Evaluation Report
Biometrics Trial
2b or not 2b

Contents

DEFINITIONS

AAS	Amsterdam Schiphol Airport
Application process	Applying for a travel document at the municipal service point
Active authentication	Preventing the chip's content being copied or the chip being substituted
Basis Access Control	Preventing the chip data being read undetected
Biometrics	Using physical or behavioural characteristics to ascertain or verify a person's identity
BioRAAS	A copy of the existing RAAS, combining the applicant's biometric data with the data from the application form. The application for a biometric test document is sent, in encrypted form, from the BioRAAS to the producer of the travel documents.
BPR	Personal Records and Travel Documents Agency
BTD	Biometric test document
CBP	Dutch Data Protection Authority
eNIK	Dutch electronic identity card
False reject	A verification that is wrongly rejected
False accept	A verification that is wrongly accepted
FAR	False Acceptance Rate, the percentage of false acceptances in relation to the total number of fraudulent verification attempts
Photo scan	Facial record based on a passport photo
FRR	False Rejection Rate, the percentage of false rejections in relation to the total number of verifications
Facial scan	A facial record on a chip
IAR card	Authorized Official Identification card
ICAO	International Civil Aviation Organization
Identification	The system whereby a live recording of a biometric identifier is compared with a number of characteristics of various persons stored in a database
ImagePerf	An ImagePerf is a second passport photo affixed to the holder page of the passport by means of perforation and visible when the holder page is held up to the light.
LDS	Logical Data Structure
Live scan	Live recording of the face
Look-alike fraud	Look-alike fraud involves an unlawful holder using a travel document of a holder to whom he or she bears a physical resemblance.

Minutiae	Identification points in the pattern of lines in a fingerprint
MRZ	Machine Readable Zone
NGTD	New Generation Travel Documents, introduced on 1 October 2001
Padding	A grey border around a picture of a face caused by converting the picture to the requisite ISO format
Passive authentication	Establishing the authenticity and integrity of the stored data
Producer	Sdu identification
PUN	Passport Regulations Netherlands
PUB	Passport Regulations Abroad
PUKMAR	Passport Regulations Royal Military Constabulary
PUNA	Passport Regulations Netherlands Antilles and Aruba
Travel document	Passports and National Identity cards
REVU	RAAS Enrolment and Verification Unit, the hardware and software enabling a biometric test document to be applied for and issued.
Secure messaging	Encrypting the flow of data between the chip and the reader to make tapping impossible
Train-the-Trainer	A training method whereby one or more people are trained enabling them to train others
Issue process	Collecting the travel document at the municipal service point
Verification	Comparing biometric identifiers 1:1 with those stored in the travel document
Fingerprint	Print made by the fingertip

1. Introduction

1.1 From NGR 2001 to biometrics in travel documents

Making travel documents secure is an ongoing process, with new ways of protecting documents against misuse constantly being sought. Travel documents are used at home and abroad to verify the holder's identity and nationality.
With the introduction of 'New Generation Travel Documents' (NGR) on 1 October 2001 the Netherlands made all Dutch travel documents highly secure against possible misuse. When the NGR model was developed it made use of the most advanced technologies available at the time, but it was realized then that biometric identifiers could be a solution to the problem of look-alike fraud (use of a travel document by a person other than the lawful holder). As the technical standards needed were not then available, following the introduction of the NGR model it was decided to carry out a study in due course into whether to include biometric identifiers in Dutch travel documents.

The study[1] was concerned in particular with the question of what biometric technologies would be most suitable for combating look-alike fraud. The findings were presented to the House of Representatives on 19 December 2003.[2] From these it was concluded that the finger scan would be the best biometric technology to combat look-alike fraud.

In spring 2003 the International Civil Aviation Organization (ICAO)[3] opted for the facial scan as the biometric identifier to be included in travel documents. In order to comply with the ICAO guideline it was decided to include a facial scan as well as a finger scan in Dutch travel documents. In December 2004 the European Union also laid down, in the Regulation on standards for security features and biometrics in passports and travel documents issued by Member States,[4] that the travel documents of the European Union Member States would have to include a facial scan and two fingerprints.

[1] Study into the application of biometric characteristics in the Dutch travel documents', The Hague, 6 June 2003, Biometrics Project, Personal Records and Travel Documents Agency, Ministry of the Interior and Kingdom Relations.
[2] TK 2003-2004, 25764 No. 22
[3] Letter from ICAO dated 28 May 2003, PIO 09/03.
[4] Council Regulation (EC) No. 2252/2004 of 13 December 2004.

In preparation for the introduction of biometric identifiers in Dutch travel documents a trial was conducted by the Ministry of the Interior and Kingdom Relations (BZK), under the name of '2b or not 2b', the aim of which was:

1. to look into how the application and issue process would have to be organized once biometrics were included;
2. to see whether the biometrics (facial scan and finger scan) in the travel documents could be verified.

The Ministry of BZK evaluated the trial. This report sets out the findings of the evaluation.

1.2 Organization of the Report

This report is organized as follows.

Chapter 2 describes the design of the trial, including monitoring and evaluation. Chapter 3 sets out the results, discussing the quality of the biometrics recorded as well as numbers of participants, test documents and successful and unsuccessful recordings and verifications. Chapter 4 sets out the conclusions and describes how the biometrics (facial scan and fingerprints) can be included in Dutch travel documents and how they can be verified when the documents are issued.

The report includes the following Appendices:

- References
- Specifications of Biometric Test Documents
- Phasing of Trial
- Detailed Analysis of Data from Municipal Trial
- Analysis of Schiphol Test Documents
- TNO Report

2. The Trial

2.1 Design of trial

The trial comprised three parts:

- municipal trial to try out the application and issue process and verify the biometric identifiers;
- trial at Schiphol Airport to ascertain the effects of frequent verification on the biometric test document;
- trial (carried out by TNO) to find out whether it was possible to obtain record biometric identifiers from children under 14.

For the purpose of the trial the current application and issue process at the municipalities was left unchanged wherever possible. A person applying for a regular travel document 'merely' had additional biometric identifiers recorded and verified; he or she did not have to undergo a completely separate application process. For the purpose of the trial the existing document scanners were therefore used to send the travel document application forms to the producer of the documents. Also, no additional requirements were laid down for photos to be supplied by the applicant vis-à-vis the current Dutch photo matrix.

The figures below show the application process and issue process in schematic form.

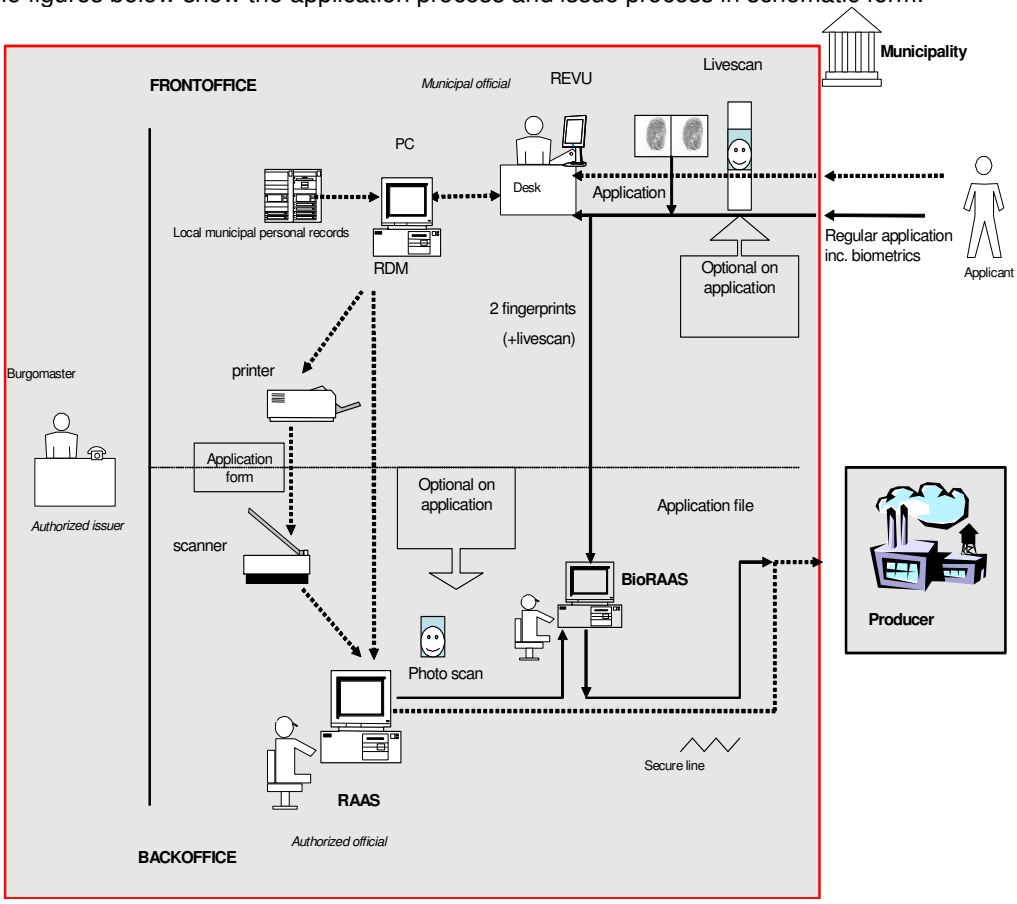

Fig. 1, Application process

The application process is as follows: the person's identity is ascertained by verifying the identity documents submitted, then a new application is drawn up. The passport photo is affixed to the application form, which the applicant signs. The form is scanned and once the application has been checked it is sent in encrypted form via a secure line to the producer. For the purpose of the trial two fingerprints were taken at the desk. The facial scan was included in the biometrics application, using the scanned passport photo, in three of the trial municipalities; in the others a live recording of the applicant's face was made at the desk using a camera.

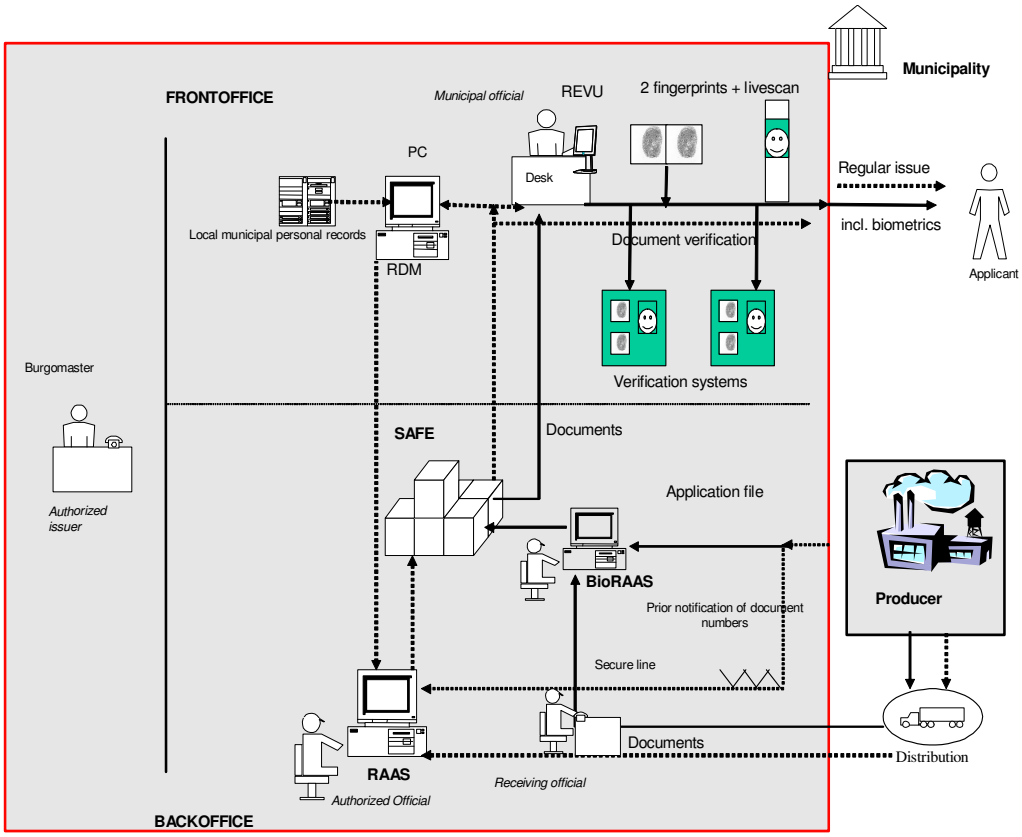

Fig. 2, Issue process

The issue process is as follows: the travel document is received, checked and entered in the travel document records. The person's identity is ascertained again before the document is issued to the person. For the purpose of the trial the biometrics recorded were verified by making a live recording of the face and fingerprints and comparing these with the biometrics stored on the chip in the test document. The biometrics were then verified again using verification systems from various suppliers of such systems.

For the purpose of the trial the Interior Ministry of BZK commissioned two different biometric test documents (BTD), one based on the passport (ID-3 format) and one based on the Dutch identity card (ID-1 format). The chip for storing the biometrics is affixed to the holder page of the passport and incorporated in the identity card.

The test documents were produced and personalized in the normal way by the producer of Dutch travel documents (Sdu Identification), based on the International Civil Aviation Organization standards [ICAO2004], i.e. using Basic Access Control (BAC), Secure Messaging, Passive Authentication and Active Authentication. A contactless chip (ISO 7816) with a storage capacity of 72 kBytes was used. The chip's data storage structure, known as 'Logical Data Structure' (LDS), was based on the ICAO and EU specifications (for the test document specifications see Appendix 2).

The purpose of Basic Access Control (BAC) is to prevent the chip data being read undetected.[5] Secure Messaging is part of Basic Access Control and ensures that data interchange between the chip and the reader is encrypted. Passive Authentication ascertains the authenticity and integrity of the stored data, and Active Authentication prevents the data being copied or the chip being substituted.
Additional requirements[6] under the EU Regulation [EU2004], e.g. Extended Access Control to encrypt fingerprints, were not included in the trial, as the European Union technical specifications were not yet available when the trial was in preparation and the test documents were produced in a single batch prior to the trial.

For the purpose of the trial the producer of the travel documents developed a RAAS Enrolment and Verification Unit (REVU). The following peripherals were connected to the REVU:

- a smartcard reader to sign the recorded biometrics digitally using an IAR card[7] so that the irrefutability of the application is clear to the official in question;
- a bar code scanner to read the number on the application form;
- a machine-readable zone (MRZ) reader to access the chip;
- a chip reader to read the data stored on the chip;
- a finger scanner to record and verify fingerprints[8];
- a digital camera in a column to enable a live scan of the face to be made and verified[9];
- a smartcard with the key material for encrypting fingerprints when the application is made and decrypting the encrypted fingerprints when the document is issued.

The trial municipalities also set up a grey backdrop and an adjustable-height stool.

The producer also produced a modified version of the existing Travel Document Application and Records Station (RAAS),[10] known as the 'BioRAAS'. This was connected to the REVU so as to add the biometrics recorded to the application file that was sent to the producer of the travel documents. The BioRAAS was equipped with a smartcard reader for the IAR cards.

[5] The chip reader has to authenticate itself to the chip before it can open the requested files. This authentication is based on cryptographic technologies.
[6] The EU specifications require Extended Access Control to be used when reading out fingerprints.
[7] Authorized Official Identification Card
[8] The finger scanner was by Sagem.
[9] The camera was by Viisage.
[10] RAAS (Travel Document Application and Records Station), where the applicant's personal data are combined with the data from the scanned application form (photo and signature) to form an application, which is sent to the supplier of the travel documents in encrypted form.

2.2 Municipal trial

The biometrics trial began on 30 August 2004 and ended on 28 February 2005. Six municipalities, viz. Almere, Apeldoorn, Eindhoven, Groningen, Rotterdam and Utrecht,[11] participated. They are referred to in the remainder of this report as the 'trial municipalities'. The agreements between the trial municipalities and the Interior Ministry on duration, input and reimbursement were set out in a covenant.

Persons applying for a regular travel document during the trial were able to take part on a voluntary basis. Participants were recruited with a letter from the Minister for Governmental Reform and Kingdom Relations12 (BVK) and a leaflet. As recompense for taking part, each applicant received €10 discount on the regular price of the travel document.

In line with the provisions of the Personal Data Protection Act the participants gave written consent for their personal data and biometrics to be used in the trial. Prior to the trial the Interior Ministry consulted the Dutch Data Protection Authority (CBP) on the matter.

Application and issue process

All the trial municipalities used two biometric identifiers, a facial scan and fingerprints. The facial scan was produced in two different ways. In three municipalities it was produced by scanning the photo that the applicant was required to submit when applying for a travel document; in the other three a 'live scan' was made at the municipal service point using a camera.[13] In the trial municipalities two fingerprints were taken from the participants, as a rule of the left and right index finger.

In the trial municipalities the biometrics were also verified using other equipment than that used to record them.[14] Hardware and software from six suppliers of biometric verification systems was used (finger scanner: Precise Biometrics, Nec, BioScrypt and Identix; camera: Biodentity, Cognitec and Identix).

[11] These municipalities were selected because of the numbers of travel documents regularly issued and the technical suitability of the location (network plus enough space for the test equipment on and around the counter).
[12] This letter was enclosed with the compulsory (since 2001) municipal reminder that the person's travel document will expire in the near future.
[13] The EU Regulation leaves the Member States free to choose the method of facial scanning (photo scan or live scan).
[14] The same hardware and software was used to record the biometrics in all the municipalities.

2.3 Schiphol trial

The Schiphol trial was conducted to ascertain the effect on the test documents of frequent use. A trial took place from September 2004 to February 2005 in collaboration with Amsterdam Schiphol Airport (AAS) in which 193 of the airport's staff used the test document developed by the Ministry of BZK to gain entry to the Schiphol building at a staff entrance. The aim was to carry out some 10,000 verifications during the trial.

2.4 Children's trial

As the Ministry of BZK anticipated that only a few children would apply for documents in the trial municipalities, a separate study was conducted to ascertain whether it was possible to make a facial scan and take fingerprints from children under 14 years of age. The study was commissioned by the Ministry of BZK and conducted by TNO. TNO also carried out a literature review into the possible effects of facial changes on recognizability when using automatic face recognition.

2.5 Monitoring and evaluation

During the trial the Ministry of BZK inserted four interim evaluations to monitor the conduct of the trial and modify it where necessary. These took place one week, two weeks, two months and four months after the start of the trial[15] and resulted in various modifications being made during the trial, both to the software and to the instructions for the officials and participants.

As far as possible data were collected and recorded automatically during the trial. Where automated data collection was not feasible, municipal officials used logbooks. Municipal officials were additionally interviewed and trial participants polled.

[15] The system data were collected in weeks 37, 38, 45 and 53 of 2004.

2.6 Funding of trial

The trial was funded from the Ministry of BZK budget and cost €3,427,713. The cost broke down as follows:

• Municipalities, including €10 to participants	€	531,000
• Producer of the travel documents	€	1,265,930
• Suppliers of verification systems, including hiring-in of experts	€	1,451,130
• TNO study into children and biometrics	€	26,775
• Other, including information (leaflet etc.)	€	152,297

3. Results

This chapter outlines the results of the municipal trial, the trial at Schiphol and the TNO study. The analyses that form the basis of this report can be found in Appendices 2-6.

3.1 Municipal trial

3.1.1 Application and issue process

14,700 persons took part in the municipal trial.[16] A total of 14,735 applications were made, of which 14,504 documents were personalized and supplied to the municipalities. The discrepancy between the numbers of participants, applications and actual documents produced is due to the following:

- 35 persons applied for two documents.
- 217 passport photos were not able to be converted to the required ISO-19794 format because the software used was unable to locate the eyes correctly in every case (1.5%).
- 14 applications could not be sent from the REVU to the BioRAAS owing to technical problems (0.1%).

Biometrics included

Of the 14,504 documents produced:

- 14,038 (96.8%) included the facial scan and two fingerprints.
- 192 (1.3%) included the facial scan and one fingerprint.
- 274 (1.9%) included only the facial scan, as it was not possible to record fingerprints that met the quality standards.

Attempts to record biometrics

In about 10% of cases more than one attempt was needed to record biometrics of the required quality. Of these 10%, 9 out of 10 times the reason was that the person had difficulty following the instructions for positioning the face (39 applications) or finger (1,567 applications). In the remaining cases the failure to record biometrics was due to technical problems.

[16] The six burgomasters/aldermen of the trial municipalities and the Minister for Governmental Reform and Kingdom Relations, and the test documents issued to them at the start of the trial, were not included in the analysis.

Biometric test documents issued (verified)

Of the 14,504 documents produced, 14,165 (97.7%) were verified when they were issued. Verification did not take place in 339 cases (2.3%), for the following reasons.

Technical problems:

- In 178 cases the REVU was not available owing to technical problems, so verification upon issue could not be carried out. In these cases verification did however take place using other verification systems;
- 2 documents were not produced until about a month after the application because the BioRAAS 'held onto' the application file;
- In 11 cases the test documents were delivered too late;
- In 20 cases municipal officials noted various reasons (in the logbooks), e.g. MRZ fault, BTD reader fault, equipment broken, technician working on the equipment at the time of verification;

Procedural problems:

- One test document was unable to be found by the trial municipality when the participant reported for verification;
- In one case the participant's health did not permit verification;

Unknown problems:

- The reason was unexplained in the case of 126 documents (0.9%).

Successful and unsuccessful verifications

In 99.2% of the test documents verified at least one of the three biometric identifiers recorded was successfully verified. The identifiers recorded were successfully verified in 93.6% of cases. In 4.3% of cases one fingerprint was able to be verified (4.1% including the face and 0.2% without the face). In 2.9% of cases the face was successfully verified but verification of the fingerprints was completely unsuccessful. In 2.2% of cases the facial scan could not be verified.

Verification attempts

Over 4% of the participants needed more than one attempt to achieve successful verification. In half the cases this was due to technical problems and in the other half to the way the biometrics were offered for verification (incorrect positioning of finger and/or face, finger too dry/wet, out-of-date passport photo etc.).

Overview of applications/issues

Error! Reference source not found., Overview of municipal trial

Fig 3 gives a schematic overview of the figures for participants, test documents applied for and test documents verified.

3.1.2 Breakdown of participants

Age of participants

The trial participants were relatively old, compared to the age structure of the Dutch population in general. The figure below[17] shows how the population of the trial relates to the structure of the Dutch population.

[17] No requirements were laid down for participation in the trial. The age pattern was monitored during the trial, but it was not found possible to exert much if any influence on this aspect. The number of participants aged 13 and 14 went up sharply in the last quarter of 2004, owing to the introduction of the Compulsory Identification Act. This explains the big discrepancies in Fig. 4.

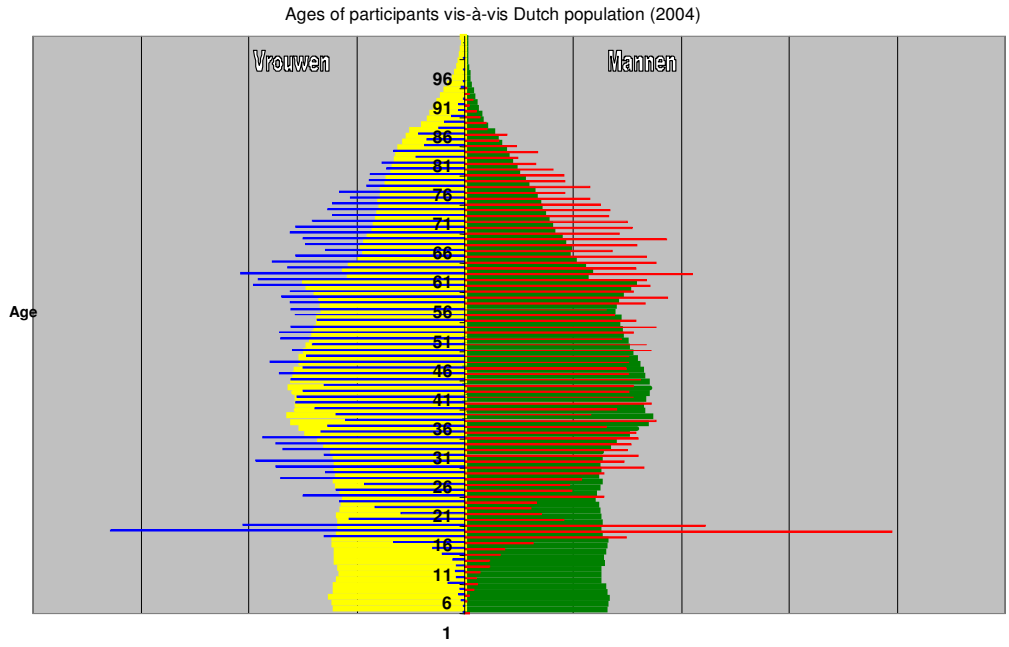

Fig. 4: Age structure of trial participants compared to Dutch population
(lines represent trial participants, solid area represents Dutch population)

Participants aged 50-80 were overrepresented in the trial population, and the over-80s were hardly represented at all.

The percentage of children under 13 who took part in the municipal trial was lower than would be expected, based on the age structure of the Dutch population, so TNO carried out a separate study, in which 161 children took part.

Sex
47% of the participants were male and 53% female. The distribution in the Dutch population is 49% male and 51% female.

Photo scan municipalities vis-à-vis live scan municipalities
Of the total participants, 52% (7,676) made applications at the 'photo scan' trial municipalities and 48% (7,064) at the 'live scan' municipalities.

3.1.3 Facial scan

The following factors were assessed as regards the facial scan:

- scan quality: what was the quality of the photo scan and live scan?
- verification results: was there a difference in verification results upon issue?
- design of desks and issue points: what effect did the design of the service points have on a photo scan and a live scan?

- participant's personal characteristics: did wearing spectacles, having a beard/moustache etc. affect successful verification of the face upon issue?

Facial scan quality

The facial scan stored in the test documents—both the photo scan and the live scan—complied with the technical ICAO and ISO[18] specifications (number of pixels between the eyes, fill factor, eye coordinates, both eyes on a horizontal line). When the facial scan was being recorded, images that did not comply with these specifications were brought up to specification by the software (by zooming in or out and/or rotating the image). Depending on the extent of deviation from the specifications, and thus the size of the correction, this caused 'padding' in some cases (a grey border round the facial image). An example is given below.

Fig. 5: Facial scan with padding

Padding does not affect automated biometric verification but it did adversely affect the quality of the visual image aesthetically in the test documents.

In 1.5% of cases (217) the photo submitted did not meet the requirements, with the result that the software was unable to locate the eyes. As already indicated, the requirements for photos to be submitted were not changed for the trial, so as to leave the existing application process unchanged as far as possible.

There is no objective[19] automated standard system for measuring the quality of a facial scan. To gain some idea of this, however, a number of parameters were set based on the 'photo matrix'[20] currently in force (e.g. shadow, brightness, contrast, background, rotation, size of face). All the facial scans (both photo scans and live scans) made upon application were rated (see Appendix 3). The photo scans rated unsatisfactory on a number of parameters, e.g. shadow and brightness. The live scans rated unsatisfactory on the parameters relating to contrast and rotation of the head: the participant's head was not always centred in the image and the participant was not always looking straight into the camera.

The quality of the facial scans was also affected by the resolution, which was lower in the case of the photo scanner than the camera.[21]

[18] ISO-19794 format.
[19] An objective standard of this kind does exist for fingerprints.
[20] Article 28 of the Passport Regulations (Netherlands) 2001 requires photos to meet various requirements, which are set out in detail in a 'photo matrix'.
[21] So as to leave the regular application and issue process unchanged as far as possible, the existing scanners were used: these have a resolution of 300 dpi, unlike the cameras, which have a resolution of 500 dpi.

Verification results

Facial scans produced by scanning photos resulted in about 4% dropout upon verification, due in particular to the resolution at which the photos were scanned (300 dpi).

Another cause of dropout was the fact that photos for automatic face recognition have to meet more stringent requirements than those currently set for photos.[22] The dropout upon verification of facial scans based on live scans was 0.1%.

Recording of facial scan					Verification of facial scan				
Face	Photo scan	Live scan	Total	%	Face	Passport photo	Live scan	Total	%
+	7,439	7,065	14,504	100.0	+	6,896	6,842	13,738	97.8
					-	300	10	310	2.2
Total	7,439	7,065	14,504	100.0	Total	7,196	6,852	14,048	100.0

Table 1 Recording and verification of facial scan

Design of desks

Producing good-quality live scans requires major changes at the issuing authorities, as the lighting, camera settings and background have to be controlled to enable a good quality recording of the face to be made. An official also needs a professional photographer's know-how to make a live scan at the desk. These requirements do not apply in the case of a photo scan.

Personal characteristics

Reflections from spectacles can adversely affect automated face recognition. About 45% of spectacle-wearers were more likely to get an error message on verification of the face than non-spectacle-wearers.

Having a beard or moustache did not have any effect on whether a facial scan could be recorded or verified. The trial was inconclusive when it came to the effect on verification of different skin colours, as the number of trial participants with different skin colours (1% black, 7% coloured) was too small. Facial expression, on the other hand, was a major factor in the probability of successful verification: a participant who was smiling on the recorded scan and looking into the camera with a neutral expression upon verification was likely not to be positively verified. The current stricter ICAO standards for facial scans include facial expression.

3.1.4 Fingerprint

The following factors were assessed as regards fingerprints:

- number of successful and unsuccessful recordings;
- number of successful and unsuccessful verifications;
- fingerprint quality throughout the trial;
- fingerprint quality in relation to the participant's age;
- fingerprint quality in relation to the of recording the fingerprint;

[22] The ICAO has drawn up guidelines including requirements for facial scans, including fill factor, facial expression etc.

- effects of hobbies/occupation/scars on fingerprint quality.

The quality of the fingerprints recorded was analysed using the 'NIST Fingerprint Image Software 2 (NFIS2)' provided by the National Institute of Standards and Technology (NIST). The NIST has developed a classification system for fingerprints enabling fingers to be classified in five categories, with 1 standing for 'excellent', 2 for 'very good', 3 for 'good', 4 for 'fair' and 5 for 'poor'. According to the NIST [NIST2004], categories 1, 2 and 3 permit adequate verification.[23]

The trial fell into two periods as regards fingerprinting. In the first period (phases 1-3 of the trial) the software did not include a quality parameter for taking the original fingerprints (this period covered the first three months of the trial). In the second period of the trial a quality parameter was incorporated in the software, which assessed the quality of the fingerprints before they were recorded. Also, a number of officials of the trial municipalities were given additional training on how to take fingerprints.

[23] According to the NIST, fingerprints in quality categories 1, 2 and 3 produce few if any false rejections upon verification.

Number of successful and unsuccessful recordings

In 96.8% of applications two fingerprints were taken successfully. In 1.3% one fingerprint was successfully taken and in 1.9% it was impossible to take a fingerprint from the applicant at all.

Fingerprint recording			
Finger 1	Finger 2	Total	%
+	+	14,038	96.8
+	-	63	0.4
-	+	129	0.9
-	-	274	1.9
		14,504	100.0

Table 2: Fingerprint recording

Number of successful and unsuccessful verifications

When the test documents were issued, one or two fingerprints were successfully verified in 97% of them. Verification of one or two fingerprints failed in 3% of cases.

Fingerprint verification			
Finger 1	Finger 2	Total	%
+	+	13,037	92.8
+	-	323	2.3
-	+	279	2.0
-	-	409	2.9
		14,048	100.0

Table 3: Fingerprint verification

Introducing the quality parameter when taking fingerprints resulted in a slight improvement in verification upon issue (see Appendix 3). This improvement did not occur when verifying using the other systems: one reason for this could be that the improvement occurs particularly when verification is done using the same system used to take the fingerprint.

If only fingerprints in NIST categories 1, 2 and 3 are verified using systems other than the one used to take the fingerprints there is an improvement in most verifications, however (see Appendix 3). If an open standard—NIST—is used to assess fingerprint quality, the probability of successful verification by systems not used to take the fingerprints would seem to be greater.

Fingerprint quality throughout the trial

The figure below shows the quality of the fingerprints taken in each phase. Before the quality parameter was introduced (phases 1, 2 and 3) the quality of the fingerprints slowly declined (the NIST quality scores were higher in phase 3 than in phase 1). Interim analysis of the fingerprints revealed that the quality was unsatisfactory[24] and that a threshold needed to be set before the software would accept a fingerprint recording, as the officials—rightly—trusted the software ratings.[25] Once the quality parameter had been incorporated in the software the quality of the fingerprints recorded improved: the NIST quality improved from phase 4 onwards.

[24] The quality of the fingerprints recorded was assessed in collaboration with the NFI and other bodies.
[25] The system emitted a beep when a fingerprint had been recorded.

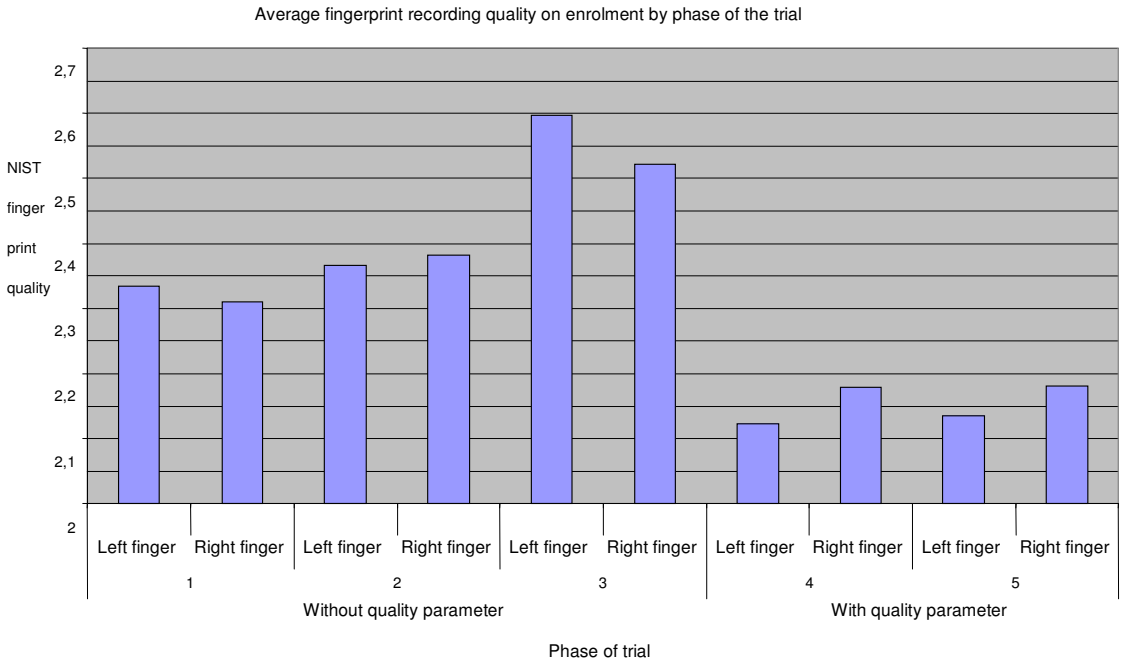

Fig. 6: Average NIST fingerprint recording quality by phase

Fingerprint quality in relation to the participant's age

The quality of the fingerprints recorded was found to go down with age. Over 65 years of age the probability of fingerprint quality being higher than 3 on the NIST scale steadily increases, which means, according to NIST, that the probability of verification failure is reasonable to high.

The figure below shows graphically the relationship found between average fingerprint quality and the age of the participant.

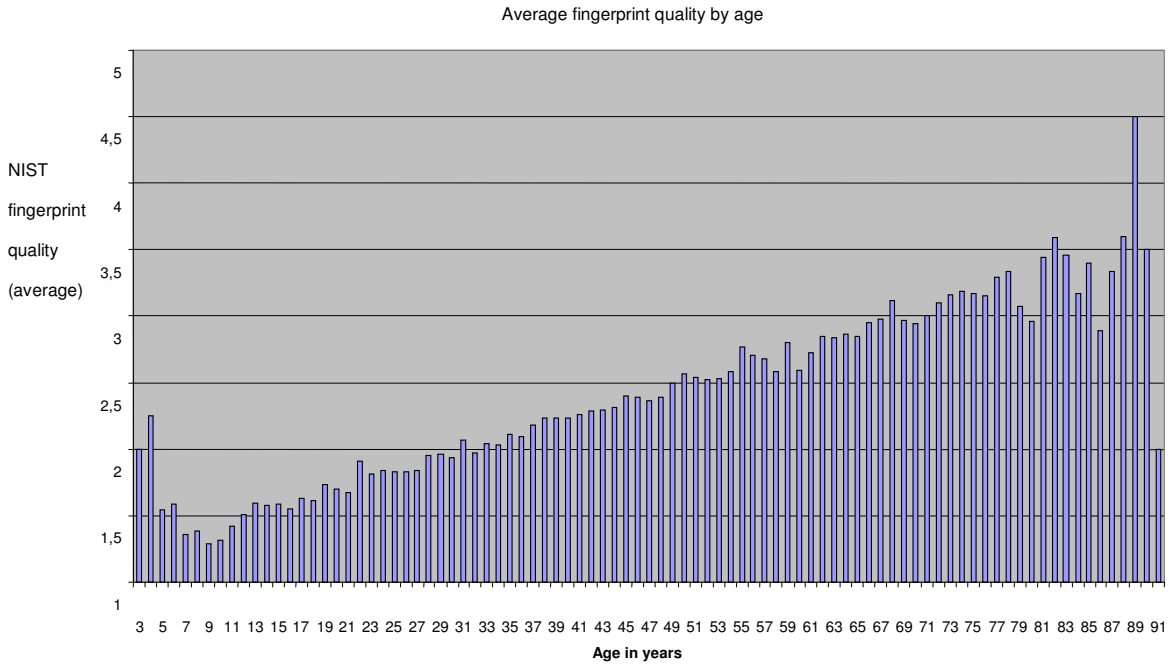

Fig. 7: Average fingerprint quality by age

Fingerprint quality in relation to the time fingerprinting took

Including a quality parameter in the fingerprint recording software caused fingerprinting to take longer (about twice as long).[26] A print of the right-hand finger with a NIST quality of 1-3 takes about 15 seconds; a print of the left finger takes about 25 seconds.[27] Taking a fingerprint with a NIST quality of 4 or 5 takes about 40 or 48 seconds (right and left-hand finger respectively). The difference in the time needed to take a print of left and right-hand fingers is probably due to the fact that most people are right-handed: right-handed people are likely to position a right-hand finger correctly more quickly than a left finger.

Fingerprint verification upon issue takes about 17 seconds.

Effects of hobbies/occupation/scars on fingerprint quality

The results of the trial did not indicate that participants with an occupation or hobby that could cause damage to the fingers had a significantly lower fingerprint quality.

[26] See Appendix, Detailed Analysis of Data from Municipal Trial.
[27] This includes applying the quality parameter.

3.1.5 Readout speed

Reading the data on the machine-readable zone on the test documents and the data stored on the chip took 15-25 seconds. The theoretical minimum readout time that could be achieved would be about 3.8 seconds.[28] The discrepancy is due to the fact that the security measures (Basic Access Control with Secure Messaging) affect readout speed, and a number of cryptographic functions required were not integrated in the operating system on the chip.

3.1.6 Experiences of officials

24 municipal officials who had taken part in the trial were interviewed, both individually and in groups.

Those officials who had taken the producer's training course did not always pass on the knowledge they had acquired to their colleagues, partly owing to pressure of time. As a result, officials were sometimes unprepared when dealing with applications for biometric test documents and issuing them. It also transpired that, with a few exceptions, officials did not use the written training material provided (both that handed out before the trial and the additional material issued to improve fingerprint recording) for reference during the trial.

The current photo matrix in force was used in all the trial municipalities when assessing photos submitted or making live scans. In a few cases passport photos were not accepted by the municipal official or live scans were retaken.
The officials said that they were unable to fathom why:

- a photo was rejected by the BioRAAS;
- the BioRAAS rotated the facial scan;
- the BioRAAS added crosshairs to the facial scan (marking the eye coordinates to detect the eyes).

The fingerprint recording software was configured in such a way that standard practice was to ask for the left index finger first. This caused confusion, as most participants automatically placed their right index finger on the finger scanner first. The officials also rated finger scanners that could be moved around on the desk higher for ease of operation than those which could not be moved by the participant.

The camera used to take live scans of the face was not user-friendly, according to the officials. The participants had to position themselves correctly in front of it to enable a live scan to be made. The official was not able to assist in the process, e.g. by adjusting the camera. Nor was the stool supplied adequate, said the officials: it was not sufficiently adjustable and it was difficult to operate, especially in the case of very young, old or tall people.

[28] The minimum time needed for this can be calculated by dividing the average size of the files stored on the chip (approx. 40 kBytes) by the transmission speed (approx. 10.4 kB/s).

As regards the fingerprint recording software, the officials put forward the following findings/suggestions:

- the software should provide clear instructions;
- the quality parameter was useful, albeit it made taking fingerprints from older people more difficult;
- the official taking the fingerprints needs to be able to look 'over the shoulder' of the person whose prints are being taken so as to assist him or her where necessary by giving instructions;
- steps need to be taken to prevent fingerprints being recorded in the documents with the wrong description (e.g. the right index finger is stored in the document but the description says 'left index finger');
- the software should indicate at each stage in the process whether the biometrics recorded are of the required quality;
- when technical faults occur, clear help screens are needed giving instructions on how to remedy the fault.

3.1.7 Experiences of participants

For two weeks during the trial, questionnaires were handed out to the participants. 861 participants completed them. The questionnaires for the municipalities that used photo scans were different from those that used live scans.

The main findings from the poll were:

- a substantial majority of the participants (89%) gave a positive verdict on the information supplied and the explanations given by the municipal officials;
- 82% of the participants found taking fingerprints easy and 80% found verification upon issue easy;
- 90% of the participants found taking a live scan easy and 80% found verification upon issue easy;
- 74% of the participants found taking the biometrics quick and 73% found verification upon issue quick.

3.2 Schiphol trial

In the Schiphol trial 7663 verifications of 232 test documents were carried out during the period from September 2004 to the end of January 2005. The same test document was used for these verifications as in the municipal trial. Given the relatively large number of verifications, the Schiphol trial gave an indication of how robust the test document was. To ascertain this, he test documents were analysed and 83% of them were found to have hairline cracks in the top layer of the polycarbonate. Investigation of the cause revealed that this was due to mechanical stresses occurring in the material of the test documents.[29]

[29] Hairline cracks developed in the test documents owing to the different coefficients of expansion of the polycarbonate and the metal of the chip casing.

3.3 Children's trial

Fingerprinting

Based on the study conducted for the Ministry of BZK, TNO came to the conclusion that it is virtually impossible to obtain fingerprints from children aged under 4 years. Where it was possible to obtain one fingerprint from children aged 3 or 4 this was generally of the thumb, presumably because it has a larger surface area than the other fingers.

The following points were also noted when taking fingerprints:

- babies (below the age of 8 or 9 months) can make a strong fist which is very difficult to open. This can substantially hamper fingerprinting, as it is impossible to place the finger on the sensor properly. A similar situation can occur, for that matter, in people with spasticity of the hands;
- in children who suck their thumbs a lot the skin of the finger is very soft, and it is often impossible to take a good print from such fingers;
- children's fingers are often very moist and need to be dried if a good quality print is to be obtained.

Live facial scanning

Live facial scanning of children is successful in most cases. Where it is not succesfull this is because children are crying or fidgety, so it is impossible to get them to look straight into the camera for long enough. Another reason is where the camera has a relatively slow shutter speed and the children are unable to sit still, causing the image to be out of focus and therefore unusable.

TNO also did research into facial recognition in children aged twelve years and below based on reference pictures that are a few years old (travel documents are valid for five years). Recognition is problematical because of the major changes that occur in relationships between characteristic facial points as children grow. These changes are part of a complex process determined to a large extent by sex and genetic background. It is unlikely, therefore, that facial recognition software will be able in the near future to compensate for the effects on growth in children's faces.
There are not only technical considerations here but also practical ones: in the strange (to them) environment of a town hall or the hectic conditions of a border control young children may well be unwilling or unable to cooperate with a facial scan, causing delays.

The table below shows the age structure of the group of children and whether the biometrics were taken successfully. Fingerprinting is considered to be successful if valid enrolment and verification prints were able to be taken from at least one finger.

Age	Number	Fingerprint successful	%	Face successful	%
0	15	0	0.0%	12	80.0%
1	16	0	0.0%	12	75.0%
2	17	0	0.0%	13	76.5%
3	24	2	8.3%	22	91.7%
4	10	5	50.0%	9	90.0%
5	12	8	66.7%	12	100.0%
6	18	16	88.9%	16	88.9%
7	8	8	100.0%	8	100.0%
8	7	7	100.0%	7	100.0%
9	13	13	100.0%	13	100.0%
10	5	5	100.0%	5	100.0%
11	8	8	100.0%	8	100.0%
12	6	6	100.0%	6	100.0%
13	2	2	100.0%	2	100.0%
Total	**161**	**80**	**49.7%**	**145**	**90.1%**

Table 3: Success of obtaining biometrics by age

4. Conclusions

4.1 Recording biometrics upon application for travel documents

Facial scan

The trial showed that facial scanning was successful in almost all cases (98.4%). If high-quality facial scans are to be produced, however, modifications to the current application process or additional facilities are needed.

Two steps are needed when it comes to making facial scans by scanning the photos that applicants are required to submit when applying for a travel document: (a) the photo matrix[30] needs to be revised so that photos meet the international requirements (which have now been amended), and (b) the photo scanning hardware/software needs to be modified. These steps need to be taken before the European Union deadline for introducing the facial scan (28 August 2006) and will require relatively limited efforts, organizationally and financially.

At present, software-based checking of photos submitted by applicants takes place when the travel document application is scanned and the applicant is no longer present. If the check indicates that the photo is not satisfactory the applicant has to be contacted. This could be avoided by carrying out quality control of photos at the desk. If the photo is not satisfactory the applicant can be told and he or she can take action to obtain a photo that does meet the requirements. Photo shops will also have to be informed of the stricter requirements for photos.

If live recordings that meet the quality standards are to be made at the issuing authorities, modifications to the facilities at the desk will be required. We need to bear in mind the fact that there are no 'standard' facilities (the circumstances differ from one location to another) and there are a large number of service points (around 4,200) which would all need to be equipped with recording equipment. This would require substantial investment on the part of both central government and the municipal issuing authorities. In view of this, live scanning is not currently regarded as a realistic option.

Fingerprints

A standard (NIST) for the quality of fingerprints and a quality threshold for fingerprinting proved to be useful tools. Applying them resulted in more successful verifications (upon issue) and ensured that the quality of the prints included in the travel documents will be constant.

Support needs to be provided to people whose fingerprints are being taken. The finger has to be placed right in the middle of the scanner, the correct pressure has to be exerted and so on. The support should be visual (e.g. an on-screen display of how to place the finger) so that the instructions can be understood by large sections of the population.

It is not possible to take fingerprints from everyone. The reasons for this are various, related to both personal characteristics and the limitations of the technology.

[30] A new, stricter photo matrix has been drawn up for facial scans by the ISO, to which the ICAO refers.

Personal characteristics that can play a part are the applicant's age, handicaps and wear and tear or damage to the fingertips. In general it is virtually impossible to take fingerprints from children under 6 years of age.

Given these findings, allowance needs to be made for the fact that there will be people (or categories of people) from whom it is not possible to take one or more fingerprints. It needs to be decided at EU level how to deal with this.

Length of time
Recording a fingerprint takes 20 seconds per finger on average. Recording fingerprints from people with damaged fingers etc. takes substantially longer (about 44 seconds).

4.2 Verifying biometrics upon application for and issue of travel documents

Facial scan
Facial scans made using the existing scanners with the current photo matrix were found to result in 4% dropout upon verification. This rate needs to be reduced by revising the photo matrix (see above) and modifying the scanners. No modifications are needed, on the other hand, at the issuing authorities' desks.

The dropout upon verification of facial scans based on live scans (in the trial) was 0.1%. On the other hand, producing a live scan that meets the quality standards would require a lot of effort and modifications to the service point facilities.

Reflections in spectacles and the position of the rim in relation to the eyes can adversely affect verification, as can facial expression. If the facial expression at the time of verification is not the same as in the stored facial scan there is a substantial probability that verification will fail.

Fingerprints
The quality of the stored fingerprints is a decisive factor when it comes to successful verification. Also, the probability of successful verification is determined by the same factors as that of successful recording: i.e. personal characteristics such as age, handicaps and wear and tear or damage to the fingertips affect verification.

Robustness of the electronic documents
The trial showed that the test documents used developed hairline cracks at the place where the chip was incorporated. The identity cards in particular were also found to display warping. These defects must not occur when travel documents with biometric identifiers are introduced.

Readout speed
Reading the chip took 15-25 seconds. It was found that this could be speeded up considerably by using faster readers and integrating security functions in the chip's operating system.

Appendix 1: References

[EU2004] Applicable EU Regulation 'on standards for security features and biometrics in passports and travel documents issued by Member States' (Council Regulation (EC) No. 2252/2004, 13 December 2004).

ICAO2004] Applicable ICAO guidelines:

[1] Biometrics deployment of Machine Readable Travel Documents 2004
[2] Annex A - Photograph Guidelines
[3] Annex B - Facial Image Size Study #1
[4] Annex C - Facial Image Size Study #2
[5] Annex D - Face Image Data Interchange
[6] Annex E - Iris Image
[7] Annex F – Fingerprint Image
[8] Annex G - Fingerprint Minutiae
[9] Annex H – Fingerprint Pattern
[10] Annex I - Use of Contactless Integrated Circuits
[11] Annex J - ICAO May 2003 Press Release
[12] Annex K - ICAO Supplementary Requirements to ISO14443 -v2
[13] Annex L – ePassports Data Retrieval Test Protocol
[14] Logical Data Structure (LDS), version 1.7
[15] PKI for Machine Readable Travel Documents offering ICC read-only access v1.1

[NIST2004] 'Fingerprint Image Quality', E. Tabassi, C.L. Wilson and C.I. Watson, National Institute of Standards & Technology, NISTIR 7151, August 2004. Including: User's Guide to NIST Fingerprint Image Software 2 (NFIS2), C.I. Watson et al., 2004

Appendix 2: Specifications of biometric test documents

For the purpose of the trial two different biometric test documents were developed, based on the passport model (ID-3 format) and the Dutch identity card (ID-1 format) respectively. The specifications of the two test documents are set out below.

Specifications of biometric test document: passport model

FEATURES	CURRENT 2001 PASSPORT MODEL	BIOMETRIC TEST DOCUMENT
Design and Format		
Format	ID-3 = 125 x 88 mm	ID-3 = 125 x 88 mm
Colour of cover:	Maroon	Dark blue
Colour of holder page	Blue and yellow	Green and purple
Personalization	Laser engraving	Laser engraving
Authenticity features		
Visa pages	Watermark	Watermark
Holder page	Integrated kinegram	Integrated kinegram
	ImagePerf	ImagePerf
	Tactile relief	-
Storage medium		
Medium	-	Contactless chip
Manufacturer	-	Philips
Type	-	Smart MX
Model	-	P5CT072
Capacity	-	72 kB
Operating System		
OS	-	Java
Version	-	JCOP
Inlay		
Material	-	Polycarbonate
Thickness		400 microns
Antenna coil	-	Wire embedded copper wire
Antenna format	-	ID-3
Unloaded resonance frequency	-	16.5 MHz
Operating frequency	-	13.56 MHz
Setup		
Model	-	Logical Data Structure, version 1.7
Data groups	-	DG1: Machine Readable Zone
		DG2:Token image of face
		DG3:Two fingerprints of the index fingers
		DG15:Public key Active Authentication
Biometrics		
Face	-	Image
Compression	-	JPEG 2000
Compression factor	-	Less than 15 kB
File size	-	Approx. 15 kB
Fingerprints		Images
Compression	-	WSQ
Compression factor	-	11-14
File size	-	11-18 kB
Security		
Chip access	-	Basic Access Control
Communication between chip and reader	-	Secure Messaging
Authentication	-	Passive Authentication
Anti-copying	-	Active Authentication
Fingerprints	-	3DES encryption
Security Object Document	-	Document Signer Certificate forms part of this.

Specifications of biometric test document: Dutch identity card model

FEATURES	CURRENT IDENTITY CARD MODEL 2001	BIOMETRIC TEST DOCUMENT
Design and Format		
Format	ID-1 = 86 x 54 mm	ID-1 = 86 x 54 mm
Colour of ID card	Blue and yellow	Green and purple
Personalization	Laser engraving	Laser engraving
Authenticity features		
ID card	Integrated kinegram	Integrated kinegram
	ImagePerf	ImagePerf
	Tactile relief	-
Storage medium		
Medium	-	Contactless chip
Manufacturer	-	Philips
Type	-	Smart MX
Model	-	P5CT072
Capacity	-	72 kB
Operating System		
OS	-	Java
Version	-	JCOP
Inlay		
Material	-	Polycarbonate
Thickness		400 microns
Antenna coil	-	Wire embedded copper wire
Antenna format	-	ID-1
Unloaded resonance frequency	-	16.5 MHz
Operating frequency	-	13.56 MHz
Setup		
Model	-	Logical Data Structure, version 1.7
Data groups	-	DG1:Machine Readable Zone
		DG2:Token image of face
		DG3:Two fingerprints of the index fingers
		DG15:Public key Active Authentication
Biometrics		
Face	-	Image
Compression	-	JPEG 2000
Compression factor	-	
File size	-	Approx. 15 kB
Fingerprints		Images
Compression	-	WSQ
Compression factor	-	11-14
File size	-	11-18 kB
Security		
Chip access	-	Basic Access Control
Communication between chip and reader	-	Secure Messaging
Authentication	-	Passive Authentication
Anti-copying	-	Active Authentication
Fingerprints	-	3DES encryption
Security Object Document	-	Document Signer Certificate forms part of this.

Appendix 3: Phasing of Municipal Trial

During the municipal trial a number of changes were made, based on interim evaluations, to the hardware, software and instructions to municipal officials and participants. As a result, the trial breaks down into six phases.

The changes were not all made at the same time by the various municipalities. The table below shows when they were made.

	Almere	Apeldoorn	Eindhoven	Groningen	Rotterdam	Utrecht
Phase 0	31/8/2004	31/8/2004	31/8/2004	31/8/2004	31/8/2004	31/8/2004
Phase 1	18/9/2004	n/a	18/9/2004	n/a	n/a	18/9/2004
Phase 2	12/10/2004	12/10/2004	12/10/2004	12/10/2004	12/10/2004	12/10/2004
Phase 3	29/10/2004	28/10/2004	29/10/2004	3/11/2004	28/10/2004	26/10/2004
Phase 4	1/12/2004	30/11/2004	1/12/2004	25/11/2004	1/12/2004	1/12/2004
Phase 5	7/12/2004	7/12/2004	7/12/2004	7/12/2004	7/12/2004	7/12/2004

Table 1: Starting dates of phases by trial municipality

Phases

The following six phases were identified in the municipal trial:

Phase	Change vis-à-vis previous phase
Phase 0	Start of trial
Phase 1	Optimization of BioRAAS software at photo scan municipalities
Phase 2	Additional instructions to municipal officials and participants
Phase 3	Update 1
Phase 4	Update 2
Phase 5	Training by fingerprinting equipment supplier

Table 2: Phasing of trial

Phase 1: Optimization of BioRAAS software at photo scan municipalities

The dimensions of the facial image in the BTD were originally 320*240 pixels. The ICAO guidelines require a minimum of 60 pixels between the eyes.[31] The software was updated to increase the number of pixels to 640*480, resulting in 85-95 pixels between the eyes. This change only needed to be made in the photo scan municipalities.

[31] ISO/IEC CD 19794-5.

Phase 2: Additional instructions to municipal officials and participants

An interim evaluation revealed that fingers were not being placed properly on the finger scanner in a relatively large number of cases, so the municipal officials were given additional instructions on how this should be done. The trial municipalities were also supplied with 'placemats', which could be placed on the applicant's side of the counter, providing visual instructions to applicants on how to place their fingers on the scanner.

Phase 3: SDU Update 1

The change comprised three elements:

1. introducing a measurement of the time it took to record each biometric identifier;
2. the option of skipping fingerprinting. In the photo scan municipalities one of the settings in the software was incorrect, making it impossible to apply for a test document if the fingerprint quality was unsatisfactory;
3. improving the stability of the recording equipment.

Phase 4: SDU Update 2

The aim of update 2 was to improve fingerprint recording quality by setting a threshold that would yield better verification results. Only fingerprints that passed the threshold would be recorded. In addition to the changes to the software, the municipalities were given 'prescan pads' for participants with dry fingers.

Phase 5: Training by fingerprinting equipment supplier

The supplier of the fingerprinting hardware and software for the application and issue process provided additional training on positioning the finger on the finger scanner, as the training courses provided hitherto proved inadequate for municipal officials to take good-quality fingerprints.

Appendix 4: Detailed Analysis of Data from Municipal Trial

Introduction

The table below gives an overview of the distribution of participants and biometric test documents among the participating municipalities.

Photo scan/live scan		BTDs	Test document	No BTD	Double BTD	TOTAL Participants
		(2)	(3)	(4)	(5)	(2)+(3)+(4)-(5)
Passport photo	Almere	2,584	1	67	10	2,642
	Eindhoven	2,621	2	99	5	2,717
	Utrecht	2,234	1	51	2	2,284
TOTAL: photo scan		*7,439*	*4*	*217*	*17*	*7,676*
Live scan	Apeldoorn	1,902	1	0	2	1,901
	Groningen	2,651	1	5	8	2,649
	Rotterdam	2,512	1	9	8	2,514
TOTAL: live scan		*7,065*	*3*	*14*	*18*	*7,064*
GRAND TOTAL		**14,504**	**7**	**231**	**35**	**14,707**

Table 1: Participants and BTDs

The trial involved 14,700 participants and produced 14,504 biometric test documents (excluding the seven documents for the Minister for Governmental Reform and Kingdom Relations and the burgomasters/aldermen). The following reasons were found for the discrepancy between numbers of participants and documents issued.

1. A photo scan was not able to be converted to ISO-19794 format in 217 cases (1.5%), so the producer was not sent a digital application to personalize a BTD. This problem, of course, only occurred in the photo scan municipalities.
2. A copying problem between the REVU equipment and the BioRAAS in 14 cases. It was not possible to copy the data from the REVU to the BioRAAS, so the BioRAAS did not receive any data to deal with the application.
3. Participants in the trial applied for 35 documents as second documents (they applied for both a passport and a Dutch identity card). Interestingly, one participant was able to enrol fingers for one document but not the other: no reason was found for this.

1. For the photo to be recorded on the chip, the photo scan has to be converted to the required ISO format. When converting the photo, the algorithm determines whether the image contains a face: in order to do this it has to locate the eyes, which it was not able to do in every case.

2. The copying problem was due to an incorrect setting in the software, and was remedied by update 1.

Inclusion of biometric identifiers upon application

The table below shows which biometrics were included in the 14,504 test documents.

Biometrics included						
Face	Finger 1	Finger 2	Passport photo	Live scan	Total	%
+	+	+	7,267	6,771	14,038	96.8
+	+	-	22	41	63	0.4
+	-	+	68	61	129	0.9
+	-	-	82	192	274	1.9
Total			7,439	7,065	14,504	100

Table 2: Biometrics included: distribution among BTDs

Verifying biometrics upon issue

Of the 14,504 personalized test documents, 14,165 (97.7%) were verified upon issue. The remaining 339 were not verified upon issue for technical (211) or procedural (2) reasons. In the case of 126 documents it was impossible to ascertain why they were not verified upon issue.

In 99.2% of the test documents verified at least one of the three biometric identifiers recorded was successfully verified. All the biometric identifiers recorded were successfully verified in 93.6% of cases. In 4.3% of cases one fingerprint was able to be verified (4.1% including the face and 0.2% without the face). In 2.9% of cases the face was successfully verified but verification of the fingerprints was completely unsuccessful. In 2.2% of cases the facial scan could not be verified. The table below shows the relationship between biometric identifiers included and verification of the biometric identifiers included.

Recorded biometric identifiers						Verification of the recorded biometric identifiers					
Face	Finger 1	Finger 2	Photo scan	Live scan	Total	Face	Finger 1	Finger 2	Photo scan	Live scan	Total
+	+	+	7,267	6,771	14,038	+	+	+	6,493	6,257	12,750
						+	+	-	130	136	266
						+	-	+	75	97	172
						+	-	-	41	74	115
						-	+	+	278	9	287
						-	+	-	5	-	5
						-	-	+	8	-	8
+	+	-	22	41	63	+	+	-	16	31	47
						+	-	-	1	8	9
						-	+	-	4	1	5
+	-	+	68	61	129	+	-	+	58	36	94
						+	-	-	5	23	28
						-	-	+	5	-	5
+	-	-	82	192	274	+	-	-	77	180	257
Total			7,439	7,065	14,504	Total			7,196	6,852	14,048

Table 3: Relationship between recording and verification of biometrics

The table below shows the relationship between recorded biometric identifiers and verification of recorded biometric identifiers; the fingerprints that were included were ones that met the quality parameter.

Recorded biometric identifiers						Verification of the recorded biometric identifiers					
Face	Finger 1	Finger 2	Photo scan	Live scan	Total	Face	Finger 1	Finger 2	Photo scan	Live scan	Total
+	+	+	2,952	3,168	6,120	+	+	+	2,728	2,999	5,727
						+	+	-	50	66	116
						+	-	+	5	28	33
						+	-	-	5	17	22
						-	+	+	115	2	117
						-	+	-	1	0	1
						-	-	+	0	0	0
+	+	-	17	32	49	+	+	-	14	25	39
						+	-	-	1	5	6
						-	+	-	1	1	2
+	-	+	63	56	119	+	-	+	55	33	88
						+	-	-	4	21	25
						-	-	+	4	0	4
+	-	-	78	167	245	+	-	-	75	158	233
Total			3,110	3,423	6,533	Total			3,058	3,355	6,413

Table 4: Relationship between recording and verification of biometrics (with quality parameter for fingerprints)

Applying a quality parameter when taking fingerprints resulted in more successful verifications upon issue: one of the biometrics included was able to be verified in 98.2% of verifications, as against 95.8% without the quality parameter.

Attempts to record upon application and verify upon issue

The table below shows the number of attempts made when recording and verifying biometrics in the 14,504 test documents. The conclusion is that over 95% of verifications are successful after one or two attempts.[32]

Attempts	Recording, resulting in a document	In percent	Verification upon issue	In percent
1	12,719	87.7%	13,437	92.6%
2	1,390	9.6%	430	3.0%
3	248	1.7%	137	0.9%
4	94	0.6%	34	0.2%
5	22	0.2%	5	0.0%
6	16	0.1%	3	0.0%
7	6	0.0%	2	0.0%
8	4	0.0%	-	
9	4	0.0%	-	
12	1	0.0%	-	
Verification unsuccessful			117	0.8%
Not verified			339	2.3%
TOTAL	14,504	100.0%	14,504	100.0%

Table 5: Attempts per BTD (recording and verification)

Time taken to record biometric identifiers

The graph below shows how much time it took on average to record the biometrics (face and two fingerprints) in the various age groups. Taking biometrics from children under about 6 and older people over 60 took longer than from the in-between age group. The time shown includes the time taken for the municipal official to put the research questions to the participant.

[32] 'Successful verification' refers to situations where at least one biometric identifiers is able to be verified positively.

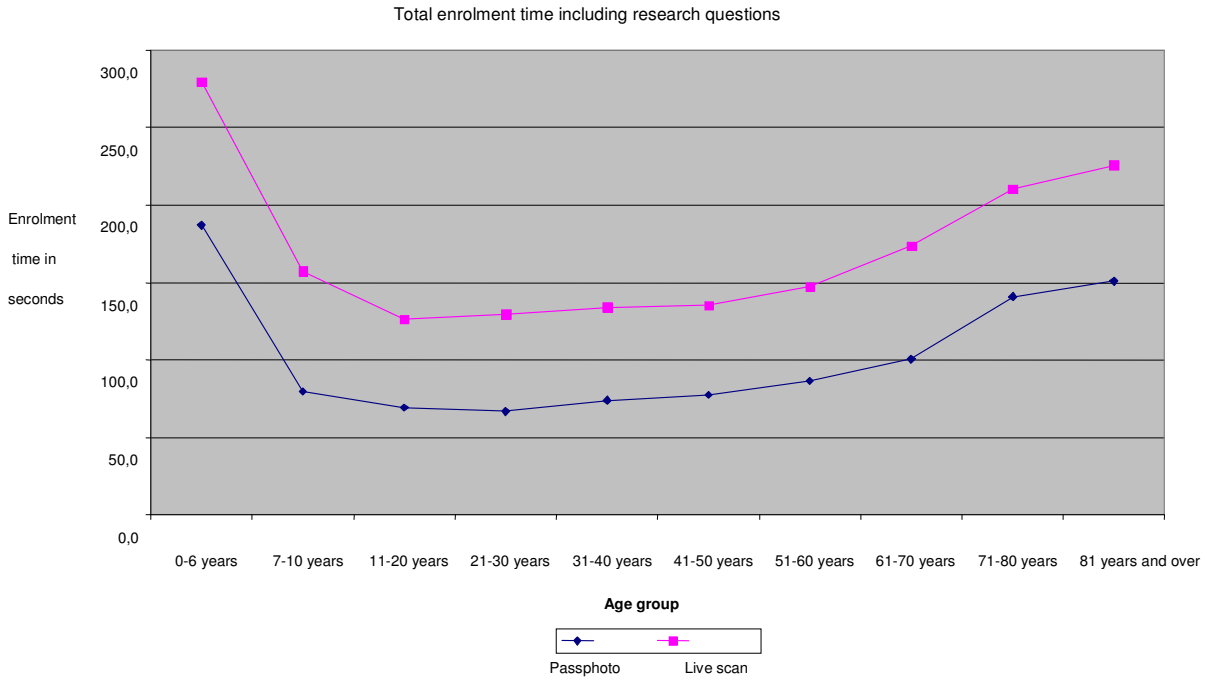

Fig. 1: Time taken to record biometrics (including explanation and research questions)

The times measured in the photo scan municipalities were naturally shorter than in the live scan municipalities, as only fingerprints were taken in the former; photo scanning was not done at the desk and was not included in these times measured.

Time taken for verification upon issue

The figure below shows the time it took to verify the stored biometric identifiers upon issue. As with recording the biometric identifiers, verification took longer in the case of children and older people. Verifying a face (average 25 seconds) took longer than verifying fingerprints (average 17 seconds). The right-hand finger took less time than the left-hand finger.

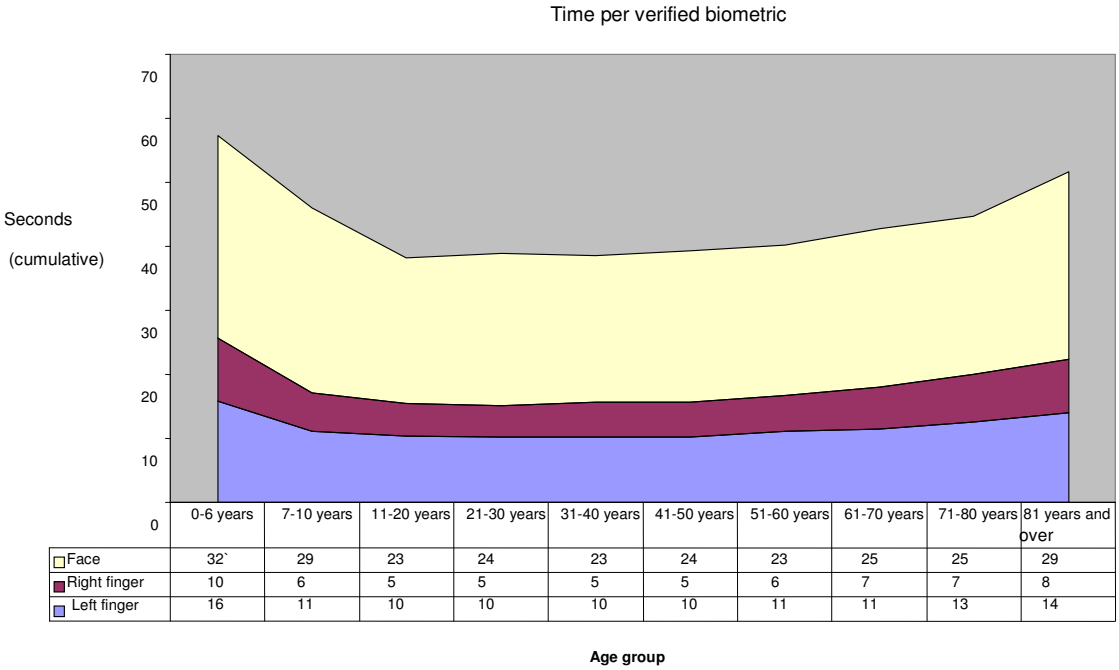

Fig. 2: Time taken to verify each biometric

Facial scan

Facial scan quality

There is no standard software available to check the quality of stored facial scans as there is for fingerprints. For the purpose of the trial the Interior Ministry, in collaboration with one of the suppliers, set a number of parameters by which to assess the facial scans automatically. The table below shows these parameters, including thresholds (upper and lower limits).

Parameter	Threshold Lower limit	Threshold Upper limit
Head rotation (looking left/right)	-6°	6°
Head inclination (looking up/down)	-7°	7°
Brightness (scale 1-100)	30	80
Distance between eyes (pixels)	35	140
Reliability of eye detection (scale 1-100)	55	100
Size of face (percentage of area)	25	50
Face centred	0	40
Shadow on face (scale 1-100)	30	100
Shadow on eyes (scale 1-100)	45	100
Brightness of background (scale 1-100)	30	90
Evenness of background (scale 1-100)	65	100
Background shadow (scale 1-100)	0	30
Contrast (scale 1-100)	45	100
Focus (scale 1-100)	35	100
Colour balance	65	100

Table 6: Parameters of quality assessment for face (with threshold)

The stored facial scans were assessed on the basis of these parameters, distinguishing between those made by scanning photos and those made by the camera at the desk. The table below shows for each parameter what percentage of facial scans would be rejected with the given limits.

Reasons for rejecting facial scans	Passport photo	Live scan	Total, average
Head rotated (looking left/right too much)	9.4%	10.9%	10.1%
Head inclined (looking up/down too much)	2.7%	1.4%	2.0%
Brightness too low	10.2%	1.0%	5.8%
Distance between eyes too small or too large	0.1%	3.3%	1.7%
Reliability of eye detection	12.4%	1.0%	6.8%
Size of face (too small/large)	0.8%	0.7%	0.7%
Face centred	0.2%	0.5%	0.3%
Shadow on face (too much)	16.7%	1.1%	9.1%
Shadow on eyes (too much)	10.3%	0.7%	5.6%
Brightness of background (too low)	49.4%	0.4%	25.5%
Evenness of background (uneven)	60.5%	11.3%	36.5%
Background shadow (too much)	34.9%	6.4%	21.0%
Contrast (too low)	0.1%	10.2%	5.1%
Focus (too low)	2.7%	3.9%	3.3%
Colour balance (too low)	0.2%	1.9%	1.0%

Table 7: Rating of facial scan quality by parameter

The photo scans largely failed to meet the parameters ‘brightness of background’, ‘evenness of background’, ‘background shadow’ and ‘reliability of eye detection’. Analysis of the stored photo scans revealed that one reason was ‘padding’, a grey border around a picture of a face caused by converting the stored facial scan to the requisite ISO format. In order to convert the scan, the eyes are straightened by rotating the image. Padding can be avoided by laying down stricter requirements for the quality of photos submitted by applicants. Another possibility is making manual corrections if the software wrongly locates the eyes (e.g. it interprets the rim of a pair of spectacles as an eye).

Fingerprints

The following points were analysed as regards the fingerprints:

- the quality of the fingerprints recorded;
- the distribution of fingerprint quality among the test documents;
- fingerprint quality in relation to the participant’s age;
- fingerprint quality in relation to the time fingerprinting took;
- fingerprint quality in relation to information on hobbies/occupation/scars;
- fingerprint quality in relation to the time fingerprinting took place during the working day.

After phase 3 of the trial a quality parameter from the supplier of the finger scanner used to take fingerprints for applications was incorporated in the recording software. From then on only fingerprints that passed the quality threshold were recorded and stored in the biometric test documents.

The quality of the fingerprints recorded

The National Institute of Standards and Technology (NIST) has developed software to check the quality of fingerprints, known as NIST Fingerprint Image Software 2 (NFIS2). This is an open standard made available by the NIST. The software classifies fingerprints in quality categories on a scale from 1 to 5, where:

- 1 stands for 'excellent',
- 2 for 'very good',
- 3 for 'good',
- 4 for 'fair' and
- 5 for 'poor'.

According to the NIST, fingerprints in quality categories 1, 2 and 3 produce few if any false rejections upon verification; categories 4 and 5 produce a large or fairly large number of false rejections. This software was used to analyse all the fingerprints taken in the trial.

The chart below shows the average NIST quality of the fingerprints included in the BTDs. Without the quality parameter the quality of the fingerprints recorded is seen to deteriorate (on average 10% lower fingerprint quality was found in phase 3 compared with phase 1). Introducing the quality parameter improved the quality of fingerprint recordings: compared with phase 3 the average quality went up by 15-20% (right-hand finger 15%, left-hand finger 20%) and it was better on average than in the earlier phases of the trial.

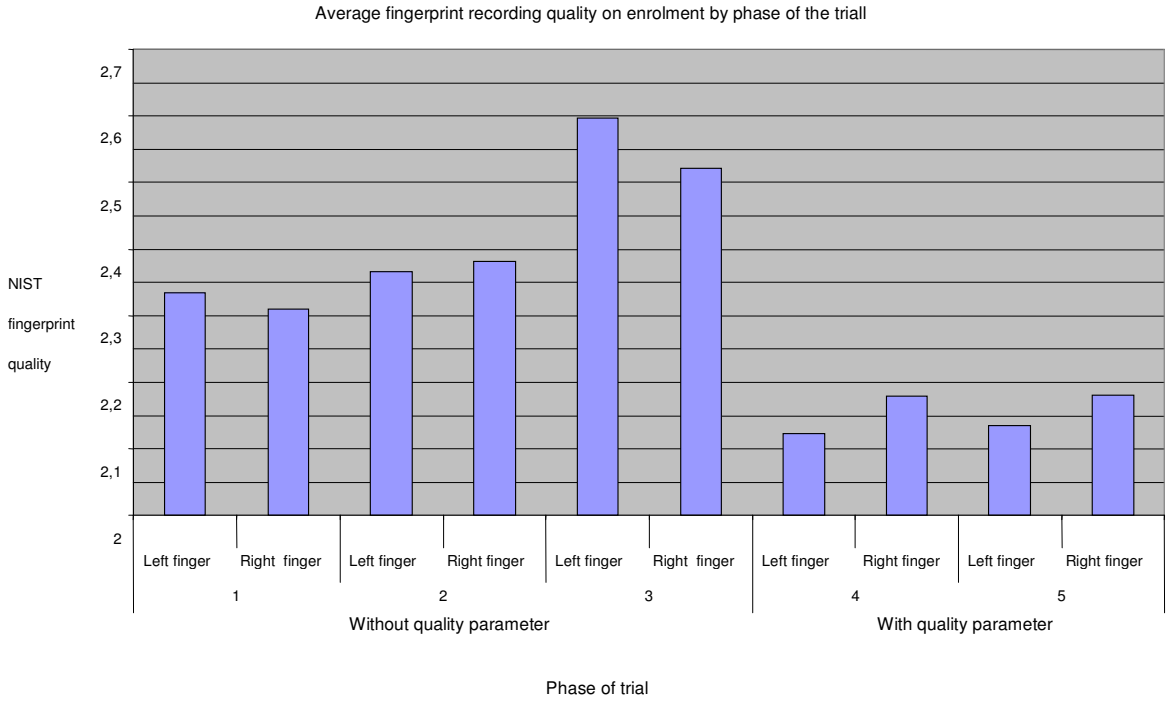

Fig. 3: Average NIST fingerprint recording quality by phase

The chart suggests that the quality of the fingerprints recorded would have gone down during the trial if the quality parameter had not been introduced (fingerprint quality declined during phases 1-3). Officials—rightly—trusted the software[33] and seldom checked the quality of the fingerprints themselves, as the interviews with them confirmed.

Using the NIST quality classification seems to have resulted in an improvement in the verifications done by verification systems other than the one used to take the fingerprints (see table below). Only in the case of Vendor 3 did the false rejection rate (FRR) differ greatly from the others. Vendor 3 indicated that the software was not correctly configured. Prior to the trial the suppliers, based on their own tests, set a limit at which a comparison of biometrics would be assessed as successful or unsuccessful. It was not possible to change these settings during the trial, for the sake of the analysis. These FRRs, incidentally, were not adjusted to take account of verifications that took place with fingerprints other than those stored in the test documents.

FRR (%)		Municipalities											
		Almere		Apeldoorn		Eindhoven		Groningen		Rotterdam		Utrecht	
		Vendor 4	Vendor 3	Vendor 5	Vendor 6	Vendor 3	Vendor 6	Vendor 4	Vendor 6	Vendor 3	Vendor 4	Vendor 3	Vendor 6
Finger 1	all images	5.4	49.9	17.7	7.7	50.5	17.8	5.4	18.3	23.3	9.8	49.6	7.5
Finger 1	NIST 1, 2 and 3	2.4	49.1	11.4	3.4	44.2	8.7	3.1	8.6	14.1	4.4	45.9	4.5
Finger 2	all prints	6.1	50.4	20.9	8.5	47.5	17.3	7.3	19.8	17.8	9.9	43.5	8.3
Finger 2	NIST 1, 2 and 3	2.2	46.8	9.8	3.0	44.2	9.4	6.0	9.4	10.0	4.1	39.4	4.8

Table 8: Comparison between FRR for all fingerprints with FRR for fingerprints only in NIST categories 1, 2 and 3

Introducing the quality parameter when recording fingerprints did not have a clear effect on verifications using systems other than the one used to take the fingerprints. This may be due to the fact that a particular supplier's recording and verification software are developed together.

FRR (%)		Municipalities											
		Almere		Apeldoorn		Eindhoven		Groningen		Rotterdam		Utrecht	
		Vendor 4	Vendor 3	Vendor 5	Vendor 6	Vendor 3	Vendor 6	Vendor 4	Vendor 6	Vendor 3	Vendor 4	Vendor 3	Vendor 6
Phase 1	Finger 1	6.0	48.7	23.6	14.5	47.9	11.6	8.4	14.6	11.6	8.5	46.6	12.6
	Finger 2	11.9	44.4	18.6	12.7	45.2	17.8	10.9	20.0	18.0	10.5	46.9	12.6
Phase 2	Finger 1	5.4	49.9	17.7	7.7	50.5	17.8	5.4	18.3	23.3	9.8	49.6	7.5
	Finger 2	6.1	50.4	20.9	8.5	47.5	17.3	7.3	19.8	17.8	9.9	43.5	8.3

Table 9: FRR phase 1 (without quality parameter) and phase 2 (with quality parameter)

The distribution of fingerprint quality among the test documents

The table below shows the NIST figures for the fingerprints (left and right-hand finger) stored in the test documents. The category 'Other' in the two tables below relates to fingerprints whose quality the NIST software was not able to assess.

[33] The software gives an indication when a fingerprint has been recorded, even without the quality parameter.

Percentage of documents	Quality of right-hand finger							
Quality of left-hand finger	Excellent	Very good	Good	Fair	Poor	None Right-hand finger	Other	Grand total
Excellent	11.7%	8.2%	1.7%	0.5%	0.0%	0.0%	0.1%	22.3%
Very good	7.0%	17.9%	7.1%	0.7%	0.1%	0.1%	0.1%	32.9%
Good	2.0%	8.4%	15.7%	4.3%	0.4%	0.2%	0.6%	31.6%
Fair	0.5%	0.8%	4.1%	2.2%	0.1%	0.1%	0.1%	8.0%
Poor	0.1%	0.1%	0.6%	0.2%	0.2%	0.0%	0.1%	1.4%
No left-hand finger	0.0%	0.2%	0.5%	0.2%	0.0%	1.3%	0.1%	2.4%
Other	0.1%	0.1%	0.6%	0.1%	0.1%	0.0%	0.4%	1.4%
Grand total	21.5%	35.7%	30.4%	8.2%	0.9%	1.8%	1.5%	100.0%

Table 6: The quality of the fingerprints stored in the BTDs

This table shows that:

- about 80% of the test documents contained two fingerprints with a NIST quality of 1-3 (excellent, very good or good);
- about 12% contained two fingerprints, one of which had a NIST quality of 1-3 and the other a NIST quality higher than 3;
- about 1% contained one fingerprint with a NIST quality of 1-3;
- about 7% contained no fingerprints at all, or the NIST software was not able to assess the quality;

2.7% of the fingerprints stored had a NIST quality of 4 or 5 (fair or poor).

The table below gives an overview of the foregoing.

Percentage of documents	Right hand				
Left hand	Fingerprint 1, 2 and 3	Fingerprint 4 and 5	No fingerprint Right-hand finger	Other	Grand total
Fingerprints 1, 2 and 3	79.8%	5.9%	0.3%	0.7%	86.8%
Fingerprints 4, 5	6.3%	2.7%	0.1%	0.2%	9.4%
No fingerprint	0.7%	0.3%	1.3%	0.1%	2.4%
Other	0.7%	0.2%	0.0%	0.4%	1.4%
Grand total	87.6%	9.2%	1.8%	1.5%	100.0%

Table 7: Overview of stored fingerprint quality

Fingerprint quality in relation to the participant's age

The quality of the fingerprints recorded goes down as the participant's age goes up, as shown in the figure below.

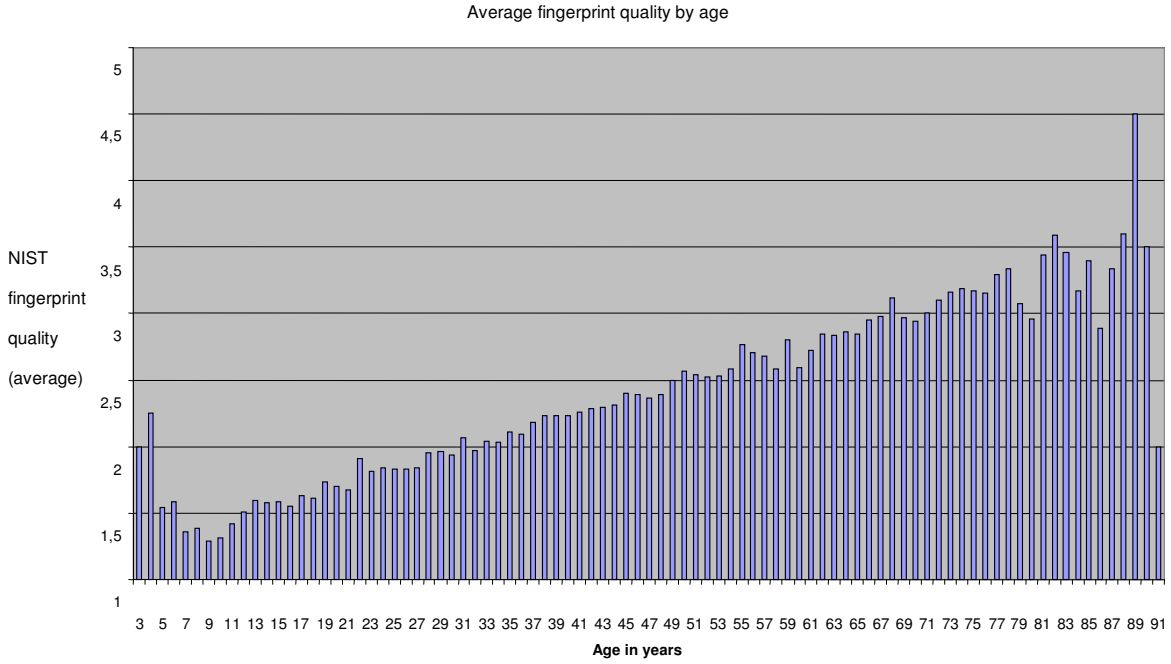

Fig. 4: Fingerprint quality in relation to age

As the figure below shows, taking one or two fingerprints with a NIST quality of 1-3 was particularly unsuccessful in the 0-11 and over 60 age groups in particular.

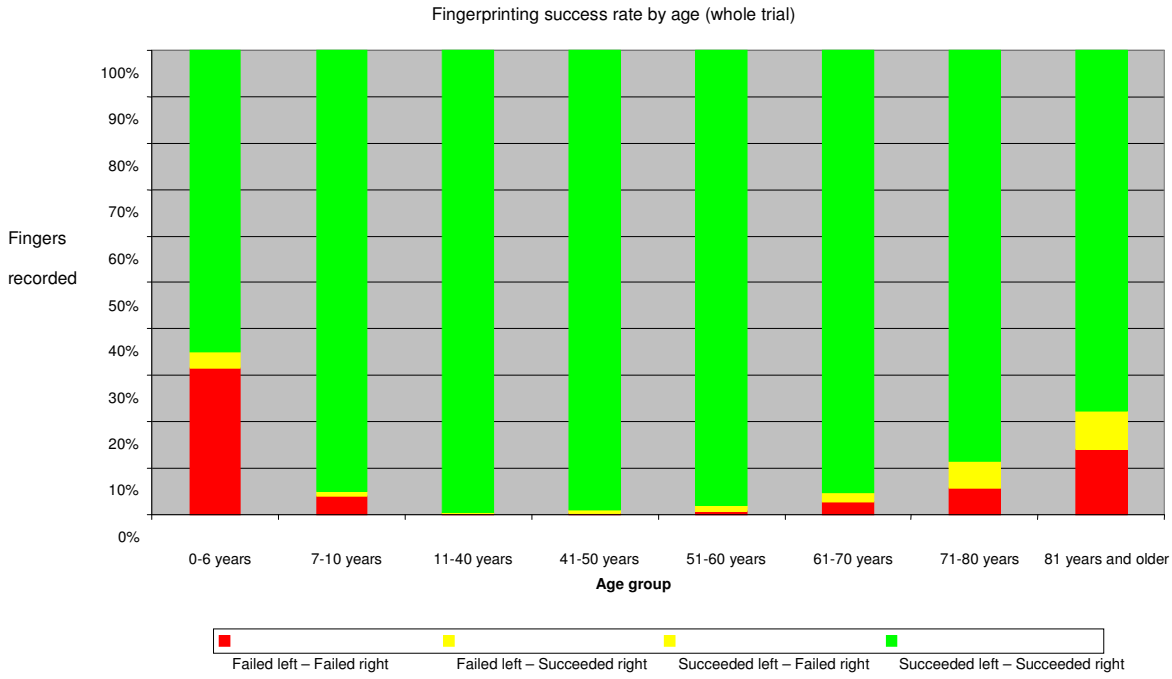

Fig. 5: Fingerprinting success rate by age group

Once the quality parameter was introduced, only fingerprints that passed the quality threshold were stored in the test documents. This increased the probability of successful verification and reduced the probability of 'poor' fingerprints being successfully recorded.

The figures below show the relationship between successful fingerprinting and the introduction of the quality parameter. Fig. 6 shows the probability of successful fingerprinting without the quality parameter and Fig. 7 the probability of successful recording with the quality parameter.

Fig. 6: Fingerprinting success rate without quality parameter

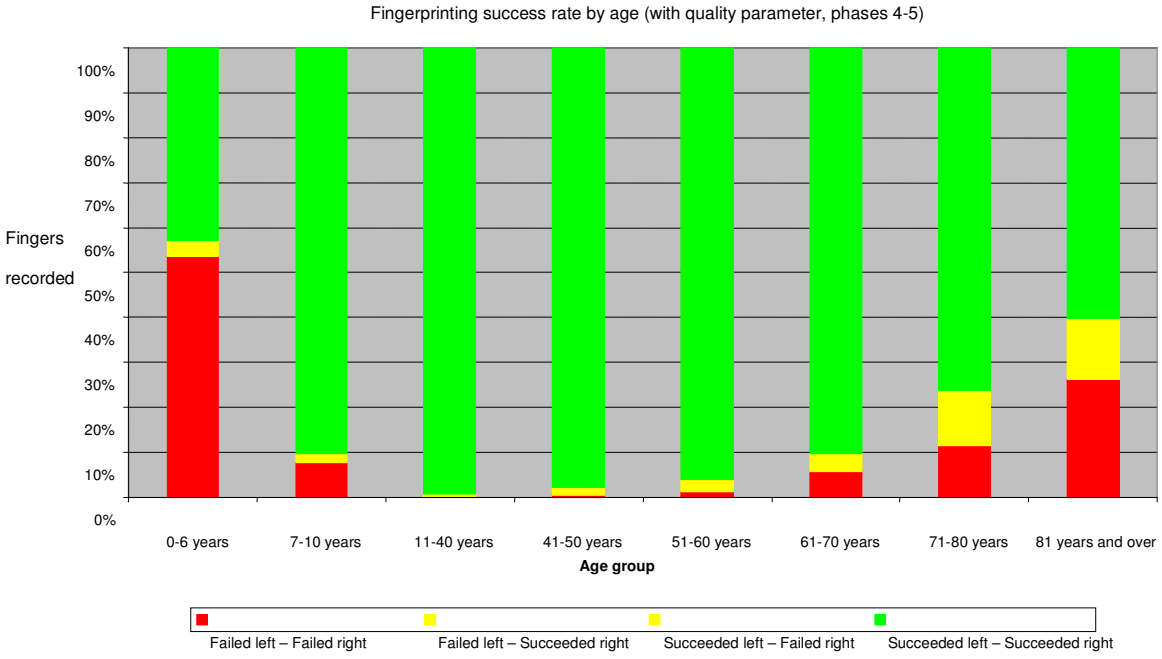

Fig. 7: Fingerprinting success rate with quality parameter

In the under-10 and over-60 age groups in particular there was less possibility of taking a fingerprint of adequate quality if the quality parameter was applied.
Analysis of the stored fingerprints revealed that virtually all the test documents where one fingerprint did achieve a NIST quality of 3 (or better) and the other did not had been applied for by persons aged over 60.

Fingerprint quality in relation to the time fingerprinting took

As part of the trial, the time it took to take two fingerprints and check the recorded fingerprints was recorded.

The average time needed to take a fingerprint was found to differ between the left and the right-hand finger: a left-hand fingerprint took about twice as long as a right-hand fingerprint. There was less difference in the time it took to check the left-hand and right-hand fingerprints once they had been recorded.
Incorporating the quality parameter in the software increased the average time fingerprinting took, as shown in the table below.

Fingerprint recording [in seconds]	Without quality parameter	With quality parameter
Recording left-hand finger	13	25
Recording right-hand finger	7	16
Subtotal: recording fingers	*20*	*41*
Checking left-hand finger	7	8
Checking right-hand finger	5	5
Subtotal: checking fingers	*12*	*13*
Total: enrolment of fingers	32	54

Table 8: The time fingerprinting took without and with the quality parameter

The reason for the difference in the time needed to take a print of left and right-hand fingers was not investigated. A possible explanation is the fact that most people are right-handed (about 90% worldwide[34]) and therefore able to place the right-hand finger correctly more quickly than the left-hand finger. The interviews with the municipal officials indicated that the participants automatically wanted to put their right-hand finger on the finger scanner first.

[34] This percentage is given on various web pages, e.g. www.handresearch.com.

The table below shows the time fingerprinting took in relation to the five NIST categories. The difference in the average time by NIST classification was greater if the fingerprint was required to meet the quality parameter than without the quality parameter (the time is shown in brackets).

NIST fingerprint quality classification	Left-hand finger [recording time in seconds]		Right-hand finger [recording time in seconds]	
1 (Excellent)	18	(13)	11	(6)
2 (Very good)	21	(13)	12	(6)
3 (Good)	33	(13)	19	(7)
4 (Fair)	45	(14)	27	(7)
5 (Poor)	51	(15)	53	(8)

Table 9: The time fingerprinting took for NIST quality 1-5 (the time taken without the quality parameter is shown in brackets)

Fingerprint quality in relation to information on hobbies/occupation/scars

When a test document was applied for, three characteristics of the participant that could affect the possibility of taking a good fingerprint were recorded, viz.:

- occupation and/or hobby that, in the participant's opinion, could affect wear and tear on the fingers[35] and
- scars on the fingers (the official recorded this in the logbook if fingerprinting was unsuccessful).

A small number of participants said they had an occupation or hobby that involved a substantial risk of damage to the fingers (see table below).

	Risk of finger deterioration/damage due to hobby			
Risk of finger deterioration/damage due to occupation	Large	Small	Nil	Total
Large	0.5%	0.3%	0.2%	1.0%
Small	0.6%	10.0%	7.2%	17.8%
Nil	0.6%	6.0%	74.6%	81.2%
Total	1.7%	16.3%	82.0%	100.0%

Table 10: Effect of hobby/occupation on fingerprint according to participant

Scars on the fingers were recorded in the logbooks in the case of 91 applications. The analysis did not indicate that scars resulted in unsuccessful fingerprinting, so no conclusions can be drawn on the relationship between occupation/hobbies/scars and the quality of the fingerprints recorded.

[35] The letter accompanying the invitation to take part in the trial asked the applicant to sign a consent form for the use of biometric information. Applicants were also asked whether the risk of damage to/deterioration of the skin of the finger due to hobby/occupation was large, medium or small.

Fingerprint quality in relation to the time fingerprinting took place during the working day

The time of day when fingerprinting was done did not affect the quality of the fingerprints recorded. Separate times for applying for travel documents (e.g. morning, as in Apeldoorn) and issuing them (afternoon) do not therefore improve the quality of the fingerprints stored. The figure below shows this for the various age groups.

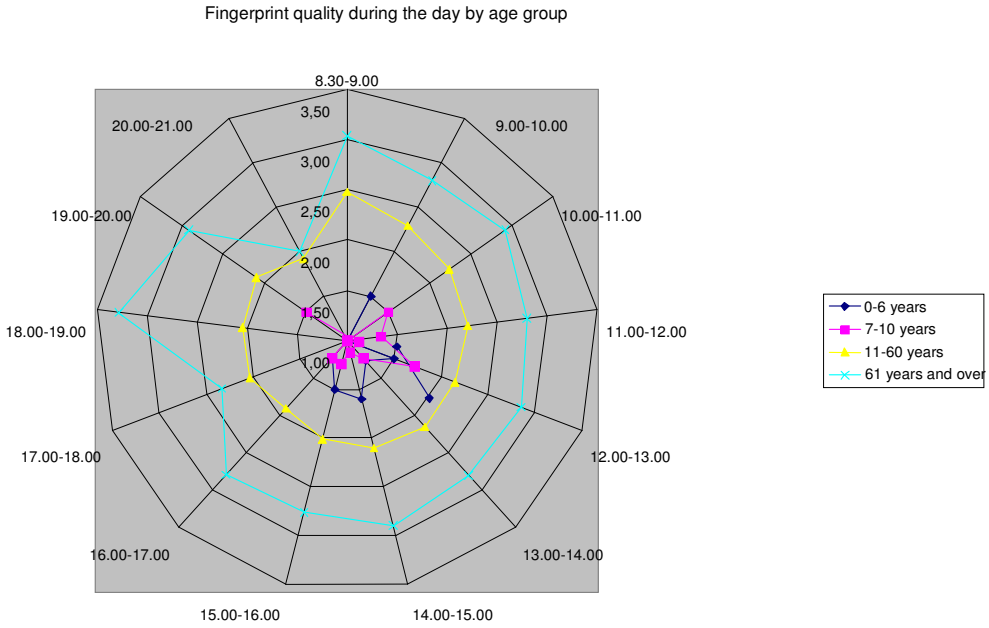

Fig. 8: Fingerprint enrolment quality during the day

APPENDIX 5: Analysis of Schiphol Test Documents

Checkpoints	Schiphol trial BTDs	%	Phase 1	%	Phase 2	%
Total BTDs examined	142	*100*	46	*100*	44	*100*
Appearance of card						
Slight damage	28	*20*	5	*11*	5	*11*
Dull surface	39	*27*	12	*26*	17	*39*
Deformation	52	*37*	30	*65*	5	*11*
ImagePerf detached	1	-	-		-	
Personalization						
Photo in grey border	142	*100*	46	*100*	44	*100*
Padding/black bars	94	*66*	35	*76*	30	*68*
Incorporation of chip						
Hairline cracks	45	*32*	20	*43*	13	*30*
Bad cracks	73	*51*	21	*46*	25	*57*

Appendix 6: TNO Report

TNO Report

IS-RPT-050040

How do you measure a child?

A study into the use of biometrics on children

Date	29 April 2005
Author(s)	Dr J.E. den Hartog Dr S.L. Moro-Ellenberger R.J. van Munster
Client	Personal Records and Travel Documents Agency
Project No.	033.10396
Report classification	Unclassified
Title	Unclassified
Summary	Unclassified
Report text	Unclassified
Appendices	Unclassified
No. of pages	1 (inc. appendices)
No. of appendices	0

Executive Summary

Title: How do you measure a child? A study into the use of biometrics on children

Author(s): Dr J.E. den Hartog
Dr S.L. Moro-Ellenberger
R.J. van Munster

Date: 29 April 2005
Project No.: 033.10396

Report No.: IS-RPT-050040

This report aims to provide the Personal Records and Travel Documents Agency (BPR) with information on the feasibility of using biometrics on children aged 0-12 years, looking at the taking of fingerprints and facial scans. As regards the latter, a literature review was also conducted into the effects of the growth of children's faces on the reliability of facial recognition.

For the project biometric data were taken from 161 children aged 0-13 years, using the TEVU system, which has been specifically developed for taking biometrics and is being used by the Agency in its '2B or not 2B' trial to evaluate the use of biometrics in passports.

With the system and settings used it was not possible, however, to obtain clear fingerprints from children under 4 years of age. At least one clear fingerprint could only be obtained using this system from the age of 6 upwards (this was the case with virtually all children).

The trial showed that a biometric facial scan can be taken irrespective of age in most cases. Virtually all the cases where this was not possible involved children aged 5 years or under who started crying while being scanned or refused to look straight into the camera.

There are a number of particular points to be considered when taking fingerprints from young children, in particular the strong fist a baby can make and the moistness of children's fingers. There are specific requirements for obtaining good facial biometrics from children, such as variable positioning of the camera, very short shutter speeds and proper quality control of the facial scan.

As regards the feasibility of facial recognition in children, the scientific literature does not provide enough information on the ‘durability’ of biometric data to predict the results in the real world.

As the growth of children’s faces is a complex and not entirely predictable process, it is very difficult to express this growth in terms of a facial recognition algorithm, and we are indeed not aware of any providers of facial recognition software who claim to be able to compensate for the growth of children's faces. One of the providers states that facial recognition is not reliable in the under-5s; it is not until the age of 13 that ageing ceases to have any marked effect, as the facial form is then stable. Medical research does indeed indicate that most facial features are stable from this age onwards.

Facial recognition in children based on reference pictures that are a few years old is likely to be problematical. It is unlikely that facial recognition software will be able in the near future to compensate for the effects on growth on children’s faces.

There are not only technical considerations here but also practical ones: in the strange environment of a town hall or the hectic conditions of a border control young children may well be unwilling or unable to cooperate with a facial scan, causing delays.

Nor is there enough information on the useful life (durability) of biometric data when it comes to using facial recognition in children over 12. We cannot rule out the possibility that the useful life of a facial scan will be shorter in the case of younger people than older people.

Contents

1. Introduction

1.1 Background

From September 2004 to the end of February 2005 the Dutch government conducted a trial, known as '2B or not 2B', to evaluate the use of biometrics in passports. In 2006 all newly issued passports will be fitted with a chip containing biometric information on the holder.

Under EU Regulation No. 2252/2004 of 13 December 2004 biometric information will eventually have to be stored in the passports of all EU citizens. This implies that it also applies to all children, irrespective of age. Although biometrics is being used ever more widely and on an increasing scale, little is known about its use in young and very young children. The Personal Records and Travel Documents Agency (BPR) of the Ministry of the Interior and Kingdom Relations (BZK) therefore asked TNO to conduct a study into the feasibility of using biometrics to establish the identity of children, specifically whether it is possible to take fingerprints and the effects of the growth of children's faces on recognition.

1.2 The work

The work the project entailed fell into two parts:

1. *Taking biometric identifiers*. In order to ascertain the feasibility of taking biometrics from children, the TNO tried to take finger and facial biometrics from at least five children in a group of 161 children aged 0-13.
2. *Review of the literature on facial recognition.* This part involved identifying the information in the literature on the changes in young children's faces and their effect on recognizability when using automatic facial recognition. A limited experiment was also conducted on the facial scans collected in the first part.

1.3 Organization of this report

Chapter 2 discusses taking biometrics from children. Chapter 3 gives a brief introduction to the technology of facial recognition. Chapter 4 deals with the effect of growth on facial recognition in children, followed by a discussion of the conclusions in Chapter 5.

2. Taking biometrics.

2.1 Introduction

For the purpose of the project the TNO tried to take biometric data from 161 children aged 0-13 years, two fingerprints and a facial scan. The biometrics taken were supplied to the Personal Records and Travel Documents Agency for analysis.

The TEVU system developed by SDU Identification was used for this purpose. It consists of a standard PC with a Windows operating system, a column containing a digital camera and flash unit for facial scanning, and a finger scanner.

To take the facial biometrics SDU used Viisage products. The fingerprints were taken using software and hardware from Sagem. As it had already been found that Sagem's standard software did not work well with children, for this trial SDU provided a version of the TEVU system that used the 'juvenile version' of the fingerprinting and recognition software. Sagem developed this juvenile version specially for taking fingerprints from children. The software was adapted for fingerprinting small fingers and should be able to compensate for the changes in scale that occur as part of the growth process.

In consultation with SDU and Viisage the TNO changed one setting of the TEVU system, the zoom setting of the digital camera. At the start of the trial it was found that there was a relatively high rejection rate for children's faces. This was due to the fact that, for the camera to be focused correctly, children had to be at the same distance from the camera as adults, and in the case of young children this made the face too small for the system to take good biometrics. The problems were resolved by a slight adjustment to this setting.

2.2 Procedure of taking biometrics

The TEVU system has a standard procedure for taking biometrics. First a facial scan is made, then biometrics are taken from two fingers. As a check a fresh facial scan is taken, followed by fingerprints from the two fingers used before. The procedure is completed by collecting additional information on the visibility of the forehead and side of the face, any scars on the face and the condition of the fingers.

Biometrics were collected at five locations using the system. Although the flash was used for facial scanning the local lighting conditions did affect recording quality, so steps were taken at each location to ensure that there was no direct sunlight, the face was adequately and evenly illuminated and there was a restful background.

The system assesses the quality of the biometrics recorded both when taking fingerprints and scanning faces. The quality of the biometrics is heightened by checking their reproducibility with a second recording: the first recording is only accepted if the first and second recordings are sufficiently similar.

For facial scanning it is very important that the child looks straight into the camera. In the case of very young children it is not possible to give adequate instructions on how to look, so a hand doll held right next to the camera was used.

2.3 Date and place

The biometrics were taken from the children in the last two weeks of February and the first three weeks of March at five different locations, at TNO, two day care centres and two primary schools.

2.4 Age structure

The table below shows the age structure of the group of children and whether the biometrics were taken successfully. Fingerprinting is considered to be successful if valid enrolment and verification prints were able to be taken from at least one finger.

Age	Number	Fingerprint successful	%	Face successful	%
0	15	0	0.0%	12	80.0%
1	16	0	0.0%	12	75.0%
2	17	0	0.0%	13	76.5%
3	24	2	8.3%	22	91.7%
4	10	5	50.0%	9	90.0%
5	12	8	66.7%	12	100.0%
6	18	16	88.9%	16	88.9%
7	8	8	100.0%	8	100.0%
8	7	7	100.0%	7	100.0%
9	13	13	100.0%	13	100.0%
10	5	5	100.0%	5	100.0%
11	8	8	100.0%	8	100.0%
12	6	6	100.0%	6	100.0%
13	2	2	100.0%	2	100.0%
Total	**161**	**80**	**49.7%**	**145**	**90.1%**

Table 1: Success of obtaining biometrics by age

2.5 Taking biometrics

As Table 1 shows, the system used did not enable clear fingerprints to be taken from children under the age of 4 years. In the case of children of 3 and 4 where it was possible to take a print of at least one finger this was usually the thumb, presumably because of the larger surface area. The area of the fingerprint is often taken as one of the measures of quality. When taking fingerprints it was normally the two forefingers that were tried first; if this proved unsuccessful the other fingers were tried. In the case of children aged up to 9 years it was frequently necessary to use the thumb or middle finger for biometrics. Problems with taking fingerprints were few and far between in the children over 9.

As Table 1 also shows, taking biometric facial scans from children does not cause problems in most cases. Those cases where this was unsuccessful

involved children who started crying or were very mobile: in the latter case it was usually not possible to get the child to look straight into the camera for long enough for the enrolment or verification scan. Another problem was the relatively slow shutter speed of the camera system, which resulted in scans that were out-of-focus, therefore unusable, in the case of children who are fidgety.

2.6 Observations on fingerprinting

The following points were noted when taking fingerprints:

- Babies (below the age of 8 or 9 months) can make a strong fist which is very difficult to open. This can substantially hamper obtaining the biometrics as it is not possible to place the finger on the sensor properly. A similar situation could occur in people with a handicap such as spasticity of the hands.
- In children who suck their thumbs a lot the skin of the finger is locally very soft, and it is often not possible to take a good print from the finger concerned.
- Children's fingers are often very moist. To take good prints it is important to dry them properly first, e.g. using a tissue.

2.7 Observations on facial scanning

The following points were noted when taking facial biometrics:

- Because of the children's widely varying heights it was necessary to be able to vary the height of the camera. An adjustable-height seat is not very practical as small children get annoyed if you keep moving them. If it is decided to use an adjustable seat, it needs to be able to be set much higher than a standard office chair. It should be a child's seat that provides sufficient support to children who have only just learned to sit by themselves, and it must also be possible for a parent to sit with the child on his or her lap.
- The quality control provided by the facial scanning system was not always reliable. Sometimes it accepted an unsuitable facial scan (e.g. with the face sharply rotated) or photos where the position of the eyes was not detected correctly. Recognition will not be possible based on a poor reference image unless the person adopts exactly the same pose as on enrolment.
- There is a delay of about half a second between the operator giving the command to scan the face and the actual taking of the photo. This is undesirable in the case of small children as they often sit still looking into the camera for only a short time. A similar problem could occur with mentally handicapped adults. A number of digital cameras are able to take a photo without delay.
- The experiments showed that the distance from the camera to the person being photographed needs to be adjustable. Young children needed to be brought much closer to the camera than bigger children or adults. This is presumably due to the fact that the system requires the face to be of a minimum size.
- Young children are often fidgety, which can result in photos that are out of focus. One solution to this problem is to reduce the shutter speed. This can only be done if there is adequate lighting. Although the system was equipped with a flash, the ambient lighting did affect the exposure of the photo. Solutions to this problem could be to change the system as regards the flash or change the ambient lighting.

- To get young children to look straight into the camera there needs to be an object that attracts their attention, so it would be desirable to incorporate an eye-catcher in the system.

2.8 Observations on the use of the system

The following observations were made on the use of the system:

- The programme only allows incorrect input (e.g. false acceptance of a poor facial scan) to be corrected by manually aborting the procedure and starting all over again. In some cases this may entail having to retake the biometrics unnecessarily.
- There is no way of storing incorrect input as such, so as to use it to improve the system.
- The flash for facial scanning sometimes remains charged and can spontaneously discharge while being moved.

3. Introduction to Facial Recognition

This chapter gives a brief introduction to the technology of facial recognition.

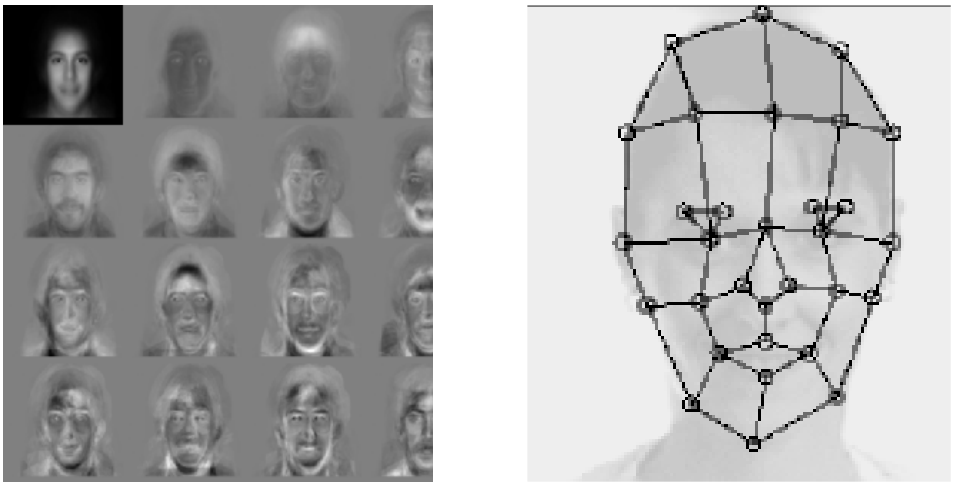

Fig. 3: Impression of Eigenfaces (left) and Local Feature Analysis (right)

3.1 The technology behind facial recognition

Any facial recognition system is a succession of different steps:

1 Image acquisition. First an image containing the face is obtained. This could be a still picture, a frame from a video stream or an image from a database.
2 Face detection. This step involves detecting the position and size of the face. The orientation of the face is usually also determined from the position of the eyes.
3 Standardization. The size and orientation of the face are scaled to a default size and orientation. Corrections are also made for lighting effects.
4 Feature extraction. It is in this step that the essential differences between the various suppliers are found. Broadly speaking there are two approaches. The Eigenfaces method represents a face as a sum of 64-128 standard faces. The second system, known as Local Feature Analysis, identifies a few dozen characteristic points such as the eyes, the corners of the mouth and the tip of the nose: the relationships between them are characteristic of a person. See also Fig. 3.
5 Comparison. This involves comparing the features found with those of one or more reference faces of one person. In the case of border controls the reference face is stored on a chip in the passport; the user himself carries his own biometrics.

3.2 Terminology

In order to discuss the feasibility of facial recognition we need to introduce a few terms that will be used in the rest of this report. They apply to all types of biometrics but will be explained using the example of facial recognition.

3.2.1 Verification versus identification

Facial recognition can be used in a number of ways. In the case of verification the system has prior knowledge of the person that the camera is looking at, and here the task is relatively simple: someone reports to the system, e.g. with his passport, and it has to verify whether the person is who he says he is. In the case of identification the task is more difficult: the system has no prior knowledge and has to select which person it is from a database of possibly thousands of people or decide that the person is not known. In the case of border controls it is usually verification that will be used, as it is more reliable and takes less time than identification.

3.2.2 Enrollment

Before a facial recognition system can recognize a person, that person must be registered with the system for the first time and the biometric data must be made available to the system. This can be done by having the person sit in front of the same system that will subsequently do the recognition. If this is not possible the system could process a scanned photo. The facial image is then turned into a template that can be stored in a database (for access control or surveillance) or on a smartcard (for access control). The entire process of registering the person, taking the biometrics and storing them in the database is referred to as 'enrollment'.

3.2.3 Evaluation

When evaluating the system technically, i.e. ascertaining the quality of recognition, three terms are used:

1. False Rejection Rate (FRR). This is the percentage of persons wrongly not recognized, or rejected in the case of verification.
2. False Acceptance Rate (FAR). In the case of verification this is a measure of the risk of an intruder wrongly being recognized as the person he claims to be.
3. Failure to enrol. This is a measure of how many persons cannot be enrolled (abbreviated to FTE). Although it is always possible to make a recording of the face, situations are conceivable where it is not possible to make a recording of adequate quality at the time of enrolment, e.g. where a child is too small to be able or willing to cooperate.

The FAR and FRR are interrelated, so they cannot be optimized at the same time. Both of them depend on the same system sensitivity configuration, so optimizing the former goes at the expense of the latter and vice versa.

3.3 The particular use of facial recognition studied

Facial recognition can be used in various ways, but this report only looks at the use of the technology in the context of border controls, based on verification of identity under controlled conditions.

4. Facial Recognition in Children

4.1 Introduction

This chapter looks at the effect of the growth development of children's faces on the feasibility of facial recognition. To put it another way, the question is 'How long does a developing child look like itself as far as this technology is concerned?'. This question is relevant because the current passport has a validity of five years, so the technology needs to be able to establish a child's identity reliably from a reference image that can be up to five years old.

First in this chapter we shall look at relevant research that has already been published. As we found little relative literature on the subject, we then discuss the effects that the growth process has on facial changes so as to ascertain whether it is likely that automatic facial recognition can compensate for these effects.

4.2 Literature survey

The literature survey we carried out showed that very little has been published on the feasibility of facial recognition in children (especially young children). This conclusion is supported by e.g. [GROS01], which points to the fact that hardly anything is known about this. The information from Identix, one of the three best-performing suppliers of facial recognition products (source: [FRVT02]) is also relevant: the information below is taken from a FAQ on the Identix web site [IDENT].

> **Question:** 'Can Identix' face recognition match accurately an image created with an aging product against an actual image?'
>
> **Answer:** 'Face recognition does not work optimally on images of children under the age of 5. We have studied the effect of aging from adolescence through adulthood using our technology and have found invariance with respect to aging beyond the completion of feature growth (roughly 13 years of age).'

Identix is the only well-established provider to make a pronouncement on this subject. We are not aware of any providers of facial recognition software who claim to be able to compensate for the growth and ageing of children's faces.

It is clear from [FRVT02] and [GIVE02] that age affects recognition, but the experiments were conducted using biometrics from—young—adults and cannot therefore be applied to the situation regarding children. Both studies indicate that older persons are recognized better than younger persons. The precise reason for this is not clear. Research described in [LANI02] and [OTOO99] suggests that a face becomes increasingly characteristic as it ages and is thus easier to recognize automatically.

If this hypothesis is correct, younger children ought to look more alike than older children. This hypothesis was tested, as the project included making facial scans of 145 children distributed among 13 age groups. It was

investigated what the average similarity between the various children was in the various age groups. If the hypothesis is correct, this average similarity should go down as the children get older. The limited experiment, however, did not provide support for this hypothesis.

4.3 The development of children's faces

4.3.1 Introduction

Given the lack of proper research into the usefulness of the face as a biometric identifier in children, research was also done into the development of children's faces. This section looks at the information available on this subject.

It seems reasonable to assume that facial recognition will be possible on children over a lengthy period if the changes in their faces obey distinct rules and the relative positions of characteristic points remain more or less the same. Only in this case could the recognition software possibly allow for growth.

To gain some understanding of the ageing of children's faces we first discuss the work of forensic artists, who are able to produce a picture of what long-term missing children would look like after a few years. Then we look at the information in the medical literature on the growth of children's faces.

4.3.2 Missing children and forensic artists

When looking for missing children there are software programs available that can generate a picture of the child at a later age from old photographs. This means that there are a number of regular changes which take place that can be expressed as algorithms. It should be noted, however, that to obtain a good picture of a child at a later age a forensic artist is brought in: he draws a picture of the missing child based on the original pictorial matter and photographs that show the development of parents, brothers and sisters over time. The changes that the forensic artist depicts, then, are based only partly on laws of nature and to a substantial extent on genetic factors.

4.3.3 Anthropometric data

Bone does not grow by the generic, uniform deposition of new bone on the outer surfaces, as is commonly—wrongly—assumed. Some regions of a bone may grow faster or slower. Bones change shape over time. Their relative positions can also change in order to enable them to grow. It cannot necessarily be assumed, therefore, that the interrelationships between the characteristic points of the face remain the same as the hard tissue grows.

A study into the development of various regions of children's faces [FARK92] includes data on North American Caucasian children aged 1-18 years. The main aim of the study was to gain a medical understanding of children's normal development so as to detect growth abnormalities and thus be able to treat them. It looked at the development of a large number of features that are also relevant to facial recognition, including the following:

- breadth and length of head;
- breadth and height of forehead;
- breadth of face;
- morphological face height;
- breadth and height of jaw;

- depth of face.
- Distance between the eyes (outer and inner corners)
- Depth, length and breadth of nose
- Upper lip height

Some 1500 children were examined, with no significant difference between the numbers of boys and girls. About 160 of them were under 4.

The study showed that boys and girls develop differently, and the various regions of the face obey very different growth curves. A few examples:

- Forehead breadth experiences a growth spurt in boys aged 3-4 and 5-6; in the case of girls the spurt occurs earlier, between 2 and 3, and 5 and 6.
- Head height experiences a growth spurt in boys between 2 and 3 and in girls between 3 and 4.
- Head breadth develops continuously, with no growth spurts.
- Jaw breadth experiences a growth spurt in boys between 3 and 4, 7 and 8, and 12 and 13; in girls the only growth spurt is detected between 6 and 7.

The study also ascertained at what ages particular facial regions reached 'adulthood'. In general, girls' facial regions reach adulthood sooner. There is a large spread between the regions: e.g. 3 years for the height of the upper lip and 14 years for head breadth. In boys the face reaches adulthood between 6 years (height of upper lip) and 16 years (nose depth).

The study clearly shows that the growth of a child's face is non-linear. In other words, the growth process does not involve a simple increase in the scale of the face: different regions develop differently. The biggest changes take place up to the age of about 7, after which they are more gradual, except in the case of jaw breadth (growth spurt in boys aged 12-13), nose height (growth spurt in boys aged 11-12) and nose depth (growth spurt between 11 and 12, and 15 and 16).

4.4 Practical considerations

On top of the technical limitations of facial recognition as a biometric technique, there are also practical considerations that need to be taken into account. Facial recognition is fairly reliable if the person looks straight into the camera with a neutral expression. Under the often hectic conditions of a border control, e.g. at an airport, many young children will be tired after a long journey and not feel at ease, with the result that they will often refuse to cooperate properly with facial scanning. Coercion (by the parents) will produce crying, with predictable effects on the neutrality of the facial expression. It is reasonable to assume, therefore, that using facial recognition on young children under border control conditions could produce a fairly high false rejection rate (FRR), with adverse effects on throughput speed at the border crossing.

4.5 Conclusions

Based on the above data, facial recognition in children aged 12 or under based on reference pictures that are a few years old is likely to be problematical because of the major changes that occur in relationships

between characteristic facial points as children grow. These changes are part of a complex process determined to a large extent by sex and genetic background. It is unlikely, therefore, that facial recognition software will be able in the near future to compensate for the effects on growth on children's faces.

There is not enough information on the useful life (durability) of biometric data when it comes to using facial recognition in children over 12. Initial research suggests that this is shorter in younger people than in older people.

There are not only technical considerations here but also practical ones: in the strange (to them) environment of a town hall or the hectic conditions of a border control young children may well be unwilling or unable to cooperate with a facial scan, causing delays.

5. Summary and Conclusions

In this chapter we comment on the conclusions and recommendations in previous chapters. We shall first consider data acquisition, then the study of facial recognition in children.

5.1 Data acquisition

- Attempts were made to take biometrics from the fingers and face in 161 children aged 0-13 years. One or two fingerprints were able to be taken from 80 children. Facial scans of sufficient quality were able to be taken from 145 children. There were at least five children of each age.
- With the system and settings used it was not possible to obtain clear fingerprints from children under 4 years of age. One or more clear fingerprints could only be obtained using this system from the age of 6 upwards, this was the case with virtually all children.
- A biometric recording of the face was able to be taken in most cases. Virtually all the cases where this was not possible involved children aged 5 years or under who started crying while being scanned or refused to look straight into the camera.
- There are a number of particular points to be considered when taking fingerprints from young children, in particular the strong fist a baby can make and the moistness of children's fingers.
- Specific points when it comes to obtaining facial biometrics from children are variable positioning of the camera, minimizing shutter speeds, quality control of the facial scan and the time that elapses between the command and the actual scan.

5.2 Facial recognition

- There is not enough information in the scientific literature on the feasibility of facial recognition in children as regards the 'durability' of the biometric data.
- The anthropometric data available indicate that the growth of children's faces is a complex process that differs between boys and girls. Growth takes place in spurts, and the proportions do not remain constant, making it very difficult to express the effect of growth in a facial recognition algorithm.
- We are not aware of any providers of facial recognition software who claim to be able to compensate for the growth and ageing of children's faces. One of the providers states that facial recognition is not reliable in the under-5s; it is not until the age of 13 that ageing ceases to have any marked effects, as facial form is then stable.
- Anthropometric research indicates that most facial features have indeed matured by about the age of 13, though this is not true of all the important ones.
- Facial recognition in children based on reference pictures that are a few years old is likely to be problematical. It is unlikely that facial recognition software will be able in the near future to compensate for the effects on growth on children's faces.
- There are not only technical considerations here but also practical ones: in the strange (to them) environment of a town hall or the hectic conditions

of a border control young children may well be unwilling or unable to cooperate with a facial scan, causing serious delays.

- Independent research indicates that ageing continues to play a role in facial recognition throughout life. Older people are generally easier to recognize than younger people.
- There is not enough information on the useful life (durability) of biometric data when it comes to using facial recognition in children over 12. We cannot rule out the possibility that the useful life of a facial scan will be shorter in the case of younger people than older people.

6. References

[ENLO82] *Handbook of facial growth*, Donald H. Enlow, W.B. Saunders Company, ISBN 0-7216-3386-2, 1982.

[FARK92] *Growth and development of regional units in the head and face based on anthropometric measurements*, L.G. Farkas, J.C. Posnick, , Cleft Palate Craniofac J., 29(4), 1992.

[FRVT02] *FRVT 2002: Overview and Summary*, P.J. Phillips, P. Grother, R.J Micheals, D.M. Blackburn, E Tabassi, and J.M. Bone., March 2003. Available from http://www.frvt.org.

[GIVE02] *A statistical assessment of subject factors in PCA recognition of human faces*, G.J. Givens, et al., NIPS Workshop on statistics for computational experiments, 2002.

[GROS01] *Quo vadis Face Recognition?,* R. Gross, J. Shi, and J. Cohn. Technical report CMU-RI-TR-01-17, Robotics Institute, Carnegie Mellon University, June, 2001.

[IDENT] *Identix FAQ*, http://www.identix.com/trends/faqs/recog.html

[LANI02] *Toward Automatic Simulation of Aging Effects on Face Images*, A. Lanitis, C.J. Taylor, and T.F. Cootes.. IEEE T-PAMI Vol. 24, No. 4, pp. 442-455, April 2002.

[OTOO99] *3D shape and 2D surface textures of human faces: the role of "averages" in attractiveness and age,* A.J. O´Toole, T. Price, T. Vetter, J.C. Bartlett, and V. Blanz.. Image and Vision Computing 18, pp. 9-19, 1999.