

# FS26E

## FIPS201/PIV Compliant USB2.0 Fingerprint Scanner with Encrypted USB communication

### เครื่องสแกนลายนิ้วมือ สำหรับการตรวจสอบ บุคคลที่ต้องการความปลอดภัยสูงมาก

- FS26E เป็นเครื่องสแกนลายนิ้วมือที่ได้รับมาตรฐาน FBI สหรัฐอเมริกา
- มีความปลอดภัยสูง เพราะข้อมูลลายนิ้วมือและข้อมูลอื่นๆเกี่ยวกับผู้ใช้จะถูกเข้ารหัสไว้อย่างแน่นหนา
- ทำงานบน Web browser
- ตรวจสอบลายนิ้วมือได้ถูกต้องแม่นยำ รวดเร็ว
- หน้าสัมผัสตัวเครื่องทนทาน ใช้งานได้นานกว่าใคร
- เหมาะสำหรับหน่วยงานที่ต้องการความปลอดภัยของข้อมูลสูง เช่น ทหาร, ตำรวจ, หน่วยงานความมั่นคง, ระบบสมาชิก, ธุรกรรมทางการเงิน ฯลฯ

Futronic FS26E เป็นเครื่องสแกนลายนิ้วมือแบบ USB ที่ได้รับมาตรฐาน FBI มีความปลอดภัยสูงเพราะข้อมูลต่างๆ เช่น ภาพลายนิ้วมือ, minutiae, ข้อมูลเจ้าของลายนิ้วมือ ฯลฯ ที่จะถูกส่งผ่าน USB นั้น จะถูกเข้ารหัสอย่างแน่นหนาด้วย AES256 Algorithm ผู้ที่ไม่มีรหัสปลดล็อคจะไม่สามารถอ่านข้อมูลได้

นอกจากนี้ FS26E มีระบบ Digital signature สำหรับตรวจสอบความถูกต้องของ FS26E แต่ละเครื่อง นั่นคือหากไม่ใช่เครื่องที่ได้รับอนุญาตจะไม่สามารถอ่านข้อมูลได้ จึงมั่นใจได้ว่าข้อมูลสำคัญจะปลอดภัย ไม่รั่วไหลแน่นอน

### Fingerprint scanner spec

- Scan fingerprint and send to USB host real time.
- Fingerprint scanning window size is 16x24mm
- Image resolution is 320x480 pixel, 500 DPI
- 8 bit grey level
- Light source: Infrared LED
- Optical system, lifetime up to one million scans.
- Live Finger Detection (LFD)

### Encrypted USB channel

- AES256 according to FIPS197
- Diffie-Hellman key exchange algorithm, DH2048, according RFC5114.
- SHA256 for key generation

### Build-in Digital Signature

Elliptic Curve Digital Signature Algorithm (ECDSA) according to FIPS186-4. Use 256bit at FS26E and 512bit at PC.



### General spec

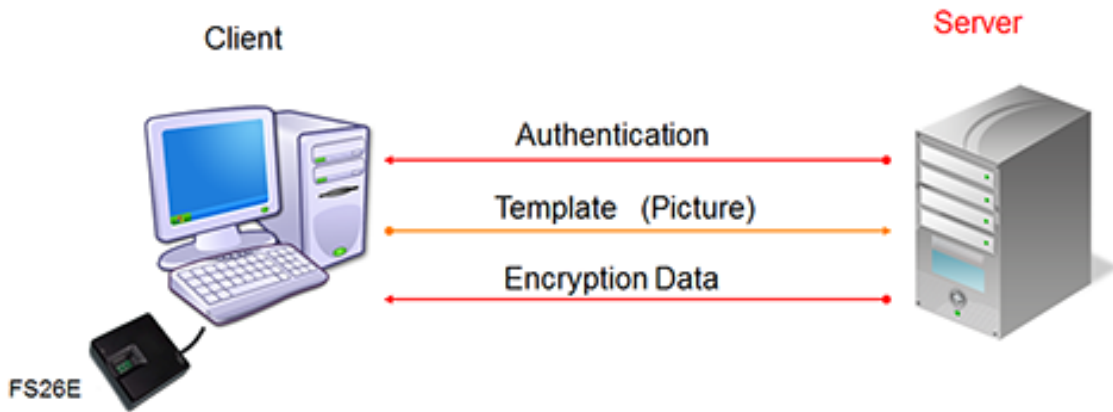
- USB 2.0 compatible interface, plug and play device.
- Work on Windows, Linux and Android.
- 2 meter standard USB cable
- Size, 98 x 98 x 35 mm
- Weight, 200 gram
- Operation temperature: -10 to +55 Degree Celsius
- Supply voltage: DC 4.5-5.5V via USB port
- Power consumption: active is 150mA and standby is 70mA.
- ESD contact - 8KV and air discharge - 16KV, no permanent damage

WAC RESEARCH CO.,LTD.

Tel : 025303809-10, 025381038

E-mail : [sales@wacinfotech.com](mailto:sales@wacinfotech.com)

[www.wacinfotech.com](http://www.wacinfotech.com)



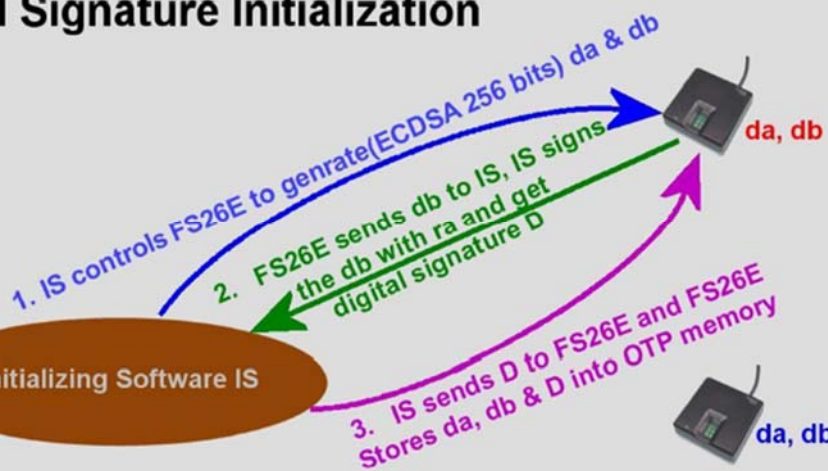
## Digital Signature Initialization

Futronic  
Initializes each  
FS26E in factory



Generate  
(ECDSA 512 bits)  
Digital Signature  
root key ra/rb.  
ra in IS, rb in API

Initializing Software IS



Remarks :

1. Each FS26E has its unique set of da, db and D.
2. OTP memory is OneTime Programable Memory.

# FS26E Authentication Process

1. When FS26E is power up, it generates DH key pair  $y_a$  &  $y_b$ . FS26E signs  $y_b$  with  $d_a$ (pre-stored) to get the digital signature  $Y$ .



2. FS26E sends  $Y$  and  $D$  (prestored) to PC



3. PC uses  $rb$ (in API) to check and confirms  $db$  is from authenticated FS26E.

PC uses  $db$  to check  $Y$ ( $y_b$  signed by  $d_a$ ) and confirms  $y_b$  is from the same FS26E.

PC continues to use  $y_b$  to start the standard DH key exchange process.

