small device

BIG POSSIBILITIES

Smufs, Secure Mobile Universal Fingerprint Scanner, is a compact, self-powered, standalone fingerprint scanner, capable of running over Bluetooth and USB interfaces. It turns your peripherals into precise, sufficient and secured biometric POB, which one can use anywhere. The device can be extensively used in remote areas where access to computers/laptops and internet is limited. SMUFS is suitable for demanding 1: N identification challenges, on the field, through biometric, server over GPRS network. SMUFS handles tasks from standalone identity to large scale AFIS requirements. SMUFS can also work with regular computers and laptops over the USB port

- **Banking and Mobile payments**
- **Insurance and finance**
- **health Centers and Hospitals**
- **Paperless ID**
- **Access Control**
- **Remote workforce attendance**

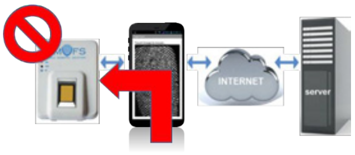
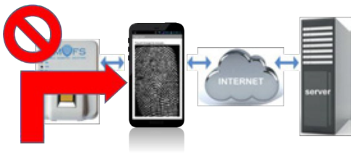
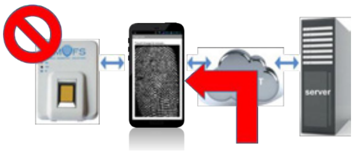
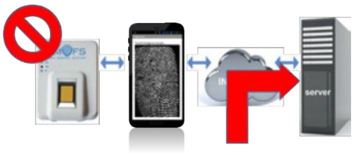
- **Governmental & UN food and benefits**
- **law enforcement**
- **Border Control**
- **Forensics**
- **Disaster scene management**

	Functionality	Technology	Customer Benefit
Interfaces	Bluetooth	Class 2 Bluetooth 2.1 Compatible with both Android and iOS	Image capture and transfer < 3sec Encrypted into 256-bit AES
	USB	OTG capabilities Micro USB connector	Plug & Play capabilities For both data transfer and charging
Hardware specifications	Long-life rechargeable battery	3.7V 1240 mAh Li-Ion battery Charge gauge Rechargeable via USB connection (3-5 hrs.)	~800 fingerprints on a single charge
	Memory	32MB FLASH memory (optional) 2MB SRAM memory	Can store up to 5000 templates ('Pro' device only) **Extraction** &Identification on device capabilities ('Pro' only) User programmable area of 4 KBs
	High processing capacity	ARM based DSP 192 MHz Programmable device	Allows flexibility and adaptability to various needs and applications. Firmware can be updated through our website.
	Notification	3 LED Buzzer	Immediate status indication on the device
Image Formats	Raw image	256 grayscale image (8 bit) Improved image quality	Customer may use any algorithm for extraction/matching.
	Compressed image	TIFF, JPEG, WSQ	Customer can use his preferable format
	Template (available for 'Pro' device only)	ISO/IEC 19794-2:2005 ANSI/INCITS 378-2004 SBS extraction algorithm	Image capture and transfer - 1 ~ 2 Sec
Sensor Specifications	Biometric Fingerprint Sensor	Capacitive TCS1CT – Gold-Coat Certified: FIPS 201 PIV > 1,500,000 finger capturing Capacitive TCS1ST Steel-Coat for enhanced durability(for moisture conditions) > 2,500,000 finger capturing Resistance to electro-static discharges, scratches and shocks, +/-15KV ESD	IP 65 (water, dust protection), Enhanced Image Mode (EIM) High signal-to-noise ratio, excellent robustness, suited for high quality capture across a wide range of fingerprint types. The image quality is resilient to various environmental conditions encountered in the field, like sunlight, dust, residual latent prints, etc.
	Image size	508 dpi, 8bit grayscale 256 x 360 Pixels (12.8x18mm)	Allows only live finger scans (no fake finger detection) Suitable for all 1: N and AFIS tasks
SDK	Operating Systems Supported	IOS, Android, Windows, Linux, Mac	SDK has a consistent interface across all versions. NFIQ is available through our SDK
	Security	MAC list features Template Signature (X9.84 standard) Connection Password IO packet encryption	Manage list of authorized phones Guarantee the origin and the integrity of the data sent to the Host System Additional password (optional) to establish connectivity Additional security layer of security on top of BT session
Physical Specifications	Handheld Device	6.5 x 8.3 x 1.5 cm / 2.5 x 3.2 x 0.6 inches 85gr/0.2lbs	Compact, portable mobile device
	Durable	Sealed ABS plastic Dust proof Water resistant Operating temperature -30 to +70°C / 5% to 93%RH Storage temperature -30 to +125°C / 5% to 93%RH	Suitable for outdoor and harsh conditions

Certifications	**FIPS 201 PIV compliance** **USBIF**	**BT SIG (D033153)** **FCC**

Security Features

For any SMUFS mobile biometric scanner

	• Sealed box – breaking is the only way to open the device, every physical opening leaves evidences. • Physical switch – every opening will lead to erasure of all sensitive data. • Fusing – the SMUFS is un-crackable, every attempt to make firmware changes will lead to a permanent destruction. • No sensitive data in the SMUFS – at its default operation mode, the SMUFS does not store the data. It collects the fingerprint image and send it to the host. In this function, if the device was hacked, it cannot serve any malicious use. • Detect only “live” fingerprint. “Fake finger” will be rejected. • Soft lock – the SMUFS unit can be locked and released using the fingerprint of pre-authorized person.
	• Data transfer over Bluetooth 256-bit AES encryption. • Addition security layer on top of the link session (optional). • Sending irreversible template only (optional) – recovery and “theft” of the fingerprint image is impossible. • MAC list - Managing a list of authorized phones in the SMUFS device. • Using Bluetooth 2 link limits the connectivity radios, and reduces the risk of an intruder or “listener”. • Additional security code – Blocking un-authorized phone.
	• MAC list - Managing a list of authorized scanners. • Using Bluetooth 2 link limits the connectivity radios, and cuts the danger of intruders or “listener”.
	• **SSL connection for sever identification.** • Low-friction solution – enable working with the customer’s secured network. • Working over GPRS and Wi-Fi, which have a strict secured protocol. • Sending irreversible template only (optional) – recovery and “theft” of fingerprint image is impossible.
	• **SSL connection for sever identification.** • Low-friction solution – enable working with the customer’s secured network. • Locked and secured groups of identities, using pre-authorized fingerprints. • Manage and Limit the information receives from the server for each identification (person picture only, “identified/not identified” only, etc.).