Demystifying OSDP
(Open Supervised Device Protocol)
The advancement of physical access control technology continues to evolve as new threats emerge, vulnerabilities are identified, security protocols are updated, and requirements for integration increase. In step, the standards governing the development and testing of Physical Access Control Systems (PACS), have continued to evolve, improving security and interoperability among access control and security products.

The introduction of Open Supervised Device Protocol (OSDP) 10 years ago significantly shifted the world of access control capabilities and offered an option other than the long antiquated Clock-and-Data and Wiegand protocols, which have been found to leave organizations vulnerable to attack. As more information is available regarding the vulnerability of legacy PACS it’s increasingly critical for organizations to adopt protocols like OSDP that enhance their overall security posture and support current and future technology requirements.

End users often aren’t aware of the vulnerabilities that exist in legacy systems but find that upgrading to an access control system that adheres to newer standards is a significant initiative. However, there are a number of advantages to adopting updated protocols that are more flexible and offer increased security and operational efficiency for security and facility departments across organizations for the long term.
Vulnerabilities and Challenges of Legacy Systems

In the early 1980s, as more and more companies sought to shift from traditional lock-and-key access control to a more centralized approach, Chief Security Officers (CSOs) sought ways to continually protect premises from outside threats. Clock-and-Data and Wiegand protocols were widely adopted as the de facto standard as they enabled interoperability between access control readers and physical access controllers. Those de facto standards were later formalized and adopted into industry standards by the Security Industry Association in the 1990s.

Clock-and-Data

For magstripe card readers, the Clock-and-Data signaling method was introduced, which utilizes two wires called "clock" and "data." The data line is used to send all the binary data to the panel, while the clock line is used to tell the panel when to sample the data line. Each time a bit of data is sent down the data line, a pulse is sent down the clock line, which instructs the panel to take a “sample” of the data line and record that bit. Magstripe signaling is supported by many of the new access control panels, as well as older, Wiegand systems. However, this outdated communication protocol is insecure and magstripe cards can be cloned easily. It also allows readers and credentials to be upgraded without a complete overhaul of the back-end system of controllers and software.
Wiegand

More than 90 percent of the PACS installed today use the Wiegand protocol, making it the most common communication method used by access control devices to send information from the card reader to the controller. This means that the potential vulnerabilities that this protocol exposes can have a significant effect on the safety of transmitted data as it continues to be widely used.

The Wiegand standard was not designed to keep pace with the security demands of today’s enterprise organizations and the increasingly complex threats that are emerging, exposing far more challenges for these organizations to keep data transmission secure. At its core, Wiegand lacks the security that is essential for today’s access control systems, as it is unencrypted, offers limited distance options, and is operationally inefficient in preventing the controllers from communicating with readers for firmware upgrades, configuration changes, state changes, and other critical updates. Additionally, anyone who can learn the protocol language developed for Wiegand, or procure one of the readily-available off-the-shelf hacking devices, can easily exploit its vulnerabilities creating significant security issues for the organization it is tasked to protect.

Although widespread in use, Wiegand vulnerabilities are known to most end users. In a survey of IT professionals, facility managers and physical security leaders conducted by HID Global, respondents said they were aware (39 percent) or somewhat aware (36 percent) of the security risks associated with the Wiegand protocol, yet continue to utilize, while the remaining respondents (25 percent) reported being completely unaware of the security risks.

Do you believe there are security risks associated with the Wiegand protocol?

- Yes, I am aware of the security risks: 39%
- I am somewhat aware of the security risks: 36%
- No, I am not aware of the security risks: 25%
The Weak Links

Several weaknesses for these early PACS exist, including the lack of encryption protocol to protect from “man in the middle” attacks and vulnerabilities from reader to controller. Also, the retrofitting installation alongside a legacy system is complicated for integrators and expensive for organizations, as the vast majority of readers require dedicated home-run wiring. Extensive wiring on a large-scale project, such as a school or corporate campus, results in considerable — and at times, prohibitive — costs for installation of a PACS.

The weaknesses identified in the Clock-and-Data and Wiegand protocols have pushed the security industry to adopt a new protocol, bolstering the protection of critical data as it is transmitted.
Recognizing the shortcomings of Wiegand and other legacy protocols, it was critical for the industry to come together and develop a new standard on which to heighten the communication protocols and protect critical data being collected through a PACS. The result was OSDP: an access control communications standard first developed by Mercury Security and HID Global in 2008. OSDP was then donated, free of intellectual property, to the Security Industry Association (SIA) to improve interoperability among access control and security products.

Why Implement OSDP as a Standard?
It's common knowledge that today's organizations value system interoperability — especially with regard to security. The rise of IP-networked devices, such as video and physical access control, has opened up a world of possibilities; however, the security of the data being collected from these devices is paramount to keeping the organization safe from attack. OSDP is the only protocol that is secure and open for communication between readers and controllers and is also being widely adopted by manufacturers, including the industry-leading manufacturers for readers and controllers.
The fact that OSDP is also an evolving, ‘living standard,’ similar to many others that streamline the development of connected devices, makes it a safer, more robust, future-proof option for governing physical access control systems.

However, a continued need for awareness and education around the vulnerabilities of the Wiegand protocol and the advantages of upgrading to OSDP is required. In a recent HID Global survey, of those respondents that did not have OSDP-enabled devices, lack of awareness was significantly high as 80 percent of respondents said they had never heard of OSDP, while 20 percent said they had, but opted for a system using an alternative protocol.

80 percent of respondents said they had never heard of OSDP, while 20 percent said they had, but opted for a system using an alternative protocol.

The tide may be turning, however. Of those respondents aware of OSDP, 33 percent reported a plan to install or upgrade to OSDP-enabled devices (45 percent didn’t know of plans and only 22 percent said they did not plan on doing so).
OSDP Offers Extensive Benefits

Increased Security
Implementing OSDP standards can result in higher levels of security, as OSDP with Secure Channel Protocol (SCP) supports AES-128 encryption that is required in U.S. federal government applications. Additionally, OSDP constantly monitors wiring to protect against tampering, removing the guesswork since the encryption and authentication are predefined. OSDP helps overcome and address the growing threat of “man in the middle” attacks, such as when a “bad actor” uses a tool to penetrate and secretly alter the communication between reader and controller to gain access to a secured location.

Bidirectional Communication
OSDP standards support bidirectional communications among devices. Early on, communication protocols such as Wiegand were unidirectional, with external card readers sending information one way to a centralized access control platform. However, OSDP has transformed the ability for information to be collected, shared and acted upon with the addition of bidirectional communication. This means that not only can the readers “talk” directly to the centralized management platform, but the system can also communicate directly with the readers. As a result, this two-way communication offers a host of advantages, including:

- Reader configuration can be specified in the PACS software and sent to the reader via the controller
- Continuous reader status monitoring, polling and querying
- Tampering and malfunction detection and indication without needing to physically inspect the reader
- Advanced user interfaces, including welcome messages and text prompts can be displayed by the reader
Open and Interoperable
Numerous advantages exist for open-platform protocols, including the ability to deliver an increasingly flexible solution for end users over time as more and more peripheral devices are added — and not necessarily from the same manufacturer. OSDP supports IP communications and point-to-point serial interfaces, ensuring the ability for customers to enhance the functionality of their systems with additional tools over time as needs change and new threats to an organization emerge. The open-platform nature of OSDP can offer the chance for organizations to bring new technology to the table that more greatly enhances the ability for companies to protect incoming and outgoing data collection through a physical access control system. This allows companies to remain proactive in their approaches to the safety and security of employees, visitors, and assets.

Reduced Installation Costs
OSDP’s use of two wires (as compared to a potential of 11 wires with Wiegand) allows for multi-drop installation, supervised connections to indicate reader malfunctions, and scalability to connect more field devices. Multi-drop capabilities mean one length of a two-conductor cable can be daisy-chained to accommodate many readers connected to a single controller, eliminating the need to run home-run wiring for each reader. With two data lines, OSDP enables the use of a four-conductor cable, which can achieve up to 10x longer distances between reader and controller than Wiegand; and it powers the reader and can send/receive data. The reduction in wiring costs has a direct effect on an organization resulting in lower-cost implementation on an embedded device. The installer also benefits from less cable to run throughout a building, meaning less time on a project overall.
User Friendly
For credential holders, OSDP provides greater ease of use, with audio and visual feedback such as colored lights, audible beeps, and the ability to display alerts on the reader. For security administrators, managing and servicing OSDP-enabled readers also becomes increasingly convenient, as OSDP-enabled readers can be remotely configured from network-connected locations. Users can poll and query readers from a central location, eliminating the need to physically visit malfunctioning devices to diagnose, thus saving time and reducing costs.

Unlimited Application Enhancements
OSDP supports advanced smartcard technology applications, including PKI/FICAM and biometrics, as well as other enhanced authentication protocols used in applications that require Federal Information Processing Standards (FIPS) compliance and interactive terminal capabilities. Audio-visual user feedback mechanisms provide a rich, user-centric access control environment.
Demystifying OSDP

OSDP in Practice

As organizations consider OSDP, the broad range of benefits outweighs the cost to upgrade, a fact supported by the survey data. In fact, 85 percent of respondents said they strongly agree (44 percent) or agree (41 percent) that using OSDP-enabled devices has made a positive impact on their overall organizational access control experience.

Survey respondents who implemented OSDP within their organization confirmed that a number of benefits are realized, including increased security (70 percent), convenience in management (45 percent), greater functionality (43 percent), and more flexibility with features (27 percent).

While the increased security of OSDP gives organizations added protection against attacks, the real world efficiencies will be immediately evident to those managing the security infrastructure. The interoperability of OSDP ensures that customers can utilize systems from numerous manufacturers, a factor crucial in today’s security landscape as CSOs seek to upgrade systems and invest in infrastructure that maximizes protection of critical data being transmitted across various channels.

Do you agree or disagree with the following statement?
“Using OSDP devices has made a positive impact on our overall organizational access control experience.”

- Strongly Agree: 44%
- Agree: 41%
- Somewhat Agree: 15%
- Disagree: 0%
In a campus environment — whether a hospital or school — when readers are added using traditional Wiegand protocols, additional wiring is required, along with costly installation fees to effectively scale. Under OSDP, however, security leaders can realize significant cost savings as a result of more streamlined installations. This open functionality also makes adding new feature-rich readers easier and saves organizations the added expense of requiring all readers to be replaced if a new access control solution is implemented.

Users transitioning to OSDP also see realized benefits in service and maintenance, as OSDP encourages continuous monitoring of system uptime and allows for remote configuration or upgrades to a reader. OSDP enables a user to remotely change the configuration of a reader (i.e. security keys or LED color) from any network-connected location. Integrators can also capitalize on the introduction of OSDP by encouraging open standards, which can, in turn, help build new customer relationships and win more projects.

How has OSDP impacted your organization? (Select all that apply)

- Increased security: 70%
- Convenient to manage: 45%
- Greater functionality: 43%
- Easier to install: 32%
- More flexibility with features: 27%
- Integration with other systems: 23%
The Future of OSDP

Advancements in the delivery and protection of physical access control data have taken center stage over the last decade as OSDP has become more widely adopted to achieve security, efficiency and flexibility for end-user customers. "We know the adoption of OSDP is on the rise, but education efforts must be ongoing to help organizations maximize their PACS investments. With OSDP, more of these companies can ensure their ongoing security investments are future-proofed in order to truly protect people and assets well into coming decades,” said Brandon Arcement, Director of Product Marketing at HID Global.

Industry leaders, such as HID Global, have played a key role in the development of these standards in an effort to deliver physical access control solutions to customers that ensure the highest levels of security from outside threats. HID Global is a true partner, providing guidance and innovation within the security industry. Working with integrator partners and end-user customers, HID offers the enhanced protocols in a wide variety of products aimed at increased levels of protection.