AN002: OSDP Security

Open Supervised Device Protocol (OSDP) is a standard developed by the Security Industry Association (SIA) as a replacement for the ageing Wiegand protocols. Some of the key benefits of OSDP include the supervision of peripheral devices by the controller, a more robust communication link over RS-485, multi-drop installations and advanced functionality such as file transfer, giving the ability to update products in the field where supported. OSDP can also include an encryption layer utilising symmetric keys, to make the life of an attacker much more difficult.

All of Third Millennium's top-shelf products are OSDP Verified and support the latest OSDP standards. We also hold positions in multiple OSDP working groups, allowing us to influence, guide and observe any new directions the standard may take, ensuring that our products are at the leading edge for compatibility and security.

The OSDP encryption layer has recently come under scrutiny following media reports of a talk by security research group Bishop Fox at the Blackhat Convention 2023. The main concerns expressed during the talk were:

- Encryption is Optional
- Downgrade Attack
- Install-mode Attack
- Weak Keys
- Keyset Capture

To address them in turn:

Encryption is Optional

Encryption is not a requirement of OSDP though while running in unsecured mode, there are still benefits over a Wiegand installation such as supervision and liveness from polling. Using Secure Channel is recommended whenever possible, which all shipping Third Millennium readers support. The OSDP Verified product list is a good resource to make sure you purchase a controller which is compliant with the OSDP V2.2 specification and may be configured for Secure Channel use.

Downgrade Attack

A controller may request a response from a reader indicating what that reader can do. This attack implies a hypothetical scenario where this reply is intercepted and modified to indicate that the secure communications channel is not supported. It is up to controller manufacturers to ensure that once a secure channel is established, the controller will not fall back to unencrypted communication without requiring user input to confirm that this is valid. Third Millennium readers take an additional security precaution and may only be paired one time, refusing to fall back to the open channel unless special configuration steps are taken to confirm that the line is secure.

Third Millennium Systems Ltd.

18 / 19 Torfaen Business Centre Panteg Way New Inn PONTYPOOL NP4 0LS United Kingdom
tel: +44 (0) 1495 751 992 web: www.tm-readers.com contact: info@tm-readers.com

Install-mode Attack

Installation mode is widely used throughout the industry for the initial key-sharing process to take place between the reader and controller. It avoids the onus of trust required to implement an asymmetric key system, as well as reducing the computational power required to calculate more complicated encryption functions. Instead, the trust is placed on the installation environment and controllers should require a proactive step to pair with a reader using this mode. After pairing is complete, in this trusted environment, the key can no longer be observed and a production rollout is permitted. The controller should also ensure that this installation environment is disabled after pairing is completed.

Weak Keys

Keys are determined by the access controller and weak keys should not be used in production. Some systems allow the user to enter their encryption key which should be securely generated and distributed. If the controller generates the key a user may reach out to the controller manufacturer for additional information to ensure they can confirm that they are using secure random number generators.

Keyset Capture

It is possible to observe the key exchange if you already know the key in use – for example, when in installation mode. This is why installation should be performed securely – and why Third Millennium has taken the extra step to ensure that this mode will not unintentionally be entered a second time to allow capture to take place in production.

When correctly installed, OSDP can be used in a secure configuration, mitigating against message replay or 'sniffing' attacks which plague Wiegand installations.

Third Millennium Systems Ltd.

18 / 19 Torfaen Business Centre Panteg Way New Inn PONTYPOOL NP4 0LS United Kingdom
tel: +44 (0) 1495 751 992 web: www.tm-readers.com contact: info@tm-readers.com

Appendix 1: ACU Best Practice Guide

Some Access Control Units require specific configurations to ensure that they are being used securely. The following will outline a few steps for some of the market-leading devices employed by the world's largest corporations.

If you would like your ACU to be added to this list, please email support@tm-readers.com allowing us to process the request further.

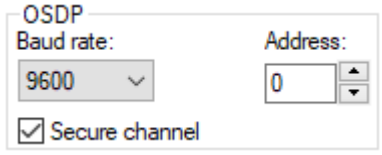
General Guidance

Where possible pairing using installation mode may be performed using a short fly lead directly to the ACU to ensure that the environment is strictly controlled. The reader may then be removed from this temporary connection and installed in its final location for production.

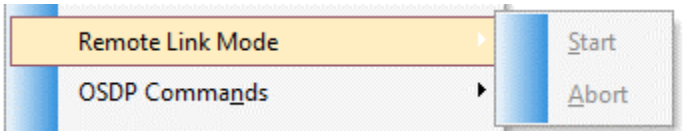
Lenel OnGuard

OnGuard supports Secure Channel, but you must make sure the following settings are used:

Secure Channel must be turned on in the reader configuration.



You can enable reader pairing in Alarm Monitor. Right-click the reader and select 'Remote Link Mode' and 'Start'. The reader should then pair.

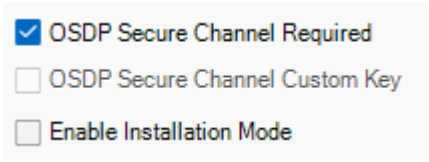


Screenshots captured in OnGuard V8.0, support may vary in other product versions.

Software House CCure

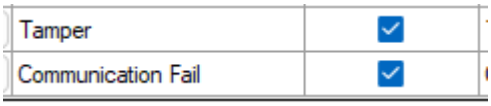
The following settings are recommended on CCure.

Enforce Secure channel required.



Installation mode will be used to initially pair the reader, but ensure that it is unticked once this first pairing has taken place.

Monitor failed communication and tamper status messages (when the reader has a tamper sensor enabled) and act when they occur.



Screenshots captured in CCure V2.90, support may vary in other product versions.

Third Millennium Systems Ltd.

18 / 19 Torfaen Business Centre Panteg Way New Inn PONTYPOOL NP4 0LS United Kingdom
tel: +44 (0) 1495 751 992 web: www.tm-readers.com contact: info@tm-readers.com