SIA OSDP for Deployment Teams

April 2017

SMITHEE SPELVIN AGNEW PLINGE

Introduction to SIA OSDP

- Introduction to badge technologies for physical and logical access
- Credential data formats and technology
- Iso stack, layer 1
- Data structures
- Protocols
- IoT Considerations
- Protocols and standards

SMITHEE SPELVIN AGNEW PLINGE

TIA/EIA-485-A (a/k/a RS-485) Signalling challenge

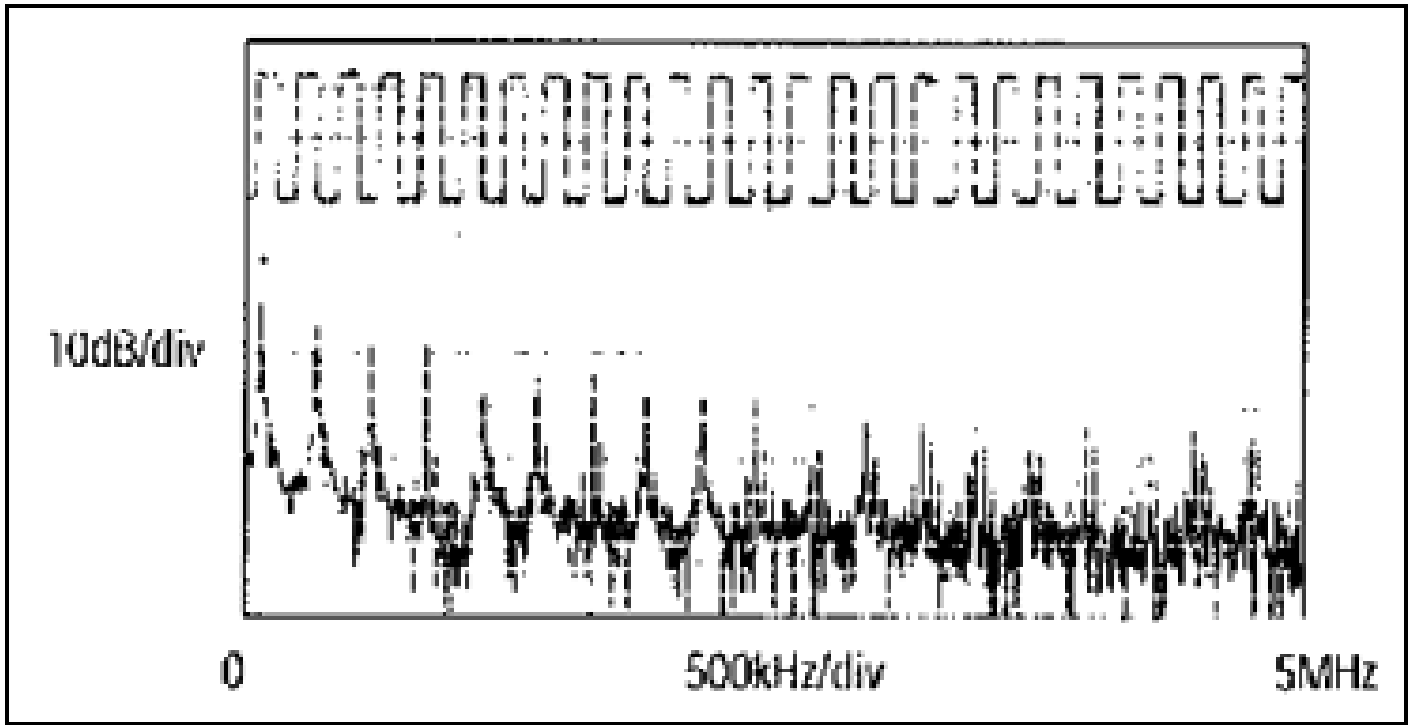
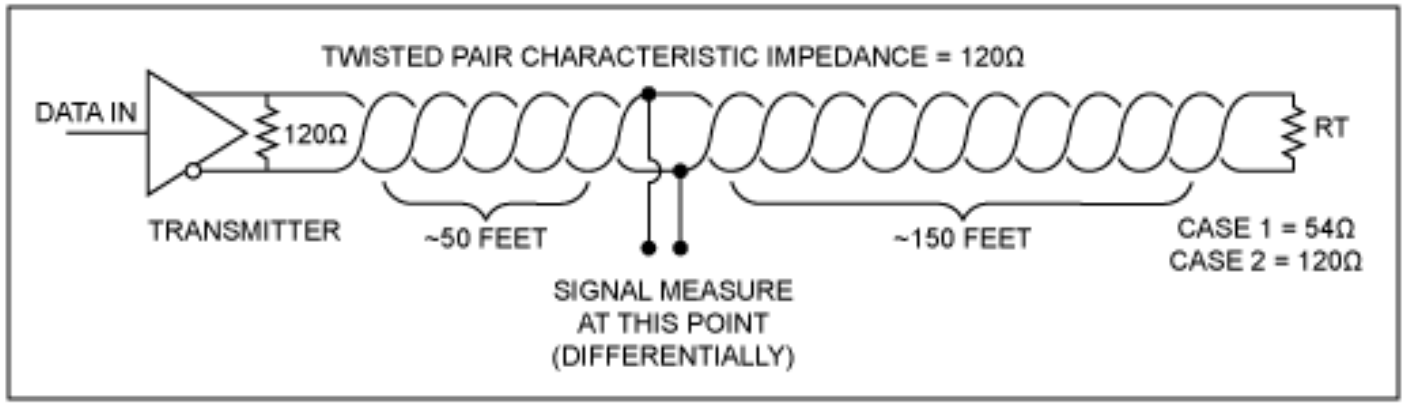


Figure 3. Waveform of a 125kHz square wave and its FFT plot.

SMITHEE SPELVIN AGNEW PLINGE

TIA/EIA-485-A (a/k/a RS-485) Terminated Twisted Pair



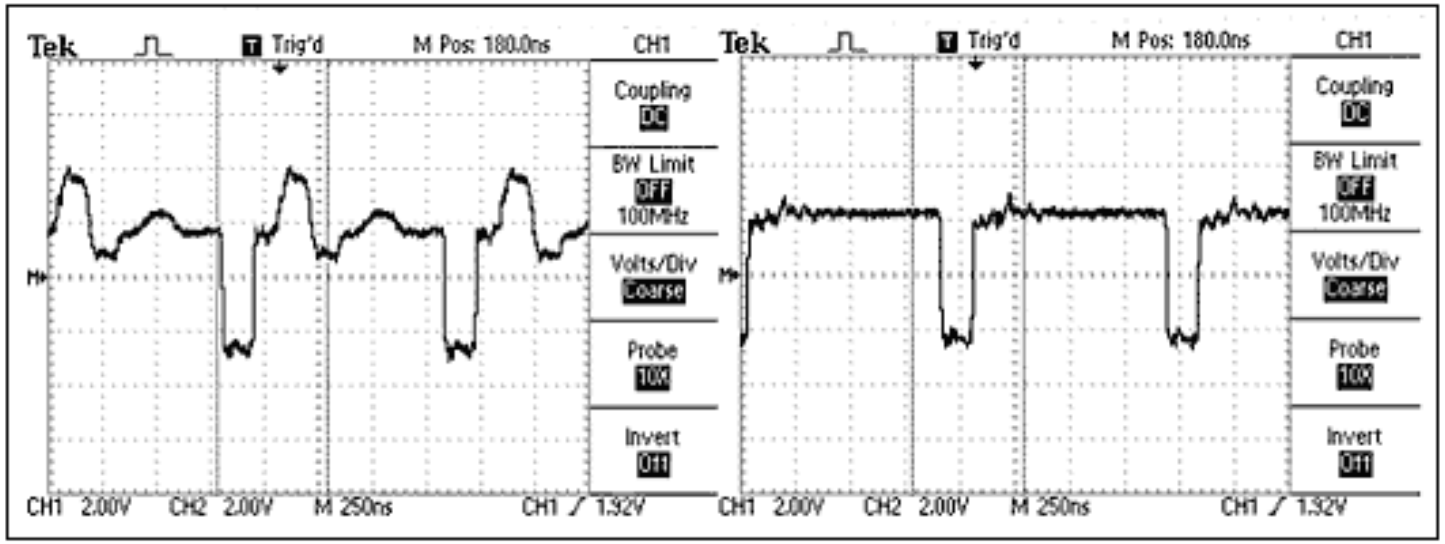


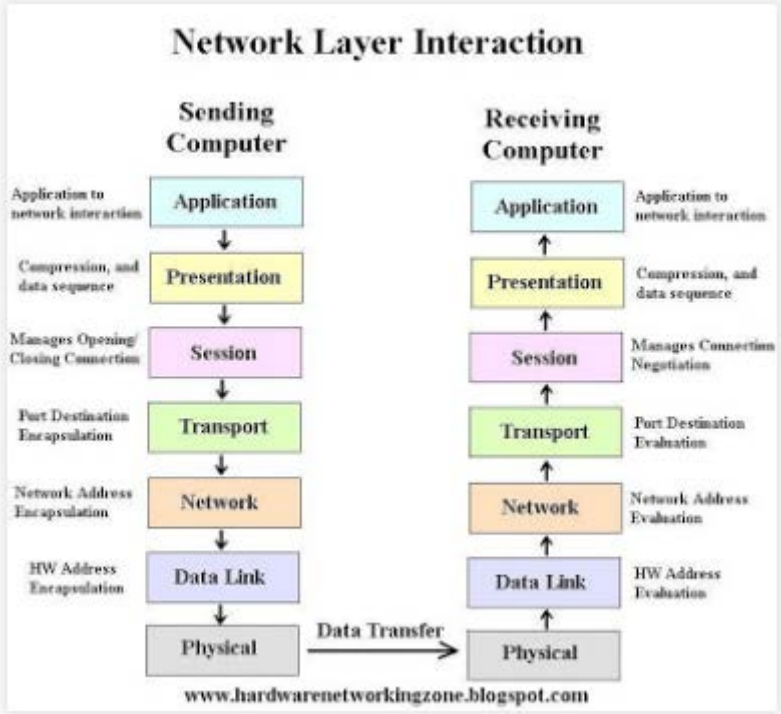
Figure 5. Using the circuit shown at the top, the waveform on the left was

SIA OSDP Use Cases

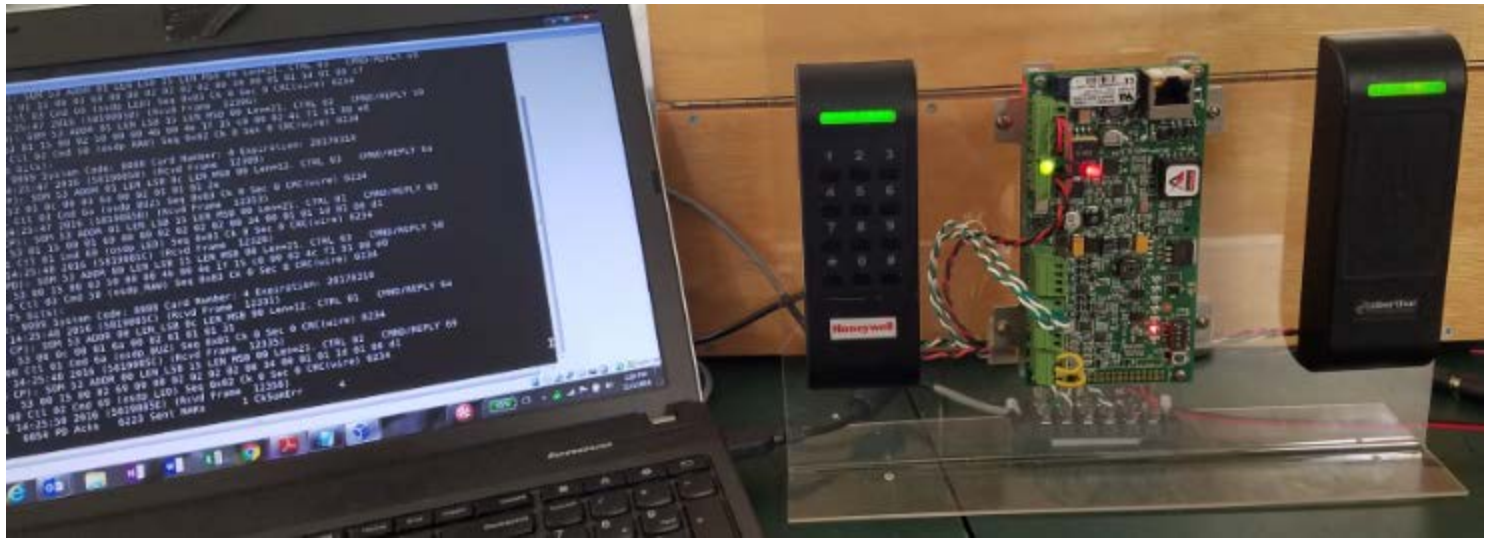
- Stock old school 26 bit wiegand
- Output signaling
- Input signaling
- Bidirectional credentials communications
- Secure card communications
- Standardized reader interface

SMITHEE SPELVIN AGNEW PLINGE

OSDP: Data Link Layer (Layer 2) protocol



Meanwhile, at Layer 2



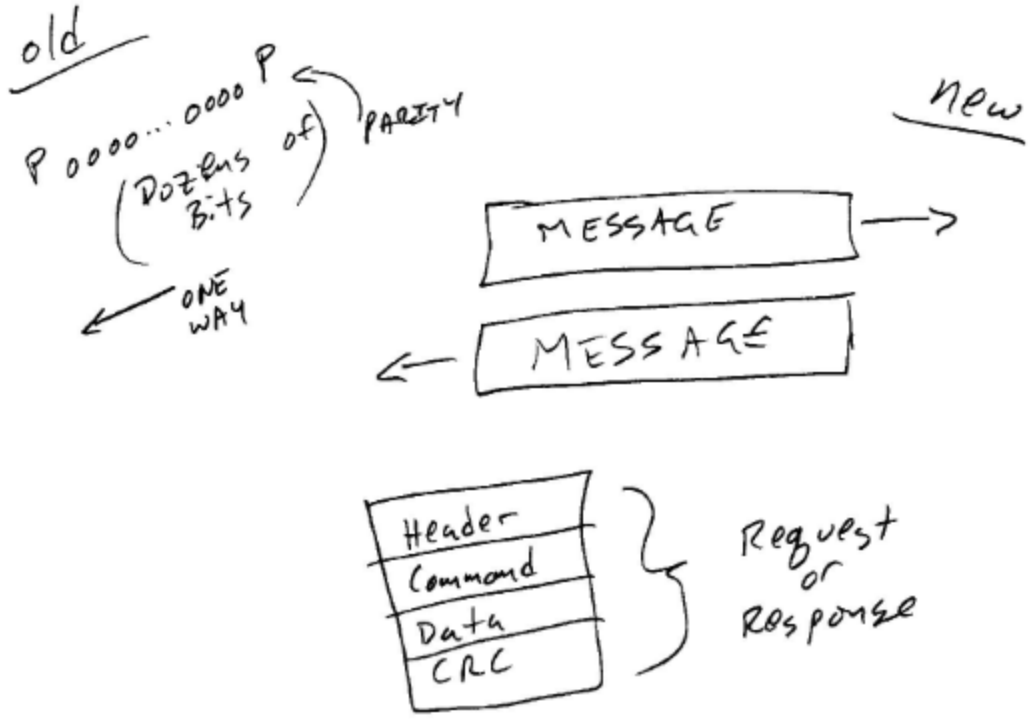
SMITHEE SPELVIN AGNEW PLINGE

SIA OSDP Protocol

There are computers in the card readers and the panels.

SMITHEE
SPELVIN
AGNEW
PLINGE

OSDP: A Computer to Computer Protocol



SMITHEE SPELVIN AGNEW PLINGE

Communications Protocol

- Document specification of message format.
- Error correction.
- message sequencing.
- acknowledgements (positive and negative.)
- Message addressing.
- Intended for public distribution.
- Meant for interoperable use.
- Implemented by multiple vendors.

SMITHEE SPELVIN AGNEW PLINGE

It's a *Standard*

- ANSI-accredited organization
- ANSI-track document standards process
- Not vendor-specific
- Not patent encumbered
- At least three genetically separate implementations exist
- Open source implementation available

SMITHEE SPELVIN AGNEW PLINGE

It's a *Thing* thing

- Intended for constrained computing platforms.
- Used in infrastructure.
- Protocol purpose-built with limited functionality.
- Works in environments too constrained for conventional (TCP/IP) networking.
- Roughly equivalent to MQTT or other low-end control protocols.
- Like an IoT thing but created in the 1990's.

SMITHEE SPELVIN AGNEW PLINGE

SIA

Published Standard

Open Supervised Device Protocol (OSDP)
Version 2.1.7

Communication Protocol for Peripheral Devices with Data Security Extension

SMITHEE SPELVIN AGNEW PLINGE

OSDP Concepts

- Taxonomy: CP and PD
- PD's can be Peripheral (minimal), Basic, Biometrics, Extended Packet Mode
- 2-wire RS-485 (TLS version proposed)

SMITHEE SPELVIN AGNEW PLINGE

OSDP Dialog

- 2-way, acknowledged, with multipart-messaging available.
- Read credentials
- Interact with credentials
- Receive input signaling (alarm points.)
- Send output signaling (relay output.)

SMITHEE SPELVIN AGNEW PLINGE

OSDP Profiles

- Peripheral – minimal device
- Basic – classic card reader (sends OSDP_RAW)
- Biometrics – supports appropriately implemented classic fingerprint-based biometric match solutions
- Credential processing – Extended Packet Mode to interact with intelligent (phone, smart card) credentials.

SMITHEE SPELVIN AGNEW PLINGE

OSDP Messages

- Poll, Ack, and Nak
- Raw Data
- Ident
- Capabilities
- Input change: Tamper, signal in, power
- Output: LED, signal out

SMITHEE SPELVIN AGNEW PLINGE

OSDP Message Format

Byte	Name	Meaning	Value
0	SOM	Start of Message	0x53
1	ADDR	Physical Address of the PD	0x00 – 0x7E 0x7F = configuration
2	LEN_LSB	Packet Length Least Significant Byte	Any
3	LEN_MSB	Packet Length Most Significant Byte	Any
4	CTRL	Message Control Information	See List
	SEC_BLK_LEN	(optional) Length of Security Control Block	Any
	SEC_BLK_TYPE	(optional) Security Block Type	See List
	SEC_BLK_DATA	(optional) Security Block Data	Based on type
	CMND/REPLY	Command or Reply Code	See List
	DATA	(optional) Data Block	Based on CMD/REPLY
	MAC [0]	(optional) Present for secured messages, dependent on SEC_BLK_TYPE; (see Appendix D)	
	MAC [1]	"	
	MAC [2]	"	
	MAC [3]	"	
	CKSUM/CRC_LSB	Checksum, or, CRC-16 Least Significant Byte	
	CRC_MSB	(optional) CRC-16 Most Significant Byte	

SMITHEE SPELVIN AGNEW PLINGE

Command Messages

Commands

Name	Value	Meaning	Data
osdp_POLL	0x60	Poll	None
osdp_ID	0x61	ID Report Request	Id type
osdp_CAP	0x62	PD Capabilities Request	Reply type
osdp_DIAG	0x63	Diagnostic Function Command	Request code
osdp_LSTAT	0x64	Local Status Report Request	None
osdp_ISTAT	0x65	Input Status Report Request	None
osdp_OSTAT	0x66	Output Status Report Request	None
osdp_RSTAT	0x67	Reader Status Report Request	None
osdp_OUT	0x68	Output Control Command	Output settings
osdp_LED	0x69	Reader Led Control Command	LED settings
osdp_BUZ	0x6A	Reader Buzzer Control Command	Buzzer settings
osdp_TEXT	0x6B	Text Output Command	Text settings
osdp_RMODE	0x6C	... removed ...	
osdp_TDSET	0x6D	Time and Date Command	Time and Date
osdp_COMSET	0x6E	PD Communication Configuration Command	Com settings
osdp_DATA	0x6F	Data Transfer Command	Raw Data
osdp_XMIT	0x70	... removed ...	
osdp_PROMPT	0x71	Set Automatic Reader Prompt Strings	Message string
osdp_SPE	0x72	... removed ...	
osdp_BIOREAD	0x73	Scan and Send Biometric Data	Requested Return Format
osdp_BIOMATCH	0x74	Scan and Match Biometric Template	Biometric Template
osdp_KEYSET	0x75	Encryption Key Set Command	Encryption Key
osdp_CHLNG	0x76	Challenge and Secure Session Initialization Rq.	Challenge Data
osdp_SCRYPT	0x77	Server Cryptogram	Encryption Data
osdp_CONT	0x79	... removed ...	
osdp_MFG	0x80	Manufacturer Specific Command	Any
	A0-EF	Reserved for Application Specific Messages	
osdp_SCDONE	0xA0	... removed ...	
osdp_XWR	0xA1	See Application Specific Messages	Defined in ASM Document
osdp_ABORT	0x7A	Stop Multi Part Message	None
osdp_MAXREPLY	0x7B	Maximum Acceptable Reply Size	

Reply Messages

Replies

Name	Value	Meaning	Data
osdp_ACK	0x40	Command accepted, nothing else to report	None
osdp_NAK	0x41	Command not processed	Reason for rejecting command
osdp_PDID	0x45	PD ID Report	Report data
osdp_PDCAP	0x46	PD Capabilities Report	Report data
osdp_LSTATR	0x48	Local Status Report	Report data
osdp_ISTATR	0x49	Input Status Report	Report data
osdp_OSTATR	0x4A	Output Status Report	Report data
osdp_RSTATR	0x4B	Reader Status Report	Report data
osdp_RAW	0x50	Reader Data – Raw bit image of card data	Card data
osdp_FMT	0x51	Reader Data – Formatted character stream	Card data
osdp_PRES	0x52	... removed ...	
osdp_KEYPPAD	0x53	Keypad Data	Keypad data
osdp_COM	0x54	PD Communications Configuration Report	Comm data
osdp_SCREP	0x55	... removed ...	
osdp_SPER	0x56	... removed ...	
osdp_BIOREADR	0x57	Biometric Data	Biometric data
osdp_BIOMATCHR	0x58	Biometric Match Result	Result
osdp_CCRYPT	0x76	Client's ID, Random Number, and Cryptogram	Encryption Data
osdp_RMAC_I	0x78	Initial R-MAC	Encryption Data
osdp_MFGREP	0x90	Manufacturer Specific Reply	Any
osdp_BUSY	0x79	PD is Busy reply	
osdp_XRD	0xB1	See Application Specific Messages	Defined in ASM Document
~~osdp_XRD~~	~~0xB1~~	~~See appendix~~	~~Defined in Appendix E~~

Poll and Ack

Message: osdp_POLL Addr:00 Lth:8. CTRL 05 Cmd 60 Seq:01 Sec 0 CRC 99da(4)

OSDP PD Frame-in:0007 Timestamp:20160824-104931 (Sec/Nanosec: 1474739371 57347661)

Raw: 53 80 08 00 05 40 68 9f

Message: osdp_ACK Addr:00 Lth:8. CTRL 05 Cmd 40 Seq:01 Sec 0 CRC 9f68(4)

OSDP CP Frame-in:0008 Timestamp:20160824-104935 (Sec/Nanosec: 1474739375 75618128)

Raw: 53 00 08 00 06 60 89 cc

SMITHEE SPELVIN AGNEW PLINGE

OSDP Basic Profile

✓ = REQUIRED TO CONFORM TO PROFILE		Basic Reader
Communication Settings		
2.1	Physical Interface	✓
2.2	Signaling	✓
2.3	Character Encoding	✓
2.4	Channel Access	✓
2.5	Multi-byte Data Encoding	✓
2.6	Packet Size Limits	✓
2.7	Timing	✓
2.8	Message Synchronization	✓
2.9	Packet Format	✓
2.10	SOM – Start of Message	✓
2.11	ADDR – Address	✓
2.12	LEN – Length	✓
2.13	CTRL - Control	✓
2.14	Security Block	✓
2.15	CMND/REPLY - Command/Reply Code	✓
2.16	CHKSUM/CRC16 - Message Check Codes	✓
2.17	Messages Supporting the Transfer of Large Data Arrays	
Commands		
3.1	Poll (osdp_POLL)	✓
3.2	ID Report Request (osdp_ID)	✓
3.3	Peripheral Device Capabilities Request (osdp_CAP)	✓
3.4	Diagnostic Function Request (osdp_DIAG)	✓
3.5	Local Status Report Request (osdp_LSTAT)	✓

SMITHEE SPELVIN AGNEW PLINGE

OSDP Basic Profile (cont.)

3.6	Input Status Report Request (osdp_ISTAT)	✓
3.7	Output Status Report Request (osdp_OSTAT)	✓
3.8	Reader Status Report Request (osdp_RSTAT)	✓
3.9	Output Control Command (osdp_OUT)	✓
3.10	Reader LED Control Command (osdp_LED)	
3.11	Reader Buzzer Control Command (osdp_BUZ)	
3.12	Reader Text Output Command (osdp_TEXT)	
3.14	Communication Configuration Command (osdp_COMSET)	
3.16	Set Automatic Reader Prompt Strings (osdp_PROMPT) *DRAFT*	
3.17	Scan and Send Biometric Template (osdp_BIOREAD)	
3.18	Scan and Match Biometric Template (osdp_BIOMATCH)	
3.19	Continue Multi-Part Message (osdp_CONT)	
3.20	Manufacturer Specific Command (osdp_MFG)	
3.21	Manufacturer Specific Command (osdp_MFG) NEW	
3.22	Stop Multi Part Message (osdp_ABORT)	
3.23	Maximum Acceptable Reply Size (osdp_MAXREPLY)	
Replies		
4.1	General Acknowledge, Nothing to Report (osdp_ACK)	✓
4.2	Negative Acknowledge – SIO Comm Handler Error Response (osdp_NAK)	✓
4.3	Device Identification Report (osdp_PDID)	✓
4.4	Device Capabilities Report (osdp_PDCAP)	✓
4.5	Local Status Report (osdp_LSTATR)	✓
4.6	Input Status Report (osdp_ISTATR)	✓
4.7	Output Status Report (osdp_OSTATR)	✓
4.8	Reader Tamper Status Report (osdp_RSTATR)	✓
4.9	Card Data Report, Raw Bit Array (osdp_RAW)	
4.10	Card Data Report, Character Array (osdp_FMT)	
4.11	Keypad Data Report (osdp_KEYPAD)	
4.12	Communication Configuration Report (osdp_COM)	
4.13	Scan and Send Biometric data (osdp_BIOREADR)	
4.14	Scan and Match Biometric Template (osdp_BIOMATCHR)	
4.15	Manufacturer Specific Reply (osdp_MFGREP)	
4.16	Manufacturer Specific Reply (osdp_MFGREP) NEW	
4.17	PD Busy Reply (osdp_BUSY)	

SMITHEE SPELVIN AGNEW PLINGE

Deployment, Maintenance, and Troubleshooting

Hang it on the wall, keep it on the wall, fix it when it falls off the wall.

SMITHEE
SPELVIN
AGNEW
PLINGE

Deployment Considerations

- Specification
- Credential Configuration
- Components: readers, mounting tools, config tools, cabling, documentation, configuration specs
- Credential, PACS, and CP preparation
- PD staging
- OSDP CP configuration
- OSDP PD configuration

SMITHEE SPELVIN AGNEW PLINGE

OSDP Deployment Check-list

- CP asset management (firmware, documentation)
- CP configuration
- Wiring, line speed, line termination, wiring topology (CP and PD)
- PD configuration
- PD asset management (firmware, documentation)
- Key management
- Installation meets specs
- Calibration

SMITHEE SPELVIN AGNEW PLINGE

Disposal

- Zeroize the keys
- Reset to factory default (which should zeroized the keys)
- External marking and identity scrub

SMITHEE
SPELVIN
AGNEW
PLINGE

SIA

Maintenance

- Reader environment
- Cabling
- Firmware updates (CP and PD)
- Key management
- Wear and tear (and vandals and hackers)
- Credential stability and evolution

Troubleshooting

- Configuration
- Telemetry
- Re-calibration
- Updates
- Diagnostic analysis

Tracing and Diagnostics

- RS-485 data trace
- Diagnostic tools
- 3-rd party OSDP tools (libosdp, others)
- Device statistics and logs
- Protocol troubleshooting

SMITHEE SPELVIN AGNEW PLINGE

Thank you!

Be safe out there.

References

- http://hardwarenetworkingzone.blogspot.com/2013/06/osi-model-concept.html
- https://www.maximintegrated.com/en/app-notes/index.mvp/id/763

SMITHEE SPELVIN AGNEW PLINGE

About Smithee…

- Consultancy based in northern California.
- Focus on network integration and security issues for physical security and infrastructure operators.
- Delivers consulting, training, technical evaluation services.
- The name comes from standardized anonymous names used for authors in the theatre world.

SMITHEE SPELVIN AGNEW PLINGE

Contact

Rodney Thayer

Smithee,Spelvin,Agnew & Plinge, Inc.

rodney@smithee.us

Office 510 488 4448