

HID® Lumidigm® V-Series Secure Line

Enhanced security with exceptional user convenience for real-world applications

It is estimated that 70% of security breaches originate at an endpoint. Don't let a fingerprint reader outside your firewall be an easy access point for bad actors looking to take control of your network or plant viruses and malware.

Endpoints are the weakest link in your network security. Connecting devices outside your well-protected internal network establishes a path for hackers to bypass standard security controls and access your network. Even the best firewalls are ineffective. Vulnerable endpoints enable cyber criminals to access your network stealing valuable data or holding data hostage.

HID's endpoint encryption is the critical layer for endpoint security. Encryption protects the data on the fingerprint readers and during

transmission, preventing cyber criminals from accessing your network. By effectively blocking threats and access attempts HID reduces your risk of:

- Downed networks and lost productivity
- Financial loss from theft, ransom or reparations to third parties
- Brand damage and lost customers

The V-Series Secure Line uses HID patented Multispectral Imaging technology to detect and reject fake finger attempts. The V-Series Secure Line provides onboard 1:1 matching, encrypted communication, and physical tamper protection. It is available in a USB desktop version and an OEM module for integration into a variety of devices.

HID PATENTED MSI WORKS ON THE MOST DIFFICULT FINGER TYPES



HID MSI ensures users have a fast, single-touch experience and authorized users are not falsely rejected.



V520



V521

KEY BENEFITS:



- Reduce Financial Losses – HID's market-leading, patented liveness detection technology, Multispectral Imaging (MSI), accurately and consistently identifies and rejects fake finger attempts
- Protect Data Assets – Encryption prevents cyber criminals from gaining unauthorized access to your networks and intellectual property
- Protect Keys – Physical tamper protection and active erase prevents cyber criminals from accessing encryption keys and data stored on fingerprint readers

SECURE LINE:

- Encrypted Communication – establishes a secure endpoint to prevent bad actors from accessing your networks
- Physical Tamper Protection – active erase technology prevents bad actors from accessing your encryption keys
- ISO Presentation Attack Detection Level 2 – detects and rejects sophisticated fake finger attempts
- Patented, HID Multispectral Imaging Technology – captures the most difficult finger types reducing false rejections and failures to enroll
- Sealed Ruggedized Housing – built to last in harsh environments
- Hard Glass Platen – withstands harsh cleaning chemicals and prevents increasing false rejections over time due to platen degradation from high-touch volumes

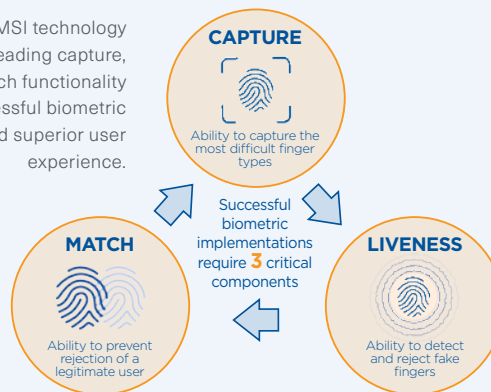
**HID Lumidigm V-Series Secure Line
V520 OEM Module**

**HID Lumidigm V-Series Secure Line
V521 USB Desktop Reader**

| | | |
|--|---|---|
| |  |  |
| | V520-01-01 | V521-01-01 |
| FINGERPRINT IMAGING SYSTEM | | |
| Technology | Patented Lumidigm® Multispectral Imaging (MSI) | |
| Output image resolution / bit depth | 500 dpi / 8-bit, 256 grayscale | |
| Platen area | 0.7" x 1.1" (17.8mm x 27.9mm) ellipse; durable, chemical resistant glass (no coatings to wear out) | |
| BIOMETRIC FUNCTIONS | | |
| Image output format | Uncompressed or WSQ compressed images (FBI Certified) | |
| Template output format | ANSI 378 and ISO 19794-2 compliant (MINEX III certified) | |
| Matching | 1:1 Matching On-Fingerprint Reader, 1:1 Matching On-Host | |
| Latent protection | User Configurable | |
| SECURITY FEATURES | | |
| Presentation Attack Detection (PAD) | ISO/IEC 30107-3, Level 2 Presentation Attack Detection (PAD) certified Multispectral Imaging (MSI) Live Finger Detection (LFD) | |
| Cryptography Ciphers/ Encrypted Communication | AES 128/256, TDES 2/3 Key, SHA-256, RSA-2048. See Secure Integration Kit data sheet for details | |
| Physical Security | Hard epoxy encapsulated electronics, detection switches, temperature sensors, tamper evident label | |
| Tamper Response | Secure battery-backed memory with active erase memory zeroization | |
| ENVIRONMENTAL RANGE | | |
| Temperature | -10 to 60°C (operating, with enclosure) | |
| Humidity | 10 – 95% RH (operating, with enclosure) | |
| ESD Immunity | IEC 61000-4-2 level 4 (+/-15kV air discharge, +/-8kV contact discharge). | |
| INTERFACE | | |
| USB | USB 2.0 high speed (480 Mbps), Mini B connector | USB 2.0 high speed (480 Mbps), 2m USB cable |
| Operating systems supported | Windows 10/11, WHQL Drivers, Linux PC (32/64-bit) Linux ARM7/8 | |
| FORM FACTOR & DURABILITY | | |
| Overall dimensions | 2.67"W x 2.85"D x 2.01"H (67.9mm x 72.5mm x 51.2mm) | 3.3"W x 3.97"D x 2.33"H (84mm x 100.9mm x 59.2mm) |
| Enclosure | Glass filled PC | Painted magnesium alloy, IP65 rating |
| Weight | 125 grams | 290 grams |
| POWER SUPPLY REQUIREMENTS | | |
| Supply current — operational | +5 VDC, 500 mA (peak) | |
| Supply current — idle | +5 VDC, 210 mA (typical) | |
| STANDARDS COMPLIANCE | | |
| Interoperability | ANSI 378, ISO 19794-2, ISO/IEC 19784-1, MINEX III-certified algorithm, WHQL Drivers | |
| EMC & Safety | Submitting = (CE, FCC, CB, UL) | |
| Environmental | Submitting = (REACH, RoHS, WEEE) | |
| Ingress | IP65 at the platen | IP65 |

Data subject to change without notice

HID patented, MSI technology delivers market-leading capture, liveness and match functionality to ensure a successful biometric implementation and superior user experience.



hidglobal.com

North America: +1 512 776 9000 | Toll Free: 1 800 237 7769
 Europe, Middle East, Africa: +353 91 506 900
 Asia Pacific: +852 3160 9800 | Latin America: +52 55 9171 1108
For more global phone numbers click here

© 2023 HID Global Corporation/ASSA ABLOY AB. All rights reserved.
 2023-02-13-eat-lumidigm-v5-series-secure-line-ds-en PLT-06372
 Part of ASSA ABLOY