BIOMETRICS

Lumidigm® M421 Fingerprint Sensor

Fingerprint readers are field-proven and widely deployed, authenticating over one billion ATM and teller transactions per year.

USE CASES:

- **ATMs —** second factor or PIN replacement
- **Tellers —** confirm customer and teller identities
- **High-value transactions —** wire transfers, portfolio management, B2B payments, secure web portal access
- **Government benefits —** pension payments, public healthcare access

TRUSTED AND SECURE FINGERPRINT AUTHENTICATION

- **Establishes Trust in Transactions —** Device enables secure communications between the sensor and a centralized account management system, ensuring that only authorized users gain access.
- **Encrypts Sensitive Data —** Cryptographic toolkit provides data security throughout sensitive transactions, preventing man-in-the-middle and replay attacks.
- **Resists Tampering —** Cryptographic keys and other data stored on the device are protected by active hardware tamper detection and response.
- **Provides Best Available Biometric Performance —** Patented Lumidigm multispectral imaging technology leads the industry in real world fingerprint authentication performance.
- **Prevents Fraudulent Verification Attempts —** Award-winning liveness detection reliably distinguishes between fake and legitimate biometric characteristics.

HID Global's Lumidigm® M421 Fingerprint Sensor combine world-renowned Lumidigm biometric performance with data encryption, tamper detection/response, and key management for trusted user authentication. Designed to simplify transactions for users while eliminating fraud for financial institutions, the M421 provides convenient and reliable biometric authentication in solutions requiring end-to-end security in transactions.

The cryptographic toolkit provides a broad set of tools that allow an organization to secure data transmissions. The M421 encrypts sensitive data for transactional security, preventing man-in-the-middle and replay attacks using mutual authentication between the host and the sensor. The tamper response capability on the M421 detects and resists physical tampering of cryptographic keys and other data stored on the device. Encrypted and authenticated firmware updates prevent malicious code loading.

The M421 offers exclusive multispectral imaging and best-in-class liveness detection that leverages the industry's best-performing fingerprint sensor platform. Known for its ability to provide a quick and easy user experience while reducing the opportunity for fraud, HID Global's Lumidigm technology gathers biometric data from the surface and subsurface of the finger to provide reliable, real world biometric authentication in any environment and with any user population. Strong, field-updatable liveness detection ensures that the person making the transaction is who they claim to be.

The M421 supports multiple standard cryptography transaction models or can be customized for a proprietary, customer-specific solution. With flexible deployment options, the M421 will reduce fraud and restore trust in transactions.

SECURE LINE FEATURES:

- Cryptographic toolkit with symmetric/asymmetric encryption/decryption algorithms, hashing functions, random number generation, and digital signature generation/verification.
- Physical tamper resistance, detection and response.
- Per-device encryption keys that can be remotely updated.
- Mutual authentication between the host and the sensor.
- Encrypted and authenticated firmware updates.
- Secure boot.
- Lumidigm multispectral fingerprint imaging technology.
- State-of-the-art liveness detection.

SPECIFICATIONS

	M421
	FINGERPRINT IMAGING SYSTEM
Technology	Patented Lumidigm optical multispectral imaging (MSI)
Output image resolution / bit depth	500 dpi / 8-bit, 256 grayscale
Platen area	0.55" x .69" (13.9mm x 17.4mm) rectangle, uncoated 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)
Match on device	ANSI 378 and ISO 19794-2 template inputs supported
Presentation Attack Detection (PAD)	Multispectral Imaging (MSI) Live Finger Detection (LFD) ISO/IEC 30107-3, Level 1 Presentation Attack Detection (PAD) certified
Latent protection	User Configurable
	SECURITY FEATURES
Physical security	Hard epoxy encapsulated electronics, detection switches, temperature sensors
Tamper detection and response	Secure battery backed memory with active erase memory zeroization
	BIOMETRIC PERFORMANCE
Finger detection to image out	1.2 sec. (typical)
Finger detection to template out	1.6 sec. (typical)
Presentation Attack Detection (PAD) enabled	ADD 0.4 sec. (typical)
	ENVIRONMENTAL RANGE
Temperature (operating, with enclosure)	-10 to 60°C
Humidity (operating, with enclosure)	0 – 95% RH
ESD Immunity	IEC 61000-4-2 level 4 (+/-15kV air discharge, 8kV contact discharge)
	INTERFACE
USB	USB 2.0 high speed (480 Mbps), 2m USB Cable
Operating systems supported	Windows 7/8/10 (32/64-bit), WHQL Drivers, Linux
	FORM FACTOR & DURABILITY
Overall dimensions	1.85"W x 3.02"D x 2.06"H (47.1mm x 76.8mm x 52.5mm)
Enclosure	ABS Plastic
	POWER SUPPLY REQUIREMENTS
Supply current — operational	+5 VDC, 400 mA Operational (peak)
Supply current — idle	+5 VDC, 200 mA (typical)
	STANDARDS COMPLIANCE
Interoperability	ANSI 378, ISO 19794-2, ISO/IEC 19784-1, MINEX III-certified algorithm, WHQL Drivers
Device certifications	CE, FCC, CB, UL
Environmental	REACH, RoHS, WEEE
Ingress	IP50, ingress at platen IP65
Other	DEA EPCS, Argentina, Australia/New Zealand, Columbia, Mexico, South Africa

The HID Global Secure Line support the following cryptographic algorithms and has been found to be fully compliant and registered with the NIST CAVP (Cryptographic Algorithm Validation Program). [https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program]

CAVP Validation Number	Implemntation	Modes/States/Key Sizes/Description/Notes
3970	AES Validation	AES (e/d: 128, 192, 256, ECB, CBC), CTR (128, 256)
2177	Triple-DES Validation	TCBC (e/d: KO 1), TECB (single block only)
2029	RSA Validation	ALG (RSASSA-PSS, PKCS #1 v1.5); KEY (Gen); RSA Sig (Ver) (1024); RSA (Gen, Ver) (2048, 3072); SHA (1, 224, 256, 384, 512)
2587	HMAC	HMAC-SHA (1, 224, 256, 384, 512); KS < BS, KS = BS, KS > BS
3273	SHS Validation	SHA (1, 224, 256, 384, 512) BYTE-only
1164	DRBG Validation	CTR-DRBG-AES (256) Prediction Resistance Enabled

For Lumidigm inquiries: lumidigm@hidglobal.com

North America: +1 512 776 9000
Toll Free: +1 800 237 7769
Europe, Middle East, Africa: +44 1440 714 850
Asia Pacific: +852 3160 9800
Latin America: +52 55 5081 1650

hidglobal.com
An ASSA ABLOY Group brand

Lumidigm® Patents - https://www.hidglobal.com/patents

2019-06-18-hid-lumidigm-m421-sensor-ds-en PLT-04549

ASSA ABLOY