VISPILOT –

Towards European Biometric Visa Border Control

Michael Schwaiger[1], Fares Rahmun[2], Oliver Bausinger[3], Mathias Grell[4]

[1]secunet Security Networks AG
Kronprinzenstraße 30, 45128 Essen, Germany
michael.schwaiger@secunet.com

[2]German Federal Office of Administration (BVA)
Barbarastraße 1, 50735 Köln, Germany
fares.rahmun@bva.bund.de

[3]German Federal Office for Information Security (BSI)
Godesberger Allee 185-189, 53175 Bonn, Germany
oliver.bausinger@bsi.bund.de

[4]German Federal Police (BPOL)
Roonstraße 13, 56068 Koblenz, Germany
mathias.grell@polizei.bund.de

Abstract: To thoroughly prepare the expected start of the European Visa Information System (VIS) in 2011, Germany has implemented and evaluated the biometric visa border control process in a dedicated pilot project. In addition to implementing all necessary software modules for the access to the VIS, the focus of the project was set on the new feature of fingerprint biometrics. Fingerprint verification is applied to the primary position during border control where the process is optimised for fast completion, high throughput and ease of use. Extended identity checks with a quality-oriented border control process are conducted at the secondary position, where also a time-consuming fingerprint identification can be applied. Several tests were conducted during the pilot project in order to evaluate the VIS border control process. Recommendations regarding the implementation and operation of VIS related systems on the national level have been derived based on the evaluation results.

1 Introduction

The introduction of the Visa Information System (VIS) based on the European Regulation No. 767/2008 [EC-767-2008] mandates European member states to issue biometric visas and check them during the border control process. While issuing of biometric visas based on captured fingerprints of the visa holder was first implemented and evaluated in the European BioDEV II pilot project, the project VISPILOT was set up by the German Federal Office of Administration (BVA), the German Federal Office for Information Security (BSI), the German Federal Police (BPOL) and the company secunet Security Networks AG as contractor to design and evaluate the border control processes of biometric visas.

The first part of the project was dedicated to the specification, implementation and installation of all necessary software modules for a biometric visa border control check against the central VIS based on fingerprints. Implementation was done according to the BSI Technical Guideline Biometrics for Public Sector Applications [TR-03121] which requires several BioAPI 2.0 [ISO-19784-1] compliant Biometric Service Providers (BSP) for the acquisition of the fingerprint data during the visa identity check processes. For fingerprint acquisition the *Dermalog ZF1* single-finger-scanner and the *Cross Match Technologies L SCAN Guardian* four-finger-scanner were used during the project. Interoperability and exchangeability of hardware devices was implemented using the BioAPI Sensor Function Provider Interface abstraction according to [ISO-19784-4]. While single-finger-scanners are only applied in verification scenarios, four-finger-scanners can be used for enrolment and identification as well. In general, a maximum of four fingerprints is allowed to be captured for verification. Due to the fact that fast processing time and high throughput is needed at the primary border control position, no additional quality assurance is conducted in this situation. For identification, a tenprint of the visa holder is captured at the secondary position. Additionally, extensive quality assurance is conducted in order to achieve the best possible fingerprint quality. To achieve this goal, multiple captures of the same finger are conducted in order to select the best fingerprint image. Besides stationary border control, verification was also implemented for full mobile scenarios.

In the second phase of the project, an evaluation environment was designed and implemented in order to import the results of all visa processes and enable a central evaluation thereof. The evaluation environment is based on the logging and evaluation requirements of the BSI Technical Guideline [TR-03121] which defines a general scheme for logging data of all visa processes. This requires all software modules to deliver the corresponding information in XML format. Consequently, this information is used to generate defined diagrams and statistics in order to monitor all visa processes. Furthermore, the implemented evaluation environment offers the possibility to apply filtering according to the location and the date of the visa issuance and border control conducted. This allows German authorities to react on problems and anomalies in the visa processes as soon as possible. During the VISPILOT project this evaluation environment was used to generate statistical project results.

The application procedure for biometric visas of the voluntary participants in the VISPILOT project was conducted at the Federal Police site in Swisttal-Heimerzheim. Until December 2010, the biometric data of about 150 participants was collected. After the implementation and integration of the software modules for visa border control into the existing systems, the evaluation of the border control processes was conducted in February and March 2011. During the pilot project records of all participants were submitted to the European testing environment, the VIS Playground, which then were used as a basis for the simulations conducted.

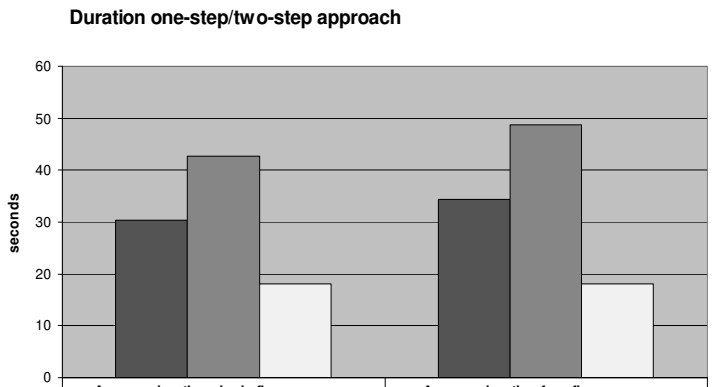
2 Border Control Simulations and Evaluation Results

In order to obtain information about the visa border control process, several simulations were conducted. The focus was set on evaluating the implemented border control processes and on gaining practical experience of the technical behaviour of the VIS and the underlying Biometric Matching System (BMS). For those simulations, several subgroups of the voluntary participants were invited to simulate visa border controls under certain circumstances and exceptional scenarios. Both scenarios at the primary position, where biometric verification is conducted, and at the secondary position, where biometric identification is used to check the identity of the visa holder, were considered during the simulations.

One focus of organisational tests was on the two possibilities of conducting biometric verifications against the VIS: the one- and two-step approach. Using the one-step approach, fingerprints of the visa holder are captured and directly sent to the VIS for verification, without knowing in advance if reference fingerprint data is available for the particular visa holder. In case no fingerprints are stored for this person, an appropriate error is returned by the VIS. Nevertheless, in such a situation the fingerprint capturing was dispensable. That could have been avoided by using the two-step approach. As the name of the approach suggests, two separate messages are sent to the VIS in this case. The first request does not contain fingerprint images. As an answer to this request, the information if fingerprints are stored for the according person is returned. Only if reference fingerprints are stored, live fingerprints are captured and sent to the VIS for verification.

As expected, the two-step approach takes all in all more time for the verification of the visa holder (see Figure 1). In average, more than 40 seconds are needed for the two-step approach if reference fingerprints of the visa holder are stored in the VIS. Using the one-step approach instead, the average duration is around 30 seconds. This means that there is a significant difference in duration between both approaches. In the case that no fingerprints of the visa holder are stored in the VIS, the average duration for such a transaction is about 18 seconds.

However, in the first years of the introduction of the VIS the two-step approach can offer advantages in duration, as the VIS rollout in the Schengen consulates and the introduction of fingerprint acquisition is carried out gradually by geographical regions, implementing a transitional period where not all visa applicants will be affected by the VIS. It is assumed that fingerprints are captured and stored for nearly all issued visas in a few years. At this point in time, the one-step approach will be much faster than the two-step approach.



	Average duration single-finger-scanner	Average duration four-finger-scanner
One-step approach with reference fingerprints in VIS	30,4	34,3
Two-step approach with reference fingerprints in VIS	42,7	48,7
Two-step approach without reference fingerprints in VIS	18	18

Figure 1: Duration one-step/two-step approach

Another focus was on the analysis of the biometric characteristics of the VIS. One option to consider is the use of repetitive verification. Repetitive verification means that live captured fingerprints are compared to all stored fingerprints of the person's record. If repetitive verification is not used, live captured fingerprints are only compared to the reference fingerprints of the indicated finger. The advantage of using repetitive verification is the decrease in false rejections if visa holders place the wrong fingers or hand on the scanner. Contrary to the expectations, the use of repetitive verification did not increase the time needed for verification[1].

[1] Timing observations are not considered relevant as testing was conducted against the VIS playground. Therefore, no conclusion regarding the response time of the real VIS in full load could be derived.

An important outcome derived from the simulations is that for the VIS/BMS only one matching fingerprint is necessary for a successful verification of a person. This means that the use of four-finger-scanners does not bring the expected advantage regarding the biometric level of security. Though the BMS specification foresees a higher threshold when verifying with two or four fingers instead of with one, an attacker only needs to spoof one fingerprint to successfully pass the border control. As a consequence of this outcome, simple fake finger dummies of some project participants were produced by the project team in order to demonstrate such fake finger attacks. To detect fake fingers, it is indispensable that the border control officer has an immediate look on the fingerprint scanner and, especially, on the fingers of the visa holder. As a result, a corresponding policy will be set up at the German border control points.

A highly interesting evaluation result is the difference in capture duration of the fingerprint scanners used (see Figure 2). Both devices support hardware- or software-based auto-capture of fingerprint images. The average acquisition duration of the four-finger-scanner was 15 seconds. Using the single-finger-scanner, in average only 6.3 seconds were needed for the fingerprint acquisition. However, there is a big duration difference among the fingerprint scanners used which was also observed by the participants of the pilot project. The whole border control process at the primary position was much faster if the single-finger-scanner was used.

Resulting from the outcome of previously mentioned simulations, the use of four-finger-scanners does not only miss the expected security enhancement regarding spoofing attacks, but brings disadvantages with regard to the duration of the fingerprint acquisition. On the other side, the usage of four-finger-scanners will obviously minimise false rejections, which might compensate or justify the increased effort, when the system will have to handle a high traffic volume in production.

All in all, the complete visa border control process starting when the visa is put on the document reader and waiting until the person is verified using fingerprint recognition takes about 31 seconds. Again, the complete process takes longer if the four-finger-scanner is used. Further evaluations showed that any deviations from a regular border control process (e. g. person has dry hands and produces bad-quality fingerprint images etc.) increase the overall visa border control duration significantly.

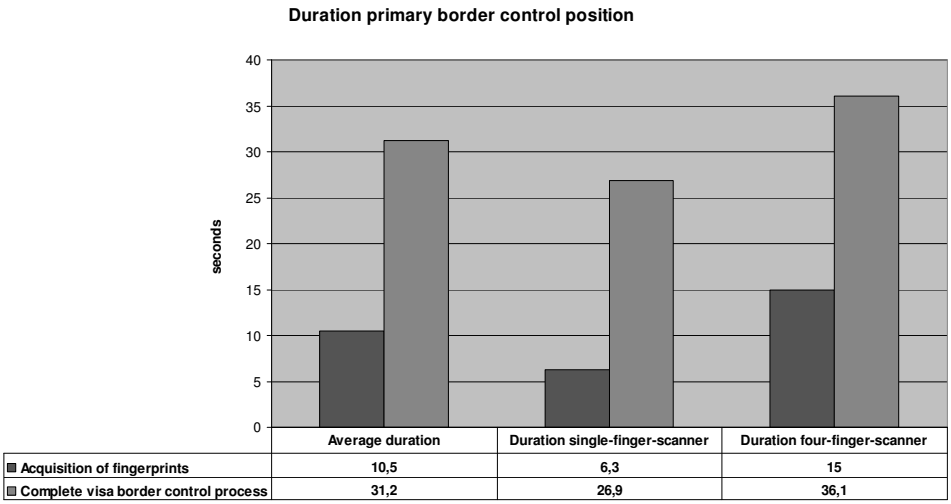


Figure 2: Duration at the primary border control position

Further evaluations showed that the verification rate at the primary position was at about 88 percent for the security settings of the VIS Playground. No big differences between fingerprint scanners used were detected. For all conducted identifications at the secondary position the appropriate visa application was returned by the VIS. Nevertheless, statistical significance is not given due to the fact that only few verifications and identifications were conducted during the pilot project.

3 Conclusions and Recommendations

The integration of all necessary software modules for biometric visa border control was successfully achieved during the project in compliance to the BSI Technical Guideline Biometrics for Public Sector Applications [TR-03121]. Outcomes of the project have influenced the further development of visa profiles of this technical guideline and will be released as version 2.3 by BSI soon.

Finally, recommendations were derived from results of the project. Outcomes of the project regarding the security of biometric verifications shall be communicated to the European Commission in order to reduce the chance of spoofing attacks and enhance the security if multi-finger-scanners are used. Considering the additional time needed for a more secure verification, this should at least be an option, helping to justify the higher amount of investment for the four-finger-scanners. Furthermore, the VISPILOT project has proven once more the importance of a standardized quality monitoring of biometric processes, as most of the statistical project results were derived from the collected logging data required by the Technical Guideline [TR-03121]. Therefore, it is highly recommended to introduce a national central evaluation environment for the VIS in operation, in order to be able to react on anomalies of visa issuance and border control as soon as possible. The implemented evaluation environment is intended to serve as a blueprint for this purpose.

Bibliography

[EC-767-2008] Regulation (EC) No. 767/2008 of the European Parliament and of the council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation).

[TR-03121] Federal Office for Information Security (BSI): Technical Guideline TR-03121 Biometrics for Public Sector Applications, Version 2.2, 2011.

[ISO-19784-1] ISO/IEC 19784-1:2006 “Information technology – Biometric application programming interface – Part 1: BioAPI specification”.

[ISO-19784-4] ISO/IEC 19784-4:2011 “Information technology – Biometric application programming interface – Part 4: Biometric sensor function provider interface”.