## Part A. System Design, Components and Parameters

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

- **The enrolment and authentication is done locally on the ACTAtek reader, ACTA3-1K-FLI-SMC. In this particular model, the fingerprint sensor module, RFID smart card, and a CMOS camera for taking picture of the user are available. The template can also be stored in a RFID smart card, such that the smart card is kept by the user and all the templates on the device are removed. The template stored in the card is read by the device and then used to match with the finger. However, the time taken for authentication is slower when compared with the case of templates stored in the device.**

Which hardware and software products from the vendor are used? Can you provide specifications for those products, besides those publicly available on the vendor's website?

- **The hardware will be the ACTAtek reader, ACTA3-1K-FLI-SMC model, and no software is required to be installed at any PCs. The system and application software are embedded in the device. It is a highly integrated all purposed built system.**

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)? The answer to this question is critical.

- **The system is capable of one-to-many matching 1:3000 templates by default, but can be expanded to 1:N but slower. If the user can accept slow response time, the ratio can be increased further without theoretical limitation.**

What is the actual number for the False Acceptance Rate (FAR) that is configured for the system? Does this number refer to a one-to-many or a one-to-one system? Is it applicable to one or two-finger scanning?

- **The FAR is 0.01%. This applies to all method of authentication. Each user can register up to 3 templates. For best performance, we recommend using the same finger. However, if a user likes to enroll 3 different finger template that is also accepted by the device but performance will be degraded.**

Does the system create a record of attendance and/or transactions? How are those data used?

- **The system creates an event log that records the time, unit, triggers, and ID when there is a user trying to do the authentication whether it's approved or not. These data can be used by different application software to generate different kind of reports and analysis depending upon the user requirement.**

## Part B. Enrollment Process

How many fingers are needed per user, and which ones (e.g., right index + left index) are enrolled?

- **We recommend using the same finger, and we recommend the index finger.**

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

- **We recommend only using 1 finger for enrolment.**

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

**- Yes, the fingerprint is one of the options of authentication. Users can also choose PIN or RFID smartcard and user name for authentication. The device also has a CMOS camera as an option to take a picture or video clip of the user upon authentication. The picture or video clip can be taken upon failed or successful authentication. In the application software, the picture or video clip can be viewed together with the registration photo to see if any buddy punch occurred.**

Some users do not have fingerprints of acceptable quality, i.e. there is a failure to enroll. How are these cases handled?

**- Again, users can choose password or smartcard for authentication.**

During enrollment, if an employee sees the fingerprint image on the monitor, can that employee capture the image using the *Print Screen* button?

**- Yes, with PC enrollment, employee can capture the image using the "print screen button".**

## Part C. Authentication Process

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

**- Depending upon the user's condo requirement and policy**

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

**- In the case of false rejection, we very often check that the user's gone through a proper registration process and placing the finger correctly on the sensor. In most cases we found this will stop further reporting of false rejection. In the very unlikely the case that a user's fingerprint is very shallow and cannot be recognized, we recommend, user name plus PIN, smart card plus PIN, and using the CMOS camera to take a picture of the user on every entry which can then be manually compared with registration photo.**

Is there a scenario where a false acceptance would have an impact on the user? Take the following example: suppose that in a one-to-many system, an enrollee is misidentified as another enrollee. Then, in a situation where there is an account for transactions, the wrong enrollee's account would be negatively affected. With a biometric, it may be more difficult to repudiate the validity of the incorrect transaction.

**- First, the false recognition does happen on the BIO readers, but the rate is very small which is around 0.0001%. Unlike our competitors, which use group matching technique i.e. they group users and only compared with templates in that group, our recognition algorithm compares with ALL the templates in the database. This means that since launching the product and with over 30,000 installation sites world-wide, we have had a single case of false acceptance report. Our largest user site is in Middle East with 30,000 users. In the situation when this case happens, through the LCD display, user can notice that an incorrect account has been recorded. (The system display the user ID and user name when the authentication occurs)**

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

**- No, user cannot see the fingerprint image during the authentication.**

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

- **The system will display the user ID and user name to confirm his identity.**

## D. Fingerprint Templates

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, ILO SID-0002?

**- No. The ACTAtek is a closed system operating within its environment. All hardware, system firmware and web-based application software are embedded in the memory of the device. Communication out of the system is limited to transactional event logs, method of entry, which terminal is used for access etc. Fingerprint minutiae can only be transferred using our SOAP based API. However, if the fingerprint module is working as an independent unit, the template can be FIPS 201 compliant after conversion.**

Does the template contain fingerprint minutiae x, y positions and directions?

- **Yes, but information is proprietary.**

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

- **No.**

Is the template size fixed or variable? What would be an approximate size of the template containing e.g., 30 fingerprint minutiae?

- **Variable, template size is maximum 1K byte, average 300 bytes, depends on the fingerprint image.**

## E. Storage and Security

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

- **When a fingerprint is scanned, the complete image is stored and encrypted for protection. In addition, the template is encrypted, as it can be stored on the user's local disk or smart card instead of being stored on the device. So the user's privacy is preserved.**

Are the fingerprint images stored on a server or somewhere else in the system? Is this option (i.e., to store the images or not) configurable? Who does the configuration?

- **The fingerprint image is not stored. By the time of the enrolment, the system automatically converts the image into a binary data and discards the image.**

Are the stored templates encrypted?

- **Yes, the templates are encrypted, and cannot be reverted to image.**

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

- **The stored data is protected by password, and different login levels.**

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

**- Only the super administrator is allow to access the stored templates.**

Does the biometric vendor regularly access the stored templates? How are the upgrades and maintenance of the biometric system performed?

**- No, the vendor has no access to the stored templates. The upgrades and maintenance of the bio system is done by the users with updated service manual and firmware from vendors.**

How and where is the template storage backed up?

**- The templates can be backed up into any PC or servers.**

Is wireless connection used anywhere in the system? If yes, is it encrypted? (This is a must.)

**- Wireless is optional and to be used to transfer transaction data back to remote server.**

Are the biometric servers connected to the Internet or an Intranet?

**- The biometric server (the unit) has the capability to connect to the internet or an Intranet. It depends on how the user is implementing the unit.**

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

**- A built-in CMOS camera is used to capture a snap shot or video clip as users are performing the authentication.**

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?

**- Yes, the biometric template can be extracted from the system. The procedure will require using our SOAP API to collect the template data. Only administrator has this capability to do so.**

## F .Data Retention Policy

How long is the biometric information retained in the system?

**- The biometric information only retained in the system as the user information exists. Once the user information is deleted, the biometric data associated with that specific user will discard.**

Can the user request the deletion of his/her biometric information?

**- Yes, user can request the deletion of his/her biometric information. The template can also be stored in a RFID smart card, such that the smart card is kept by the user and all the templates on the device are removed. The template stored in the card is read by the device and then used to match with the finger.**