



Version 2.1

Modulare Biometriearchitektur mit secunet biomiddle

White Paper Version 2.0, 25.03.10

secunet
secunet Security Networks AG

Copyright © 2010 by secunet Security Networks AG

Dieses Dokument dient zur Information. Ausdruck und Speicherung ist in vollständiger und unveränderter Form des Dokuments erlaubt. Weitergehende Veröffentlichungen, Nachdruck, Vervielfältigungen oder Speicherung - gleich in welcher Form, ganz oder teilweise - sind nur mit vorheriger schriftlicher Zustimmung der secunet Security Networks AG zulässig.

Dieses Dokument enthält neben Erläuterungen, Bewertungen und eigenen Erhebungen Beschreibungen von Herstellerprodukten, Schnittstellen und Konzepten, die auf entsprechenden Veröffentlichungen der jeweiligen Hersteller beruhen.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenzeichen usw. in diesem Dokument berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürfen. Alle Marken und Produktnamen sind Warenzeichen oder eingetragene Warenzeichen der jeweiligen Zeichenhalter.

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.

Inhaltsverzeichnis

Inhaltsverzeichnis.....	3
1 Anforderungen an biometrische Architekturen	5
2 Herausforderung: „Biometrische Interoperabilität“	6
2.1 Biometrische Datenformate	6
2.2 Biometrische Funktionen.....	7
2.3 Zugriff auf elektronische IDs.....	7
3 Leistungsmerkmale von secunet biomiddle	9
3.1 Architektur von secunet biomiddle.....	9
3.2 Vorteile von Lösungen mit secunet biomiddle	10
3.2.1 Modularität und Austauschbarkeit.....	10
3.2.2 Investitionssicherheit	11
3.2.3 Integration von Biometrie als High-Level-Funktionalität	11
3.2.4 Technologiefreiheit auf Anwendungsebene	11
4 Fallstudien mit secunet biomiddle	12
4.1 Ausweisstelle einer Organisation	12
4.1.1 Problemstellung.....	12
4.1.2 Lösungsstrategie	12
4.1.3 Umsetzung	12
4.2 Elektronische Sicherheitsprüfung eines Reisedokuments	15
4.2.1 Problemstellung.....	15
4.2.2 Lösungsstrategie	15
4.2.3 Umsetzung	15
4.3 Automatisierte Grenzkontrolle (eGate)	17
4.3.1 Problemstellung.....	17
4.3.2 Lösungsstrategie	17
4.3.3 Umsetzung	17
4.4 Identifikation zum Zutritt in einen Sicherheitsbereich	19
4.4.1 Problemstellung.....	19
4.4.2 Lösungsstrategie	19
4.4.3 Umsetzung	20
5 Leistungsmerkmale in der Übersicht.....	22

1 Anforderungen an biometrische Architekturen

Der Aufbau von biometrischen Systemen oder deren Integration in existierende Umgebungen birgt Chancen und Risiken. Aufgrund der hohen Dynamik des Biometriemarkts und kurzer Innovationszyklen kann eine realisierte Lösung unter Umständen bereits nach kurzer Zeit nicht mehr dem Stand der Technik oder sich ändernden Anforderungen genügen. Beispielsweise kann eine neue Hardware-Generation eine zeitlich oder qualitativ stark verbesserte Aufnahmeleistung bieten oder ein neuer biometrischer Vergleichsalgorithmus eine sehr viel bessere Erkennungsleistung erreichen.

Um eine anpassbare und somit investitionssichere Lösung zu realisieren, sollte von Anfang an auf ein modulares und standardorientiertes Architekturkonzept geachtet werden. secunet biomiddle bietet hierfür durch seinen modularen Aufbau und die konsequente Verwendung internationaler Standards die optimale Grundlage. Es fungiert als Middleware zwischen Client-Anwendungen und den am Markt befindlichen biometrischen Technologien. Der Funktionsumfang erstreckt sich vom optischen und elektronischen Auslesen biometrischer Daten von Ausweisdokumenten über die klassischen biometrischen Funktionen zur Merkmalsaufnahme, Qualitätsbewertung, Verifikation und Identifikation bis hin zur Anbindung komplexer Hintergrundsysteme wie Fingerabdruckdatenbanken (AFIS-Systeme) oder Berechtigungssysteme. Entscheidend ist, dass secunet biomiddle selbst keine biometrischen Verfahren umsetzt, sondern diese immer von entsprechenden Herstellern über standardkonforme Schnittstellen integriert.

Die Komplexität der vorhandenen Standards und auch der angebundener Herstellerkomponenten wird durch secunet biomiddle gegenüber den Anwendungen reduziert, indem alle Funktionen über eine serviceorientierte Schnittstelle (SOAP) angeboten werden. Dies ermöglicht außerdem die Technologiefreiheit und Skalierbarkeit gegenüber den Client-Anwendungen, welche in einer beliebigen Programmiersprache geschrieben werden können.

2 Herausforderung: „Biometrische Interoperabilität“

Im Biometrieumfeld existieren eine Reihe von internationalen Standards, die Interoperabilität von Daten und Systemen gewährleisten sollen. Diese Standards sind in der Praxis durchaus miteinander verwoben, was die Komplexität mit deren Umgang zusätzlich erhöht.

2.1 Biometrische Datenformate

Zur Kodierung biometrischer Daten wird vor allem das Format gemäß ISO/IEC 19794 verwendet. Der Standard enthält mehrere Teile, die sich jeweils auf ein gezieltes biometrisches Merkmal beschränken. Ein weiterer, wichtiger Standard zum Austausch biometrischer Daten ist die Norm ISO/IEC 19785, welche das sogenannte CBEFF-Format (Common Biometrics Exchange File-Format) definiert. Der Standard erlaubt die Definition verschiedener Ausprägungen, den sogenannten Patron Formats. Als wichtigste Patron-Formate sind hier das im Smartcardbereich verwendete Format nach ISO/IEC 7816-11 und das BIR-Format nach ISO/IEC 19784 (BioAPI 2.0) im praktischen Einsatz.

Im Kontext der elektronischen Reisepässe ist durch die International Civil Aviation Organisation (ICAO) die Logical Data Structure (LDS) definiert, welche die Kodierung biometrischer Daten auf den Pässen beschreibt.

Die Kodierung von Fingerabdruckbildern auf elektronischen Pässen ist ein gutes Beispiel, wie die verschiedenen Standards zusammenspielen: Innerhalb einer LDS-Struktur befindet sich eine CBEFF-Struktur nach ISO 19785 und 7816-11, die wiederum einen oder mehrere Datensätze nach ISO 19794-4 enthält. In diesen Datensätzen befinden sich ein oder mehrere Fingerabdruckbilder, die im WSQ-Datenformat (Wavelet Scalar Quantization-Datenformat) komprimiert und kodiert sind.

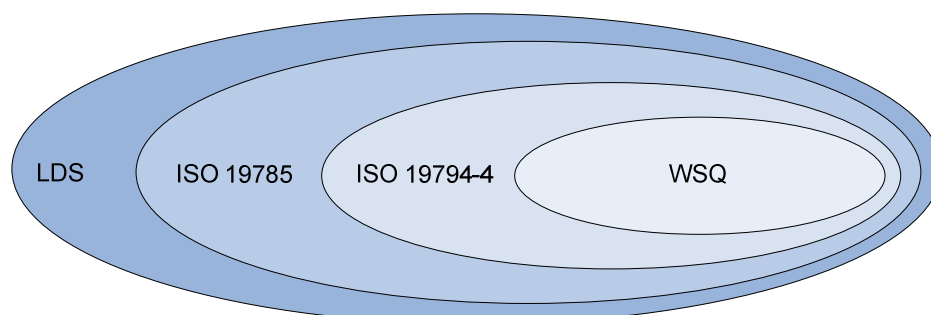


Abbildung 2-1: Kodierung von Fingerabdrücken auf Ausweisdokumenten (vereinfacht)

secunet biomiddle bietet die volle Flexibilität in der Verwendung dieser Datenformate. Wenn eine secunet biomiddle benutzende Anwendung diese Daten lediglich anzeigen möchte, kann sie die Fingerabdruckbilder in einem gängigen Bildformat, zum Beispiel BMP oder JPEG anfordern. Benötigt sie jedoch die Informationen als vollständige LDS-Kodierung, liefert secunet biomiddle die Daten in diesem Format aus.

2.2 Biometrische Funktionen

Zur Interoperabilität von Systemen und Verfahren definiert der Standard ISO/IEC 19784-1 (BioAPI 2.0) eine Architektur für biometrische Systeme. Weiterhin definiert er die Schnittstelle zu Anwendungen und zu Biometric Service Providern (BSP), die über einen Plugin-Mechanismus in die durch BioAPI spezifizierte Architektur (BioAPI Framework) eingebunden werden.

Die von BioAPI 2.0 definierten Funktionen decken den kompletten Bereich biometrischer Operationen (Enrolment, Verifikation, Identifikation) ab und sind dennoch offen für neue Technologien. Es gibt im Standard keine Festlegung auf bestimmte Datenformate, Kodierungen oder biometrische Verfahren.

Die konkrete Realisierung der biometrischen Funktionalität erfolgt über die angebotenen Provider. Diese liegen als dynamische Bibliothek vor und werden zur Laufzeit in die Umgebung eingeladen. BioAPI 2.0 definiert verschiedene Klassen von BSPs wie beispielsweise BSPs zur Aufnahme biometrischer Daten und BSPs zum Vergleich. Für jede Klasse ist festgelegt, welche Funktionen durch die entsprechende dynamische Bibliothek eines BSPs zur Verfügung gestellt werden müssen.

Die von einem BioAPI 2.0 BSP angebotenen Funktionen befinden sich auf einer „High Level“ Ebene. Der Standard darf daher nicht als „Treiberschnittstelle zu biometrischen Sensoren“ angesehen werden. Für die Verwendung eines BioAPI 2.0 BSPs ist ein durch den Standard definiertes Framework erforderlich, welches die verschiedenen BSPs einbindet und verwaltet. secunet biomiddle enthält ein solches Framework und setzt damit eine wohldefinierte, offene, modulare und transparente Gesamtarchitektur um. Sie ermöglicht es, externe zu BioAPI 2.0 kompatible Komponenten unmittelbar und ohne Integrationsaufwand hinzuzufügen oder auszutauschen. Das bedeutet, dass beispielsweise im Echtbetrieb von einem Fingerabdruckscanner auf einen alternativen Anbieter umkonfiguriert werden kann.

2.3 Zugriff auf elektronische IDs

Mit der Einführung der elektronischen Reisepässe hat das Thema Identitätsprüfung im hoheitlichen Bereich eine enge Verbindung zu biometrischen Verfahren bekommen. Die biometrischen Merkmale des Inhabers sind auf den neuen

Ausweisdokumenten gespeichert und müssen für darauf basierende Identitätsprüfungen vom Dokument ausgelesen werden. Neben den Protokollen für den Zugriff über RFID und der Kommunikation mit dem Chip sind hierfür eine Reihe von ePass-spezifischen Sicherheitsmechanismen wie Basic Access Control oder Extended Access Control erforderlich. secunet biomiddle benutzt für den Zugriff auf den Pass die ePassport API, die im Golden Reader Tool des Bundesamtes für Sicherheit in der Informationstechnik (BSI) verwendet wird. Dieses gilt international als Referenzanwendung für das Auslesen von Reisepässen und wird von vielen Herstellern zum Nachweis der Interoperabilität eingesetzt.

3 Leistungsmerkmale von secunet biomiddle

3.1 Architektur von secunet biomiddle

Die Architektur von secunet biomiddle enthält vier verschiedene Module, die Funktionen eines jeweiligen Themengebietes zusammenfassen und zur Verfügung stellen.

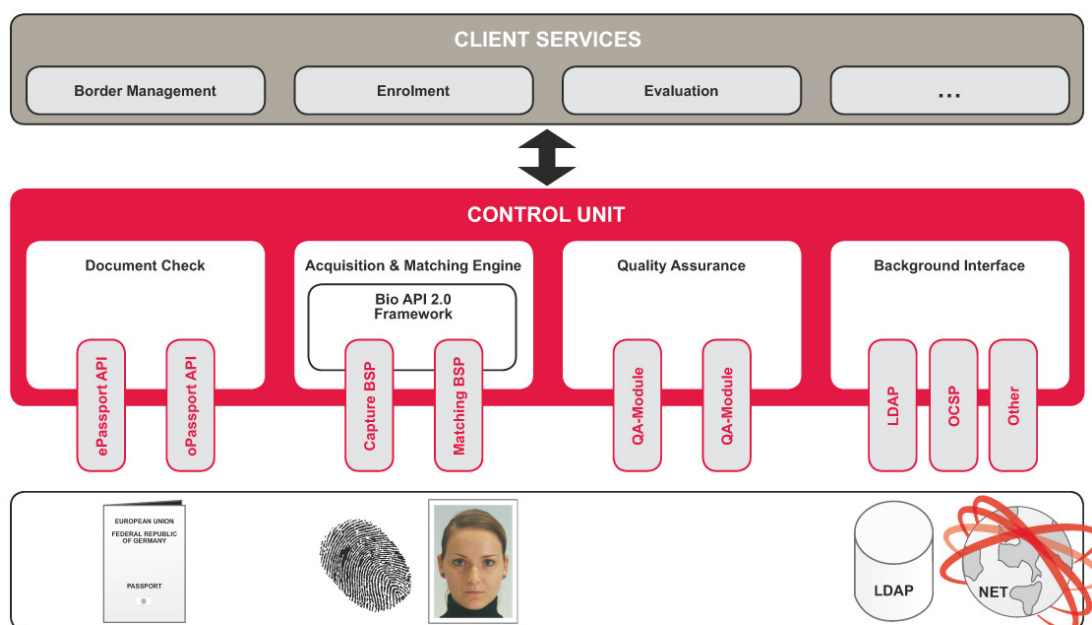


Abbildung 3-1: secunet biomiddle

Das **Document Check Modul** dient zum Auslesen und Überprüfen von Ausweisdokumenten. Für das Auslesen der elektronischen Inhalte ist die ePassport API als standardisierte Schnittstelle integriert. Sie unterstützt mit Basic Access Control (BAC), Active Authentication (AA) und Extended Access Control (EAC) alle existierenden Sicherheitsmechanismen elektronischer Ausweise. Als optische Daten können – je nach Leistungsfähigkeit des verwendeten Lesegeräts – Machine Readable Zone (MRZ), Infrarotbild (IR), ultraviolettes (UV) Bild, sichtbares Bild und zugeschnittenes Lichtbild gelesen werden.

Die **Acquisition & Matching Engine** ermöglicht einen standardisierten Zugriff zu allen biometrischen Sensoren und Vergleichsalgorithmen, die BioAPI 2.0-kompatibel sind und damit einen entsprechenden BSP bereitstellen. Auf deren Basis gestattet dieses Modul die Durchführung jeglicher biometrischer Operationen wie die Aufnahme eines Live-Bildes einer Person, das Enrolment, die Verifikation sowie die

Identifikation von Personen. Diese Funktionen werden generisch für die verschiedenen biometrischen Technologien wie beispielsweise Gesichts-, Fingerabdruck- oder Iriserkennung bereitgestellt.

Das **Quality Assurance Modul** prüft, ob biometrische Daten hinsichtlich ihrer Qualität für biometrische Vergleiche geeignet sind und/oder internationale Anforderungen (zum Beispiel ICAO-Anforderungen für Lichtbilder) erfüllen. Vergleichbar mit dem BioAPI-Ansatz werden dazu entsprechende Bewertungsalgorithmen über so genannte QA-Provider angebunden. secunet biomiddle kann dabei einen oder mehrere entsprechende QA-Provider anbinden.

Das **Background Interface Modul** dient zur Anbindung externer Systeme. Hierbei kann die Kommunikation mit den Hintergrundsystemen auf beliebige Art und Weise erfolgen, beispielsweise durch Protokolle wie SMTP, ODBC, HTTP oder SOAP. Zudem ist eine Kommunikation zu Datenbanken wie Oracle, MySQL, PostgreSQL oder MS SQL möglich. Auch hier wurde ein mit BioAPI vergleichbarer Ansatz gewählt, um die individuell erforderliche Funktionalität über Providermodule an secunet biomiddle anzubinden.

Als zentrale Instanz startet und initialisiert die **Control Unit** alle Module. Sie verwaltet die bereitgestellten Services und verarbeitet die Anfragen der Clients. Diese werden an die verantwortlichen Module weitergereicht. Zur Gewährleistung maximaler Flexibilität und Plattformunabhängigkeit basiert die Schnittstelle zu den Anwendungen auf SOAP (Simple Object Access Protocol).

3.2 Vorteile von Lösungen mit secunet biomiddle

Bei der Einführung von Biometrie muss sich ein Unternehmen sehr früh bezüglich verschiedenster Punkte festlegen. Wichtige Fragestellungen hierbei sind zum Beispiel, welches biometrische Verfahren benutzt werden soll, welche Scanner-Technologie die beste für den Einsatzzweck ist oder welcher Vergleichsalgorithmus die besten Ergebnisse erzielt. Aus oben genannten Gründen ist jedoch die Austauschbarkeit und Migrationsfähigkeit bei der Biometrie von hoher Bedeutung. Mit secunet biomiddle kann eine solche Flexibilität erreicht werden. Die Vorteile von secunet biomiddle werden nachfolgend zusammengefasst.

3.2.1 Modularität und Austauschbarkeit

secunet biomiddle ist in unterschiedliche Funktionsmodule unterteilt, welche auf dem biomiddle Server laufen. Die Verteilung der Funktionen auf verschiedene Module hat den Vorteil, dass Anforderungen von verschiedenen Einsatzszenarien erfüllt werden können. Hierbei sind verteilte Umgebungen durch die Modularität von secunet biomiddle kein Problem. Durch die Technologieoffenheit von secunet biomiddle können viele verschiedene Geräte angesprochen werden. Die Integration von Sensoren und Ausweislesern erfolgt durch eine standardisierte Schnittstelle.

Dies gewährleistet einen Austausch von Geräten unabhängig vom Hersteller. Auch das Betreiben von mehreren verschiedenen Geräten ist durch secunet biomiddle möglich. So können abhängig von der Umgebung immer die passenden Sensoren eingesetzt werden (zum Beispiel Innenbereich vs. Außenbereich). Zusätzlich besteht die Möglichkeit über secunet biomiddle multimodale biometrische Systeme (die kombinierte Verwendung verschiedener biometrischer Merkmale) zu realisieren. Dadurch kann die Erkennungsleistung eines Systems erheblich gesteigert werden.

3.2.2 Investitionssicherheit

Der Biometriemarkt wartet bereits seit Jahren mit kurzen Innovations- und Produktzyklen auf. Entsprechend sind bereits mittelfristig signifikante Leistungsverbesserungen, neue Technologien und ergänzende Methoden zur Fälschungssicherheit zu erwarten. Ebenso werden sich neue Anforderungen an biometrische Anwendungen ergeben. Durch die modulare Struktur und die Einhaltung der relevanten Standards kann eine auf secunet biomiddle basierende Anwendung mit vergleichsweise geringem Aufwand auf entsprechende Änderungen reagieren. Damit schafft der Einsatz dieser offenen Biometrieplattform Investitionssicherheit.

3.2.3 Integration von Biometrie als High-Level-Funktionalität

Die Entwicklung von Applikation bei der Verwendung von secunet biomiddle bewegt sich lediglich auf einem High Level. Das Ansprechen einzelner Sensoren oder Algorithmen entfällt bei der Implementierung und wird von secunet biomiddle übernommen. Die komplexen und gerätespezifischen Schnittstellen werden abstrahiert und deren Funktionen einheitlich und herstellerunabhängig der Anwendung zur Verfügung gestellt.

3.2.4 Technologiefreiheit auf Anwendungsebene

Anwendungen nutzen secunet biomiddle über eine SOAP-Schnittstelle. Dies hat zum einen den Vorteil, dass die Anwendung selbst in einer beliebigen Programmiersprache geschrieben sein kann. Dies vereinfacht die Integration von biometrischen Funktionen in bestehende Lösungen enorm. Zusätzlich ermöglicht dieser Ansatz, dass biometrische Funktionen als zentrale Dienste angeboten werden können. So ist zum Beispiel ein zentraler, ressourcenintensiver Vergleichsdienst realisierbar, der von vielen schlanken Anwendungen verwendet wird. Ebenso erlaubt der Ansatz, dass eine Anwendung mehrere, in der Infrastruktur verteilte biomiddle-Instanzen verwendet. Auf diese Weise lassen sich alle gewünschten Anforderungen hinsichtlich Performance, Skalierbarkeit oder Verfügbarkeit optimal umsetzen.

4 Fallstudien mit secunet biomiddle

secunet biomiddle ist für unterschiedliche Szenarien einsetzbar. Hier werden einige Fallstudien mit der Realisierung von secunet biomiddle dargestellt.

4.1 Ausweisstelle einer Organisation

4.1.1 Problemstellung

Die von einer Organisation ausgegebenen Ausweise sollen zukünftig auch biometrische Merkmale des Inhabers speichern. Für alle neuen Ausweise soll ein Foto des Gesichts gespeichert werden. Für Mitarbeiter, die Zutritt zu speziellen Sicherheitsbereichen haben, sollen zusätzlich die Fingerabdrücke gespeichert werden. Beim Enrolment sollen die biometrischen Daten qualitätsgesichert werden, um eine optimale Erkennungsleistung zu gewährleisten. Eine seit Jahren produktive Stelle zur Beantragung und Ausgabe der Ausweise muss um biometrische Verfahren erweitert werden.

4.1.2 Lösungsstrategie

Die existierende, in Java programmierte Anwendung zur Registrierung der Mitarbeiterdaten ist sehr komplex und kann aufgrund ihrer Integration mit dem Personaldatensystem und anderer Besonderheiten nicht durch eine „Standardanwendung“ ersetzt werden. Stattdessen soll die Aufnahme der biometrischen Daten in die Anwendung integriert werden. Nach der Aufnahme werden die biometrischen Daten an das Produktionssystem der Ausweise übertragen.

4.1.3 Umsetzung

Zur Umsetzung aller biometrierelevanten neuen Funktionen wird secunet biomiddle eingesetzt. Da die vorhandene Erfassungsanwendung in Java programmiert ist, wird für die SOAP-Implementierung Apache-Axis (<http://ws.apache.org/axis/>) verwendet. Aus der von secunet biomiddle bereitgestellten WSDL-Datei (Web Service Definition Language) werden mit Axis die notwendigen Java-Klassen automatisch generiert. Mit diesen Klassen können die von secunet biomiddle bereitgestellten Funktionen direkt angesprochen werden. Die Personalisierung der neuen biometrischen Ausweise übernimmt ein externes Produktionssystem. Hierfür werden die biometrischen Daten in das für die Speicherung auf dem Ausweis erforderliche Format kodiert und getrennt von den übrigen Daten in einer lokalen Datenbank bis

zum Zeitpunkt der Ausweiserstellung zwischengespeichert. Die Kodierung und Übertragung der Daten zum Produktionssystem erfolgt mit einem an secunet biomiddle angebindenen Background Interface Provider.

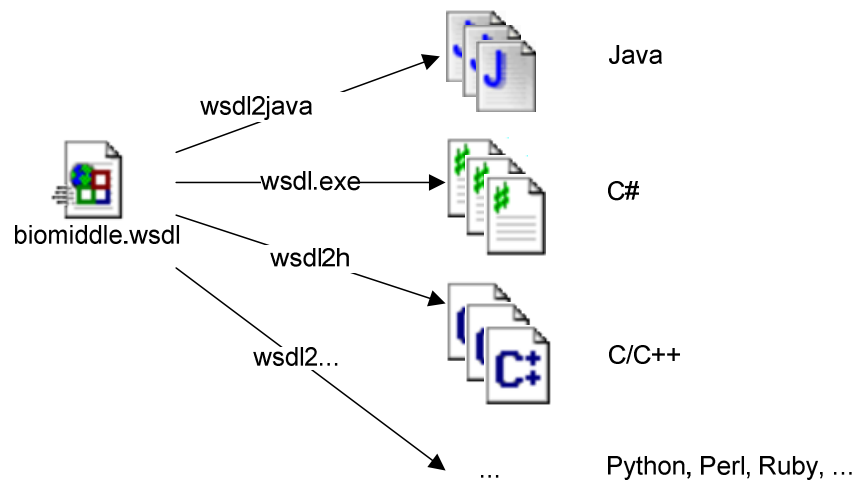


Abbildung 4-1: Generierung von Sourcecode

Auf dem System der Ausgabestelle wird secunet biomiddle installiert. Für das Enrolment sind dabei folgende Module an biomiddle angebunden:

- ein BSP zur Aufnahme eines Gesichtsbilds mittels einer Digitalkamera,
- ein BSP zur Aufnahme eines Fingerabdrucks mit einem Sensor,
- ein BSP zum Vergleich von Fingerabdrücken,
- ein Quality Provider zur Prüfung von Gesichtsbildern,
- ein Quality Provider zur Prüfung von Fingerabdrücken und
- ein Background Interface Provider zur Übermittlung der Daten an ein Produktionssystem.

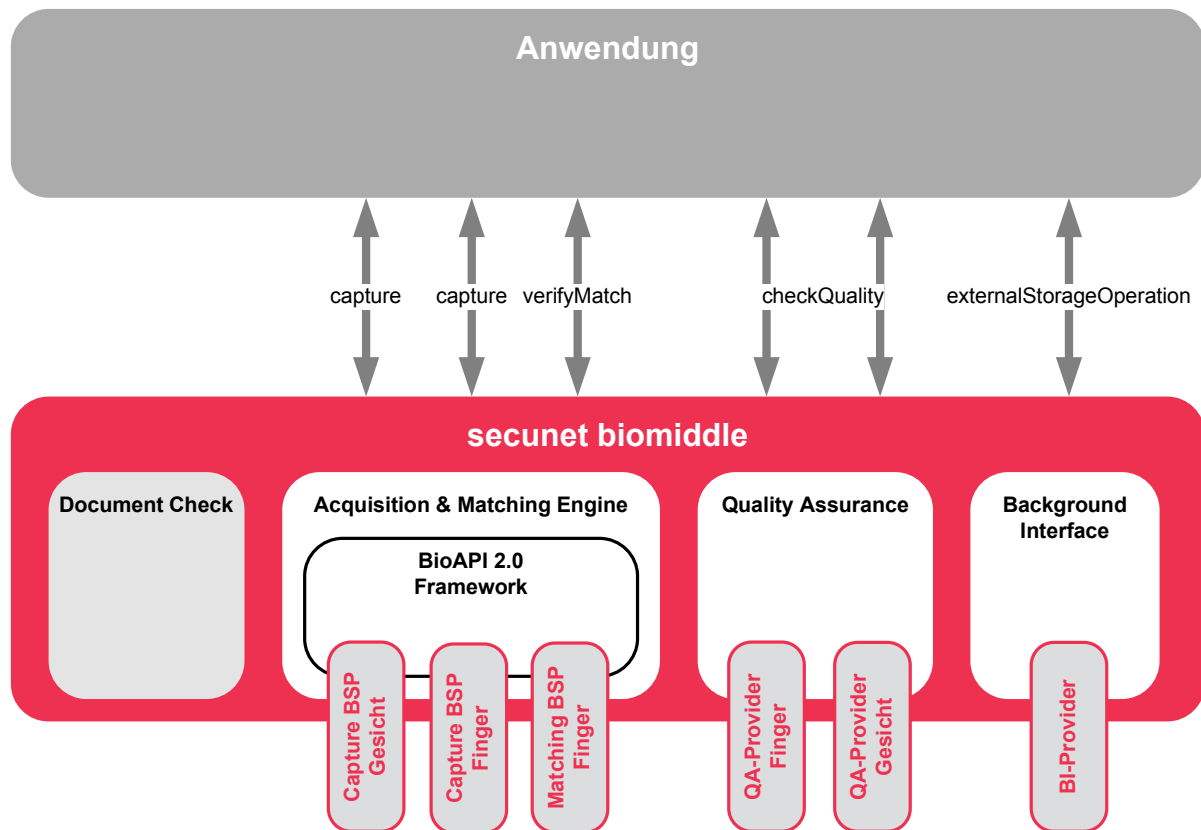


Abbildung 4-2: secunet biomiddle Setup für Ausweisstelle

Folgender Erfassungsablauf wird in die bestehende Anwendung integriert:

1. Nach Eingabe aller üblichen Daten des Ausweisinhabers wird dessen Gesicht mit einer Digitalkamera aufgenommen. Die Anwendung ruft dabei die biomiddle Funktion **capture** des BSPs auf. Dieser stellt zur Aufnahme des Bildes einen Dialog auf der Benutzeroberfläche mit dem Live-Bild der Kamera dar und löst die Aufnahme automatisch aus, sobald ein Gesicht erkannt wurde.
2. Die Anwendung übergibt das aufgenommene Bild der Qualitätsprüfung. Sie ruft hierfür die biomiddle Funktion **checkQuality** des zuständigen Providers auf. Ist das Ergebnis negativ, wird Schritt 1 wiederholt.
3. Handelt es sich um eine Person, für die auch Fingerabdrücke aufgenommen werden sollen, erfolgen drei Aufrufe der Funktion **capture** des Fingerabdruck BSPs, bei denen jedes Mal der gleiche Finger aufgenommen wird. Dies erfolgt, um eine bestmögliche Aufnahme des Fingers zu erreichen.
4. Nach der Aufnahme werden alle Fingerabdrücke miteinander verglichen und einzeln qualitätsgeprüft. Für den biometrischen Vergleich nutzt die Anwendung die Funktion **verifyMatch**. Anschließend bewertet sie die Ergebnisse und entscheidet sich für eine der drei Aufnahmen.

5. Um im Fall einer späteren Verletzung die Person weiterhin biometrisch authentifizieren zu können, werden die Schritte 3 und 4 mit einem zweiten Finger der anderen Hand noch einmal durchgeführt.
6. Nachdem die Erfassungsanwendung alle biometrischen Daten aufgenommen hat, überträgt sie diese an das Produktionssystem. Sie nutzt hierfür die biomiddle Funktion **externalStorageOperation**. Diese kodiert die Daten in das Zielformat und speichert sie im Produktionssystem.
7. Die Erstellung des Ausweises erfolgt unabhängig von der Erfassungsanwendung und secunet biomiddle.

4.2 Elektronische Sicherheitsprüfung eines Reisedokuments

4.2.1 Problemstellung

Die biometrischen Daten sind nach den internationalen Standards für Reisepässe auf dem Ausweis zugriffsgeschützt abgespeichert. Im Rahmen der Grenzkontrolle sollen diese Daten auf ihre Sicherheitseigenschaften (Echtheit, Unverfälschtheit) geprüft werden. Hierbei soll eine bestehende Grenzkontrollanwendung erweitert werden.

4.2.2 Lösungsstrategie

Die biometrischen Daten werden durch secunet biomiddle vom Ausweis gelesen, geprüft und einer Grenzkontrollanwendung zur Verfügung gestellt. Diese visualisiert das Prüfergebnis für den Kontrollbeamten.

4.2.3 Umsetzung

An der Grenzkontrollstation wird secunet biomiddle mit folgenden Komponenten installiert:

- Document Check Modul mit ePassportAPI und oPassportAPI für den eingesetzten Passleser und
- ein Background Interface Provider zur Anbindung an das nationale Zertifikatsverzeichnis (N-PKD).

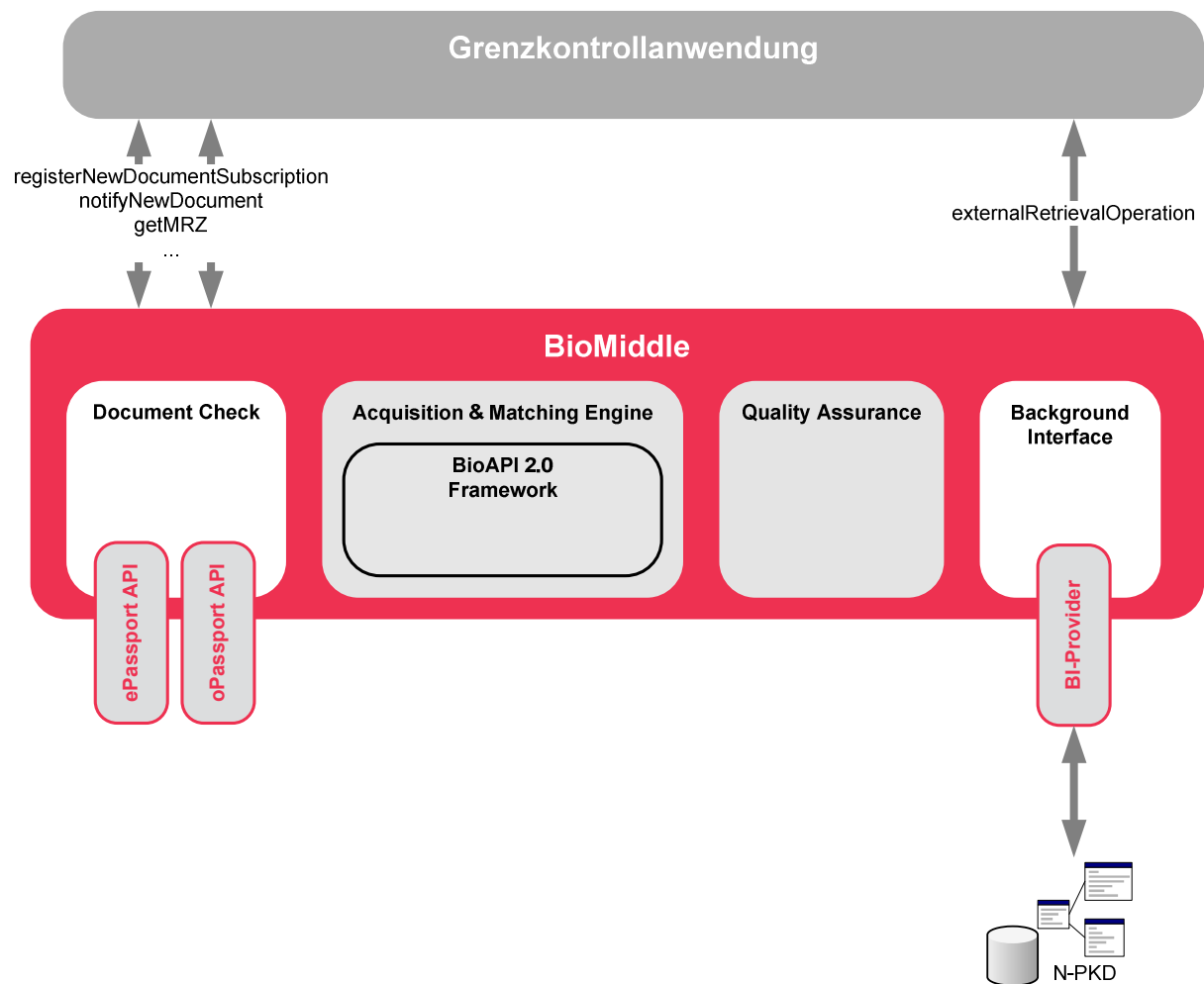


Abbildung 4-3: secunet biomiddle Setup für Grenzkontrolle

Die bestehende Grenzkontrollanwendung wird um die folgenden Prüfschritte erweitert:

1. Die Grenzkontrollanwendung registriert sich bei secunet biomiddle für eine Benachrichtigung, sobald ein neues Dokument auf den Passleser gelegt wurde. Sie ruft dazu die biomiddle Funktion **registerNewDocumentSubscription** auf und übergibt ihr die URL, auf der sie die Benachrichtigungen erhalten will. Anschließend öffnet sie den in der URL angegebenen Port und wartet auf Nachrichten.
2. Sobald ein neues Dokument aufgelegt wurde, benachrichtigt secunet biomiddle alle registrierten Anwendungen. Dabei wird die Nachricht **notifyNewDocument** verschickt.
3. Die Grenzkontrollanwendung fragt biomiddle nach der maschinenlesbaren Zeile des neu verfügbaren Ausweises. Sie ruft hierfür die Funktion **getMRZ** auf.

4. Falls ein elektronisches Dokument erkannt wird, liest die Anwendung die Datengruppen 1 und 2 aus. Hierfür nutzt sie die Funktionen **getElectronicPassportCount** und **getDatagroup**.
5. Um das für die Sicherheitsprüfung erforderliche CSCA-Zertifikat aus dem zentralen Verzeichnisdienst abzufragen, ermittelt die Grenzkontrollanwendung die Abfrageparameter mit der Funktion **getMissingCertInfo** und sendet diese über die Funktion **externalRetrievalOperation** an den BI-Provider. Als Ergebnis erhält die Anwendung das zugehörige CSCA-Zertifikat.
6. Die Prüfung der elektronischen Sicherheitseigenschaften erfolgt durch Aufrufen der Funktionen **checkDatagroup**, **checkPassiveAuth** und **getProtocolStatus**.
7. Alle Prüfergebnisse werden dem Kontrollbeamten visualisiert.

4.3 Automatisierte Grenzkontrolle (eGate)

4.3.1 Problemstellung

Mit Hilfe einer Grenzkontrollschleuse soll ein automatisierter Grenzübertritt des Reisenden realisiert werden. Dabei sollen alle Aspekte der regulären Kontrolle berücksichtigt und um einen biometrischen Vergleich des Gesichtsbilds ergänzt werden. Die Zielgruppe des Systems sind alle Bürger des Schengen-Raums.

4.3.2 Lösungsstrategie

Nach Auflage des Reisedokuments erfolgt eine Prüfung der optischen und elektronischen Sicherheitsmerkmale. Das Gesichtsbild wird durch secunet biomiddle vom Ausweis gelesen und einer Steueranwendung zur Verfügung gestellt. Diese nimmt über biomiddle ein Live-Bild des Gesichts auf und führt den biometrischen Vergleich durch. Parallel dazu erfolgt eine Abfrage des Fahndungsbestands. Sind alle Prüfungen erfolgreich, ist der Reisende zum Grenzübertritt berechtigt.

4.3.3 Umsetzung

Der Ablauf der Prüfschritte sowie die Übergabe der Informationen an einen Monitoring-Arbeitsplatz werden durch eine auf secunet biomiddle basierende Prozesssteuerung realisiert. In der Grenzkontrollschleuse wird secunet biomiddle mit folgenden Komponenten installiert:

- Document Check Modul mit ePassportAPI und oPassportAPI für den eingesetzten Passleser,

- ein BSP zur Aufnahme eines Gesichtsbilds durch die Erfassungseinheit der Schleuse,
- ein BSP zum Vergleich von Gesichtsbildern,
- ein Background Interface Provider zur Abfrage des Fahndungsbestands und
- ein Background Interface Provider zur Anbindung an das nationale Zertifikatsverzeichnis (N-PKD).

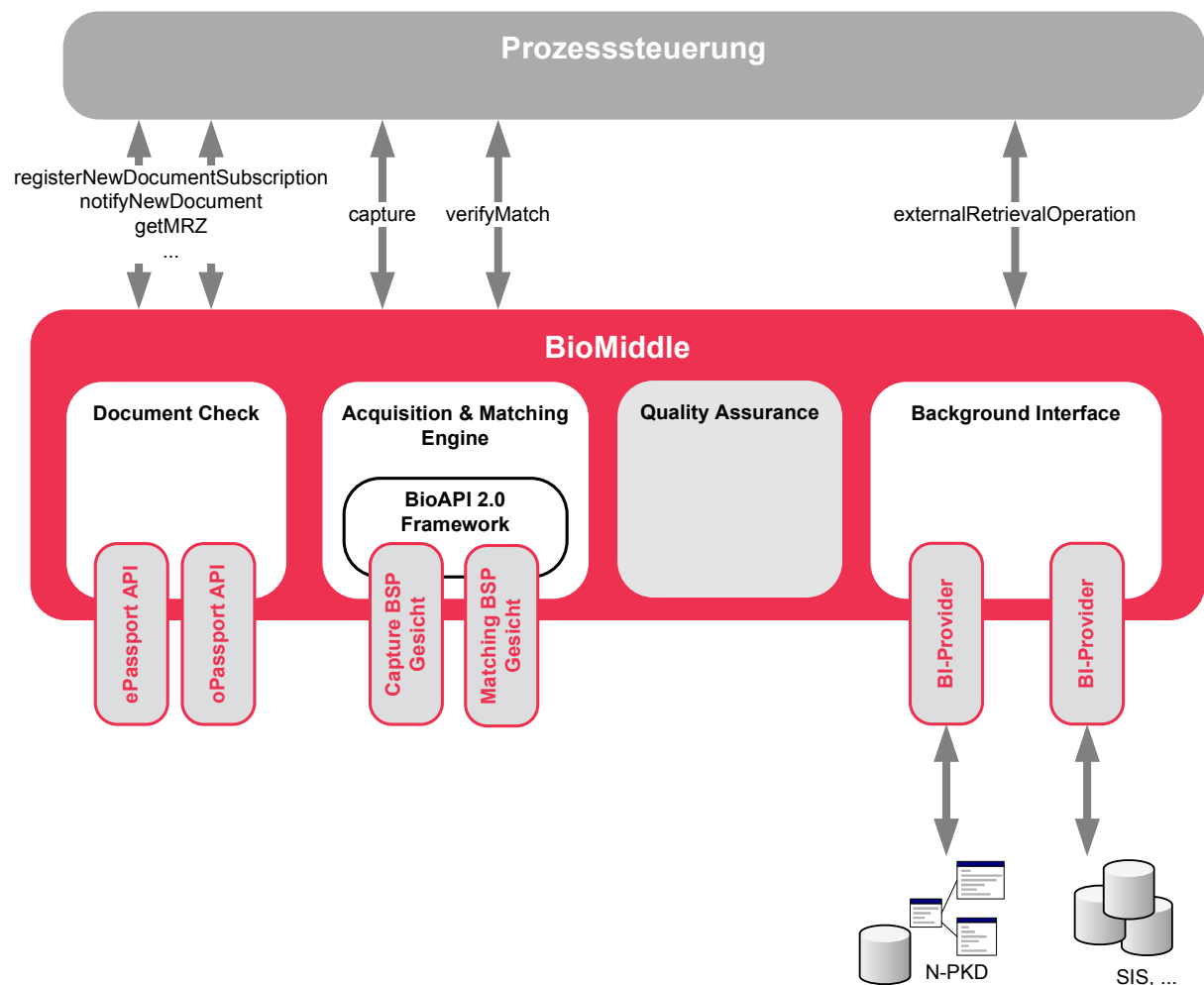


Abbildung 4-4: secunet biomiddle Setup für automatisierte Grenzkontrolle

Die Durchführung der automatisierten Grenzkontrolle hat dabei folgenden Ablauf:

1. Die Prozesssteuerung registriert sich bei secunet biomiddle und prüft nach Auflegen des Reisedokuments dessen elektronische Sicherheit wie bereits in Abschnitt 4.2 beschrieben.

2. Zusätzlich fragt die Prozesssteuerung das Ergebnis der Prüfung optischer Sicherheitsmerkmale ab. Hierzu ruft sie die Funktion **getOpticalSecurityStatus** auf.
3. Zur Abfrage des Fahnungsbestands übermittelt die Prozesssteuerung die Daten der MRZ mit der Funktion **externalRetrievalOperation** an den BI-Provider. Dieser führt die Abfragen durch und liefert das Ergebnis zurück.
4. Die Anwendung liest das Gesichtsbild vom Ausweis und nimmt gleichzeitig ein Live-Bild der Person auf. Sie benutzt dafür die biomiddle Funktionen **getElectronicImage** und **capture**.
5. Die biometrischen Daten übergibt die Anwendung mit der Funktion **verifyMatch** zum Vergleich und verarbeitet das Ergebnis.
6. Sind alle Prüfungen erfolgreich, öffnet die Prozesssteuerung die Tür der Grenzkontrollschleuse und lässt den Reisenden passieren.

4.4 Identifikation zum Zutritt in einen Sicherheitsbereich

4.4.1 Problemstellung

Ein Sicherheitsbereich eines Gebäudes soll mit einer biometrischen Zugangskontrolle ausgestattet werden. Als biometrisches Merkmal ist der Fingerabdruck vorgesehen. Die Referenzdaten sind in einem zentralen Berechtigungssystem gespeichert.

4.4.2 Lösungsstrategie

Die Zugangskontrolle wird durch eine zentrale Anwendung gesteuert. Diese verwendet secunet biomiddle für die Aufnahme des Fingerabdrucks und für die Identifikation der Person am zentralen Berechtigungssystem. Für die Identifikation gibt es grundsätzlich zwei Varianten zur Umsetzung:

1. Bietet das Berechtigungssystem eine Schnittstelle nach BioAPI 2.0 an, kann die Identifikation über einen BSP erfolgen.
2. Ist das Berechtigungssystem nicht BioAPI 2.0 kompatibel, kann eine Anbindung über das Background Interface von biomiddle erfolgen.

Im Folgenden wird die zweite Variante näher betrachtet.

4.4.3 Umsetzung

An secunet biomiddle werden die folgenden Komponenten angebunden:

- ein BSP zur Aufnahme eines Fingerabdrucks mit einem Sensor und
- ein Background Interface Provider zur Kommunikation mit dem zentralen Berechtigungssystem.

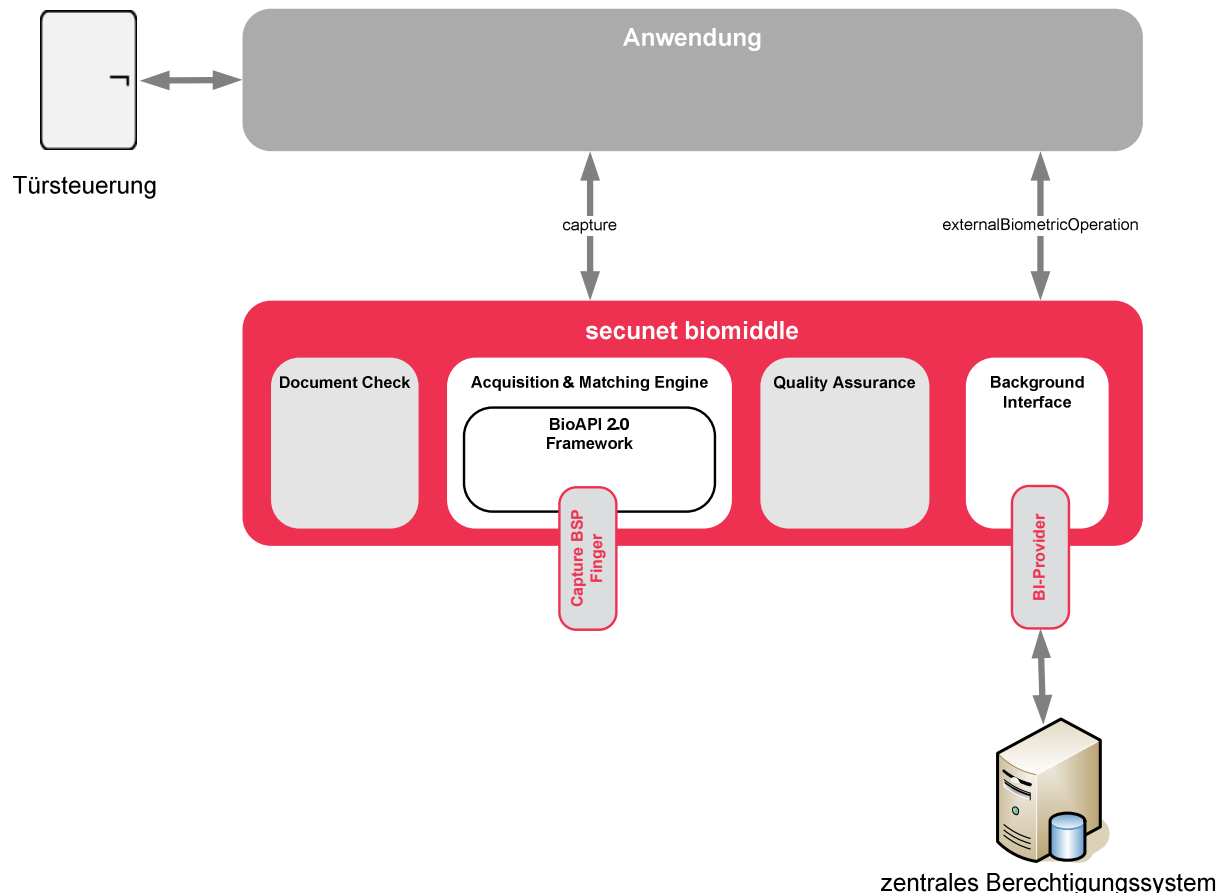


Abbildung 4-5: secunet biomiddle Setup für Zutrittskontrolle

Folgender Ablauf wird umgesetzt:

1. Die Kontrollanwendung nimmt einen Fingerabdruck auf. Sie verwendet dabei die Funktion **capture**.
2. Der aufgenommene Fingerabdruck wird an das zentrale Berechtigungssystem gesendet. Sie nutzt die Funktion **externalBiometricOperation** von secunet biomiddle. Das Ergebnis der Funktion ist die Antwort des Berechtigungssystems. Sie enthält, ob die Person identifiziert wurde und zum Zugang in den Sicherheitsbereich berechtigt ist.

3. Die Kontrollanwendung steuert die Zutrittsstür und lässt diese Person eintreten.

5 Leistungsmerkmale in der Übersicht

Leistungsmerkmal	Unterstützung
Document Check	
Unterstützung von PC/SC RFID Lesern	Ja
Unterstützung von Fullpage Lesern	Ja (div. Hersteller)
Bereitstellung MRZ	Ja
Optische Bilddaten	VIS, UV, IR, Crop
Elektronische Sicherheitsmechanismen	BAC, AA, CA, TA, EAC
Datenformate Gesichtsbild	DG2, ISO 19794-5, JPEG, JPEG2000, BMP, PNG, ...
Datenformate Fingerabdrücke	DG3, ISO 19794-2/4, JPEG, WSQ, BMP, PNG, ...
Acquisition & Matching Engine	
Aufnahme biometrischer Daten	Ja
Template-Generierung	Ja
Vergleich biometrischer Daten	Ja
Identifikation	Ja
Biometrische Merkmale	Beliebig (Gesicht, Finger, Iris, ...)
Datenformate	ISO 19794, WSQ, JPEG, JPEG2000, BMP, PNG, ...
Quality Assurance	
Qualitätsbewertung nach Schwellwert	Ja
Detaillierte Prüfergebnisse	Ja, in XML
Background Interface	

Speichern biometrischer Daten	Ja
Laden biometrischer Daten	Ja
Biometrische Operationen durch Drittsysteme	Ja
Status- und Gültigkeitsprüfung	Ja
Allgemeine Informationen	
Unterstützte Betriebssysteme	Windows XP, Windows Vista, Windows 7, Linux
Speicherbedarf	< 500KB
SSL-Unterstützung	Ja
Mögliche Programmiersprachen auf Anwendungsebene	C/C++, Java, C#, Perl, ...

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