

# TECH NOTE



access control



data collection



workforce management

**Number:** TN 100727  
**Subject:** Cogent Biometric FAQ

This frequently-asked-questions (FAQ) document answers questions about Cogent biometric devices (fingerprint readers), including:

- ◆ System Design, Components and Parameters
- ◆ Enrollment Process
- ◆ Authentication Process
- ◆ Fingerprint Templates
- ◆ Storage and Security
- ◆ Data Retention Policy

## System Design, Components and Parameters

1) What biometric options does ATS offer?

*ATS offers two biometric fingerscan reader options: e-field sensor and capacitive sensor. The main differences between these two readers include template size, storage capacity, and enrollment procedure.*

2) What are the response times of the biometric options?

*For Global Series terminals, the e-field sensor in 1:n mode can scan 150 templates in under one second. The capacitive sensor reader can scan 500 templates per second. So, if you have 1000 templates in the capacitive sensor reader, you can expect an average response time of about two seconds. However, if you have 500 or fewer, the average response time is less than a second.*

3) What are the template sizes?

*A template is the electronic data that defines the minutiae of a single fingerprint.*

*The E-Field Sensor (1:1) template is 384 bytes. The e-field sensor (1:n) template is 2352 bytes. The capacitive sensor uses a single template for both 1:1 and 1:n matching that is 784 bytes.*

*During enrollment the capacitive sensor reader takes three images of the finger and converts all three into one template. In use, the user's fingerscan is then verified against a template that contains the three stored templates created at enrolment.*

- 4) Please describe the system architecture in detail. In particular, is enrollment and authentication done locally or on a server?

*Enrollment occurs locally and can be forwarded to the host. No image is stored.*

- 5) Which hardware and software products from the vendor are used? Can you provide specifications for those products?

*ATS doesn't provide any additional specifications. Check the vendors' Websites:*

*<http://www.cogentsystems.com> and <http://www.bioscrypt.com>.*

- 6) In the case of a one-to-many identification system, how many templates is the system capable of matching (e.g., 1:3000, 1:20000)?

*For Global Series terminals, the e-field sensor reader can store up to 4,000 1:1 templates or up to 200 1:n templates. The capacitive sensor reader with 8 MB storage can locally store up to 9,000 templates.*

- 7) Does the system create a record of attendance, transactions, or both? How are those data used?

*A transaction is recorded with a date and time stamp. It is used for diagnostics as needed. See the Universal Command Set (UCS) Reference Manual for information about data and badge number formats.*

- 8) What is the durability of the biometric readers?

*The Capacitive Sensor is certified to IEC 61000-4-2 level 4 (+/- 15KV).*

*The E-Field Sensor reader is certified to IEC 61000-4-2 level 3 (+/- 8KV).*

## Enrollment Process

- 1) How does enrollment differ for the e-field sensors and capacitive sensors?

*The e-field sensor's enrollment process is more interactive, using a three-tiered approach for quality and content of the fingerprint. It returns enrollment quality and content scores, which a user's application can evaluate to determine if the enrollment is adequate for acceptance. However, the capacitive sensor's enrollment process is more automated. The sensor evaluates the finger scans taken for enrollment and takes multiple scans as necessary until reliable scans are obtained.*

- 2) How many and which fingers (e.g., right index plus left index) are needed for each enrolled user (enrollee)?

*The number of fingers enrolled is controlled by the ATS partner, but ATS recommends the enrollment of two fingers. The recommended enrollment fingers are the index finger on the right and left hands. We do not recommend enrolling the thumb or little finger.*

- 3) How many fingers and which ones are normally needed for authentication (i.e., one of the enrolled fingers or both)?

*In 1:1 mode, one of the enrolled fingers is required.*

- 4) Is submission of fingerprints voluntary for a user? What are the other options available to the user?

*In 1:1 mode, there is an option not to use the fingerscan device.*

- 5) Does dry skin affect the readers?

*If there is excessive dryness to the finger it is possible that the reader may have difficulty achieving an adequate scan. In case of these rare events, some customers have installed a moisturizing agent next to the terminal.*

- 6) Some users do not have fingerprints of acceptable quality and there is a failure to enroll. How are these cases handled?

*For the Bioscrypt sensor, there are multiple verification levels available to accommodate different quality levels. Enrollees can be placed into an exception list allowing them to pass with little or no verification. Whereas, the Cogent sensor has three levels of verification: veify, verify anything, or don't ask for enrollment. Also, in 1:n mode, there are no adjustments that will help the employee to enroll.*

- 7) Can 100% enrollment success be guaranteed?

*While there is constant improvement in biometric technologies such as fingerscan readers, there will always be a very small percentage of the population who cannot be read for one reason or another.*

- 8) During enrollment, is there a way for anyone, such as an employee, to capture the image using the Print Screen button?

*There is no image display on a screen, so image cannot be viewed nor can the image be captured with a print screen or other function.*

## Authentication Process

- 9) Is authentication done under supervision or in the presence of a security guard?

*Enrollment is typically enforced by a supervisor; authentication does not require any supervision.*

- 10) How is a false rejection handled, especially for users having difficulties with the system?

*For the e-field sensor, the false rejection rate (FRR) is 0.1% and the false acceptance rate (FAR) is 0.1% for one finger. For the capacitive sensor, FRR is 0.1% to 0.001% and the FAR is 0.01% to 0.0001%.*

- 11) Does the user see the fingerprint image during authentication (e.g., are there monitors on site to display the image)?

*No image is displayed during authentication.*

- 12) After the fingerprint authentication, does the system use any other means (e.g., a person's photo), to further confirm their identity?

*PIN and badge numbers can be used for identity; no other methods, such as photographs, are used.*

## Fingerprint Templates

- 13) Are the fingerprint templates compatible, or can they be made compatible, with one of the following standards: ANSI-INCITS 378, ISO/IEC 19794-2, FIPS 201, or ILO SID-0002?

*No, the template is only recognized by the sensor it was created on. There is no other way to extract useful information from the template.*

14) Does the template contain fingerprint minutiae (minutiae are details of interest in a fingerprint), such as x and y positions and directions?

*Yes, this information is contained in an ASCII format.*

15) Does the template contain the following data: minutiae type, quality, fingerprint core and delta positions, ridge count, and orientation field?

*No, the template is a series of ASCII characters and there is no image identifying fingerprint core, ridge count, etc.*

16) Is the template size fixed or variable? What would be an approximate size of the template containing 30 fingerprint minutiae?

*The template size is fixed by the type of sensor being used. There is no such thing as a template containing data for 30 fingerprints; instead there would be 30 templates all of the same size*

## **Storage and Security**

17) Where are the templates stored (i.e., locally or on a server)?

*Templates are stored on the terminal. Backup copies of the templates should be stored on the host.*

18) Are the fingerprint images stored on a server or somewhere else in the system? Is storing the image or not a configurable option? If so, who does the configuration?

*No image is available or stored.*

19) Are the stored templates encrypted?

*Encryption and other security methods are controlled by the ATS partner. Data transferred from the terminal to the host can optionally be set for encryption.*

20) How are the stored data protected (e.g., from an insider's attack or if the server is stolen)?

*Data protection is controlled by the ATS partner and its end users.*

21) Who has access to the stored templates? How is access controlled?

*Template access is controlled by the ATS partner and its end users.*

22) Does the biometric vendor regularly access the stored templates?

*Templates are stored on the terminal and can be accessed by the ATS partner in some situations. The vendor of the biometric device does not have direct access to data stored on any ATS device.*

23) How are the upgrades and maintenance of the biometric system performed?

*Upgrade and maintenance is at the discretion of the partner.*

24) How and where is the template storage backed up?

*Backup options are available from and controlled by the ATS partner.*

25) Is a wireless connection used anywhere in the system? If so, is it encrypted?

*ATS does not currently offer a wireless solution. Partners have the option to add wireless connectivity through a wireless router or access point.*

26) Are the biometric servers connected to the Internet or an intranet?

*The terminal can be installed in Internet mode at the discretion of the ATS partner.*

27) What are the safeguards, if any, against spoofing (i.e., applying a fake fingerprint)?

*The minutiae or swirl patterns cannot be reverse engineered. The technology eliminates the possibility of fraudulent scans.*

28) If there is a request from a law enforcement agency, can the biometric template be extracted from the system? What is the procedure? Who will perform the extraction?

*No, the template is useless to law enforcement agencies.*

29) What are the environmental requirements of the readers?

*The e-field sensor is rated for 0 to 60°C. The capacitive sensor is rated for 0 to 55°C. If operated within these temperature ranges, the performance (read rate) of each reader is independent of ambient temperature.*

30) Are biometric readers easy to clean?

*Both reader options can be easily cleaned using any mild cleaning method. Mild liquid cleaners are appropriate provided that that sensor is not exposed to excessive amounts of liquid.*

## **Data Retention Policy**

31) How long is the biometric information retained in the system?

*Information can be retained for the life of the system.*

32) Can users request the deletion of their biometric information?

*Yes, templates can be erased through a purge-templates command done by the ATS partner.*