The Power of an OPEN PROTOCOL

Interoperability and securing security lies at the heart of the revamped Open Supervised Device Protocol (OSDP). Learn the what and why of OSDP, which provides a set of commands and responses while predefining encryption and authentication.

By Stephen Sheppard

The Open Supervised Device Protocol (OSDP) is an access control communications protocol nurtured by a Security Industry Association (SIA) consortium, consisting of some of the smartest individuals from the security industry. Version 2.2 of the SIA OSDP is its most recently updated standard that improves interoperability among access control and security products such as readers and controllers. The standard also applies to peripheral devices such as card readers and other technologies at secured access doors/gates and their control panels.

Already in use by many leading manufacturers, the SIA OSDP standard is recommended for access control installations that require advanced security or will be used in government and other higher-security settings such as data facilities and drug manufacturing programs. OSDP supports advanced user interfaces, including welcome messages and text prompts. Audio-visual user feedback mechanisms provide a rich, user-centric access control environment.

A two-way channel and encryption pave the way for advanced security applications such as the handling of smart cards, biometrics and government applications that require Public Key Infrastructure or Federal Identity, Credential and Access Management requirements. Not only does OSDP provide a concise set of commonly used commands and responses, it eliminates guesswork, since encryption and authentication are predefined. How does that impact security equipment manufacturers, integrators and users?

Among other things, it lets security equipment, such as card and biometric readers from one company interface easily with control panels and equipment from another manufacturer. In other words, OSDP fosters interoperability among security devices. It also adds sophistication and security benefits through features such as bi-directional communication and read/write capabilities.

It provides the transfer of large data sets for firmware updates or graphics from an access control unit to a reader, clearer instructions for the implementation of Secure Channel, the OSDP encryption piece, to facilitate encrypted communications and updated messages for handling smartcard applications within the protocol.

OSDP importantly offers the option of secured, encrypted communications between reader and controller. This is independent of the encryption between credential and reader.

Remember, a basic definition of encryption is the conversion of information and data into a secret code. This is sometimes called a cipher. For example, let's say your access card is programmed with the number 101. You present your card to a reader and the controller also sees ID 101 but, in between the reader and the controller, the data sent looks nothing like ID 101. The card data sent in between the reader and the controller is encrypted into a secret code.

Also, significant to highlight, OSDP is a real SIA-approved industry standard. It is not a piece of technology owned by any company and, thus, not proprietary. Today, it is an open standard that is global in scope and available for use by any manufacturer.

Continue on to get the basics down and better understand how OSDP solidifies integration project integrity and opportunities. Also, a sidebar shows how a technique known as webhooks enables customized access control solutions.

Nuts & Bolts of OSDP

OSDP is built on the RS-485 serial transmission standard. RS-485 is the physical layer, laying out the actual electrical characteristics of the signal generator and receiver. Think of OSDP as communications riding on this RS-485 physical layer.

Key advantages include that RS-485 requires just four conductors, two for power and two for data. A cable example might be the popular Belden 8723. Intended for control and instrument installations, it's a 22 AWG stranded cable with four conductors, each making use of color-coded polypropylene insulation, then twisted into pairs. One pair is red and black while the other pair is green and white. Next, each pair is individually foil shielded and then wrapped together with a stranded drain wire and covered, finally, by a PVC jacket.

RS-485 also provides for longer cable runs between devices, often up to 4,000 feet. Also, when compared to Wiegand, which offers simple point-to-point topologies, OSDP offers point-to-point and multidrop. Of course, multidrop also means individually naming, or addressing, the readers in the system.

Encrypted communications between a reader and controller offer a number of real-world benefits. One is that encrypted OSDP communications can be used to prevent man-in-the-middle hacks on data lines. In this type of breach, a hacker intercepts data, then secretly relays and possibly alters the communications between a reader and door controller.

Another benefit of encryption is data integrity, a concept often overlooked. Specifically, by implementing encryption, one can trust that the data being communicated is authentic and unaltered from what was originally communicated. This is a good segue over to the subject of IT.

In our IT-centric world, the concept of IT compliance, the process of meeting a specific set of requirements for digital/cyber security, is an emerging need. For example, these requirements might be generated internally by corporate IT or they may originate from outside the customer's organization.

Think of an insurance company or government entity. Perhaps, your company agrees to a standard operating procedure (SOP) of only supplying solutions as standard when encrypted. When applied, OSDP can assist in meeting this SOP.

Moving Beyond Wiegand

For years, Wiegand has been the industry standard but it is no longer inherently secure due simply to its original obscure and nonstandard nature. Plus, the multiple definitions associated with the Wiegand name have created confusion over the years.

OSDP, focused as a standardized protocol between readers and controllers, moves us forward. SIA OSDP allows devices, such as card readers, control panels or other security management systems to work together, providing the security industry with a solution that moves far beyond the widely-used Wiegand standard

Many manufacturers have already implemented OSDP and there are many other companies with OSDP devices in development. To encourage this, SIA has released tools that will ensure that these numbers continue to grow.

OSDP is recommended for access control installations that require advanced security or will be used in government and other higher-security settings.

in terms of security and functionality.

It helps ensure that numerous manufacturers' products will work with each other. Interoperability can be achieved regardless of system architecture. For instance, the specification can handle smartcards by constantly monitoring wiring to protect against attack threats and serves as a solution for high-end encryption such as required in federal applications. The specification for handling LEDs, text, buzzers and other feedback mechanisms provides a rich, user-centric access control environment.

To again emphasize, OSDP provides the option for encrypted channel communications. Wiegand does not. Known as a secure channel, OSDP lets communications traffic between a reader and controller be encrypted. Specifically, this traffic can be encrypted via Advanced Encryption Standard (AES) with a 128-bit key.

Compared to Wiegand, which offers simple point-to-point topologies, OSDP offers point-to-point and multidrop. Of course, multidrop also means individually naming, or addressing, the readers in the system.

This is real encryption, not just a data scramble. AES is itself a recognized and widely adopted specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology.

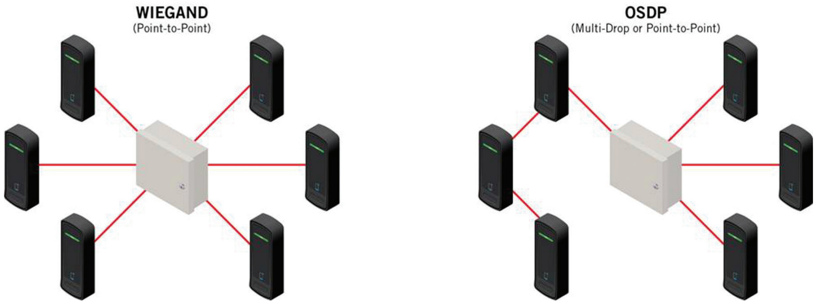
OSDP provides two-way communications. Wiegand is a one-way street for data. For example, this lets the reader be queried as to its status. Think of this as a health check. It's standard with OSDP, but not that easy to do with Wiegand.

OSDP riding on RS-485 provides longer cable runs while Wiegand is shorter. OSDP offers optional configurations of wiring topology while Wiegand only offers one. This flexibility can be very beneficial in minimizing installation and retrofit operations.

Wiring requirements are also different. An OSDP cable only requires four conductors. Wiegand cabling may require five, or even more, conductors. This makes them larger, heavier and, often, more expensive.

Finally, OSDP lets the data rate be adjusted. With Wiegand, that is not the case. The advantage is that larger quantities of data can be transmitted quicker with OSDP. Think of a personal identity verification (PIV) card. This data could be transmitted in less time than it would take with Wiegand.

WIRING TOPOGRAPHY



WEBHOOKS EMPOWER EXPANDED INTEGRATIONS *By Evan Tree*

▶ It's said that change is the only constant. For those who work with access control, that maxim has never felt more true. Cloud and mobile platforms are quickly becoming standard in the industry, allowing users to interact with their access control in ways never before possible.

Behind-the-scenes integrations among Cloud platforms allow data to be exchanged, further lightening the burden from users of these platforms. As the sophistication of these integrations grows, so does the need for the platforms to quickly notify each other of changes. These notifications have been standardized as "user-defined HTTP callbacks," or as they're more commonly called, webhooks.

Before webhooks became standard, integrations often exchanged information by blindly copying over every piece of information in one platform to the other whether or not it was needed. Why? It was because the platform sending information was completely in the dark about what the other platform finds important.

While this arrangement works in principle, it quickly becomes unsustainable as the information contained in each system grows. To combat the growing expense of this data transfer, these integrations are often limited to only transferring information perhaps once an hour, or in extreme cases, once a day.

Webhooks overcome these problems by creating a standard way for platform A to explicitly tell platform B what information A values. Platform B will then notify A when the information A values becomes available.

This principle should be familiar to any parent with a child repeatedly asking, "Are we there yet?" on a road trip. Fortunately, computers, unlike children, are perfectly satisfied to hear the response, "I'll let you know when we're there."

These requests to be notified are called subscriptions. They contain a list of events for which the receiver will be notified, and to which HTTP endpoint they will be delivered.

Once a subscription is established, events will immediately begin flowing as they're regenerated with no need to renew the subscription.

Cybersecurity Convenience

Users of physical access control systems certainly desire convenience but, as equally, expect security. So first and foremost, OSDP is more cybersecure than the most common access control communications protocol. The key is the option of encryption. OSDP typically requires less wiring, which saves money. Users may request integrators utilize existing wiring for retrofits. Additionally, OSDP constantly monitors wiring to protect against attack threats.

Looking for a traditional point-to-point topology for increased flexibility? OSDP provides it. Want the cost savings associated with multidrop? Done, using the addressability of OSDP readers. How about standards? OSDP is a SIA data communications standard built on the RS-485 serial standard. And, it offers the option to support the high end AES required in federal government applications.

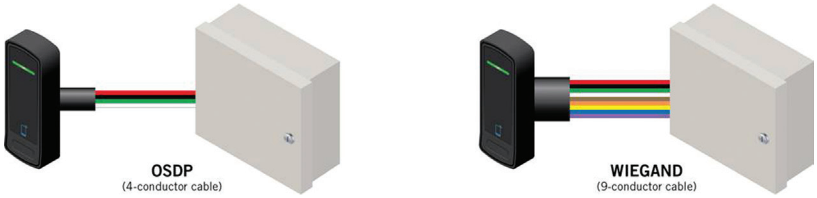
With other legacy communication protocols, such as Wiegand, there are three main physical ways to assault a card-based electronic access control system — skimming, eavesdropping and relay attacks. With OSDP Secure Channel, AES128 is used to secure the transmission of data from reader to controller.

Many manufacturers have already implemented OSDP and there are many other companies with OSDP devices in development. To encourage this, SIA has released tools that will ensure that these numbers continue to grow.

To make things easier, the SIA Open OSDP Test Tool is open-source software that lets manufacturers of OSDP-compatible equipment test their products against the specification. The test tool emulates an OSDP peripheral device or an OSDP control panel or acts as a message sniffer between two “real” OSDP devices.

The test tool runs on several widely available and low-to-no-cost platforms and hardware. It reduces physical barriers to achieving interoperability such as shipping prototypes to numerous vendors for testing. The underlying source code, also available, is another aspect of the tool that can be leveraged by device manufacturers in developing their OSDP interoperable products.

Also, there are emerging compliance initiatives pertaining to OSDP. For instance, “OSDP Verified” is being championed jointly by SIA and IDmachines, creator of the Eidola technical automation platform. SIA OSDP Verified is a comprehensive testing program that vali-



An OSDP cable only requires four conductors. Wiegand cabling may require five, or even more, conductors. This makes them larger, heavier and, often, more expensive.

When data is shared across platforms in this way, businesses benefit from streamlined workflows and efficient performance. Webhooks also allow for the creation of highly reactive interfaces. Some platforms come with the ability to utilize incoming events over webhooks natively, while others require modest programming to construct the appropriate connection.

Fortunately, the webhooks protocol is fairly straightforward, and most integrators with some technical knowledge can create an integration on their own. Consequently, webhooks open new opportunities to service clients through creative, easy-to-implement integrations.

Unexpectedly, the most common use for webhooks is in keeping two databases constantly synced. Webhooks can also be used for linking access control with nonsecurity platforms, like time and attendance, membership management, facilities management, and HR software.

Health club membership platforms, for example, want to know each time there’s a valid read at the front door. A webhook subscription can push a notification with the identity of the cardholder to an application running on the welcome desk. This application can then retrieve the cardholder’s photo and other relevant information, allowing staff to properly greet the member and verify membership.

A similar integration can be used at daycare centers. When individuals arrive to pick up a child and swipe at a door reader, a set of photos of approved persons associated with that child is immediately presented to the staff allowing for the safe release of the child.

The security integration business is evolving and including new solutions and services made possible through the Cloud and IoT. In addition, novel health and safety technologies will be part of the post-pandemic, “new-normal” workplace. Many of these systems offer enhanced value to customers when they can harvest valuable data related to people, permissions, and access to physical spaces from onsite access control platforms. Integrators who leverage webhooks can make that happen, thereby better servicing their customers while differentiating and growing their businesses.

EVAN TREE is CEO of ProdataKey.

dates a device's conformance to the SIA OSDP standard and related performance protocols. It validates that a device conforms to the OSDP standard and the related performance profiles.

A guide is furnished to find and explore products that have been verified to meet the OSDP standards. You can find which proximity readers, smartcard readers and mobile access readers comply. Such measures will benefit device suppliers, security integrators and consumers alike by guaranteeing tested devices comply with all applicable OSDP requirements.

Why Now & What's Next?

OSDP's promise is to offer opportunities to meet customers' needs today and tomorrow. The adoption and deployment of OSDP will facilitate the development of new and advanced features for readers in the field. Basically, by being able to communicate to the reader from a controller, you unlock enhanced device control.

As security professionals, many of us feel an obligation to present the best security options available to our customers. And while some technology may leave you scratching your head, OSDP is logical, practical and imperative. Today and moving forward, OSDP will greatly influence electronic access control (EAC) reader and controller development.

OSDP is seeing adoption on a global scale and is a highly recommended consideration for new installations. It is suggested that those dealing with smart security in any format will want to start incorporating the use of the OSDP standard in their equipment and systems. Future versions of OSDP will continue to follow the IEC formatting conventions, enabling the always-evolving work of the SIA SODP Working Group to be more easily adopted through the IEC standards process.

In the sales arena, OSDP should be viewed as a strong selling feature. Importantly, it offers low cost of implementation on an embedded device. It's advisable to learn it and integrate it into your presentations. **SSI**

STEPHEN "SHEP" SHEPPARD is Key Accounts Sales Manager for Farpointe Data.