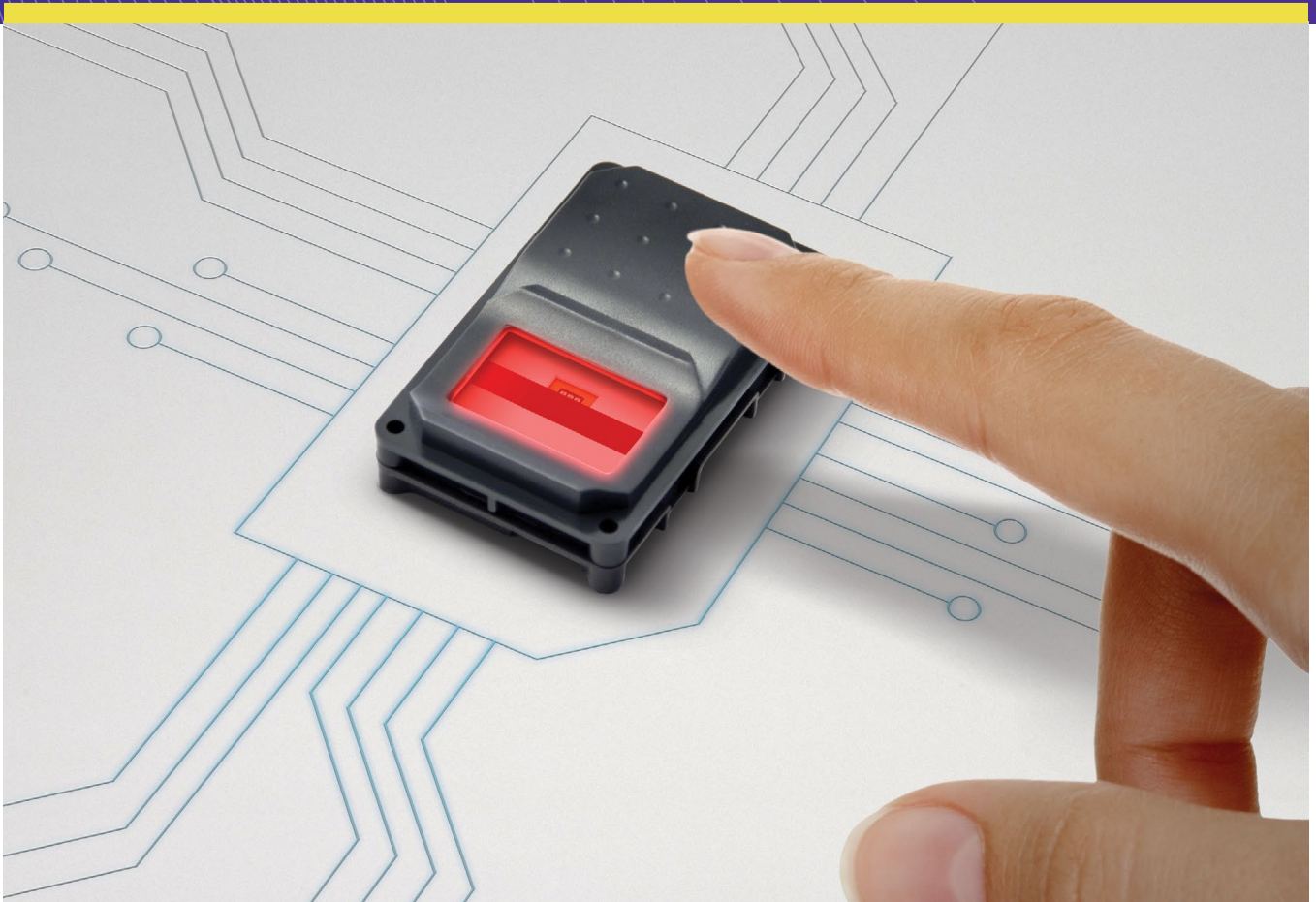


CBM Series

Compact Biometric Modules for OEM integration



Connected
Objects



The best, most compact optical modules on the market

Easy integration of biometric functions into multiple applications

High quality fingerprint acquisition

Embedded processing capabilities: MINEX compliant Coder & Matcher inside

FBI PIV IQS certification and fake finger detection available

Extensive security features, including encryption and digital signature

The CBM Series is a range of compact fingerprint modules. They use IDEMIA's patented optical technology and biometric algorithms, both acknowledged worldwide for their high levels of accuracy and performance and their exceptional robustness.

Whether used for off-the-shelf or custom-made applications, the CBM Series offers a flexible, cost-effective solution for the fast and secure processing of high quality fingerprint images.

Integrators can rapidly add the benefits of fingerprint recognition to their applications, without having specific knowledge of biometrics.

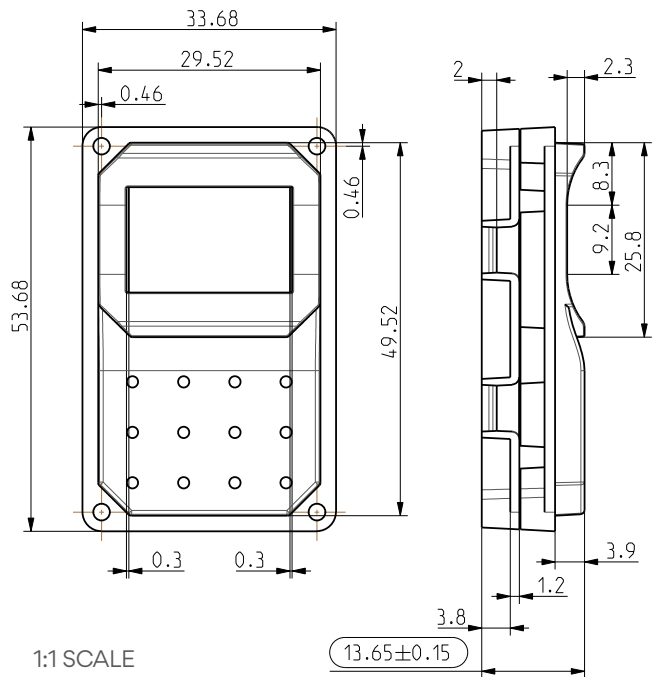
The most compact optical modules on the market

Their original flat design (13.65mm height), small footprint (53.7*33.7mm) and very light weight (20g) make them the ideal components for integration into compact and mobile products.



Why optical technology?

We selected optical technology for our sensors as it has significantly more operational and accuracy advantages compared with other technologies.



	OPTICAL	CAPACITIVE	SWIPE
Acquisition surface/resolution	●●●●	●●○○ Limited due to silicon chip cost	●○○○
Ergonomics	●●●● Visual indicator (LED light)	●●○○	●○○○ Usually requires several trials
Robustness	●●●●	●○○○ Sensitive to scratches, ESD damages, corrosion	●○○○
Fast processing time	●●●●	●●●●	●○○○ Requires image reconstruction
Performance/accuracy	●●●●	●●○○	●○○○

High quality fingerprint acquisition

Optical technology offers superior image quality

- High performance sensor: 500 dpi, 256 grey levels
- Available output formats include RAW, ISO 19794-4 or WSQ-compressed (under license) images

Lessons learnt from real world deployments put into practice

- Mechanical/visual guides ensure intuitive finger placement
- Interfaces display key information to help users: live image, messages (position, pressure etc.) and fingerprint quality score

Large acquisition surface for optimized capture and repeatable placement

The CBM's capture surface (14x22mm) ensures that the richest area on fingerprints is systematically captured time after time. Acquisition surface contributes significantly to the overall biometric performance:

- It determines the amount of minutiae data that can be captured
- Other, smaller sensors, allow different areas of the same finger to be presented with each placement, leading to poor data acquisition, narrow areas of overlap and matching errors



Richest area



CBM capture



Placement variations on smaller sensors

More than sensors, intelligent modules

While most sensors on the market are only capable of producing fingerprint images, the CBM modules are also capable of processing them internally, running powerful algorithms directly on their embedded processor.

- 1 Image Compression** using WSQ algorithm from FBI/NIST
- 2 Biometric Feature Extraction** to generate templates
 - Feature Extractor is MINEX/FIPS 201 compliant
 - Proprietary, ISO 19794-2 or ANSI 378 template formats available
 - Templates can be stored in CBM's internal database
- 3 Biometric Matching**
 - Matcher is MINEX/FIPS 201 compliant
 - 1:1 authentication or 1:N identification
 - High accuracy: the False Acceptance Rate (FAR) is configurable down to 10^{-8} (depending on the security requirements) and maintained regardless of number of users in database
 - Fast matching (refer to the table entitled "2 variants available")
- 4 CBM is capable of addressing juvenile fingers**
- 5 CBM implements an anti-latency feature** that detects fingerprint traces reactivated under certain lighting conditions

Embedded security features

When sensitive data (image or template) needs to be shared with a Host System, CBM modules are capable of securing them before dispatching.

1 Multiple security principles available:

- Symmetric and asymmetric keys,
- Key derivation,
- Hashing algorithm,
- Random number generator,
- etc.

2 Image and Template Encryption for the sake of confidentiality

3 Template Signature (X9.84 standard) to guarantee the origin and the integrity of the data sent to the Host System

4 The communication channel between CBM and Host/Distant System can be protected using either Secure Tunneling or Offered Security mode

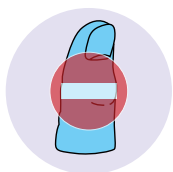
CBM-E3: best in series, best in class



Enhanced image quality

The CBM-E3's extremely fine tuned design produces a fingerprint image certified PIV IQS by the FBI.

The reference standard in terms of single fingerprint image quality (equivalent to ISO 19794-4:2011 Annexure B) was defined to ensure in particular interoperability between multiple solutions.



Fake Finger Detection

CBM-E3 detects a large panel of counterfeit fingerprints, including but not limited to those made with latex, Plasticine, Kapton, transparent film, rubber, Play-Doh, graphite or paper.

Easy integration into a wide range of applications



The CBM Series is perfectly suited for swift integration into multiple devices and applications: ATMs, kiosks, vending machines, access control and time & attendance terminals, keyboards, printers, PoS terminals, alarm systems, mobile devices, safes, locker systems, remote controls, voting machines, etc.

Robustness

- IP65 rated sensing area (sealed against dust and liquids)
- Resistance to electro-static discharges, scratches and shocks
- Operating conditions: -10°C to 50°C / 10% to 80% RH
- Storage conditions: -20°C to 70°C / 5% to 95% RH

Standard interfaces: USB and Serial (TTL Open-Collector)

Comprehensive Software Development Kit: MSO SDK

- Available for Windows, Linux and Android Platforms
- Includes a BioAPI interface

NB: Low level protocol (ILV) is also available



2 variants available

		CBM-V3				CBM-E3		
		Standard	With IDENTLITE License	With IDENTPLUS License	With IDENT10K License	Standard	With IDENTLITE License	With IDENTPLUS License
Database capacity (users)		500	3000	5000	10000	500	3000	5000
Database capacity (templates or fingers)		1000	6000	10000	20000	1000	6000	10000
Matching capability (1:N)		1:500	1:3000	1:5000	1:10000	1:500	1:3000	1:5000
Matching speed		0.6s in 1:1 mode / 0.7s in 1:500 mode						
Fake Finger Detection		—				Yes		
Security Layer		Optional						
Certifications	FBI PIV IQS / ISO 19794-4: 2011 (Annex. B)	—				Yes		
	MINEX & FIPS 201 compliant algorithms					Yes		
	STQC	—				Yes		
	CE, CB, FCC, UL					Yes		
	IP65 rated capture surface					Yes		
	RoHS, REACH, WEEE					Yes		
	WHQL drivers					Yes		



© Copyright 2019 All rights reserved. IDEMIA | EN - 01/19 | Photos: Thinkstock and IDEMIA