

The reader on that pedestal is one end of a wire whose interface was published in 1996.

NLC ACADEMY · EPISODE 28

≈952 bit/s. In 2026.

One typical Wiegand timing example, on a reader interface published in 1996 and never revised. Replace it, and check the card too: the link and the credential are separate risks.

NOT WITHDRAWN, ORPHANED

Thirty years. Still no revision.



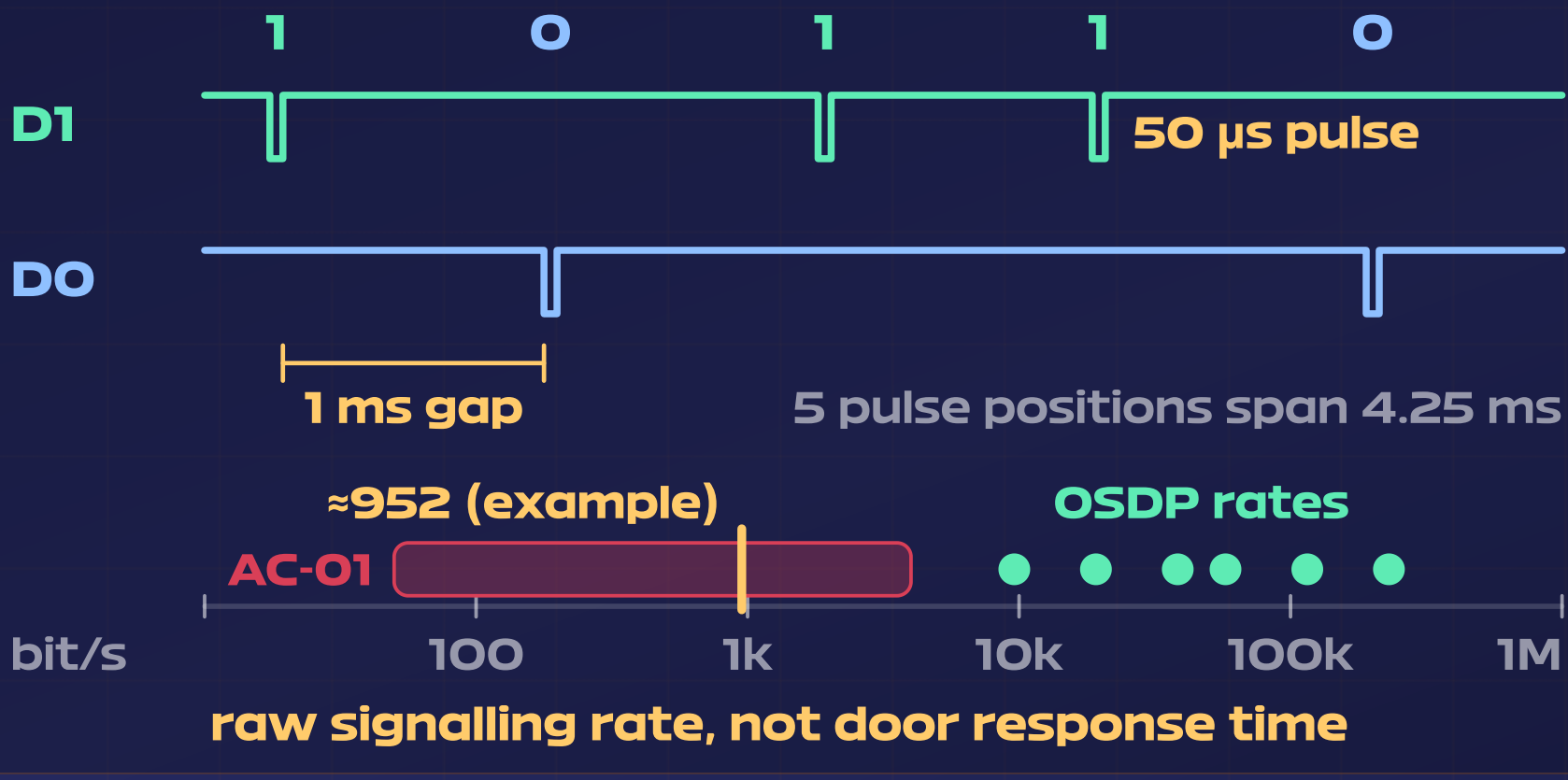
1	1996	AC-01 published
2	2008	tap tool shown
3	2011	SIA OSDP group
4	2015	BLE tap shown
5	2020	IEC 60839-11-5
6	2023	5 flaws published
7	2024	v2.2.2, errata only
8	2026	still no v2.3

SIA's catalogue (archived June 2026) lists **AC-01-1996.10** as published in **1996**, not an ANSI standard, subcommittee **disbanded**. No revision has been published. [2]

OSDP is separate and active: SIA v2.1.7 (2015), v2.2 (2020), v2.2.2 (October 2024), and IEC 60839-11-5:2020. As of 4 October 2026 we found no later SIA release; the 2023 security findings were referred to a future v2.3. [1][4]

QUANTIFY "SLOW"

≈952 bit/s is a timing example, not a Wiegand rate

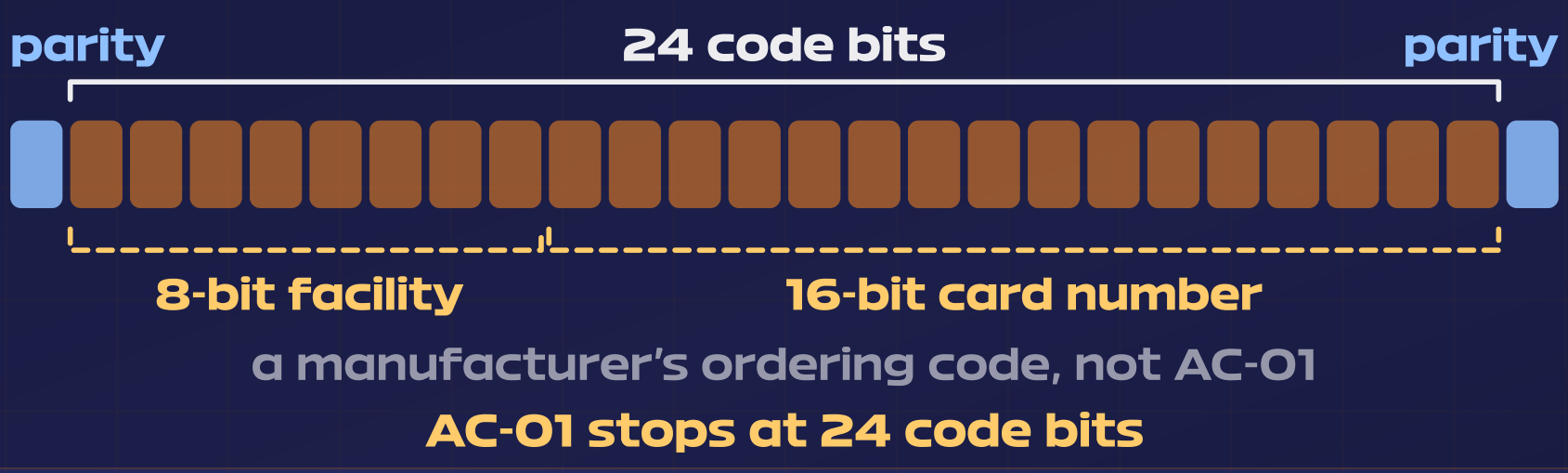


AC-01 sets a window: 20 to 100 µs pulses, and a 200 µs to 20 ms pulse interval, which reader makers define as the pause between pulses. The typical example, a **50 µs** pulse plus a **1 ms** gap, is ≈1.05 ms per bit: ≈**952 bit/s**. [2][5]

That is raw signalling, not throughput or door response: a 26-bit frame at this timing lasts ≈26 ms, while one HID reader quotes 175 ms to read and report a card. OSDP does not make doors ten times faster. [5]

THE SPLIT THAT IS NOT IN THE STANDARD

AC-01 defines the frame, not its meaning



a manufacturer's ordering code, not AC-01

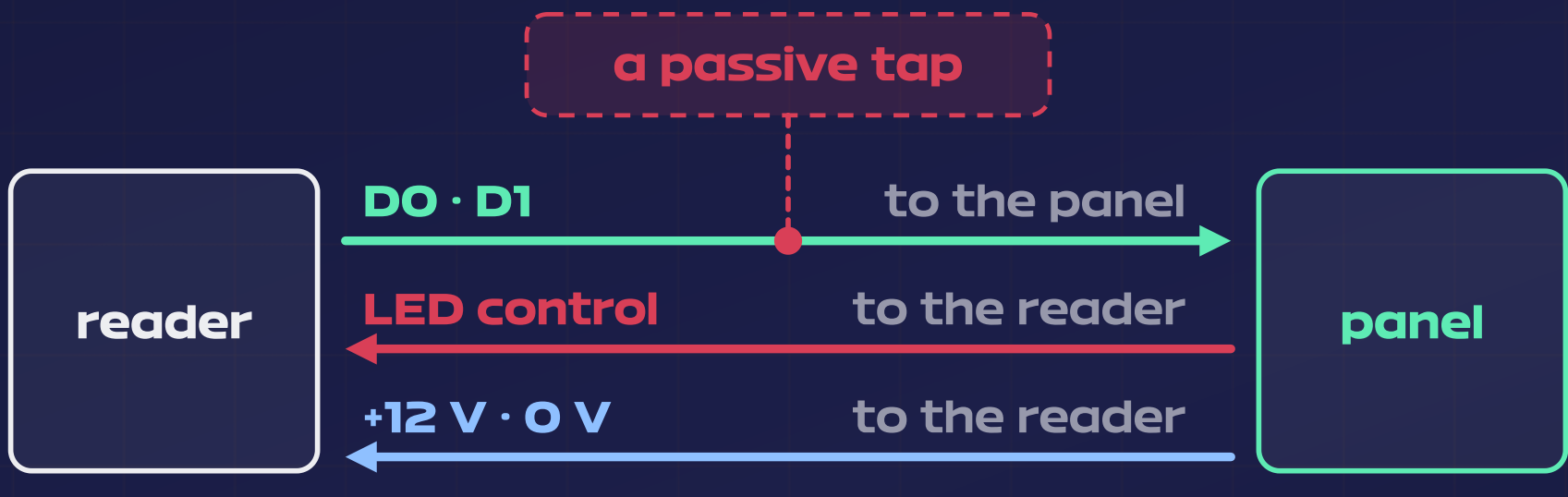
AC-01 stops at 24 code bits

AC-01 clause 5 defines the 26-bit frame as 2 parity bits plus **24 code bits**, and leaves the split to the manufacturers. The familiar **8-bit facility code + 16-bit card number** is one manufacturer format, H10301, not part of AC-01. [2]

So "Wiegand 26" does not always mean 8 + 16, and longer formats exist. The interface carries no length field and no integrity check beyond the two parity bits. [2][5]

THE FIFTH WIRE

Wiegand data is one-way. The cable isn't.



AC-01: no built-in passive-tap detection

Card data on D0/D1 runs reader to controller. The LED control conductor (clause 3.2.5) and the power pair run the other way. **AC-01 provides no built-in mechanism to detect a passive tap on D0/D1.** [2]

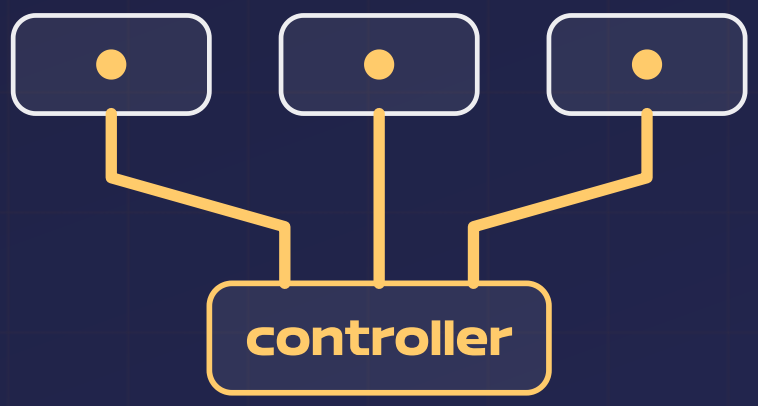


The other end of the same wire, in the riser. Keep it locked, tamper-supervised and out of public reach.

WIRING, NOT CRYPTOGRAPHY

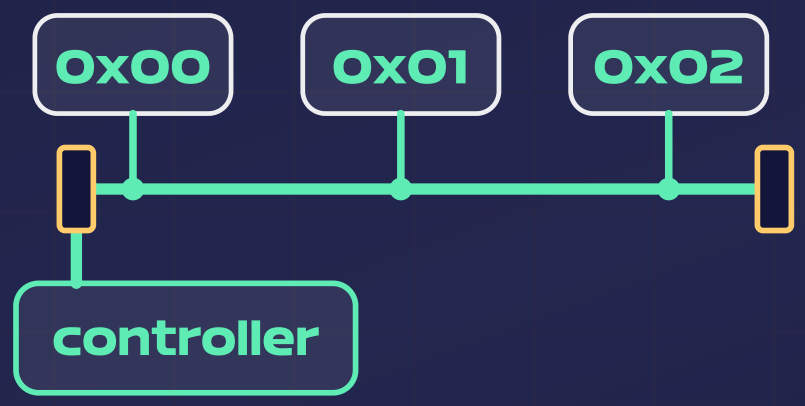
Home run against multidrop

Wiegand, home run



one cable per reader
8 terminals in practice
61 to 153 m by gauge

OSDP, multidrop



one pair plus power
terminated daisy chain
200 m controller-powered

Topology is not security; Secure Channel is. Wiegand runs one cable per reader. OSDP shares one RS-485 pair as a daisy chain terminated at both ends; HID's Signo guide calls for 120 Ω termination on OSDP runs over 61 m. The controller polls each address, so a silent reader shows as offline. [7]

Address space is not port capacity: OSDP addresses run 0x00 to 0x7E (127 devices), while the HID Mercury MP1501 takes 2 OSDP devices per reader port. Check each controller's own limit. [7]

THE COMPARISON EVERYONE OVERSTATES

Physical-layer distance is not powered-door distance

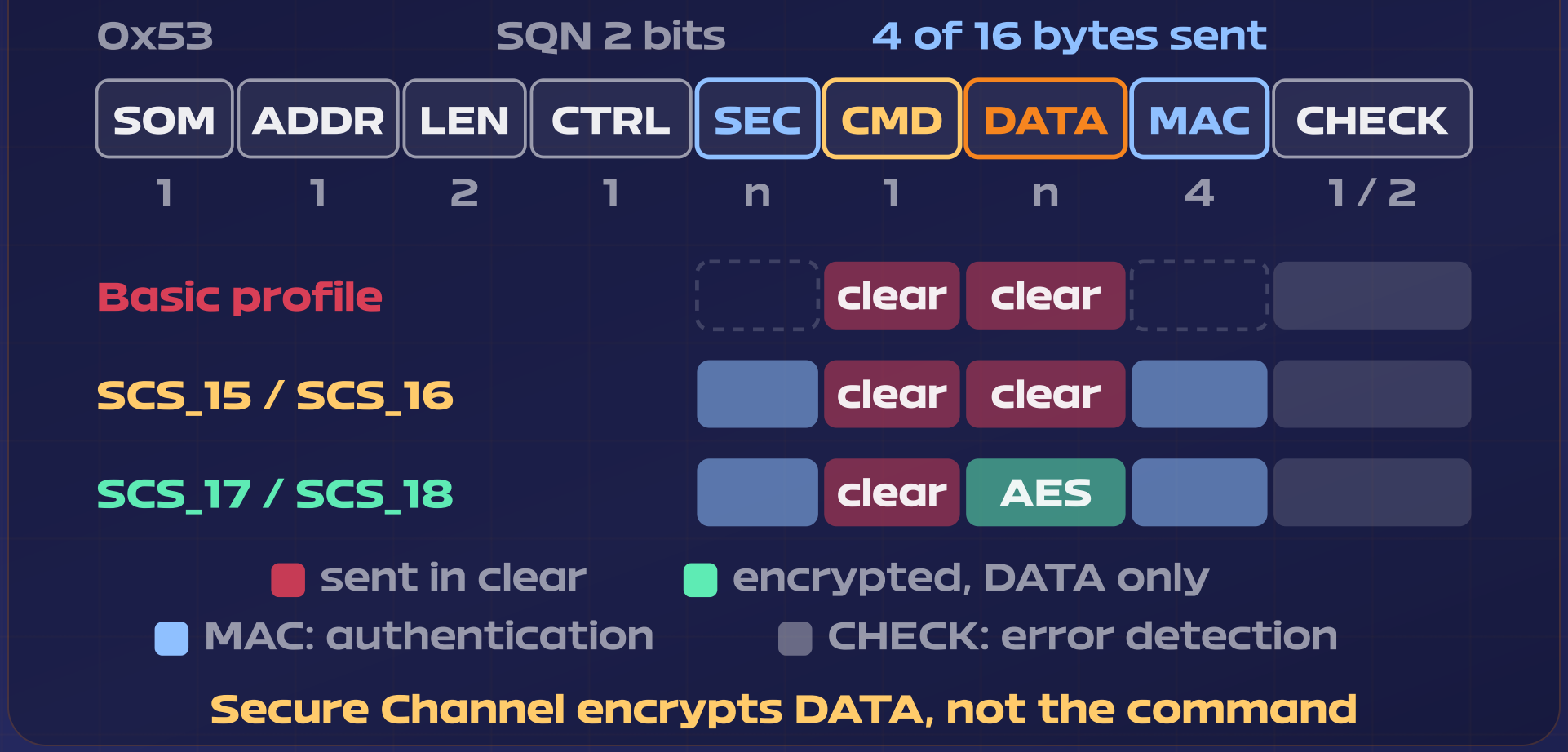


AC-01 guidance for Wiegand: **61 m at 22 AWG, 91 m at 20 AWG, 153 m at 18 AWG**. Axis's A1610 guidance for OSDP: **200 m to a controller-powered reader**, up to 1,000 m for data with a locally powered reader. ≈1,200 m is the RS-485 physical-layer guideline, not an OSDP limit. Product examples. [2][7]

Against 18 AWG Wiegand: ≈7.8× on paper, ≈1.3× at a controller-powered door.

THE SENTENCE THAT SELLS FALSE COMFORT

OSDP does not automatically mean encrypted traffic. Read the packet.



Three protections, three jobs. A checksum or CRC on every packet detects errors. In Secure Channel, a MAC over the packet authenticates it. Only SCS_17/18 also encrypt the **DATA field** with AES-128; header and command stay visible. Basic OSDP has only the first. [4][7]

SCS_15/16 carry a MAC with readable data and are meant for POLL and ACK. Specify Secure Channel **enforced**: the controller rejects readers without it. [7]

THE MOST CHECKABLE THING ON A COMMISSIONING WALK

The site key can travel under a published one



Three keys: **SCBK-D**, the published install-mode default; the **SCBK**, each reader's persistent base key; and session keys derived from it every session. Pair in install mode over untrusted wiring and a recording can reveal the SCBK. Refusing SCBK-D later does not undo that. [4][7]

Provision on physically trusted wiring or by the manufacturer's out-of-band method, then confirm SCBK-D is refused. [7]

BITS OF SECRECY, NOT BITS OF KEY

A 128-bit key can be worth 0 bits

SCBK-D, the default — **0 bits**

to anyone who has the specification

install mode left open — **0 bits**

to a device on the wire that asks

Bishop Fox's 3 tested patterns — **9.6 bits**

768 candidates, this set only

a uniformly random 128-bit key — **128 bits**

only if truly random and kept secret

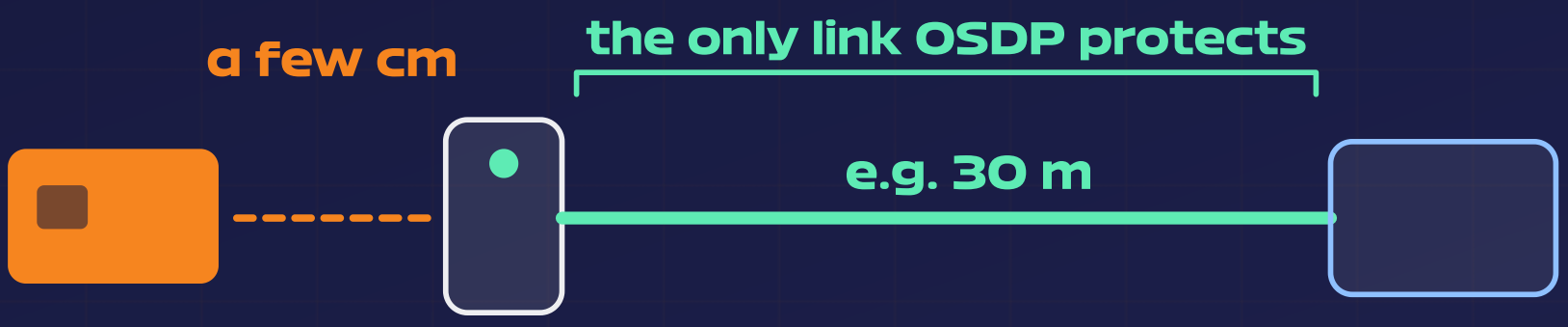
a key is worth its search cost, not its length

AES-128 is not broken; key management is the weak point. A published default is worth 0 bits to anyone with the specification, and install mode left open can hand the key to a device on the wire. Bishop Fox's three tested patterns give 768 candidates: log2(768) ≈ 9.6 bits for that set only. [4]

Only a key drawn uniformly at random from all 2^{128} values, and kept secret, is worth 128 bits. "Site-generated" does not prove that.

THE REORDERING THIS EPISODE EXISTS FOR

OSDP protects the reader-controller link. Credential cloning is a separate risk.



credential	reader	wire	controller
clone or downgrade the card	defaults, legacy on	tap, downgrade, capture the key	firmware flaws
keyed file, legacy off	high security only	unique keys, tamper alarmed	vendor patches applied

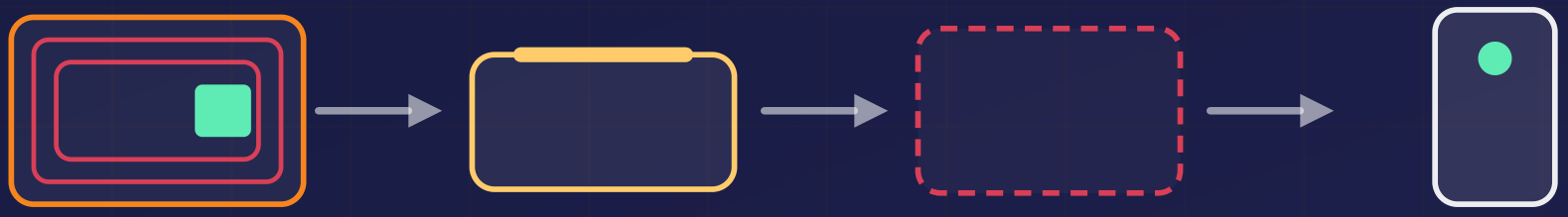
■ the published attack ■ the control that closes it

Secure Channel protects the reader-to-controller link. It does not secure the credential, legacy 125 kHz cards, open formats, reader configuration or controller firmware. **Fix the link and the credential: neither replaces the other.** [1][6]

Firmware is in the chain: CVE-2023-21406, an OSDP parser flaw in AXIS A1001 firmware 1.65.4 or earlier, was fixed by an Axis update. [9]

THE CRYPTOGRAPHY IS NOT THE TARGET

A downgrade attack never needs to break AES-128



one card 125 kHz and AES-128

an encoder reads the legacy number

a blank card written with it

the reader opens the door

the AES-128 chip is not attacked

HID describes attackers who cannot copy a Seos or DESFire credential and "use migration mode in reverse": the credential data is read and re-encoded onto a legacy card. It works only where the legacy technology stays enabled and the reader accepts it. [6]

Exposure depends on configuration. HID's fix: disable legacy credentials in the reader once migration ends, or order readers in a **high-security-only profile** that cannot enable migration mode. [6]

THE PART CRYPTOGRAPHY CANNOT FIX

A credential number alone is not proof of authenticity

open	tracked	restricted
H10301	H10302	Corporate 1000
anyone can order a number	HID controls issuance	authorised buyers only
duplicates possible	duplicates prevented	duplicates prevented

issuance control is not proof of authenticity
that needs card authentication

A credential number identifies a user; it does not prove the card is genuine. That takes card authentication, protected credential data, controlled issuance and correct controller authorisation. HID still asks for credential numbers to be protected like passwords. [6]

Open formats such as H10301 "may be ordered by any individual", so duplicates are possible. Tracked and restricted formats control issuance; they do not authenticate the card. [6]

TWO LADDERS, AND NEITHER OPENS THE DOOR

Grade is not the same as Level. And the standard excludes the lock.

IEC 60839-11-1

1	2	3	4

set by risk assessment, per access point

UL 294

I	II	III	IV

set by type testing, per product

two ladders, two different bases

1. **IEC 60839-11-1** Grades 1 to 4 are set per access point by risk assessment; **UL 294** Levels I to IV come from product testing. Separate systems: do not read Grade 4 as Level IV. [3]
2. IEC 60839-11-1 sends locks, openers, turnstiles and barriers to other standards. Power-loss behaviour, fail-safe (unlocks) or fail-secure (stays locked), is defined in 11-2 but not mandated. [3]

Escape doors follow SBC 201-CR-2024 and SBC 801-CR-2024, Section 1010, and Civil Defence escape-route rules: opening without a key or special knowledge, and manual opening if automatic means fail. Check each door. [8]

THE SAUDI ANSWER, HONESTLY

No explicit OSDP requirement was identified in the Saudi references reviewed (4 October 2026)

access, CCTV logs	NCA ECC-2:2024, 2-14
GSO standards found	11-1:2014, 11-2:2016
OSDP part, 11-5	not found in GSO search
OSDP on the wire	no explicit requirement found

projects and clients can still specify it
references reviewed 4 October 2026

NCA **ECC-2:2024** applies to government entities and private operators of critical national infrastructure. Control 2-14 requires authorised access to critical areas, access and monitoring logs (CCTV) and their protection; it names no reader protocol. [8]

A GSO store search on 4 October 2026 listed IEC 60839-11-1 and 11-2 as Gulf standards; 11-5 did not appear. A GSO standard is not by itself a Saudi mandate, and projects or clients can still require OSDP. [8]

WRITE THIS INSTEAD

Six checks before handover

1. **Credentials:** Specify secure technology; disable legacy credentials unless justified.
2. **Issuance:** Control issuance and protect credential numbers as sensitive data.
3. **Link:** Enforce OSDP Secure Channel; reject unsecured reader connections.
4. **Keys:** Use unique random reader keys; provision securely and reject SCBK-D in normal operation.
5. **Supervision:** Test tamper and offline alarms; apply vendor firmware updates.
6. **Door:** Set the grade and power-loss behaviour to meet fire, life-safety and building requirements.

Handover: test results and key-generation records, never the keys. OSDP Verified confirms conformance, not installation security. [1]

SOURCES

Where each claim comes from

[1] SIA OSDP v2.2.2 (Oct 2024); IEC 60839-11-5:2020, Ed. 1.0 SIA statements 10 Aug 2023, 18 Mar 2026; OSDP Verified list, Jun and Jul 2026

[2] SIA AC-01-1996.10, 26-Bit Wiegand Reader Interface cl. 3.2, 3.3, 4.3, 5; SIA catalogue entry, archived Jun 2026

[3] IEC 60839-11-1:2013, cl. 1; IEC 60839-11-2:2014, cl. 7.3.1 UL 294:2023, 8th edition

[4] Bishop Fox, Badge of Shame: Breaking into Secure Facilities with OSDP DEF CON 31, 9 Aug 2023

[5] US 8,358,783 B2, Table 1A; BALTECH, Wiegand specification HID ThinLine II manual 5395-901, p.5; Gecko (2008); BLEKey (2015)

[6] HID Global, Safeguarding Against Legacy Downgrade Attacks (2024) pp.1 to 4

[7] ICT AN-321 (Nov 2024), pp.9 to 27; HID Mercury MP1501 Axis A1610, TA1101-B; HID Signo installation guide; TIA-485-A

[8] NCA ECC-2:2024, 2-14; SBC 201-CR-2024 and 801-CR-2024, Section 1010 Civil Defence escape-route rules, ch. 3; GSO store search, 4 Oct 2026

[9] Axis security advisory and NVD record, CVE-2023-21406 AXIS A1001, firmware 1.65.4 or earlier

Links: the Sources section of the article (QR on the next slide).

PRACTICAL ACCESS CONTROL ENGINEERING

Save this. Send it to a colleague.

Read the full episode article

https://nlc.com.sa/academy/access-control-osdp.html

Next episode
Public Address and STI