Biometric identity verification for large-scale high-security apps

Face Verification SDK
The Face Verification SDK is designed for integration of facial authentication into enterprise and consumer applications for mobile devices and PCs. The simple API of the library component helps to implement solutions like payment, e-services and all other apps that need enhanced security through biometric face recognition, while keeping their overall size small for easy deployment to millions of users.

Different liveness detection functionalities are included to implement anti-spoofing mechanism with the possibility of configuring the balance between security and usability of the application.

Available on Android, iOS, Microsoft Windows, Mac OS X and Linux platforms.

- Compact library for deployment on mobile devices.
- Based on VeriLook technology with millions of deployments worldwide.
- Live face detection prevents spoofing.
- Android, iOS, Microsoft Windows, Mac OS X and Linux supported.
- Programming samples in multiple languages included.
- Reasonable prices, flexible licensing and free customer support.
Features and Capabilities

The Face Verification SDK is intended for developing applications which perform end-user identity verification in mass scale systems like:

- online banking and e-shops;
- government e-services;
- social networks and media sharing services.

The Face Verification SDK is based on the VeriLook algorithm, which provides advanced face localization, enrollment and matching using robust digital image processing algorithms based on deep neural networks. The SDK offers these features for large-scale identity verification systems:

- **Live face detection.** A conventional face identification system can be tricked by placing a photo in front of the camera. Face Verification SDK is able to prevent this kind of security breach by determining whether a face in a video stream is “live” or a photograph. The liveness detection can be performed in passive mode, when the engine evaluates certain facial features, and in active mode, when the engine evaluates user’s response to perform actions like blinking or head movements.

- **Face image quality determination.** A quality threshold can be used during face enrollment to ensure that only the best quality face template will be stored into database.

- **Tolerance to face position.** The Face Verification SDK allows head roll, pitch and yaw variation up to 15 degrees in each direction from the frontal position.

- **Multiple samples of the same face.** Biometric template record can contain multiple face samples belonging to the same person. These samples can be enrolled from different sources and at different times, thus allowing improvement in matching quality. For example a person might be enrolled with and without beard or mustache, etc.

- **Features generalization mode.** This mode generates the collection of the generalized face features from several images of the same subject. Then, each face image is processed, features are extracted, and the collections of features are analyzed and combined into a single generalized features collection, which is written to the database. This way, the enrolled feature template is more reliable and the face recognition quality increases considerably.
### SDK Contents

Face Verification SDK is intended for developers who want to use biometric facial verification in their applications or projects. The SDK allows rapid development of services and applications using functions from the Face Verification library for **Android**, **iOS**, **Microsoft Windows**, **Mac OS X** and **Linux** platforms. Developers provide video streams from cameras as data input, and have complete control over the output data; therefore Face Verification functions can be used with any user interface.

Face Verification SDK distribution package contains these components:

- Server components for Windows and Linux with REST API
- Face Verification component
- 1000 Person Registration Transactions (PRT) licenses
- 1000 Liveness + ICAO Transactions (LIT) licenses
- Java programming samples for Android platform
- Objective C programming samples for iOS platform
- Face Verification SDK documentation
Technical Information and Specifications

The Face Verification SDK provides certain capabilities for facial recognition applications, including high-level API for all operations and face liveness check. There are also certain requirements for facial image and posture.

General specifications

The SDK architecture requires to account the performed operations on integrator’s or end-user’s server:

- Integrators should ensure that encrypted connection is used for communications with the server.
- No face images or templates are sent to the server during all operations, which require communication with the server. The biometric data is kept on the client-side, only transaction accounting information is sent to and received from the server.

The following operations are available via the high-level API:

- **Face template creation** – a face is captured from camera and the face template is extracted for further usage in the face verification operation.
  - The server returns proprietary encrypted data as a result of an enrolment transaction that has been completed successfully.
  - Face liveness can be optionally checked during this operation. ICAO compliance check can be optionally used to strengthen the liveness check.
  - A token image of the enrolled face in accordance with ISO 19794-5 criteria can be optionally generated.
  - The template may be saved to any storage (database, file etc) together with custom metainformation (like person’s name etc.). Note that the storage functionality is not part of the Face Verification SDK, although the programming samples include an example of such implementation).

- **Face verification** – a face is captured from the camera and is verified against the face template which was created during the face template creation operation.
  - Face liveness can be optionally checked during this operation. ICAO compliance check can be optionally used to strengthen the liveness check.

- **Template import** – a face template, which was created with VeriLook algorithm, can be imported into the application, based on Face Verification SDK. Later this template can be used for face verification operation in the same way, as the native templates from the face template creation operation.

- **Liveness check** – this operation perform only liveness check of the provided face and only returns the result of the check. See the recommendations for the liveness check on the next page.
  - If the liveness check succeed, a token image of the enrolled face in accordance with ISO 19794-5 criteria can be optionally generated.
  - ICAO compliance check can be optionally used to strengthen the liveness check.

*continued on the next page*
Basic Recommendations for facial image and posture

The face recognition accuracy heavily depends on the quality of a face image. **Image quality during enrollment is important**, as it influences the quality of the face template.

- **32 pixels is the recommended minimal distance between eyes** for a face on a video stream to perform face template extraction reliably. **64 pixels or more** recommended for better face recognition results. Note that this distance should be native, not achieved by resizing the video frames.

- **Several face enrollments** are recommended for better facial template quality which results in improvement of recognition quality and reliability.

- **Additional enrollments** may be needed when **facial hair** style changes, especially when beard or mustache is grown or shaved off.

- The face recognition engine is intended for usage with near-frontal face images and has certain tolerance to face posture:
  - head roll (tilt) – ±15 degrees;
  - head pitch (nod) – ±15 degrees from frontal position.
  - head yaw (bobble) – ±15 degrees from frontal position.

Live Face Detection

A live video stream from a camera is required for face liveness check:

- When the liveness check is enabled, it is performed by the face engine before feature extraction. If the face in the stream **fails** to qualify as “live”, the features are **not extracted**.

- Only **one face should be visible** in these frames.

- Optionally, **ICAO compliance** check can be used to **strengthen** the liveness check.

- Users can enable these liveness check modes:
  - **Active** – the engine requests the user to perform certain actions like blinking or moving one’s head.
    - 5 frames per second or better frame rate required.
    - This mode can work with both colored and grayscale images.
    - This mode requires the user to perform all requested actions to pass the liveness check.
  
  - **Passive** – the engine analyzes certain facial features while the user stays still in front of the camera for a short period of time.
    - Colored images are required for this mode.
    - 10 frames per second or better frame rate required.
    - Better score is achieved when users do not move at all.
  
  - **Passive then active** – the engine first tries the passive liveness check, and if it fails, tries the active check. This mode requires colored images.
  
  - **Simple** – the engine requires user to turn head from side to side while looking at camera.
    - 5 frames per second or better frame rate recommended.
    - This mode can work with both colored and grayscale images.
  
  - **Custom** – the engine requires user to turn head from side to side while looking at camera.
    - 5 frames per second or better frame rate required.
    - This mode can work with both colored and grayscale images.
    - This mode requires the user to perform all requested actions to pass the liveness check.
System requirements

There are specific requirements for each platform which will run applications based on the Face Verification SDK.

Microsoft Windows platform requirements

- Microsoft Windows 7 / 8 / 10, 32-bit or 64-bit.
- PC or laptop with x86 (32-bit) or x86-64 (64-bit) compatible processors.
  - 2 GHz or better processor is recommended.
  - SSE2 support is required. Processors that do not support SSE2 cannot run the Face Verification SDK algorithm. Please check if a particular processor model supports SSE2 instruction set.
- At least 512 MB of free RAM should be available for the application.
- A camera or webcam which is accessible using DirectShow interface.
- Microsoft .NET framework 4.5 or newer (for .NET components usage).
- One of following development environments for application development:
  - Microsoft Visual Studio 2012 or newer (for application development under C/C++, C#, Visual Basic .Net)
  - Sun Java 1.7 SDK or later.
- Internet connection required for managing the Face Verification transaction licenses

Android platform requirements

- A smartphone or tablet that is running Android 4.4 (API level 19) OS or newer.
  - API level 22 is the recommended target for code compilation.
  - If you have a custom Android-based device or development board, contact us to find out if it is supported.
- ARM-based 1.5 GHz processor recommended for face processing in the specified time. Slower processors may be also used, but the face processing will take longer time.
- At least 256 MB of free RAM should be available for the application.
- 30 MB of free storage space (built-in flash or external memory card) required for the component deployment for each separate application.
- Any smartphone’s or tablet’s built-in camera which is supported by Android OS. The camera should have at least 0.3 MegaPixel (640 x 480 pixels) resolution.
- PC-side development environment requirements:
  - Java SE JDK 6 (or higher)
  - Eclipse Indigo (3.7) IDE
  - Android development environment (at least API level 19 required)
  - Gradle 4.6 build automation system or newer
  - Internet connection for managing the Face Verification transaction licenses
ios platform requirements

- One of the following devices, running iOS 8.0 or newer:
  - iPhone 5S or newer iPhone.
  - iPad 2 or newer iPad, including iPad Mini and iPad Air models.

- At least **256 MB of free RAM** should be available for the application.
- **30 MB of free storage** space (built-in flash or external memory card) required for the component deployment for each separate application.

- **Development environment** requirements:
  - a Mac running Mac OS X 10.10.x or newer.
  - Xcode 6.4 or newer.

Mac OS X platform requirements

- A Mac running **Mac OS X 10.7.x** or newer. 2 GHz or better processor is recommended.

- At least **512 MB of free RAM** should be available for the application.

- A **camera or webcam** which is accessible using **GStreamer** interface.

- Specific requirements for **application development**:
  - XCode 4.3 or newer
  - GNU Make 3.81 or newer (to build samples and tutorials development)
  - Sun Java 1.7 SDK or later.

Linux x86 / x86-64 platform requirements

- **Linux 3.10 kernel** or newer is required.

- PC or laptop with **x86 (32-bit)** or **x86-64 (64-bit)** compatible processors.
  - 2 GHz or better processor is recommended.
  - **SSE2 support is required**. Processors that do not support SSE2 cannot run the Face Verification SDK algorithm. Please check if a particular processor model supports SSE2 instruction set.

- At least **5128 MB of free RAM** should be available for the application.

- A **camera or webcam** which is accessible using **GStreamer** interface.

- glibc 2.13 library or newer

- GStreamer 1.2.2 or newer with gst-plugin-base and gst-plugin-good is required for face capture using camera/webcam or rtsp video. GStreamer 1.4.x or newer is recommended.

- Specific requirements for **application development**:
  - GCC-4.4.x or newer
  - GNU Make 3.81 or newer (to build samples and tutorials development)
  - Sun Java 1.7 SDK or later.
Reliability Tests

We present the testing results to show the Face Verification SDK algorithm template matching reliability evaluations with the following public datasets:

- NIST Special Database 32 - Multiple Encounter Dataset (MEDS-II). - [https://www.nist.gov/itl/iad/ig/sd32.cfm](https://www.nist.gov/itl/iad/ig/sd32.cfm)
  - All full-profile face images from the dataset were removed because they are not supported by VeriLook SDK. This resulted in 1,216 images of 518 persons.

- University of Massachusetts Labeled Faces in the Wild (LFW). - [https://vis-www.cs.umass.edu/lfw/](https://vis-www.cs.umass.edu/lfw/)
  - According to the original protocol, only 6,000 pairs (3,000 genuine and 3,000 impostor) should be used to report the results. But recent algorithms are “very close to the maximum achievable by a perfect classifier” [https://people.cs.umass.edu/~elm/papers/LFW_survey.pdf](https://people.cs.umass.edu/~elm/papers/LFW_survey.pdf). Instead, as Neurotechnology algorithms were not trained on any image from this dataset, verification results on matching each pair of all 13,233 face images of 5,729 persons were chosen to be reported.
  - All identity mistakes, which had been mentioned on the LFW website, were fixed. Also, several not mentioned issues were fixed.
  - Some images from the LFW dataset contained multiple faces. The correct faces for assigned identities were chosen manually to solve these ambiguities.

Two experiments were performed with each dataset:

- **Experiment 1** maximized matching accuracy. Face Verification 11.0 SDK algorithm reliability in this test is shown on the ROC charts as blue curves.

- **Experiment 2** maximized matching speed. Face Verification 11.0 SDK algorithm reliability in this test is shown on the ROC charts as red curves.

Receiver operation characteristic (ROC) curves are usually used to demonstrate the recognition quality of an algorithm. ROC curves show the dependence of false rejection rate (FRR) on the false acceptance rate (FAR). Equal error rate (EER) is the rate at which both FAR and FRR are equal. The ROC charts and the testing results are available on the next pages.

| Face Verification 11.0 SDK algorithm testing results with face images from public datasets |
|----------------------------------|--|--|
|                                 | MEDS-II | LFW |
|                                 | Exp. 1 | Exp. 2 | Exp. 1 | Exp. 2 |
| Image count                     | 1216   |       | 13233  |
| Subject count                   | 518    |       | 5729   |
| Session count                   | 1 - 18 |       | 1 - 530|
| Image size (pixels)             | variable | 250 x 250 |
| Template size (bytes)           | 7128   | 5066  | 7128   | 5066  |
| EER                             | 0.9247% | 1.0550% | 0.6135% | 0.9895% |
| FRR at 0.1% FAR                 | 2.1770% | 3.8100% | 2.2920% | 5.2150% |
| FRR at 0.01% FAR                | 5.9860% | 10.1100% | 7.5900% | 14.6700% |
| FRR at 0.001% FAR               | 15.1900% | 16.2400% | 17.9700% | 29.3900% |
Face Verification SDK

Face Verification 11.0 SDK matching engine with face templates from NIST Multiple Encounter Dataset (MEDS-I):
- Experiment 1, maximized matching accuracy scenario
- Experiment 2, maximized matching speed scenario

Face Verification 11.0 SDK matching engine with face templates from the University of Massachusetts Labeled Faces in the Wild (LFW) dataset:
- Experiment 1, maximized matching accuracy scenario
- Experiment 2, maximized matching speed scenario
Face Verification Trial SDK and Related Products

The Face Verification SDK Trial is available for downloading at [www.neurotechnology.com/download.html](http://www.neurotechnology.com/download.html).

These products are related to the Face Verification SDK:

- **VeriLook SDK** – for developing systems that perform facial identification. The Face Verification SDK is based on the VeriLook technology and allows to import face templates which were created with VeriLook SDK.

- **MegaMatcher On Card SDK** – a product for fingerprint, iris and face matching on smart cards.

- **MegaMatcher Automated Biometric Identification System (ABIS)** – a turnkey multi-biometric solution for national-scale identification projects. Available as on-premise solution and as cloud service.

- **MegaMatcher SDK** – for development of AFIS or multi-biometric face, fingerprint, iris, voiceprint and palm print identification products.

- **Free Fingerprint Verification SDK** – a freeware SDK intended for adding fingerprint verification functionality into various applications.
Licensing Face Verification SDK

The Face Verification SDK licensing model is based on transactions that are accounted directly on the integrator or end-user server(s). The server does not use any biometric data for the accounting, only proprietary encrypted data is used.

**Product Development**

An integrator should obtain Face Verification 11.0 SDK (€ 1,390) to develop services or end-user products based on the Face Verification technology. The SDK needs to be purchased just once and may be used for all projects and by all the developers within the integrator’s company. The Face Verification component can be used on all computers or devices within the integrator’s company for the development process.

Face Verification 11.0 SDK includes:

- 1000 PRT (Person Registration Transaction) licenses;
- 1000 LIT (Liveness + ICAO transaction) licenses;
- 3 dongles for license management.

Integrators can obtain additional transaction licenses if those are required for the development process.

**Product Deployment**

To deploy their developed services and/or products, an integrator need to obtain the required amount of PRTs and LITs licenses to be assigned to the specific set of dongles used for the deployment. The Face Verification component can be installed on every computer or device, which runs the integrator’s product, based on the Face Verification SDK.

Integrators can purchase additional transaction licenses to add to the existing dongle counters, if required, at anytime.

*continued on the next page*
Transaction Licenses and their Activation

The transaction licenses are copy-protected and they can be installed just on a specific set of dongles purchased by the customer.

The transactions are accounted directly on the integrator or end-user servers. It is necessary to plug in at least two USB dongles, which store both the total number of transactions purchased by the integrator and the number of transaction that were already used, to a server. The server component should have constant access to the connected dongles.

A license for a particular transaction is activated each time, when an application or a service, based on Face Verification SDK, requests the server for a permission to perform this transaction. Each transaction license allows to perform only one particular transaction.

The Face Verification SDK handles two types of transactions:

- **PRT – Person Registration Transaction:**
  - The transaction is accounted on the server component every time when a person is enrolled on a particular mobile device or PC, and communication with the server component happens.
  - The enrolled face can be verified an unlimited amount of times with the client component of Face Verification. The verification process can happen off-line.
  - Liveness check can be optionally performed during the verification of a previously enrolled face. In this case the liveness check is not accounted as a transaction (LIT).

- **LIT (Liveness + ICAO Transaction):**
  - The transaction is accounted on the server component every time when a stand-alone liveness check operation is performed and not as a part of a verification operation as described above.
  - The accounted LIT are just the ones for which the liveness criteria succeeds. In case the liveness criteria is not passed, the LIT is not accounted by the server.

Licenses Validity

All SDK and component licenses are perpetual and do not have expiration. There are no annual fee or any other fees except license purchasing fee. Once used, a transaction license can’t be reverted back for another usage.

Licensing Agreement

The Licensing Agreement (https://neurotechnology.com/face_verification_sdk_sla.html) contains all licensing terms and conditions.

Note that you unambiguously accept this agreement by placing an order using Neurotechnology online ordering service or by email or other means of communications. Please read the agreement before making an order.

Enterprise License

The Face Verification SDK enterprise license allows to use the Face Verification component, without dongles copy protection, in end-user products or services for a specific territory, market segment or project. Specific pricing and licensing conditions would be included in the licensing agreement.

For more information please contact us.
Prices

- The prices are effective January 3, 2019. The prices may change in the future, so please download and review the latest version of the brochure before making an order.
- Prices do not include local import duties or taxes.
- Product shipping costs depend on delivery country
- Customers with Solution Partner status are eligible for product discounts.

Face Verification SDK and transaction licenses

<table>
<thead>
<tr>
<th>Face Verification SDK</th>
<th>€ 1,390.00</th>
</tr>
</thead>
<tbody>
<tr>
<td>Face Verification 11.0 SDK package, which includes:</td>
<td></td>
</tr>
<tr>
<td>1000 PRT licenses;</td>
<td></td>
</tr>
<tr>
<td>1000 LIT licenses;</td>
<td></td>
</tr>
<tr>
<td>3 dongles for license management.</td>
<td></td>
</tr>
<tr>
<td>Larger quantities of transaction licenses can be also ordered – see the prices below)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Additional transaction licenses for Face Verification 11.0 SDK</th>
<th>PRT licenses</th>
<th>LIT licenses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quantity</td>
<td>PRT licenses</td>
<td>LIT licenses</td>
</tr>
<tr>
<td>1000 - 1999</td>
<td>€ 0.69</td>
<td>€ 0.35</td>
</tr>
<tr>
<td>2000 - 3999</td>
<td>€ 0.53</td>
<td>€ 0.27</td>
</tr>
<tr>
<td>4000 - 7999</td>
<td>€ 0.41</td>
<td>€ 0.20</td>
</tr>
<tr>
<td>8000 - 15999</td>
<td>€ 0.32</td>
<td>€ 0.16</td>
</tr>
<tr>
<td>16000 - 31999</td>
<td>€ 0.24</td>
<td>€ 0.12</td>
</tr>
<tr>
<td>32000 - 63999</td>
<td>€ 0.19</td>
<td>€ 0.10</td>
</tr>
<tr>
<td>64000 - 127999</td>
<td>€ 0.14</td>
<td>€ 0.07</td>
</tr>
<tr>
<td>128000 - 255999</td>
<td>€ 0.11</td>
<td>€ 0.05</td>
</tr>
<tr>
<td>256000 - 511999</td>
<td>€ 0.08</td>
<td>€ 0.04</td>
</tr>
<tr>
<td>512000 - 999999</td>
<td>€ 0.06</td>
<td>€ 0.03</td>
</tr>
<tr>
<td>1000000 and more</td>
<td>Please contact us for more information</td>
<td></td>
</tr>
</tbody>
</table>

Notes:
1. The minimal number of specific transaction licenses which can be purchased for is 1000 licenses.
2. Quantity discounts are applied for the current order and do not accumulate over time.

The Face Verification SDK and related products can be ordered:
- online, at www.neurotechnology.com/cgi-bin/order.cgi
- via a local Neurotechnology distributor; the list of distributors is available at www.neurotechnology.com/distributors.html