HBUS and OSDP

Hardened Physical Access Control Systems and Secure Bi-Directional Communications

History, Comparison, and Overall System Considerations

October 2023

Prepared by IDmachines for Surveillance Trust

Surveillance Trust
SURVEILLANCE STANDARDS & REGISTRY

Table of Contents

Executive Summary

This white paper summarizes the overall requirements for secure physical access control systems (PACS). It presents the development of secure communications between card readers and door controllers[1]. It presents the history of the Open Supervised Device Protocol (OSDP) and Gallagher's HBUS.

In terms of HBUS and OSDP comparison:

- HBUS meets or exceeds the communication speed and security (encryption) functionality of OSDP secure channel as specified.
- HBUS does not meet the openness and interoperability of an OSDP deployment. [2]
- Gallagher ACUs can connect to OSDP devices if it is required functionality.
- OSDP allows for firmware downloads to devices, it does require the ACU manufacturer to support the various OSDP devices that the customer chooses to use. Support for firmware downloads to OSDP devices will vary and the customer should check for compatibility prior to purchasing the interoperable components of a system. Firmware downloads are supported on all Gallagher HBUS-based systems, requiring no additional actions from customers.
- Secure Chanel is optional with OSDP. Customers and their supply chain need to know if a product is OSDP Verified™ for the Secure, Smart Card, or Biometric profile. It is necessary to make sure if it is turned on, and securely implemented, particularly when it comes to OSDP encryption keys and their management. Gallagher takes 'secure-by-default' approach, covering unique device identification, encryption, and key management.
- Customers choosing to use Gallagher HBUS for readers and input/output devices must be aware that they will be unable to connect these devices to a different manufacturer's ACU.
- For OSDP to achieve high performance of opening doors, it is not normal to have more than a few readers on a cable pair. Not all reader ports on existing OSDP controllers support OSDP and/or require dedicated (serial) ports, reducing the capacity of the number of readers a controller can support. HBUS, on the other hand, can support up to 100 devices per cable pair while maintaining high performance.
- While other aspects of security are out of scope for OSDP, Command Centre and all Gallagher devices provide end-to-end hardened solutions that, as specified, meet modern security standards across the board.

[1] Card readers are Peripheral Devices (PDs) and door controllers/panels are Access Control Units (ACUs) in the OSDP standard.
[2] As a result of this effort, Gallagher is providing the HBUS specification to a 3rd party, not IDmachines, for a security evaluation to be made public.

Introduction: The Need for Secure Communication

The August 2023 Black Hat presentation, "Badge of Shame," highlighted possible vulnerabilities of systems using OSDP. It highlights how it is critical for implementations of OSDP to use the correct approach to installation and key initialization to achieve security goals. OSDP is different and significantly more difficult to configure than legacy systems. Not all manufacturers and their integrators have experience in deploying OSDP. If poorly initialized, configured, and/or maintained, a system utilizing OSDP Secure Channel could be compromised, resulting in unauthorized access to a facility.

Physical Access Control Systems (PACS), also known as Electronic Access Control Systems (EAC), are integral components of physical security systems used to provide access to facilities and protect people and property in a variety of global circumstances. It is critical for all PACS communications to be secure and provide the speed and functionality to support the system owner and the use case, its people, and places. Ironically, this was not the case for many systems installed following the introduction of PACS in the early 1970's; more importantly (and unfortunately), it remains true for many systems installed today.

Much of the focus of cybersecurity is on Internet Protocol (IP) and IP devices, and with good reason: IP devices comprise a significant and growing part of modern security systems. Even with the ubiquity of IP devices in security and IoT systems, there remains a significant number of devices that do not, or cannot, support IP. These devices are critical to the overall security of physical security systems as they sit in between the person attempting access and the logic and service/server that grants access.

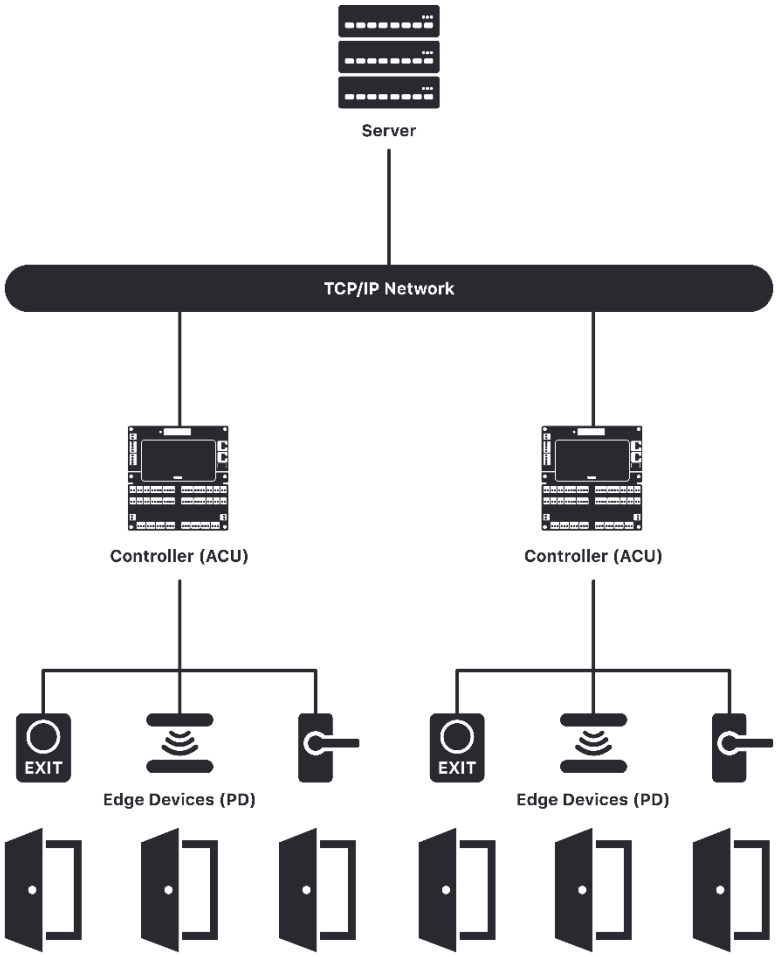
Unfortunately, even today, most card readers and door controllers still use the Wiegand method which dates back 50 years to the start of the industry. The Wiegand method is fundamentally insecure in that there is no encryption of data, and burdensome in that it does not allow bi-directional communications, prohibiting remote device management and forcing users to "roll a truck" to fix reader issues. Cybersecurity and physical security assessors and auditors will call out the use of Wiegand readers and controllers in reports, often resulting in the need for an immediate, unplanned upgrade to physical security systems to stay in compliance. This is true for many industries and government installations and is also taken into consideration in cybersecurity insurance underwriting.

As achieving effective cybersecurity becomes more and more complex, there are compelling reasons for the use of modern and secure communications between card readers and door controllers, as well as the rest of the system components.

Understanding Physical Access Control Systems

Physical Access Control Systems

For the most part, PACS today have a centralized and hierarchical architecture with an access control server and database at the top typically connected via an IP network to door controllers, which also provide control over other inputs and outputs like sensors and electronic locks/strikes. Ideally, they include bi-directional serial communication to card readers which typically communicate via a contactless interface with cards and mobile devices. All these connections - and the information they communicate - must be secured.



In all cases, PACS interact with personally identifiable information and sensitive data in addition to granting access to restricted and protected areas. As a result, there are literally thousands of regulations which require their proper design, integration, operation, maintenance, and decommissioning to ensure safe handling and compliance.

To achieve these requirements, it is critical that physical security be in synch with and leverage information technology and IT security. This so-called convergence is driven by the fact that physical security systems reside on IT resources and backbone. Hardening guides and specifications use the extensive sets of standards, compliances, and conformance frameworks that define requirements for IT privacy and security. These same requirements apply to physical security systems as a whole and specifically to HBUS and OSDP as well.

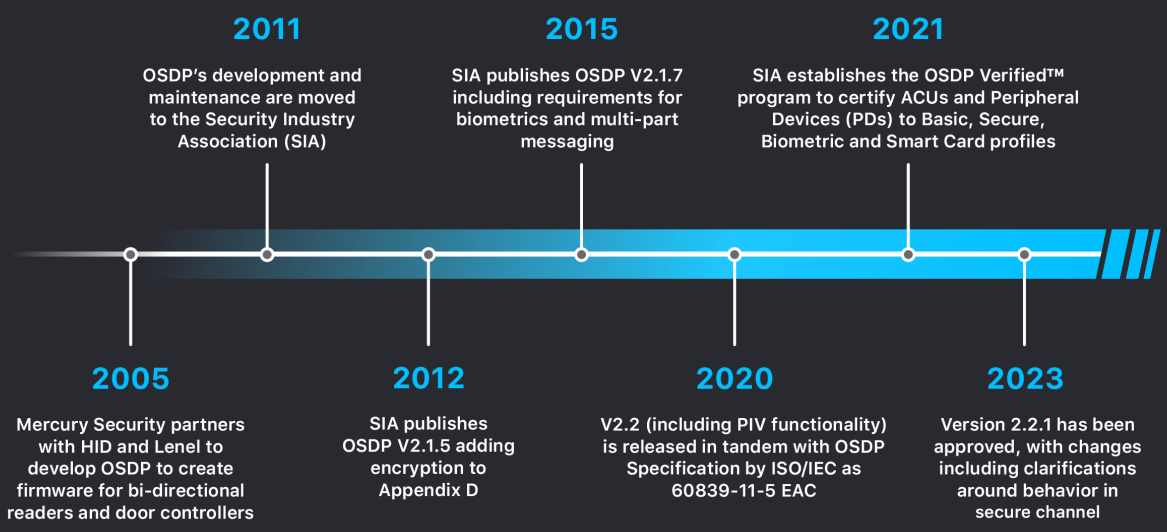
High-level system security requirements and standards common across international security frameworks

Component	Cards – Credentials	Readers	IP Devices – Controllers, Cameras, etc	Switches – Network	Servers and Workstations
Standards – Requirements	**Modern Smart Credentials and Standards Based Cryptography** • AES 128 • ECC P256 (note: attention to curve definitions) • RSA 2048	**Strong Credential Authentication and Secure Bi-Directional Communication** • Support of modern credentials e.g., EV2/ Mifare, PIV, "mobile" • 128-bit AES (e.g., OSDP / HBUS) encrypted serial communication • TLS 1.2/1.3 (2024) for IP devices • Post-quantum?	**Secure Device Authentication and Secure Communication** • TLS 1.2/1.3 (2024) • SNMP v.3 • Leverage IT Security and Privacy Controls	**Secure Smart Authentication and Secure Communication** • Managed Switches • SNMP v.3 • TLS 1.2/1.3 (2024) • Leverage IT Security and Privacy Controls	**Secure Device Authentication and Secure Communication** • Privileged Access Controls • MFA • TLS 1.2/1.3 (2024) • Leverage IT Security and Privacy Controls

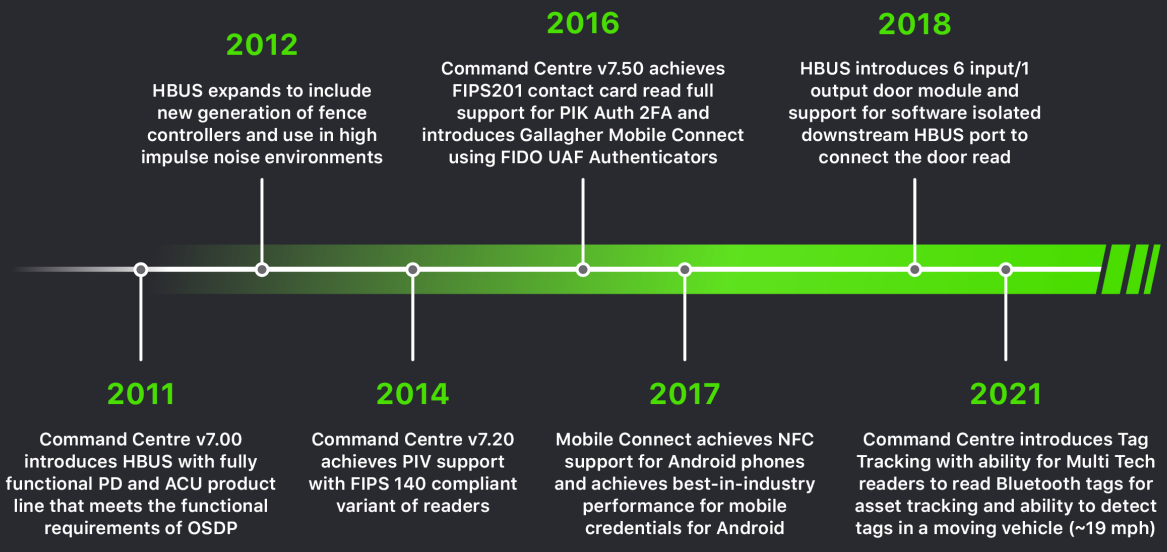
A brief history of OSDP and HBUS

Although OSDP predates Gallagher HBUS, the below timelines demonstrate that Gallagher achieved the functional equivalent of the OSDP Secure and Smart Card Transparent Model profiles for PDs and ACUs with the introduction of PIV functionality in its 7.2 release (albeit for Gallagher HBUS-supported devices). This includes secure and encrypted communications, key management, remote maintenance and configuration via file transfer and support of other functions equivalent to OSDP in terms of input/output, LED and buzzer support, and smart card challenge and response.

OSDP Timeline



HBUS Timeline



Comparing Security

The fundamental requirement for secure communications throughout an access control system is one of the main drivers behind the development, demand, and use of HBUS and OSDP. There are two aspects considered here: the encryption technique itself and the setting of the secure channel (SC) communications between the card reader (PD) and door controller (ACU). This is apart from the system level security considerations presented earlier.

(For a detailed list of other serial communication standards see Appendix C.)

Encryption

In almost all cases, encryption of serial communications sessions uses symmetric encryption, namely AES 128 which is specified as NIST FIPS 197 and was updated in 2023. There are multiple cipher suites that can be used. Both OSDP and HBUS use cipher block chaining (CBC) due to the constrained nature of devices. Galois Counter Mode (GCM) is another AES block cipher which is more robust but requires more processing power. These ciphers are updated in the latest version of FIPS 197. Updated ciphers are currently under consideration with OSDP 2.3, and HBUS is looking at upgrades in an imminent version.

The use of asymmetric key pairs and challenge and response, such as RSA and ECC, can also be used to encrypt payloads and communications. These algorithms can be used inside an OSDP SC session. Asymmetric encryption is more calculation intensive than symmetric encryption with ECC being less calculation intensive than RSA, which is why, at present, AES 128 is commonly used.

Secure Channel Session

To properly establish SC communications a very specific series of steps must be undertaken in both the case of OSDP and HBUS.

In the case of the OSDP standard, this series of steps is called out in Appendix D of the specification. This involves starting a secure session using a base key defined in the specification. This is used to begin the session after which it is required to move to a new key that is unique to the ACU and PD and cannot be reused for setting a secure channel between any other ACU and PD. While not called out in the standard, these keys need to be managed over time. This involves not only rotating - namely issuing new keys – and removing key material (also known as zeroizing) at the time of decommissioning. The initial key setting ceremony needs to be done in a secure and closed setting, and the ongoing key management needs to be established only by privileged system administrators on a secure network, or again, completely out of band, and only by privileged users.

HBUS security is always initialized when configuring a PD to be a child of an ACU. When a PD is connected to a HBUS circuit at its final install location, it will immediately advertise its presence sending a message every second. This message indicates its factory loaded unique serial number. The Command Centre configuration client will show the presence of the PD and log the entire process in the audit trail. The installer will indicate that they wish to use the device, and at this point, the ACU will validate the ECC P256 signed certificate; if valid, a secure key establishment protocol, ECDH, is used to generate a “pre-shared key”[3] that is maintained in both ACU and PD for the life of the relationship, or until it is desired to update it. The pre-shared key is used to mutually authenticate the devices at the start of each subsequent session and generate MAC and encryption keys for a session. A session will last for less than 24 hours prior to the establishment of a new session that will generate new keys.

System Level

OSDP and HBUS, as mentioned earlier, are only a part of the communication path in a PACS. It is of little benefit to have secure communications between ACUs and PDs and for the rest of the system credentials, network, servers, and database to be insecure. In addition to supporting secure components, it is critical that they are all configured, installed,

[3] The Gallagher HiSEC readers differ from this process slightly to the standard readers.

and maintained properly. This is true not only for the PD-ACU communications using OSDP or HBUS, but for all aspects of system security. The certificates used to establish the https connections, including setting up TLS, must be up to the latest specifications, as defined in associated standards and in policy. These are detailed in the certificate practice statement and must indicate that the certificate is issued from a trusted source. Very often these details are overlooked.

It is important to reinforce that IT security best practice is followed. Practices like limiting the number of servers and privileged users (administrators) are critical to security at a system level. Again, there are national and global cybersecurity and privacy frameworks (e.g., NIST and ISO) that include security and privacy controls that integrators and system operators need to follow. Ideally, these are incorporated into hardening guidance by system manufacturers.

Comparing Functionality

The comparison here of HBUS and OSDP looks at the previous security requirements as well as the functionality they deliver in supporting physical access control and related business use cases. As mentioned earlier and shown in the history timelines, the two protocols have very similar functionality with the primary difference being the extent of support by multiple manufacturers of OSDP devices versus the support of multiple HBUS devices by Gallagher Security.

Integrated Solutions vs. Interoperability

An integrated solution, where one manufacturer supplies multiple layers of the end-to-end system, can be contrasted with a system put together from interoperable components from several manufacturers.

OSDP is very device specific and really focuses on the security of communication between only the ACU and the PD. Even in the case where a manufacturer provides both ACUs and PDs, the compliance with the OSDP standard is measured on a device-by-device basis. As far as integrated solutions are concerned, anything apart from reader-to-controller communication is out of scope of the OSDP protocol. The potential benefits in an integrated system using OSDP requires the functionality to be supported by all interoperable devices, e.g., advanced functionality such as firmware updates.

HBUS is part of the integrated Gallagher Command Centre system where the end-to-end solution is provided, including all the advanced features of OSDP (remote configuration, firmware updates, key management). The overall system security architecture defines a high security stance where both the server-to-ACU communications and ACU-to-PD communications are designed to automatically configure strong authentication and encryption to best practice standards. The Command Centre system can also support interoperability of edge devices, by allowing OSDP readers to be used with a Gallagher ACU.

Specified Functionality

Comparing OSDP and HBUS is challenging in that the two solutions use different types of bus control. Since RS-485 is a serial bus and cable pair, only one device is allowed to “talk” at a time, otherwise the messages will be corrupted, and communication will fail.

One of the simplest options (and the one used by OSDP) is a master/slave approach, where the master device on the wire invites each of the other devices on the wire to talk. [4] A card reader needs to wait until invited to talk (sent a poll) before it talks to the controller (e.g., sends information on a card that has been presented). The more devices connected to the RS-485 bus, the longer it will take to detect the card read and open the door.

HBUS uses collision detection and avoidance, an alternative to polling that has been used for many years in ethernet implementations. The device will check to see if the bus is idle, and if so, will start transmission immediately; if not, it will wait for idle. Statistically, with several card readers on the same cable, the likelihood of two cards being presented to two readers at the same time is so small that with anti-collision, a card reader can tell the controller immediately it has read the card without having to wait for a poll. In some cases, this could reduce the time to open the door by ¼ - ½ a second, improving the UX.

[4] Master – Slave poling is an unfortunate choice that was used to describe the OSDP architecture. Primary and dependent among other alternatives have been offered.

Functional Comparison

Function	OSDP	HBUS
RS485 support	**Multidrop:** up to 32 **Distance:** 1000m **Communication speed:** 9600 – 230,400 bits per second (bps) **Technique:** Master - Slave Polling	**Multidrop:** up to 100 **Distance:** 500m (repeater is an option) **Communication speed:** 1 Mbps **Technique:** Anti-Collision
Credential reader support	• Single and Multi Tech readers from different brands • Biometric reader support • Beeper, keypads, LEDs, text- based LCD displays • Transparent smart card mode support (but must be licensed in the USA) and extended packet mode for PIV • Tamper protected options	• Single and Multi Tech readers from Gallagher • No biometric readers (Gallagher controllers support OSDP) • Beeper, keypads, LEDs, graphic LCD display, speaker, and sound file support • PIV and smart card processing support • Tamper protected options
Non-reader (PD) functionality support	• Input and output support ◦ Limited OSDP Verified™ hardware available • Supervised input and outputs under consideration for OSDP 2.3 • Reader sensor data as OSDP text	• 16 in 16 out • 8 in 4 out • 6 in 2 out plus logically isolated HBUS repeater port (door module) • Monitored Pulse Fence – perimeter Intrusion detection with deterrent • Tension Sensor (taut wire sensor ++) • Secure end of line module – to achieve device substitution protection for all sensors (installed within the tamper protected enclosure of sensor)
Device discovery on RS485	• Readers will default to specific polling address and need to be changed if more than one device is required	• All HBUS devices have a unique serial number and will be given a communications address for each new session • Unconfigured devices will advertise their presence on the bus
Firmware downloads The ability to update the firmware or configuration in a device based on added/changed functionality or in response to a Cyber Secuirty event	• Not required at this time by OSDP Verified™ or OSDP Standard • The ACU manufacturer must support the firmware update file management of each device manufacturer • Uses a file transfer mechanism in OSDP or manufacturer specific commands	• Built in - all HBUS devices have firmware update capability • The ACU will manage the updates to any HBUS device • All firmware updates loaded centrally • Ability to control when the updates will take place

Key Points of Difference

Physical Bus Properties	OSDP	HBUS	Why it Matters
Data speed	• Default is 9,600 bits per second • OSDP 2.2 states 9,600 – 230,400 bps	• 1Mbps	The data speed affects overall performance, particularly in the case of a high number of multi-drop devices on the bus at one time.
Maximum recommended cable distance	• 1000m • Twisted pair • 120-ohm resistance • Shielded from power	• 500m • Twisted pair • 120-ohm resistance • Shielded from power	The type and length of the cable and proper termination, particularly if multi-drop, determine how far a reader can be located from the ACU. In general, the longer the better, but practically there are very few situations that need more than 500m and potentially longer distances are better achieved by other communications options like fiber.
Number of devices supported on one cable pair	• 32 (potentially)	• 100	For high performance of opening doors, it is not normal to have more than a few OSDP readers on a cable pair. Not all reader ports on existing OSDP controllers support OSDP and/or require dedicated (serial) ports, reducing the capacity of the number of readers a controller can support. HBUS has great performance with many devices on the cable pair. For example, there have been situations where users have had over 80 of the perimeter fence tension sensors (taut wire equivalent) on the same HBUS circuit and each device reports the tension every second. If a card reader was on the same bus, it would maintain strong performance.
Bus arbitration How the bus ensures only one device talks at a time	Polling (ACU invites each PD to talk normally in round robin approach)	Anti-collision (devices are free to communicate immediately if it detects the bus is idle)	Polled systems can create a significant delay before a card reader can send its message to the controller if there are multiple readers connected. It is generally recommended with OSDP that only one or two readers be used on any OSDP connection to ensure good user experience. A HBUS reader can normally send its message within 100 microseconds as the bus is generally idle; this allows great user experience with many devices on the bus.
Manufacturers serial number and certificate in device	No	Yes	A unique identity in every device enables strong device authentication, which in turn allows detection of device substitution, an attack scenario that is important for high security.

Conclusion

Secure communications are completely dependent on the communication channel being set up properly. This needs to be carefully followed when using OSDP. The Gallagher HBUS has been designed and is set secure by default, automating all initialization and configuration tasks required. The installer, consultant, and customer must determine and trust that their supplier and operators has configured the system to be secure and that any attempt to tamper with the system will generate an alarm.

ACU-to-PD communications are just one step in an end-to-end system. Equal attention needs to be taken to ensure that the ACU-to-server communications are equally protected. The same is true for any API that connects to the access control system and to other enterprise systems. Maintaining a secure system requires an ability to quickly and easily patch any software system to mitigate any vulnerability that is found. OSDP specifies a file transfer protocol that may be used to update the firmware in the card reader in place. This file transfer mechanism requires both the ACU manufacturer to support the file transfer mechanism and any of the readers attached to the ACU. This is a 'buyer beware' situation, where specifiers and system operators need to ask the question of the integrator and system component vendors whether these features in the integrated solutions are supported. Gallagher has, from the inception of HBUS, implemented firmware updates to all its HBUS devices that ensure that all devices maintain compatibility through the patching/updating process.

In conclusion, secure communications between controllers and card readers are critical to the security and value of PACS. This is not a requirement that should be taken lightly or for granted. In the case of OSDP, it is critical to ensure that products are certified, initialized, configured, and maintained properly by experienced suppliers. Gallagher HBUS, devices, and systems provide security by default. Nothing less is acceptable for security systems, in any place, in any case.

Acknowledgements

Thanks to Steve Bell, Chief Technology Officer for Gallagher Security, for his assistance with sourcing information on HBUS and Command Centre.

Abbreviations

ACU *Access Control Unit*

AES *Advanced Encryption Standard*

ANSI *American National Standards Institute*

API *Application Programming Interface*

BACnet *Building Automation and Control*

BPS *Bits per second*

CBC *Cipher Block Chaining*

CoAP *Constrained Application Protocol*

DSS *Digital Signature Standard*

EAC *Electronic Access Control*

ECC *Elliptic-curve Cryptography*

FIDO *Fast Identity Online*

FIPS *Federal Information Processing Standard*

GCM *Galois Counter Mode*

MAC *Message Authentication Code*

ISO *International Organization for Standardization*

IEC *International Electrotechnical Commission*

IETF *Internet Engineering Task Force*

IoT *Internet of Things*

IP *Internet Protocol*

IT *Information Technology*

Mbs *Megabit(s) (Million(s) of bits per second*

NIST *National Institute of Standards and Technology*

NISTIR *National Institute of Standards and Technology Internal or Interagency Report*

OSDP *Open Supervised Device Protocol*

OT *Operational Technology*

PACS *Physical Access Control Systems*

PD *Peripheral Device*

PIV *Personal Identity Verification*

RFC – *Request for Comment (name of IETF Specifications)*

RSA – *Rivest, Shamir, Adleman*

SC – *Secure Channel*

SIA *Security Industry Association*

SP *Special Publication*

TCP/IP *Transmission Control Protocol/Internet Protocol*

TLS *Transport Layer Security*

XML *Extensible Markup Language*

XMPP *Extensible Messaging and Presence Protocol*

Appendix A

A brief history of OSDP

In the early 2000's Mercury Security, a door controller manufacturer, was integrating readers capable of bi-directional communications but needed to implement unique communications firmware in its controllers for each of the devices. To address this, Mercury, in about 2005 partnered with HID and Lenel (now LenelS2) and developed a protocol specification that resulted in the Open Supervised Device Protocol (OSDP), in the hope of addressing this.

Before and during this period and aware of the drawbacks of the Wiegand protocol, several companies had developed their own proprietary communication protocols including those by Software House (referred to as their RM series), and F2F which was and still is supported by multiple vendors, among others. In all these cases there existed drawbacks in terms of interoperability or the security of the protocol.

In 2011, at about the same time as the release of Gallagher's HBUS, the development and maintenance of OSDP was moved to the Security Industry Association (SIA), as OSDP was becoming more widely adopted. Prior to this any OSDP specification is often referred to as 1.0. In 2012 SIA published OSDP v2.1.5 which in its Appendix D included Encryption, 2.1.7, published in 2015, included addressing requirements for biometrics, and multi-part messaging.

In 2020, Version 2.2 was released in synchronization with the publication of the OSDP Specification by the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) as 60839-11-5 as part of the ISO/IEC electronic access control group of specification. Version 2.2. included file transfer functionality, as well as an expanded smart card command and reply set that included functionality to handle Personal Identity Verification (PIV) as defined in the Federal Information Processing Standard 201 (FIPS 201 now at FIPS 201-3).

In 2021, SIA established the OSDP Verified™ program to certify Access Control Units (ACUs) and Peripheral Devices (PDs) to Basic, Secure, Biometric and Smart Card profiles. Approximately 20 companies have had some of their products go through the certification process. In terms of market acceptance, lists[1] available on the Internet identify over 75 companies that have made references to OSDP products. When a device is being specified, the requirements with regards to the OSDP standard are determined by the OSDP Profiles that are publicly available on the SIA OSDP Verified GitHub repository test cases spreadsheet (.ods file). In 2023, Version 2.2.1 has been approved, with changes including clarifications around behavior in secure channel. Version 2.3 is currently open for input in the SIA OSDP Technical Subcommittee where the maintenance of the standard today, primarily, takes place.

One benefit of being a published standard is that it provides an attractive target for penetration testers and researchers (as well as white and black hat hackers). This provides a 3rd party assessment of the robustness of a protocol, and its underlying cryptography. In the case of OSDP, one recent presentation[2] pointed to some known weaknesses in the current standard, included for updates in the 2.3 release, targeted for 2024. In the same presentation of so-called OSDP deficiencies, most were not related to the protocol but rather to how the secure channel session must be executed properly, or access to the systems and thereby vulnerable to attack. The conclusion of the presentation highlights the need to implement standards properly, for product certification, and for training and documentation to support OSDP. The presentation reinforces the fact that just because a security standard exists it still needs to be implemented properly, or else the result is not security but rather security theater.

Standards and systems also need to evolve. The expansion of IoT devices, in general, is driving efforts in lightweight cryptography and encryption standards. This is important, as the reader is often a constrained device, in terms of processing, with only serial communication capabilities. In the relatively near term, there will also need to be considerations of the impact of quantum computing, given the lifetime of physical security systems. At present AES, effectively the industry standard, is believed to be post-quantum proof. Notwithstanding NIST has over the last 10 years been conducting an evaluation and selection process for lightweight cryptography algorithms which has recently been concluded. The physical security industry must continue to adapt its products to generally accepted robust cryptography and this applies across physical and IT standards.

Appendix B

A brief history of HBUS

Gallagher, founded in 1938, purchased PEC NZ in 1999, and with it, the Cardax access control business. Over time, the brand and platform transitioned to the current Gallagher Command Centre and related hardware and software. The following timeline picks up the story with the introduction of HBUS.

In 2009, Gallagher recognized that the lack of a high-performing secure device protocol was going to limit the functionality and security innovations that their customers were asking for. While starting the development of a new generation of readers - and recognizing that no suitable protocol existed - HBUS was designed and implemented.

In 2011, Command Centre v7.00 included the first release of HBUS in the Controller 6000 (ACU) on RS485 ports A and B, and in the T10, T11, and T12 card readers, both single and Multi Tech options. HBUS devices extended the process of factory loaded serial numbers and certificates used in the Gallagher controllers since 2001 to all the new devices. This allowed authentication of all devices to be performed at installation and the secure generation of pre-shared keys for the partnership of the ACU and PD. This achieved the design objective that strong security is best managed by the system and must be on by default. The other objective achieved was that all device firmware must be able to be updated in place and that the ACU ensures that each PD is updated to match the ACU's own firmware.

In 2012, Command Centre v7.05 released a series of updates and new PDs. Card readers were extended to support Mifare DESfire cards using diversified keys managed by the customer. A new range of Controller 6000 plug-in modules was released that included 8 HBUS RS485 ports to allow star connection of door readers preferred by most installers. A new Gallagher F22 perimeter fence controller was released to run HBUS in a high impulse noise environment.

In May 2014, v7.20 further extended the HBUS device family with a range of input and output modules and the T20 terminal with color LCD display, keypad, LED indicators, and of course, NFC communication. 7.20 also released support for the FIPS201 (PIV) standard US Government smart cards. From the start, Gallagher implemented the entire time of access requirements of the standard in the PIV variants of the Controller 6000 and T Series card readers. HBUS was one of the reasons for the best-in-class user experience of the system.

In 2016, v7.50 released a new T Series reader, the T15 Multi Tech in a mullion form factor. The PIV family of devices was extended by the release of the T21 contact and contactless PIV card reader that implement the true two factor mode of the FIPS201 standard.

In October 2016, v7.60 included the first release of Gallagher Mobile Connect, delivering a mobile phone credential with FIDO UAF public key authenticators for phishing-resistant security. A new version of the Multi Tech T Series card readers was released with a Bluetooth LE radio for communication with the smartphone. Version 7.70 in April 2017 saw the release of phase 2 of Mobile Connect including two factor authentication promoting the use of biometric capabilities of smartphones as the second factor. v7.70 also added more granularity of control for the Multi Tech readers with the ability to control which credential technologies could be used at the reader. v7.80 in Nov 2017 further extended Mobile Connect to use NFC on supported Android phones via an ISO-registered NFC protocol developed by Gallagher.

In June 2020, v8.30 released the ability to "roll" the Mifare DESfire keys on the card, a capability only possible with the performance of HBUS where the ACU had the ability to read and authenticate the card with the old key then update the Desire key for that card all in one presentation of the card.

Other noteworthy updates for HBUS devices include the ability to manage locker allocation on the T20 terminal and extending the Bluetooth LE functionality to read Bluetooth tags for asset/people tracking, including a use case in mining where people are reliably detected in moving vehicles.

Appendix C

Other Serial Communication Standards

The physical security and access control industry is not alone in the need to support secure communication of constrained devices. This is true across the Internet of Things (IoT) world. None have been fully adopted by the physical security community since they do not meet the specific requirements of the physical access control use case. In an oversimplification the requirements from a physical access control perspective include the need to support; communications at the link layer, symmetric speeds, and (from an OSDP perspective) at least a 1500-byte messages at a reasonable speed. The following is a quick overview of several of the protocols that are mentioned as possible, but in fact, at this time, are not viable, alternatives.

BACnet (Building Automation and Control) Network

BACnet dates to 1987 and started as a serial communication bus and protocol. The American Society of Heating, Refrigerating and Air-Conditioning Engineers is an American National Standards Institute (ANSI) Standards Development Organization (SDO) that developed the protocol. BACnet became ISO16484-5 Building automation and control systems (BACS) — Part 5: Data communication protocol in 2003. BACnet supports both RS-232 and RS-485 and multidrop and device discovery. While BACnet did receive some consideration within the access control world it never achieved any critical mass in terms of adoptions. The later versions of BACnet also incorporated IP devices.

Zigbee

Zigbee is a wireless protocol, that is popular among constrained devices, and which has been in place for about 20 years and has recently morphed into the Connectivity Standards Alliance. It has been adopted for wireless locks but not as a means of integrating the devices into the access control system. It is often found in so-called “smart home” applications. Again, the fundamental requirement that needs to be met is to provide communication between a peripheral device and door controller as part of an access control system, not simply a means to unlock a lock.

MQTT

Message queuing telemetry transport (MQTT) is a lightweight messaging protocol widely adopted on the Internet of Things (IoT). MQTT is also targeted at constrained networks. It has seen limited use, also with “smart” locks. MQTT is a simple protocol and does not support many of the features and functionality that are required for a physical access control system (like Zigbee). It is a publish/subscribe approach that does not map to the supervision of OSDP or the bus management of HBUS.

CoAP

The Constrained Application Protocol (CoAP) is mostly targeted at connecting constrained devices and accommodating a connection to the Internet. Like the other protocols here it is not well adapted to the requirement of reader to controller communication, and the supervision and security that is required. Many CoAP implementations communicate over HTTP and therefore send messages in the clear.

XMPP

Extensible Messaging and Presence Protocol (XMPP) is a messaging protocol more than a communication protocol for managing devices. The protocol has overhead from the use of XML. This is not used for physical access control but has been used for sending messages, such as the control stream, to Internet Protocol (IP) devices such as network cameras.

Bibliography

"Advanced Encryption Standard (AES)." Computer Security Resource Center, May 9, 2023. https://csrc.nist.gov/pubs/fips/197/final.

"Alarm and Electronic Security Systems - Part 11-5: Electronic Access Control Systems - Open Supervised Device Protocol (OSDP)." International Electrotechnical Commission, July 2020.

"Cybersecurity Framework." National Institute of Standards and Technology. Accessed August 22, 2023. https://www.nist.gov/cyberframework.

Dierks, T., and E. Rescorla. "The Transport Layer Security (TLS) Protocol Version 1.2." Internet Engineering Task Force, August 2008. https://www.ietf.org/rfc/rfc5246.txt.

"Digital Signature Standard (DSS)." Computer Security Resource Center, February 3, 2023. https://csrc.nist.gov/pubs/fips/186-5/final.

Dworkin, Morris J. "Advanced Encryption Standard (AES)." Gaithersburg: National Institute of Standards and Technology, May 9, 2023.

"Gallagher Command Centre Gallagher's Guide to Physical Security Levels." Hamilton: Gallagher Security, December 2022.

"Gallagher Command Centre v8.90 Hardening Guide." Gallagher Security, May 2023.

"Gallagher Command Centre Visitor Management Kiosk Hardened Installation." Hamilton: Gallagher Security, September 2022.

"Gallagher Controller 6000 and 7000 Single Door Hardening Guide." Hamilton: Gallagher Security, August 2023.

"Digital Signature Standard (DSS)." Computer Security Resource Center, February 3, 2023. https://csrc.nist.gov/pubs/fips/186-5/final.

"Information Technology — Security Techniques — Information Security Management Systems — Overview and Vocabulary." Geneva: International Organization for Standardization, February 2018.

"Information Technology - Security Techniques - Privacy Framework." Geneva: International Organization for Standardization, December 15, 2011.

"ISO 16484-5:2022(En) Building Automation and Control Systems (BACS) — Part 5: Data Communication Protocol." Online browsing platform (OBP) - ISO. Accessed August 22, 2023. https://www.iso.org/obp/ui/en/.

"ISO/IEC 27001 Standard – Information Security Management Systems." ISO, October 2022. https://www.iso.org/standard/27001.

"ISO/IEC 27002:2022." ISO, February 2022. https://www.iso.org/standard/75652.html.

"ISO/IEC 7816 - Identification Cards Package." ANSI Webstore. Accessed August 22, 2023. https://webstore.ansi.org/standards/iso/isoiec7816identificationcards.

Moriarty, K., B. Kaliski, J. Jonsson, and A. Rusch. “RFC 8017: PKCS #1: RSA Cryptography Specifications Version 2.2.” Internet Engineering Task Force, November 2016. https://datatracker.ietf.org/doc/html/rfc8017.

“OSDP v2.1.7: Open Supervised Device Protocol Standard Version 2.1.7.” Security Industry Association, 2023. https://www.securityindustry.org/industry-standards/osdp-v2-1-7/.

“OSDP v2.2: Open Supervised Device Protocol Standard Version 2.2.” Security Industry Association, 2020. https://www.securityindustry.org/industry-standards/osdp-v2-2/.

“OSDP Verified Products.” Security Industry Association. Accessed September 4, 2023. https://www.securityindustry.org/industry-standards/open-supervised-device-protocol/sia-osdp-verified/sia-osdp-verified-products/.

“PIV Standards and Supporting Documentation - Personal Identity Verification of Federal Employees and Contractors: CSRC.” Computer Security Resource Center. Accessed August 22, 2023. https://csrc.nist.gov/Projects/piv/piv-standards-and-supporting-documentation.

“Privacy Framework.” National Institute of Standards and Technology. Accessed August 22, 2023. https://www.nist.gov/privacy-framework.

Rescorla, E. “RFC 8446: The Transport Layer Security (TLS) Protocol Version 1.3.” Internet Engineering Task Force, August 2018. https://datatracker.ietf.org/doc/html/rfc8446.

“Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.” Gaithersburg: National Institute of Standards and Technology, December 2018.

rsgmodelworks. “osdp-verified Resources fr the SIA OSDP Verified Testing Program.” GitHub, August 22, 2023. https://github.com/Security-Industry-Association/osdp-verified#readme.

Saint-Andre, P. “RFC 6120: Extensible Messaging and Presence Protocol (XMPP): Core.” Internet Engineering Task Force, March 2011. https://datatracker.ietf.org/doc/html/rfc6120.

Shelby, Z., K. Hartke, and C. Bormann. “RFC 7252: The Constrained Application Protocol (CoAP).” Internet Engineering Task Force, June 2014. https://datatracker.ietf.org/doc/html/rfc7252.

“Security and Privacy Controls for Information Systems and Organizations.” Computer Security Resource Center, December 10, 2020. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.

“SIA AC-01-1996.10: Access Control Standard Protocol for the 26-Bit WiegandTM Reader Interface.” Security Industry Association, 1996. https://www.securityindustry.org/industry-standards/sia-ac-01-1996-10/.

Turan, Meltem Sonmez, Kerry McKay, Donghoon Chang, Lawrence E. Bassham, Jinkeon Kang, Noah D. Waller, John M. Kelsey, and Deukjo Hong. “Status Report on the Final Round of the NIST Lightweight Cryptography Standardization Process.” Gaithersburg: National Institute of Standards and Technology, June 2023.

“User Authentication Specifications Overview.” FIDO Alliance. Accessed August 22, 2023. https://fidoalliance.org/specifications/.