



Version 2.1

Modular biometric architecture with secunet biomiddle

White Paper Version 2.0, 25/03/10

secunet
secunet Security Networks AG

Copyright © 2010 by secunet Security Networks AG

This document is for information purposes. It is permitted to print it out and save it in full, unmodified form. Additional publishing, printing and copying or saving in any form whatsoever, in whole or in part, is permitted only with the prior written consent of secunet Security Networks AG.

In addition to explanations, assessments and our own surveys, this document contains descriptions of manufactured products, interfaces and concepts which are based on the corresponding publications of the particular manufacturer.

The replication of common names, trade names, trademarks, etc., even without special labelling, does not justify the assumption that such names should, in the sense of trademark and brand protection legislation, be regarded as unused and therefore usable by anyone. All brands and product names are trade names or registered trademarks of the particular trademark owner.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Part of the software embedded in this product is gSOAP software.

Portions created by gSOAP are Copyright (C) 2001-2004 Robert A. van Engelen, Genivia inc. All Rights Reserved.

THE SOFTWARE IN THIS PRODUCT WAS IN PART PROVIDED BY GENIVIA INC AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Contents

- Contents..... 3
- 1 Requirements of biometric architectures..... 4
- 2 Challenge: “biometric interoperability” 5
 - 2.1 Biometric data formats 5
 - 2.2 Biometric functions 6
 - 2.3 Access to electronic IDs 6
- 3 Performance characteristics of secunet biomiddle 8
 - 3.1 Architecture of secunet biomiddle..... 8
 - 3.2 Advantages of solutions with secunet biomiddle..... 9
 - 3.2.1 Modularity and exchangeability..... 9
 - 3.2.2 Security of investment10
 - 3.2.3 Integration of biometrics as high-level functionality10
 - 3.2.4 Technical freedom at application level10
- 4 Case studies using secunet biomiddle11
 - 4.1 An organisation's office for issuing ID cards11
 - 4.1.1 The problem11
 - 4.1.2 Solution strategy.....11
 - 4.1.3 Implementation.....11
 - 4.2 Verification of electronic travel documents14
 - 4.2.1 The problem14
 - 4.2.2 Solution strategy.....14
 - 4.2.3 Implementation.....14
 - 4.3 Automated Border Crossing System16
 - 4.3.1 The problem16
 - 4.3.2 Solution strategy.....16
 - 4.3.3 Implementation.....16
 - 4.4 Identification for entering a safety zone18
 - 4.4.1 The problem18
 - 4.4.2 Solution strategy.....18
 - 4.4.3 Implementation.....18
- 5 Summary of performance features.....20

1 Requirements of biometric architectures

The structure of biometric systems or their integration in existing environments presents both opportunities and risks. Because of the highly dynamic nature of biometrics and short innovation cycles, under certain circumstances a solution may no longer satisfy the requirements of the latest state of the art or of changing requirements, even after a short period. For example, a new hardware generation can provide vastly improved acquisition, in terms of time or quality, or a new comparative biometric algorithm can achieve a much better recognition performance.

In order to achieve an adaptable and thus investment-safe solution, care should be taken, right from the beginning, to achieve a modular and standards-oriented architectural concept. For this, secunet biomiddle provides the best possible basis, because of its modular structure and the consistent application of international standards. It functions as middleware between client applications and the biometric technologies on the market. The functional scope extends from optical and electronic reading of biometric data in the identity documents through the traditional biometric functions for capturing, quality assessment, verification and identification right up to the connection with complex background systems such as fingerprint databases (AFIS systems) or authorisation systems. What is decisive is that secunet biomiddle does not itself implement any biometric processing but always integrates those from suitable manufacturers via standards-compliant interfaces.

The complexity of the existing standards and also of the associated manufactured components is reduced from the applications point of view by secunet biomiddle, with all the functions being provided via a service-oriented interface (SOAP). This also makes technological freedom and scalability possible for client applications, which can be written in any programming language.

2 Challenge: "biometric interoperability"

In the field of biometrics there is a series of international standards which are meant to guarantee interoperability of data and systems. In practice, these standards are thoroughly interwoven, which considerably increases the complexity of working with them.

2.1 Biometric data formats

The format in accordance with ISO/IEC 19794 is the main one used for encoding biometric data. The standard contains several parts which are each limited to a specific biometric feature. Another important standard for exchanging biometric data is Standard ISO/IEC 19785, which specifies the "CBEFF format" (Common Biometrics Exchange File-Format). The standard permits various characteristics, the "patron formats", to be defined. The format used in the smartcard area under ISO/IEC 7816-11 and the BIR format under ISO/IEC 19784 (BioAPI 2.0) are the most important patron formats in practical use.

In the context of electronic passports, the International Civil Aviation Organisation (ICAO) has defined the logical data structure (LDS), which describes the encoding of biometric data on the passports.

The encoding of fingerprint images on electronic passports is a good example of how the various standards interact. Within an LDS structure is a CBEFF structure in accordance with ISO 19785 and 7816-11, which in turn contains one or more data records in accordance with ISO 19794-4. There are one or more fingerprint images in these data records which are compressed and then coded in WSQ (wavelet scalar quantisation) data format.

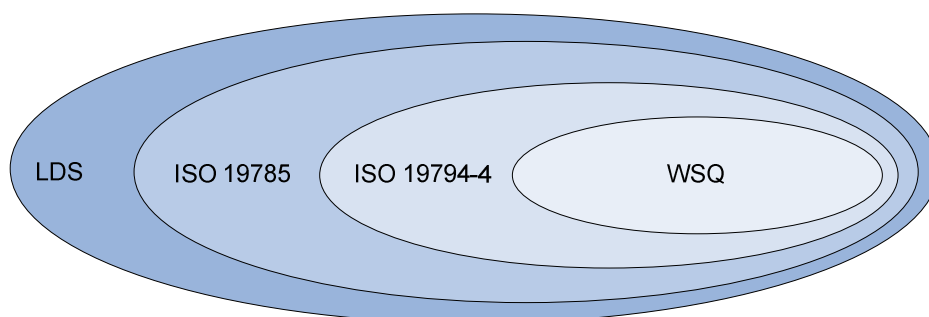


Fig. 2-1: encoding of fingerprints on identity documents (simplified)

secunet biomiddle provides complete flexibility in the use of these data formats. If an application using secunet biomiddle would like to display only these data, it can

request the fingerprint images in a commonly-used format - BMP or JPEG for example. If, however, it requires the information as complete LDS encoding, secunet biomiddle delivers the data in that format.

2.2 Biometric functions

Standard ISO/IEC 19784-1 (BioAPI 2.0) defines an architecture for biometric systems, for interoperability of systems and processes. Moreover, it defines the interface for applications and biometric service providers (BSP), which are integrated in the BioAPI-specified architecture (BioAPI framework) via a plug-in mechanism.

The functions defined by BioAPI 2.0 cover the complete range of biometric operations (enrolment, verification and identification) and are, nevertheless, open to new technologies. In the standard, there is no commitment to certain data formats, encodings or biometric processes.

The actual implementation of the biometric functionality occurs via the associated providers. They are available as a dynamic library and are loaded to the environment at the time of operation. BioAPI 2.0 defines various categories of BSPs such as, for example, BSPs for capturing biometric data and BSPs for verification purposes. It is established for each category, which functions must be provided by the appropriate dynamic library of a BSP.

The functions provided by a BioAPI 2.0 BSP are on a high level. The standard must not, therefore, be regarded as a "driver interface for biometric sensors". For the use of a BioAPI 2.0 BSP, a standard-specified framework is necessary, which integrates and manages the various BSPs. secunet biomiddle contains such a framework and thus implements a well-defined, open, modular and transparent overall architecture. It makes it possible to add or exchange external components compatible with BioAPI 2.0, directly and without the effort of integration. That means, for example, that it is possible to switch in actual operation from a fingerprint scanner to an alternative source.

2.3 Access to electronic IDs

With the introduction of electronic passports, the topic of identity checking has taken on a close association with biometric processes, in the mandatory sphere. The holder's biometric characteristics are saved in the new identity documents and must be read from the document for identity checks based on it. In addition to the protocols for access via RFID and communication via the chip, a series of ePassport-specific security mechanisms, such as Basic Access Control or Extended Access Control, are necessary. To access the passport, secunet biomiddle uses the ePassportAPI, which is used in the Golden Reader Tool of the German Federal

Office for Information Security (BSI). At international level, the latter is used as a reference application for reading passports and is used by many manufacturers as proof of interoperability.

3 Performance characteristics of secunet biomiddle

3.1 Architecture of secunet biomiddle

secunet biomiddle's architecture contains four different modules which combine and make available the functions of a particular topic.

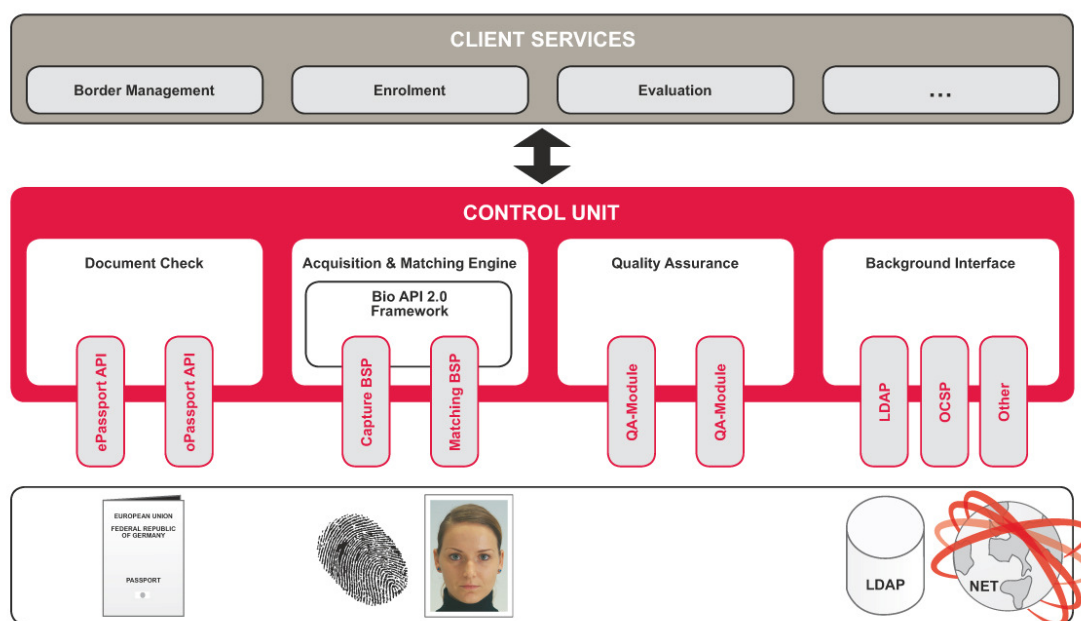


Fig. 3-1: secunet biomiddle

The **Document Check Module** is used to read and check identity documents. The ePassportAPI is integrated as a standardised interface for reading the electronic contents. Using Basic Access Control (BAC), Active Authentication (AA) and Extended Access Control (EAC), it supports all the existing security mechanisms for electronic passports. Depending on the power of the reader used, machine readable zone (MRZ), infrared (IR) image, ultraviolet (UV) image, visible image and cropped facial image may be read as optical data.

The **Acquisition & Matching Engine** enables standardised access to all biometric sensors and algorithms, which are BioAPI 2.0-compatible and thus provide a suitable BSP. Based on them, this module allows any biometric operations to be performed, such as recording the live image of a person, enrolment, verification and identification of people. These functions are provided generically for the various biometric technologies, such as face, fingerprint and iris recognition.

The **Quality Assurance Module** tests, with respect to their quality, whether biometric data are suitable for biometric comparisons and/or fulfil international requirements (ICAO requirements for photographs, for example). In a similar way to the BioAPI approach, suitable evaluation algorithms are connected via “QA providers”. During the process, secunet biomiddle can connect one or more suitable QA providers.

The **Background Interface Module** is used to connect external systems. Communication with the background systems can thus occur in any way you like, via protocols such as SMTP, ODBC, HTTP or SOAP, for example. Communication with databases such as Oracle, MySQL, PostgreSQL or MS SQL is also possible. In this case, too, an approach comparable with BioAPI has been chosen, in order to connect the functionality necessary in individual cases to secunet biomiddle via provider modules.

As a central entity, the **Control Unit** starts and initialises all the modules. It manages the services provided and processes the clients' requests. The latter are transferred to the modules responsible. To guarantee maximal flexibility and platform independence, the interface for the applications is based on SOAP (Simple Object Access Protocol).

3.2 Advantages of solutions with secunet biomiddle

On the introduction of biometrics, a business must commit itself very early, regarding the most diverse points. Important questions are, for example, which biometric process should be used, which scanner technology is best suited to the particular purpose or which verification algorithm achieves the best results. For the reasons mentioned above, however, exchangeability and migration capability are highly significant for biometrics. Such flexibility can be achieved by secunet biomiddle. The advantages of secunet biomiddle are summarised below.

3.2.1 Modularity and exchangeability

secunet biomiddle is subdivided into various functional modules running on the biomiddle server. The advantage of distributing the functions over various modules is that the requirements of various use case scenarios can be fulfilled. secunet biomiddle's modularity means that distributed environments are not a problem. As a result of secunet biomiddle's technical openness, many different devices may be addressed. Sensors and card readers are integrated by a standardised interface. This guarantees an exchange of devices, irrespective of manufacturer. secunet biomiddle also makes it possible to operate several different devices. The appropriate sensors may thus always be used, depending on the environment (e.g. interior as against exterior usage). There is the additional possibility of using secunet biomiddle to implement multimodal biometric systems (the combined use of

various biometric characteristics). This can increase a system's recognition performance considerably.

3.2.2 Security of investment

The biometric market has been operating for years with short innovation and product cycles. Accordingly, performance improvements, new technologies and supplementary methods are already to be expected for medium-term. New requirements of biometric applications will also appear. As a result of the modular structure and the observance of the relevant standards, an application based on secunet biomiddle can react to such changes with comparatively little effort. The use of this open biometric platform thus achieves security of investment.

3.2.3 Integration of biometrics as high-level functionality

The development of applications with the use of secunet biomiddle operates only at a higher level. Addressing individual sensors or algorithms no longer occurs during implementation and is taken over by secunet biomiddle. The complex, device-specific interfaces are abstracted and their functions are provided for the application in unified form, irrespective of manufacturer.

3.2.4 Technical freedom at application level

Applications use secunet biomiddle via a SOAP interface. This has the advantage that the application itself may be written in any programming language. This simplifies enormously the integration of biometric functions in existing solutions and also makes it possible for biometric functions to be provided as central services. Thus it is possible to achieve, for example, a central, resource-intensive comparative service, used by many slim applications. This approach also allows an application to use several biomiddle entities distributed within the infrastructure. In this way, all desired requirements may be implemented in the best possible way, with respect to performance, scalability or availability.

4 Case studies using secunet biomiddle

secunet biomiddle may be used in various scenarios. Shown here are some case studies involving the implementation of secunet biomiddle.

4.1 An organisation's office for issuing ID cards

4.1.1 The problem

In the future, the ID cards issued by an organisation should also contain the owner's stored biometric characteristics. For all the new ID cards, a photo of the face should be saved. For employees who have access to special safety areas, fingerprints should also be saved. For enrolment, there should be quality assurance of biometric data, in order to achieve the best possible recognition performance. An office which has been active for years in the area of application and issuance of ID cards must be extended to include biometric process facilities.

4.1.2 Solution strategy

The existing application for registering employee data, programmed in Java, is highly complex and cannot be replaced by a "standard application" because it is integrated with the personnel data system and other special applications. The acquisition of biometric data should be integrated in the application, instead. After acquisition, the biometric data are transferred to the card production system.

4.1.3 Implementation

secunet biomiddle is used for implementing all new biometric-relevant functions. Since the existing acquisition application is programmed in Java, Apache Axis (<http://ws.apache.org/axis/>) is used for the SOAP implementation. The necessary Java classes are automatically created by Axis from the WSDL (web service definition language) file provided by secunet biomiddle. Using those classes, the functions provided by secunet biomiddle may be addressed directly. An external production system takes over personalisation of the new biometric ID cards. For this purpose, the biometric data are encoded in the format required for saving to the card and saved temporarily, separately from the remaining data, in a local database until the card is issued. The data are encoded and transferred to the production system by a background interface provider connected to secunet biomiddle.

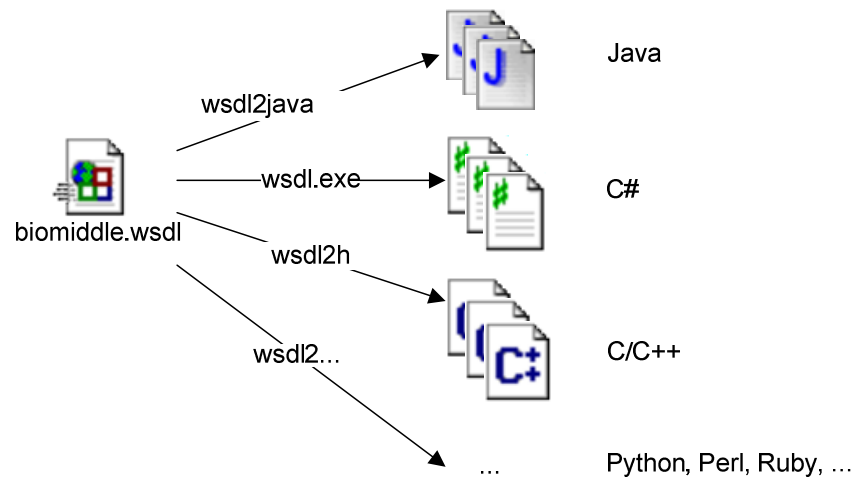


Fig. 4-1: Generating source code

secunet biomiddle is installed on the issuing office's system. In the process, the following modules are connected to biomiddle for the enrolment:

a BSP for capturing a full face shot with a digital camera,

a BSP for capturing a fingerprint with a sensor,

a BSP for comparing fingerprints

a quality provider for checking face images,

a quality provider for checking fingerprints and

a background interface provider for communicating the data to a production system.

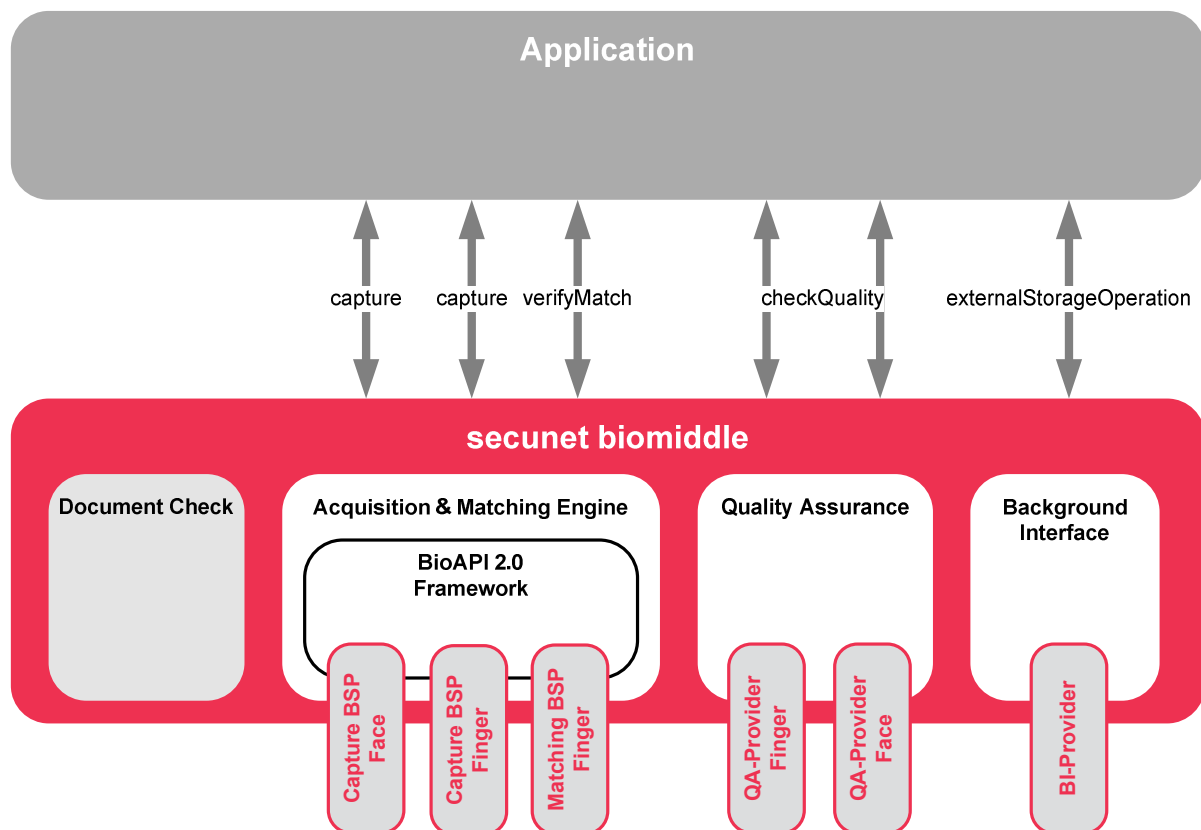


Fig. 4-2: secunet biomiddle setup for ID card application

The following acquisition process is integrated in the existing application:

1. After the cardholder's usual data has been entered, his/her face is captured by a digital camera. To do this, the application accesses the BSP's biomiddle **capture** function. To capture the image, using the camera's live image, the latter displays a dialogue on the user interface and automatically captures the photograph as soon as a face has been recognised.
2. The application transfers the recorded image to Quality Testing. To do this, it accesses the biomiddle **checkQuality** function for the provider responsible. If the result is negative, step 1 is repeated.
3. If it is a person for whom fingerprints should be taken, the **capture** function of the fingerprint BSP is accessed three times, with the same finger being recorded each time. This is done in order to achieve the best possible image of the finger.
4. After the recording, all the fingerprints are compared and individually quality-tested. The application uses the **verifyMatch** function for the biometric comparison. It then evaluates the results and decides on one of the three images.

5. In order to biometrically authenticate the person further in the event of subsequent injury, steps 3 and 4 are performed again, using a second finger from the other hand.
6. After the acquisition application has recorded all the biometric data, it transfers them to the production system. For this purpose, it uses the biomiddle **externalStorageOperation** function. The latter encodes the data in the target format and saves them in the production system.
7. The passport is produced independently of the acquisition application and secunet biomiddle.

4.2 Verification of electronic travel documents

4.2.1 The problem

In accordance with the international standards for passports, the electronic data are saved in protected form in the passport. Within a border control process, this data shall be verified. Therefore an existing border control application is required to be extended.

4.2.2 Solution strategy

The biometric data are read from the passport and verified by secunet biomiddle and submitted to a border control application. The latter visualises the results to the border control officer.

4.2.3 Implementation

secunet biomiddle is installed at the border control station with the following components:

- document check module with ePassportAPI and oPassportAPI for the passport reader and
- a Background Interface provider to access the national Public Key Directory (N-PKD).

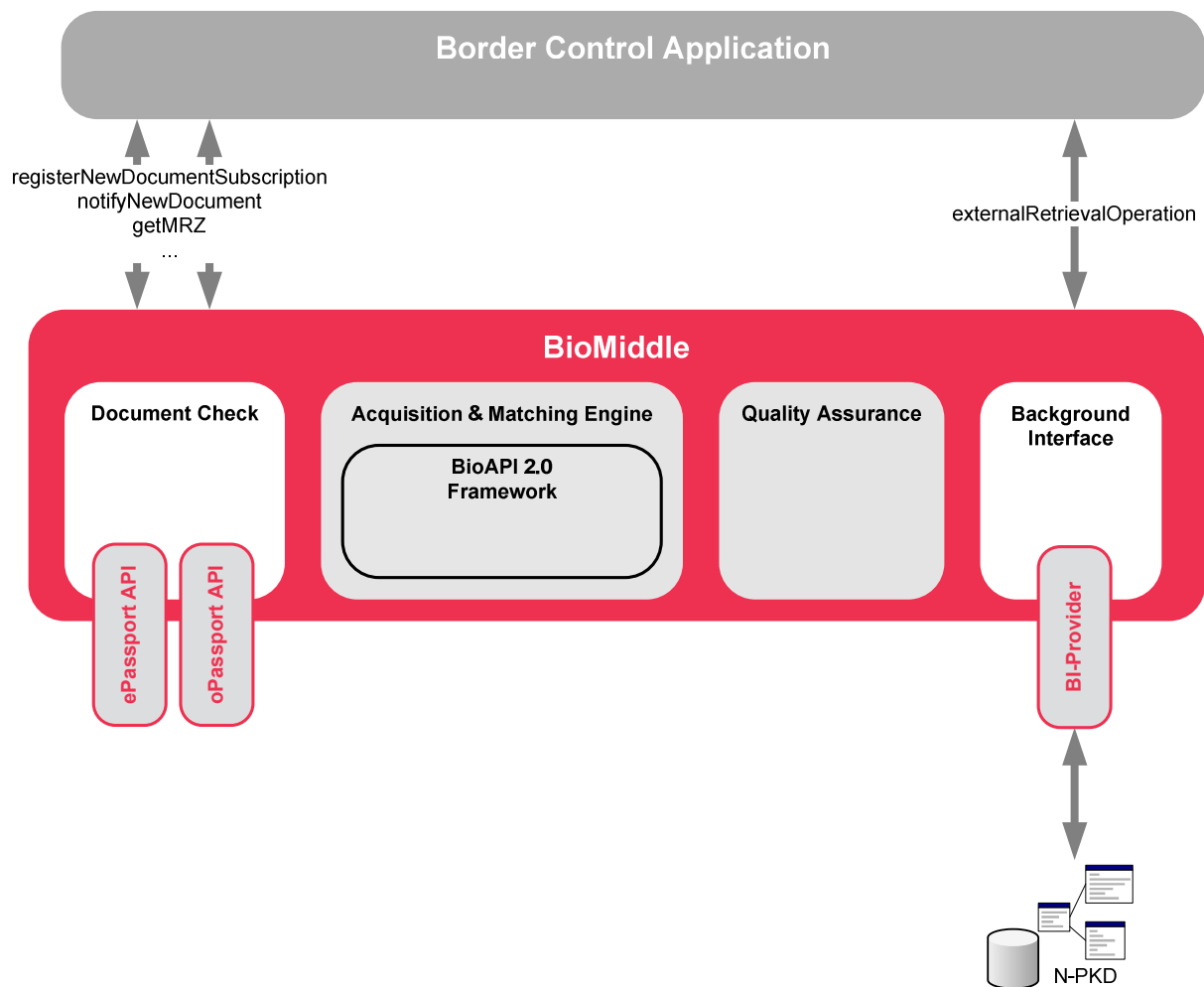


Fig. 4-3: secunet biomiddle setup for border control

The process for the biometric border check control is as follows:

1. The border control application is registered for the communication with secunet biomiddle, as soon as a new document has been placed on the passport reader. For this purpose it calls the biomiddle **registerNewDocumentSubscription** function and passes the URL on which it wishes to receive the messages. It then opens the port specified in the URL and waits for messages.
2. As soon as a new document has been placed on it, secunet biomiddle informs all registered applications. Thus the **notifyNewDocument** message is sent.
3. The border control application queries biomiddle for the machine readable zone of the newly-available passport. To do this, it accesses the **getMRZ** function. By means of the MRZ, the application decides whether biometric data should be read from the passport.

4. If an electronic document is detected, the application reads datagroup 1 and 2 from the passport. It uses the functions **getElectronicPassportCount** and **getDatagroup** to do this.
5. To retrieve the necessary CSCA certificate from the public key directory, the application asks for the search parameters by calling the function **getMissingCertinfo** and delivers them through the function **externalRetrievalOperation** to the BI provider. As result the corresponding CSCA certificate is returned.
6. To get the results of the electronic security checks, the application calls the functions **checkDatagroup**, **checkPassiveAuth** and **getProtocolStatus**.
7. All results are visualized to the border control officer.

4.3 Automated Border Crossing System

4.3.1 The problem

The border crossing of travelers is intended to be automated by using an Automated Border Crossing system (ABC system). The system shall perform all regular security checks done at the regular border control desks, supplemented by a biometric verification of the travelers face. The target user group is based on all citizens within the Schengen area.

4.3.2 Solution strategy

After the travel document is put on the reader, it's optic and electronic security features are checked. The facial image is read from the passport and delivered to a process control application. The latter takes a live image of the face and transfers the data to biomiddle for biometric comparison. In parallel, external databases are queried whether the passport has been reported as stolen or whether the traveller is on a watch list. If all security checks are successful, the traveller is allowed to cross the border.

4.3.3 Implementation

The execution of security checks and the delivery of information to a monitoring station is implemented by a Process Control Application. Within the ABC system, secunet biomiddle is installed with the following modules:

- document check module with ePassportAPI and oPassportAPI for the passport reader,

- a BSP for capturing a facial image by the capture unit of the ABC system,
- a BSP for comparing facial images,
- a Background Interface provider to query for stolen documents and wanted people, and
- a Background Interface provider to access the national Public Key Directory (N-PKD).

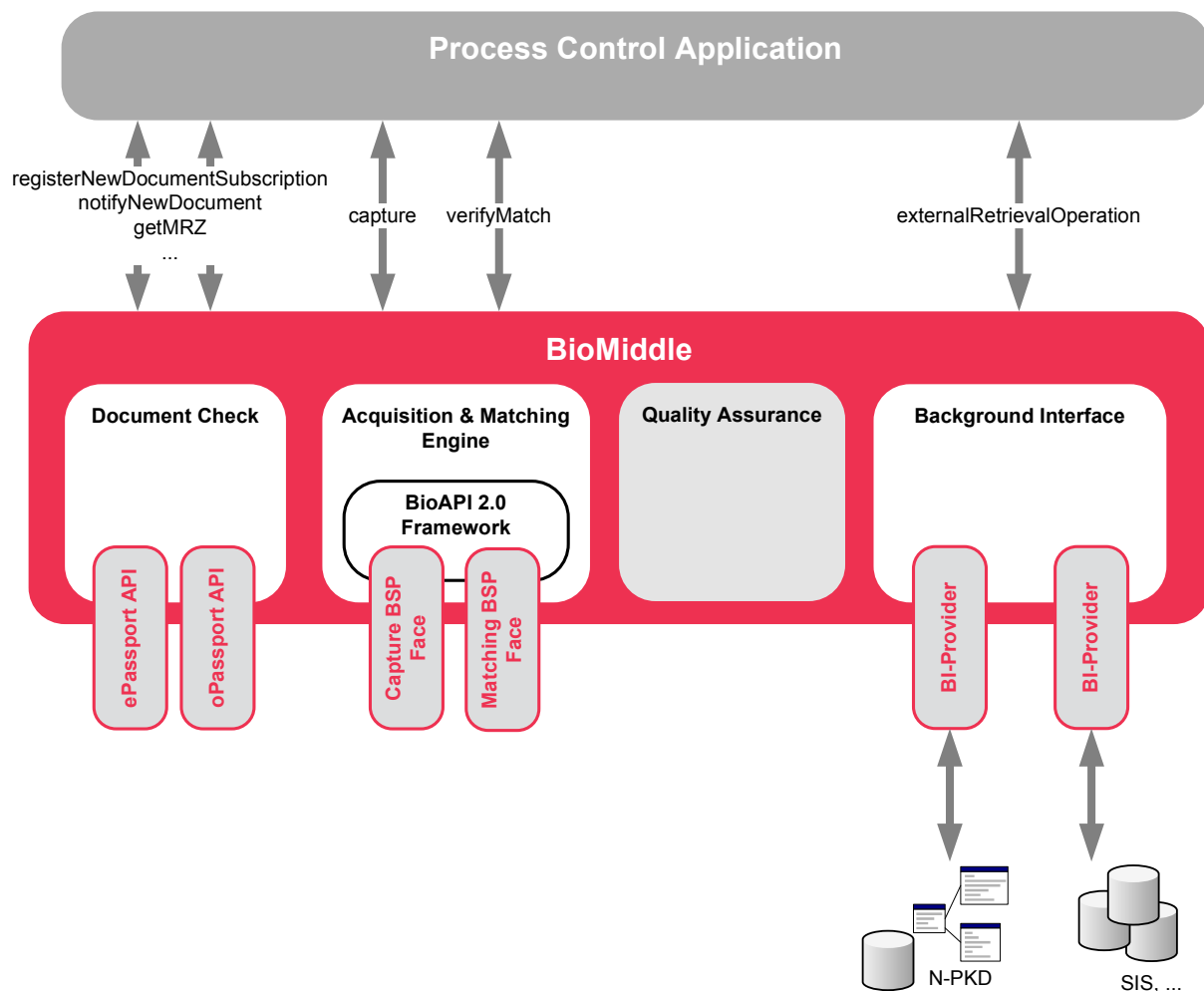


Fig. 4-4: secunet biomiddle setup for ABC systems

The workflow of the automated border crossing process is as follows:

1. The Process Control Application is registered with secunet biomiddle and verifies the electronic security features in the same way as described in chapter 4.2.

2. Additionally, the Process Control Application retrieves the result of the optic security check by calling the function **getOpticalSecurityStatus**.
3. To query for stolen passports or wanted people, the application transfers the MRZ data to the respective BI-provider by calling the function **externalRetrievalOperation**.
4. The application reads the facial image from the passport and also takes a live picture of the person. For this, it uses the biomiddle **getElectronicImage** and **capture** functions.
5. Using the **verifyMatch** function, the application transfers the biometric data for comparison and processes the result.
6. In case all security checks are successful, the Process Control Application opens the door of the ABC system and the traveler is allowed to pass.

4.4 Identification for entering a safety zone

4.4.1 The problem

A building's safety zone should be equipped with biometric entry control. The fingerprint is intended as a biometric characteristic. The reference data are stored in a central authorisation system.

4.4.2 Solution strategy

The entry control is operated by a central application. It uses secunet biomiddle to record the fingerprint and for the identification of the person in the central authorisation system. There are basically two variants for carrying out the identification:

1. If the authorisation system provides an interface in accordance with BioAPI 2.0, the identification can be done by a BSP.
2. If the authorisation system is not BioAPI 2.0-compatible, a connection can be established via biomiddle's background interface.

The latter variant is considered in greater detail below.

4.4.3 Implementation

The following components are connected to secunet biomiddle:

- a BSP for capturing a fingerprint with a sensor and
- a background interface provider for communicating with the central authorisation system.

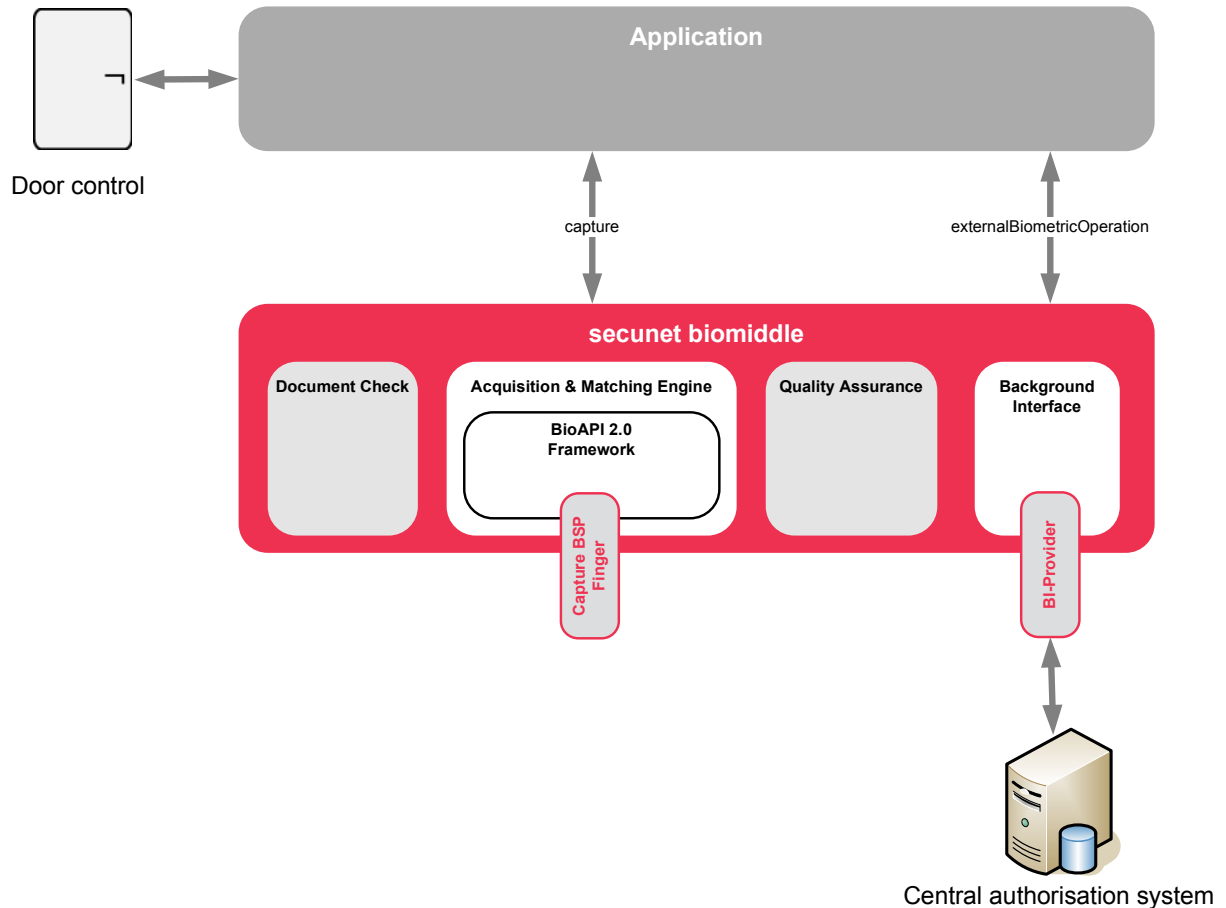


Fig. 4-5: secunet biomiddle setup for entry control

The following procedure is implemented:

1. The control application captures a fingerprint. To do this, it uses the **capture** function.
2. The captured fingerprint is sent to the central authorisation system. It uses secunet biomiddle's **externalBiometricOperation** function. The result of the function is the authorisation system's answer. It contains information as to whether the person has been identified and has authority to enter the safety area.
3. The control application operates the entrance door and allows this person to enter.

5 Summary of performance features

Performance feature	Support
Document check	
support for RFID PC/SC readers	yes
support for full-page readers	yes (various manufacturers)
providing MRZ	yes
optical image data	VIS, UV, IR and cropping
electronic security mechanisms	BAC, AA, CA, TA and EAC
face image data formats	DG2, ISO 19794-5, JPEG, JPEG2000, BMP, PNG, etc.
data formats for fingerprints	DG3, ISO 19794-2/4, JPEG, WSQ, BMP, PNG, etc.
Acquisition & Matching Engine	
recording biometric data	yes
template creation	yes
biometric data comparison	yes
identification	yes
biometric characteristics	any (face, finger, iris, etc.)
data formats	ISO 19794, WSQ, JPEG, JPEG2000, BMP, PNG, etc.
Quality Assurance	
quality assessment according to threshold value	yes
detailed test results	yes - in XML

Background Interface	
saving biometric data	yes
loading biometric data	yes
biometric operations via third-party systems	yes
status and validity test	yes
General Information	
supported operating systems	Windows XP, Windows Vista, Windows 7 and Linux
memory requirement	< 500 kB
SSL support	yes
possible programming languages at application level	C/C++, Java, C#, Perl, etc.

secunet Security Networks AG

Kronprinzenstraße 30

45128 Essen

Tel.: +49-201-5454-0

Fax: +49-201-5454-123

e-mail: biometrics@secunet.com

www.secunet.com