Biometric identity verification for large-scale high-security apps

Face Verification SDK
Face Verification SDK

Biometric identity verification for large-scale high-security applications

Document updated on October 29, 2019

CONTENTS
Features and capabilities .................................................. 3
SDK contents ................................................................. 4
Supported cameras ......................................................... 5
Technical information and specifications ............................... 6
System requirements ....................................................... 8
Face Verification Trial SDK and related products ..................... 10
Licensing Face Verification SDK ......................................... 11
Prices ............................................................................. 13

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.

- Compact library for deployment on mobile devices.
- Based on VeriLook technology with millions of deployments worldwide.
- Simple, high-level API.
- Privacy and security.
- Live face detection prevents spoofing.
- Android, iOS, Microsoft Windows, macOS 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:

- **Simple, high-level API.** The API provides operations for creating face templates from camera or still image, face verification against a specific previously created face template, importing face templates which were created with VeriLook algorithm, as well as performing face liveness check.

- **Privacy and security.** The face images and biometric templates are kept on the client-side and do not leave the end-user device. The face images are required only for template creation and face liveness detection, thus they can be disposed just after performing these operations.

- **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 during face detection and up to 45 degrees in each direction during face tracking.
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, macOS 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
**Supported Cameras**

These cameras are supported by the Face Verification SDK:

- Any **webcam** or camera that is accessible using:
  - **DirectShow**, **Windows Media** or **Media Foundation** interfaces for Microsoft Windows platform.
  - **GStreamer** interface for Linux or Mac platforms.

- Any built-in **smartphone** or **tablet** camera that is supported by **iOS** or **Android** OS. The camera should have at least 0.3 MegaPixel (640 x 480 pixels) resolution.

- Cameras, which can operate in **near-infrared** spectrum, can be used for image capture. The Face Verification SDK algorithm is able to match faces, captured in near-infrared spectrum, against faces, captured in visible light.

- These advanced cameras are supported:
  - Akiyama Akys-10 Biometric Camera
  - CMITech EMX-30 – face & iris camera (Microsoft Windows only)
  - Iris ID iCAM TD100 – face & iris camera (Microsoft Windows only)
  - VistaFA2 / VistaFA2E / VistaEY2 face & iris cameras (Microsoft Windows only)

- These models of **still cameras** are supported:
  - Canon EOS family still cameras (Microsoft Windows only; the supported camera models are EOS M50, EOS 200D, EOS 4000D, EOS M100, EOS 6D Mark II, EOS 200D, EOS 77D, EOS 80D, EOS M6, EOS M5, EOS 5D Mark IV, EOS-1D X Mark II, EOS 80D, EOS 1300D, EOS M10, EOS 5DS, EOS 5DS R, EOS 760D, EOS 750D, EOS 7D Mark II)
  - Nikon DSLR still cameras (Microsoft Windows only; a specific camera model should support video capture)
  - Fujifilm X-T2 still camera (Microsoft Windows only)

- Integrators can also write **plug-ins to support their cameras** using the plug-in framework provided with the Device Manager from the Face Verification SDK.

Simultaneous capture from multiple cameras is possible.
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.
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 **x86-64 (64-bit)** compatible processors.
  - 2 GHz or better processor is recommended.
  - x86 (32-bit) processors can still be used, but the algorithm will not provide the specified performance.
  - **AVX2 support is highly recommended.** Processors that do not support AVX2 will still run the Face Verification SDK algorithm, but in a mode, which will not provide the specified performance. Most modern processors support this instruction set, but please check if a particular processor model supports it.
- 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.
- 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 11.0 or newer:
  - iPhone 5S or newer iPhone.
  - iPad Air or newer iPad models.
- At least 256 MB of free RAM should be available for the application.
- Development environment requirements:
  - a Mac running macOS 10.12.6 or newer.
  - Xcode 9.x or newer.

macOS platform requirements

- A Mac running macOS 10.12.6 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 6.x or newer
  - GStreamer 1.10.x or newer with gst-plugin-base and gst-plugin-good is required for face capture using camera/webcam or rtsp video.
  - GNU Make 3.81 or newer (to build samples and tutorials development)
  - Sun Java 1.8 SDK or later.

Linux x86-64 platform requirements

- Linux 3.10 kernel or newer is required.
- PC or laptop with x86-64 (64-bit) compatible processors.
  - 2 GHz or better processor is recommended.
  - x86 (32-bit) processors can still be used, but the algorithm will not provide the specified performance.
  - AVX2 support is highly recommended. Processors that do not support AVX2 will still run the Face Verification SDK algorithm, but in a mode, which will not provide the specified performance. Most modern processors support this instruction set, but please check if a particular processor model supports it.
- At least 512 MB of free RAM should be available for the application.
- A camera or webcam which is accessible using GStreamer interface.
- glibc 2.17 library or newer
- GStreamer 1.10.x or newer with gst-plugin-base and gst-plugin-good is required for face capture using camera/webcam or rtsp video.
- Specific requirements for application development:
  - GCC-4.8 or newer
  - GNU Make 3.81 or newer (to build samples and tutorials development)
  - Sun Java 1.8 SDK or later.
Face Verification Trial SDK and Related Products

The Face Verification SDK Trial is available for downloading at 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 11.2 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 11.2 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 11.2 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 11.2 SDK</th>
<th>PRT licenses</th>
<th>LIT licenses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quantity</td>
<td>1000 - 1999</td>
<td>€ 0.69</td>
</tr>
<tr>
<td></td>
<td>2000 - 3999</td>
<td>€ 0.53</td>
</tr>
<tr>
<td></td>
<td>4000 - 7999</td>
<td>€ 0.41</td>
</tr>
<tr>
<td></td>
<td>8000 - 15999</td>
<td>€ 0.32</td>
</tr>
<tr>
<td></td>
<td>16000 - 31999</td>
<td>€ 0.24</td>
</tr>
<tr>
<td></td>
<td>32000 - 63999</td>
<td>€ 0.19</td>
</tr>
<tr>
<td></td>
<td>64000 - 127999</td>
<td>€ 0.14</td>
</tr>
<tr>
<td></td>
<td>128000 - 255999</td>
<td>€ 0.11</td>
</tr>
<tr>
<td></td>
<td>256000 - 511999</td>
<td>€ 0.08</td>
</tr>
<tr>
<td></td>
<td>512000 - 999999</td>
<td>€ 0.06</td>
</tr>
<tr>
<td></td>
<td>1000000 and more</td>
<td>Please contact us for more information</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