

Control iD

iDFace

Facial Identification
Features and Benefits



iDFace

Facial Identification Features and Benefits

Contents

1. What is iDFace?	3
2. In what configurations can iDFace be used?	3
2.1. Standalone	4
2.2. Embedded Web Server	4
2.3. OEM integration	4
2.4. iDSecure Cloud	4
2.5. API integration	5
3. What type of Personal Identifiable Information (PII) is stored by iDFace?	5
3.1. Default	5
3.2. Template only	5
3.3. Template on card	5
4. What is a biometric template?	6
5. Does iDFace support encryption for data in transit?	6
6. What methods are used to authenticate users accessing iDFace?	6
7. What type of logs does iDFace offer?	6
8. Is there video recording when authentications take place?	6
9. What is the fallback if a user cannot/does not want to use facial identification?	7
10. How does the system work when exposed to the elements such as direct sunlight?	7
11. Is facial identification for access control legal in the US?	7

iDFace

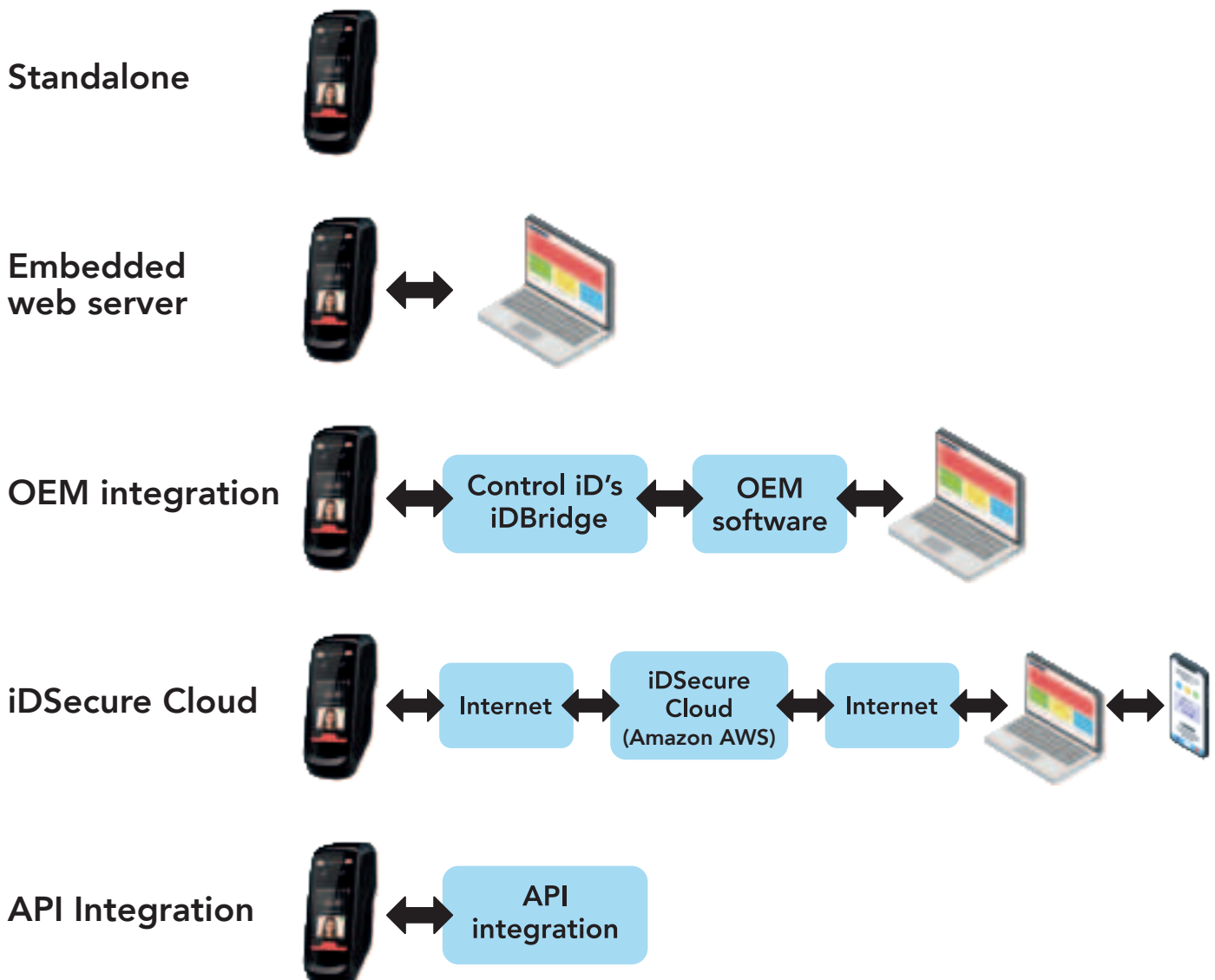
Facial Identification Features and Benefits

1. What is iDFace?

iDFace is an access controller capable of identifying users through facial validation, Mifare RFID cards, QR codes or PINs/passwords. The product is fully manufactured by Control iD, a company of the ASSA ABLOY Group.

2. In what configurations can iDFace be used?

iDFace supports 5 different modes of operations, described below:



iDFace

Facial Identification Features and Benefits

2.1. Standalone

In the standalone configuration, iDFace does not need to be connected to a network, and all configurations are performed on the device's Graphical User Interface (GUI). Data can be imported or exported by using a standard USB flash drive.

2.2. Embedded Web Server

For small-scale deployments (i.e. just a few devices), users may opt to use the embedded web interface available on iDFace to manage users and logs (i.e. export/import data). The only requirement for this operation mode is to connect an Ethernet cable to the iDFace.

2.3. OEM integration

Control iD products integrate with major access control software providers. In this mode, all iDFaces must be connected to the network and Control iD's iDBridge integration software package must be installed.

2.4. iDSecure Cloud

iDFace natively integrates with iDSecure Cloud. No on-premises software components are necessary for a true plug-and-play experience. iDSecure Cloud also comes with a mobile app for iOS and Android. In this mode, all iDFaces must have internet connection.

iDSecure Cloud (www.idsecure.com.br) is an access control software developed by Control iD and hosted on Amazon AWS. The software can be accessed over the internet and enables the management of users, devices, access rules, schedules and many other configuration options.

iDFace

Facial Identification Features and Benefits

2.5. API integration

iDFace offers an open API allowing customers to connect directly to the device and manage all access control functions (e.g. users, logs, rules etc.). Although this option requires some development, it offers maximum flexibility.

3. What type of Personal Identifiable Information (PII) is stored by iDFace?

As a minimum, iDFace requires an identification number (ID) per user. Optionally, the user's name and the user's RFID card number may also be stored in iDFace.

For facial identification, the user may choose from 3 different scenarios:

3.1. Default

By default, iDFace stores a picture of the user and his/her corresponding biometric template.

3.2. Template only

In this mode, iDFace receives the picture of the user for enrollment (i.e. template extraction), but the device only saves the corresponding biometric template (i.e. the picture is never saved in non-volatile memory).

3.3. Template on card

In this mode, iDFace saves the biometric template of the user in a RFID card and no biometric data is stored in the device. For validation, the user will have to present his/her card to the iDFace, and the device will confirm that whoever is in front of the terminal matches the template stored in the card (no biometric data will be saved in the device's non-volatile memory and the credential holder is also the sole owner of the biometric data).

iDFace

Facial Identification Features and Benefits

4. What is a biometric template?

Each template consists of a selection of significant features of a facial scan (for example, the distance between facial elements). In that sense, a biometric template is a binary representation of a person's face but contains much less information than a picture. Control iD's facial template is about 1kB in size where a typical cell phone picture is usually 4000KB or more.

A biometric template, on its own, is useless outside this system. The user data points cannot be reconstituted to create an entire facial scan. Also, companies cannot cross reference users' biometric templates with national registries or any other external databases. In short, the secured template serves one sole purpose: to identify the user onsite and grant access.

5. Does iDFace support encryption for data in transit?

Yes, iDFace supports HTTPS and TLS 1.3.

6. What methods are used to authenticate users accessing iDFace?

iDFace implements username/password authentication over HTTPS for granting access to the API.

7. What type of logs does iDFace offer?

iDFace provides an audit log (system modifications etc.), an access log and an alarms log (tamper, door forced etc.).

8. Is there video recording when authentications take place?

No, iDFace doesn't record any video internally during authentication or otherwise.

iDFace

Facial Identification Features and Benefits

iDFace supports the ONVIF (Open Network Video Interface Forum) protocol and optionally allows NVRs (Network Video Recorders) to record videos in real time from the device.

9. What is the fallback if a user cannot/does not want to use facial identification?

iDFace supports Mifare RFID cards, QR codes and PINs/passwords for users that can't or don't want to use facial identification.

10. How does the system work when exposed to the elements such as direct sunlight?

As with any facial identification solution, direct sunlight is not ideal but Control iD's iDFace implements a HDR (High Dynamic Range) camera that enables the product to perform well in adverse scenarios (direct sunlight or low light at night). Testing and environmental deployment examples have proven competitive advantages versus comparable facial identification models in the market.

11. Is facial identification for access control legal in the US?

Facial identification for access control is legal in the US in most cases if customers and users comply with applicable federal, state, and municipal laws and regulations, which may include compliance obligations such as providing notice, obtaining consent, etc. Each deployment is unique and we advise you to consult your company's Legal team.