ADT60
Frequently Asked Questions

BioSIMKey
Fingerprint Scanner & Plug-in Smart Card Reader
BioSIMKey FAQ

1. What are the possible applications using BioSIMKey?

Home-banking, E-commerce, PC security, Electronic Voting, etc. BioSIMKey is an idea device to be used as a personal device, although it can also be used as a public device such as in a public information kiosk.

2. What is the accuracy of the fingerprint?

Fingerprint technology today is roughly equivalent to a 4 digits PIN i.e. a false acceptance in the range of 1 in ten thousand.

3. Is the BioSIMKey able to distinguish between a dead finger and a live finger?

The fingerprint image is based on capacitive characteristics of the live finger. A live finger and a dead finger have different capacitive characteristics. However there can be more things related to live finger detection and one can expect more security features to come in the future.

4. Am I able to access the raw fingerprint?

There is no need for the solution house to have the raw fingerprint because the template extraction and matching are the part of API provided. It makes the usage more simple and secure.

5. Will authentication be affected by dry and wet finger?

Frankly speaking, no fingerprint sensors can capture full range from extreme dry to extreme wet. However, this range can be improved by auto-regulation through the quality feedback from the image captured.

If the fingerprint is very dry or fine:
The quality will depend how good on image performance of the sensor itself, sure the direct scanning like solid state as TouchChip will be better than indirect solution by optical, unless to use CCD but not cost-effective.

If the fingerprint is too wet:
Optical is better because it can put better coating on the len. But for ST, we will have next generation TouchChip to overcome this kind of residual finger and robustness.
6. What are the advantages of silicon sensor?

The advantages of silicon sensor are:

- compact in size
- less chance of cheating by a hardcopy of fingerprint compared with a camera type optical solution
- power saving and ease of implementation.

7. Is the matching algorithm one-to-one or one-to-many?

One to one algorithm is to match the fingerprint with one or a few templates. Technically if the template is in the smart card, the template belongs to the cardholder. If the template is the PC, a one-to-one algorithm can also be used to match a few different templates. The algorithm of the BioSIMKey is one-to-one. Many-to-one algorithm is typically used by police for criminal and forensic type of applications, which require sophisticated computers to match a fingerprint with huge database.

8. Error message is shown during the Demo kit running:

(a) “The function AC_ADT_Init was not called” during fingerprint scanner initialization for enrollment.

(b) “The smartcard is not a valid ID card”

In fact, this problem is the driver problem. The demo programs cannot recognize the device even the driver is installed successfully. The correct name of device under registry is “ACS ADT60 0”.

Suggestion actions:

i) Check the device name in registry
   [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\Readers\]

ii) If the device name is not “ACS ADT 60 0”, please uninstall the drive and re-install the driver by using provided installer.

iii) Re-start the system