# SUPREMA BIOENTRY PLUS FINGERPRINT SCANNER

## FREE EXCERPTED TEST


**Óbuda University, Donát Bánki Faculty of Mechanical&SecurityEngineering, AppliedBiometrics Institute**

www.abibiometrics.org ● info@abibiometrics.org

## TABLE OF CONTENTS

# 1 A SHORT SUMMARY OF THE SUPREMA BIOENTRY PLUS TEST RESULTS

The Suprema BioEntry Plus is an IP based fingerprint scanner for access control systems. It can store two prints per person and is able to read RF cards.

It can be easily integrated to an already present access control system, the reader simply has to be connected to the controller through a standard interface (e.g. TCP/IP, RS485 or Wiegand).

Being a biometric system, fingerprint identification may not work with every user at any given time, due to the fact that fingerprints are vulnerable to external damage, and about 5% of the population does not have a fingerprint at all.

Enrolment time for the average user is less than 8 seconds, while pass-through time – considering the human factor as well – stays under 5-6 seconds, which is fairly average. From this point of view, the device can be recommended for any corporation that has average requirements.

Our tests revealed that the device is exceptionally vulnerable to any contaminants on the sample, no matter whether it is liquid or powder-type, identification capability deteriorated radically. The device, however, can cope with minor injuries (like those that happen in an average office environment), thus we recommend its usage mainly in office environment where heavy contamination of the sample is not expected to occur.

Our tests have also revealed that positioning errors are only mildly tolerated by the device, bigger twists or rotations can't be handled, and with certain users, it required especially accurate positioning. We thus recommend informing the users about this limitation when installing the device. Also, due to this, one should only use the device where sufficient level of user cooperation can be expected.

Altogether, the device can be used well in an office environment, where there is no high risk of contamination and no exceptional security risks exist.

## 2 TECHNICAL DETAILS AND TEST RESULTS

The Suprema BioEntry Plus is an IP based fingerprint scanner for access control systems, which is equipped with an optical sensor and an RF card reader. The optical sensor creates a 2D picture of the fingerprint. The device can store two prints per person.

Technical details given by the manufacturer[1]:

- Model no.: 45279
- Dimensions: 160x50x37 mm (HxWxD)
- CPU: 400MHz DSP
- Memory: 4MB flash + 8MB RAM
- Fingerprint sensor: 500 dpi optical
- Legitimacy check: 2000 check/second
- Storage capacity: 10.000 templates (5.000 users)
- Event storage capacity: 50.000 events
- Operational modes: Fingerprint, RF card, RF card + fingerprint
- Operational temperature range: -20°C - 50°C
- Network interface: TCP/IP, RS485
- Wiegand output: programmable (64 bit)
- TTL I/O 2 output for external sensors
- Built-in relay for door control
- Power supply: 12V DC
- Frimware: v1.51 (update: 2012.ápr.)
- PC software: v1.36 (latest version: v1.63)

Connectors:

- Wiegand output: 3 pin connector
- Power and RS485: 5 pin connector
- Ethernet (TPC/IP): 4 pin connector
- Digital input and relay output: 7 pin connector
- DIP switch and RS485 closing

The device was given a firmware update in April, 2012. As of early 2014, it is still the most up to date version. As for the control software, the most up to date version is Biostar 1.62 (a rather good and easy to use software), which was updated in April, 2013. For our tests, we have used 1.36.

The device has no tamper alert system, so if it is removed, it does not send any alerts.

## 2.1 OPERATIONAL TIMES

When choosing a device, one of the most important parameters is the time needed to operate the device, which includes enrolment and everyday use. During our research, we have tested these parameters, which concluded that the average enrolment time for a new user is 6-7 seconds and the pass-through time (through an access point equipped with the device) is an average of 5-6 seconds. The actual scan of the sample takes up less than 3 seconds of this interval. These values are fairly average and should cause no interruptions in any processes – thus, from this respect, we recommend it for an average office use.

## 2.2 CONTAMINATION AND DAMAGE OF THE FINGERPRINT

Different identification systems have to face different challenges. There are certain workplaces where the hands – and thus the fingerprints – get contaminated. It is very important to know how much contamination or lesser injuries will affect identification performance, even if only a smaller percentage of the staff will face such situations. For this reason, we have tested how the device will handle a variety of contaminants and simulated injuries.

We have also tested how much any injury to the print will affect performance. Smaller sized injuries to the centre of the print raises FRR only for a few subjects. Medium or large size injuries, however, significantly deteriorate usability. Identification time slightly increases, but even significant distortion yields acceptable times. Altogether, it can tolerate injuries that are most common in an office environment (e.g. paper cuts), but it is not advised to use the device where there is a constant risk of larger injuries.

## 2.3 REQUIRED USER COOPERATION/AUTOMATISATION

These tests examine a rather subjective factor. We wished to know how much user cooperation is required to operate the device. To clarify and measure, we defined this term as the time spent by the user in a half meter radius from the device. It consists of the time required to access the device, to complete the identification process and to leave. The acquired data can then be used to deduct how much the user has to cooperate with the device due to certain design and operational parameters.

A single person has an average 5-6 sec pass through time. Subtracting the identification time, we can see that, among other things, preparing the sample takes an average 4-5 seconds.

Closely related to the subject is how many degrees of freedom is granted to the user – for example to misplace the sample. In this case, the number of degrees are 6 (3 directional rotation and displacement). The number of restrictions is 2, as the sample can't be tilted, and lifting it is not valid.

Based on this, one has to consider that using the device with larger crowds might not yield the desirable results, as it requires some cooperation from the users and thus it is not fully "fool proof".

Our tests show that even a small rotation of the sample results in a noticeable rise in FRR rates. Detailed examination of test data showed that the rise could be attributed to certain test subjects. Significant increases were experienced over 20°, however, that can't be considered as an accidental positioning error. We also have to note that such errors did not result in a notable increase of identification time. Altogether we can say that the device can tolerate random positioning errors, but some users may be required to be more precise with positioning than others.

Displacement of fingers also result in a rather low FRR rate, provided that the extent of said displacement is low. If we consider the difference between a random and a deliberate positioning error, we can say that random displacement errors are tolerated quite well by the device. Significant displacement, however, notably increases FRR. We can also assert, that the device will make every decision in 2-3 seconds, no matter how much the sample is distorted and/or displaced.

Altogether the device can only handle low level distortion or displacement and some people are required to be more precise when placing the sample than others. Thus it is advised to either educate users about this before installing the system, or only use it where the expectable user cooperation will be present.

## 2.4 HUMAN FACTORS

The following tests are trying to explore factors, that can't be directly measured. Most of these are subjective, we can only define evaluation standpoints. The following results reflect the consensual opinion of test subjects.

### 2.4.1 REQUIRED USER CONTACT

The device has to be physically touched multiple times during normal use. There is no need to operate any buttons or other control measures, however, the fingerprint sensor requires placing the finger directly on it. Our experience shows moderate user resistance against this.

### 2.4.2 CLEANABILITY

The device scored an average result on cleanability tests. The external cover features multiple geometric shapes, but most of them are flat and easily cleaned. Meeting lines of said surfaces are rounded, which allows for better cleaning. The sensor is easily accessed by most simple cleaning tools.

### 2.4.3 MISCONCEPTIONS ABOUT THE TECHNOLOGY

Biometric identification technologies – despite the common beliefs – are not unaffordable. Fingerprint scanning does not provide 100% security, as samples can be stolen and replicated. Reading fingerprints is not feasible with every person at all times, as some people (around 5% of the whole population) lack fingerprints due to genetical reasons, while others may lose prints temporarily or permanently due to contaminants, occupational influences and accidents.

# 3 TEST RESULTS

Tests were conducted in Applied Biometrics Institute (ABI) laboratories hosted at Óbudai Egyetem, during 2013. Test environments were created with respect to manufacturer requirements, as well as usage.

Please note that unique personal differences may influence test results. Every fingerprint is unique to the person, thus measurements conducted by different test populations may yield slightly different results.

Every test was conducted with real persons and real fingers. Numbers provided are not result of theoretical calculations.

## 3.1 OPERATIONAL TIME

Time required by a user for identification and pass through can be one of the most important factors when selecting the proper device. The average time needed for enrolment can also influence the choice.

The following tests seek to answer these questions.

### 3.1.1 ENROLMENT

Upon installing the system or during an organizational transformation, enrolment of large number of users is unavoidable. This usually happens in an office environment in parallel with other processes. Elapsed time during the enrolment process was also measured. This data can be a relatively important factor for those companies where the enrolment of several users is frequent and have to be finished in a relatively short time interval. In other cases this parameter may be negligible.

Time is measured from placing the finger on the sensor to the end of the enrolment process. If the device requires multiple sample presentations during AETD[1] (Average Enrolment Transaction Duration) measurements, all presentations are included, until the device successfully enrols the user. Results are only accepted when enrolment is successful. Prior to the test, we have uploaded the database to 10% of the theoretical capacity.

Only one read is required for enrolment, which considerably speeds up the process, however, there is a trade-off between the number of reads and accuracy. Due to this, we recommend creating an enrolment environment that is free of disturbances.

[1]AETD: (Average Enrolment Transaction Duration) shows the average enrolment time. From the positioning to the end of enrolling the biometric sample (of which we get feedback during the process). It is measured in [s] seconds.

We conducted our tests in such an environment, simulating an average office. Testers were required to position their fingers with maximum precision to achieve optimal positioning.

1. Table Average enrolment time

| AETD (s) | |
|---|---|
| **Average** | **7.0** |

The 1st table shows that the average enrolment of a new user takes 6-7 seconds in the environment mentioned above, deviating between 5.3 and 8.3 seconds. This, of course is influenced by both the quality of the print and the environment in which the enrolment takes place. Such results can be considered good, as other similar devices yielded similar results.

### 3.1.2 THROUGHPUT

Access points equipped with this reader have an average of 5-6 second pass through time. Out of this, reading and identifying the sample usually takes less than 2 seconds. Test results and measurement data can be found above, in the "Required user cooperation/Automatisation" section.

## 3.2 ENVIRONMENTAL PARAMETERS

The manufacturer suggests indoor use. During our tests, we have adhered to this suggestion, tests were conducted in a usual office environment.

*Temperature*

Tests were conducted in a controlled, laboratory environment. Temperature during tests varied between 20 °C and 25 °C and the device performed as per specifications.

*Humidity*

During tests, relative humidity was in range of an average office environment. The device performed as per specifications.

*Illumination*

Illumination was between 300-700 lux, and the device performed as per specifications.

## 3.3 CONTAMINATION, INJURIES

Different identification systems have to face different challenges. There are certain workplaces where the hands – and thus the fingerprints – get contaminated. It is very important to know how much contamination or lesser injuries will affect identification performance, even if only a smaller percentage of the staff will face such situations. If this circumstance is not considered prior to installation, the

system might not be able to perform its duty at all. For this reason, we have tested how the device will handle a variety of contaminants and simulated injuries.

### 3.3.1 SAMPLE CONTAMINATION WITH POWDER

As human fingers can easily get contaminated during everyday life, we tested how common powder-type contaminations affect performance.

During the "contaminating with powder" tests, we applied a thin layer of different grain size powders to the finger (one type at a time), and measured FRR values.

We used contaminants that can be easily encountered in everyday life, ranging from the finest wheat flour through coarser chalk powder up to very coarse quartz sand. Contamination patterns were designed to match those of real life examples.

Each test batch consists of several tests by the same test subject. Both sample and sensor are cleaned between individual tests. The sample is contaminated, then positioned optimally. After each batch, respective FRR values are calculated.

Measurements were performed with many different test subjects, each doing a full test batch. Out of these results, we calculated the average, which can be seen in the following, 2nd table:

**2. Table Powder contaminants**

| FRR values with contaminated fingerprints (%) | | | | |
|---|---|---|---|---|
| | Contaminants | | | |
| | Flour | Chalk powder | 0,2-0,6mm quartz sand | 0,4-1mm quartz sand |
| **Average** | 63 % | 57 % | 83 % | 40 % |

As we can see, powder-type contamination degrades performance considerably, thus the device should not be used in dusty environments. With respect to these results, we suggest that the device should only be used in office environments, where such powder-type contaminants would not be routinely encountered.

### 3.3.2 SAMPLE CONTAMINATION WITH LIQUIDS

This test was aimed to measure how much contaminating the sample with liquids of different viscosities affect performance. The testing method is very similar to the powder tests described in detail above. Cooking oil, body lotion, sunscreen, hand lotion, liquid soap and as reference, water was used as contaminants. Tests were conducted with the same test subjects, each of them doing a full test batch with every material. Out of these results, we calculated the average, which can be seen in the following, 3rd table:

3. Table Liquid contaminants

| FRR values with contaminated fingerprints (%) | | | | | | |
|---|---|---|---|---|---|---|
| | Contaminants | | | | | |
| | Cooking oil | Body lotion | Sunscreen | Hand lotion | Liquid soap | Water |
| **Average** | 95 % | 79 % | 70 % | 67 % | 75 % | 75 % |

The results show that liquid contaminants are not tolerated by the device. Any contamination results in FRR rates that make the device unusable.

We can conclude from these results that the device is very sensitive to fingerprint contamination. Except for one result, average FRR is well beyond 50%, which means that half of the attempts will result in failure. We also have to note that many contaminants produced 100% FRR, so altogether, using the device in environments where the sample can be contaminated is not advised.

### 3.3.3 SENSITIVITY TO DISTORTION (INJURIES)

It often happens that a previously enrolled person suffers some kind of injury affecting the particular sample – for example, in this case, cuts his finger. This will, of course, change the overall pattern of the sample, thus degrading identification efficiency. For this reason, we have tested how much does an injury affect identification performance.

During tests, we have simulated injuries on an otherwise perfect fingerprint. To that end, we attached black duct tape stripes of varied width to the centre of the print, then measured FRR and identification times. We conducted the test batch on the same subjects and we took the average of the FRR and ARAD values as result, which can be found in the 4$^{th}$ and 5$^{th}$ tables.

4. Table Fingeprint distortion sensitivity test results (FRR)

| FRR values with masked fingerprints (%) | | | | | |
|---|---|---|---|---|---|
| | Mask size | | | | |
| | 1mm | 2mm | 3mm | 4mm | 5mm |
| **Average** | 14 % | 24 % | 34 % | 45 % | 65 % |

5. Table Fingeprint distortion sensitivity test results (ARAD)

| ARAD values with masked fingerprints (s) | | | | | |
|---|---|---|---|---|---|
| | Mask size | | | | |
| | 1mm | 2mm | 3mm | 4mm | 5mm |
| **Average** | 1,9 s | 1,8 s | 2,3 s | 2,3 s | 2,3 s |

We found that small injuries increased FRR with only a small percentage of the test subjects. Larger injuries, however, significantly affect performance and usability. Identification times are also increased, altough not significantly, even with bigger injuries. Altogether, we can state, that injuries that can happen in an average office environment are well tolerated by the device, but using it in environments where the risk of larger injuries happening is not advised.

## 3.4 REQUIRED COOPERATION, AUTOMATISATION

Every system that requires human interaction has a fundamental weakness the human itself, who operates and uses the system and biometric identification systems are not an exception. This makes it imperative to discover the parameters that will objectively define this factor. The more „fool-proof" the system is, the better cost efficiency, usability and user satisfaction will be experienced.

### 3.4.1 REQUIRED COOPERATION

Cooperation requirements show how much time it takes to pass through an access point equipped with the device. This of course depends on any other protective equipment installed at the point (i.e. turnstiles, doors), so every time it needs to be evaluated for the particular setup. However, for every device, there is a base value that depends on the devices' own design, performance, and its ideal installation.

The purpose of this test is to measure the average time spent in a 0.5 m radius of the device. This includes approaching, identification (which consists of sample presentation and processing) then leaving the device (unhindered, i.e. without any doors, turnstiles or similar devices). Although these values depend somewhat on user behaviour, the design and properties of the device allow for a good estimation as to how much the user has to cooperate for a successful identification. In case of fingerprint scanners, users have to place their fingers properly, which can be hard, depending on the device and environment.

The results are an average from several measurements.

6. Table Average pass through time

| Pass through time (s) | |
|---|---|
| **Average** | **5,7 s** |

The 6th figure shows that a person needs 5-6 seconds on average to pass through, and it takes about 3 seconds to prepare and position the sample.

### 3.4.2 AUTOMATISATION

In automatisation, we are looked for answers about how many errors users can face due to incorrect sample presentations. We can define restrictions and degrees of freedom, which always have a sum of 6 – 3 directions of movement and 3 axes of rotation. We count features which help proper placement as restrictions, and any other that do not as degrees of freedom.

Devices that have fewer degrees of freedom can be better automatized.

The following table contains the degrees of freedom and restrictions of the device:

7. Table Numbers of restriction and degrees of freedom

| | | |
|---|---|---|
| **Number of restrictions:** | 2 | Tilting of finger<br>Lifting of finger |
| **Degrees of freedom** | 4 | |

The device does not allow for tilting the finger, because it has to be put firmly on the sensor. Furthermore, lifting the finger is not considered, because direct contact is required for device operation. Since the sensor can be found in a gap, only one direction of movement can be considered.

Our tests about improper placement can be read in the **Stress test – Misplacement and positioning errors**

Based on the above data, we can safely say that a single user can complete the full identification process in about 6 seconds. This, however, does not include the time required to pass through any physical barriers (e.g. turnstile, door, etc.). This time is not bad; however, when selecting the device and setting it up, one has to consider that with the base settings, 10-20 people will require minutes to pass through if they arrive at the same time.

One should consider using different settings when a large throughput is required. Due to the small number of restrictions, the device requires user cooperation, and as such, cannot be described as completely 'fool proof'. A good design, however, does not prompt any user resistance, and physical qualities of the users do not influence the amount of cooperation the device requires.

### 3.4.3 ROTATION AND DISPLACEMENT OF THE FINGER

As defined in the base tests, every device has its restrictions and degrees of freedom. Any degree of freedom allows the positioning of the sample in a less-than-ideal way, which can influence performance.

Let us define restrictions and degrees of freedom, which always have a sum of 6 – 3 directions of movement and 3 axes of rotation. We count features which help proper placement as restrictions, and any that do not as degrees of freedom.

Devices with fewer degrees of freedom can be better automatized.

The following table contains the degrees of freedom and restrictions of the device:

The device does not allow for tilting the finger, because it has to be put firmly on the sensor. Furthermore, lifting the finger is not considered, as direct contact is required for device operation. Since the sensor can be found in a gap, only one direction of movement can be considered, as one can only push a finger so far into the gap.

We displaced the sample in the following ways

- Twisting the finger around its horizontal axis from 10° to 50° in both directions, simulating a careless or intentional wrong sample placement
- Rotating the placed finger with respect to the top of the sensor area as much as the device permitted, in such a way that no twisting occurred.
- Pulling the finger inwards and outwards with respect to the sensor

**8. Table FRR values for rotation**

| **FRR values on rotation [%]** | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | **Rotation in degrees** | | | | | | | | | |
| | **10°** | | **20°** | | **30°** | | **40°** | | **50°** | |
| | *right* | *left* | *right* | *left* | *right* | *left* | *right* | *left* | *right* | *left* |
| **Average** | **2 %** | **21 %** | **4 %** | **18 %** | **27 %** | **27 %** | **63 %** | **51 %** | **69 %** | **62 %** |

9. Table ARAD for rotation

| ARAD values for rotation [s] | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Rotation in degrees | | | | | | | | | |
| | 10° | | 20° | | 30° | | 40° | | 50° | |
| | *right* | *left* | *right* | *left* | *right* | *left* | *right* | *left* | *right* | *left* |
| **Average** | **1,9 s** | **1,6 s** | **1,9 s** | **1,8 s** | **2,0 s** | **2,0 s** | **2,5 s** | **2,5 s** | **2,9 s** | **2,8 s** |

One must understand, when talking about rotation, that 10-20° of rotation can be considered as accidental in everyday use, larger angles might mean purposeful misplacement. Our tests, in light of this, not only sought the answer on how the device tolerates accidental positioning errors, but how it tolerates sabotage as well.

The results show that even with small rotations, FRR values rise to a noticeable level, albeit it heavily depends on the direction of the rotation.

Over 20° of rotation, the device quickly becomes unable to identify the prints. However, as we can see, the identification time does not rise. Altogether, we can say that the device should not cause problems if improper positioning happens in everyday use.

The following tests seek the answer for how putting too far in or pulling the finger out affects identification.

10. Table FRR values for Pulling/Pushing displacement on the sensor

| FRR values for pulling and pushing the finger inwards and outwards on the sensor (%) | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | „Towards the device” | | | | | „Towards the tester” | | | | |
| | 2mm | 4mm | 6mm | 8mm | 10mm | 2mm | 4mm | 6mm | 8mm | 10mm |
| **Average:** | **13 %** | **15 %** | **33 %** | **55 %** | **80 %** | **0 %** | **0 %** | **2 %** | **7 %** | **38 %** |

11. Table FRR values for sideways displacement on the sensor

| FRR values for sideways displacement on the sensor (%) | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Right | | | | | Left | | | | |
| | 2mm | 4mm | 6mm | 8mm | 10mm | 2mm | 4mm | 6mm | 8mm | 10mm |
| Average: | 0 % | 1 % | 3 % | 47 % | 90 % | 0 % | 4 % | 19 % | 55 % | 90 % |

12. Table ARAD values for Pulling/Pushing displacement on the sensor

| ARAD values for Pulling/Pushing displacement on the sensor (s) | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | „Away from oneself" | | | | | „Towards oneself" | | | | |
| | 2mm | 4mm | 6mm | 8mm | 10mm | 2mm | 4mm | 6mm | 8mm | 10mm |
| Average: | 1,7 s | 1,8 s | 2,6 s | 2,3 s | 4,7 s | 1,6 s | 1,7 s | 1,9 s | 1,8 s | 1,9 s |

13. Table ARAD values for sideways displacement on the sensor

| ARAD values for sideways displacement on the sensor (s) | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Right | | | | | Left | | | | |
| | 2mm | 4mm | 6mm | 8mm | 10mm | 2mm | 4mm | 6mm | 8mm | 10mm |
| Average: | 1,5 s | 1,7 s | 1,8 s | 3,1 s | 2,1 s | 1,6 s | 1,8 s | 2,6 s | 1,9 s | 1,7 s |

The results show that the device produces relatively low FRR values, should the size of displacement be small. Smaller displacements, up to 4 mm, cause problems with only a few users, while larger displacements deteriorate operation severely. Identification times, however, did not rise, similarly to the previous tests. Large displacements caused the device to not even detect the sample, causing no attempt to identify. This means that a larger portion of the sample has to be correctly positioned to start the identification process.

Altogether, positioning errors are not really tolerated by the device, significant displacement of any kind will hamper identification performance. During installation, users must be properly trained and the device should only be installed to locations, where users can be expected to cooperate this much.

## 3.5 HUMAN FACTORS

The following sections examine factors that have no direct, quantifiable measurement results associated with them. These factors are subjective, we can only give points of view. The following results are the consensual opinion of our test subjects.

### 3.5.1 PHYSICAL CONTACT WITH THE DEVICE

To operate the device, physically touching the sensor is necessary due to the technology. There are no controls to be operated, and we have experienced no bigger resistance than with other technologies.

### 3.5.2 CLEANING AND MAINTENANCE

Acceptance towards a freshly introduced fingerprint scanning system is influenced by the speed of the device getting dirty and the ease of cleaning. This test was conducted to discover how much effort and equipment is needed to clean the device. We conducted these tests along with the stress tests, where we contaminated the device with various contaminants. You can read about these tests further in our **Stress test – Contamination** chapter. We evaluated the device based on its geometric features, the ease of cleaning, and resistance against contaminants.

- **The device has rather elaborate geometric features**. Although its design is clean, and mostly consists of easily cleaned straight surfaces, the sensor and its immediate surroundings are prone to accumulating contaminants. This area is harder to reach during cleaning.
- **The sensor is not well placed in terms of cleaning**. The previously stated problems are true for the sensors as well. They are not easy to access for cleaning and require some attention.
- **The materials used are easy to clean**. Plastic can be easily cleaned with neutral cleaning materials. Since the device is not IP protected, this requires some caution.

### 3.5.3 MISBELIEFS REGARDING THE TECHNOLOGY

Biometric identification – contrary to popular belief – is not unaffordable. Fingerprint scanning does not provide 100% security as it can be spoofed, and doesn't work at all times. Some fingerprints, due to genetic reasons or permanent injuries, are unusable for identification. Some materials and jobs may also render fingers unusable for optical fingerprint scanning (e.g. moving bricks by hand, using hand lotions, and injuries).

# 4 LITERATURE

[1] http://www.midpoint.lt/en/online-store/readers/ip-biometric-readers/bioentry-plus-capacitive

[2] ABI test methodology, 2014, Budapest

[3] ISO/IEC 19795-6:2012