RECFACES

ID-GATE

TECHNICAL DESCRIPTION

IDGT.TI.DOC.990

CONTENTS

1 INTRODUCTION (PURPOSE)

The Id-Gate system (hereinafter referred to as the “System”) is a software product for biometric identity verification in access control and management systems.

Id-Gate enriches the existing or newly created ACS with additional modern functions using facial recognition technology, improves the accuracy of identification and increases the ease of passage for employees/guests.

The Id-Gate system is intended to control access to areas and facilities using biometric identification. With the opportunities provided by the System, you can organize access control or improve the process of granting access to employees in organizations or enterprises. The System provides joint operation of ACS, biometric terminals and devices at passage points, as well as turnstile controllers and other access equipment.

The System provides:

- Control, accounting and management of access to the facility by means of biometric identification
- The ability to create and maintain specialized lists of employees and visitors (VIP, blacklist, etc.)
- Sending instant notifications to the security service when an unauthorized person who is not on the access list or, for example, is on the "black list" attempts to enter the facility
- Analytics on the number of visitors and time they spend at the facility
- Access rights differentiation both for the employees and the visitors to separate areas of the building
- Possibility of ACS functioning with integrated face recognition System to reduce the risk of employee card forgery, loss, transfer to third parties, access of several people with one card
- Integration with ACS with synchronization of information on employees: names, access cards, photos, etc. Ready integrations with Bosch Building Integration System, Honeywell Pro-Watch, Lenel OnGuard, Schneider Electric Security Expert, Dormakaba, Moxa, Robos

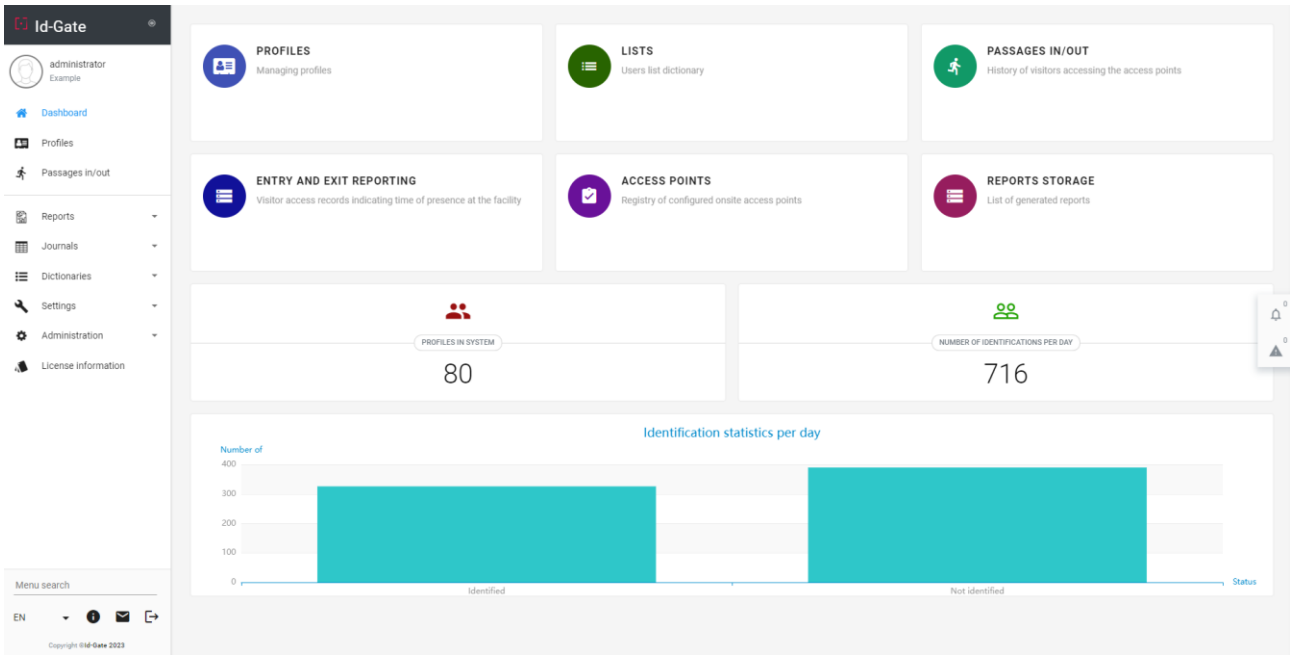

Figure 1. System dashboard

2 SOFTWARE DESCRIPTION

2.1 SYSTEM COMPONENTS

For the correct functioning of the System, the following minimum equipment is required:

- Server for the System Core
- Video preprocessing server(-s) (if necessary)
- Operators' PC (if necessary)
- Network or USB cameras, depending on the purpose and architecture of the System
- Access control terminals
- Network switches to provide data transmission between the System components

The detailed description of the equipment recommended characteristics is indicated below.

2.2 ARCHITECTURE

The System consists of the following components:

- **Id-Gate Core** — the server part of the System, consisting of separate services, including the System settings interface, recognition algorithms, database and reports
- **Id-Gate Tracker** — video preprocessing server
- **ACS Adapter** — service providing data exchange with an external system and sending notifications
- **Id-Gate Terminal** — an Android OS application for interaction with terminals installed at the entrance to the facility and access control in offline mode

The System can be integrated with:

- ACS
- Turnstile relay or other access control devices
- Terminals
- Wiegand

System architecture schemes for different use cases are presented below.

2.3 ARCHITECTURE DEPLOYMENT PATTERN

Before deploying the System and configuring the integration with an ACS, you need to determine the main sources of master data, depending on the planned algorithms of the System functioning in general. Namely: determine where the primary data (Master) will be input, in what order and with which systems it should be synchronized. In general, Id-Gate allows you to configure the integration by defining the external connected systems in Master, Slave and combined modes.

2.3.1 EXTERNAL SYSTEM IN MASTER MODE

For cases where the ACS being is the source of master data about profiles, access cards and profile pictures, the **Master** mode is enabled in the Id-Gate settings for the adapter of the corresponding ACS. For such an integration, there is a bilateral data exchange between the systems. The scheme of such a solution is shown below (**Figure** 2).

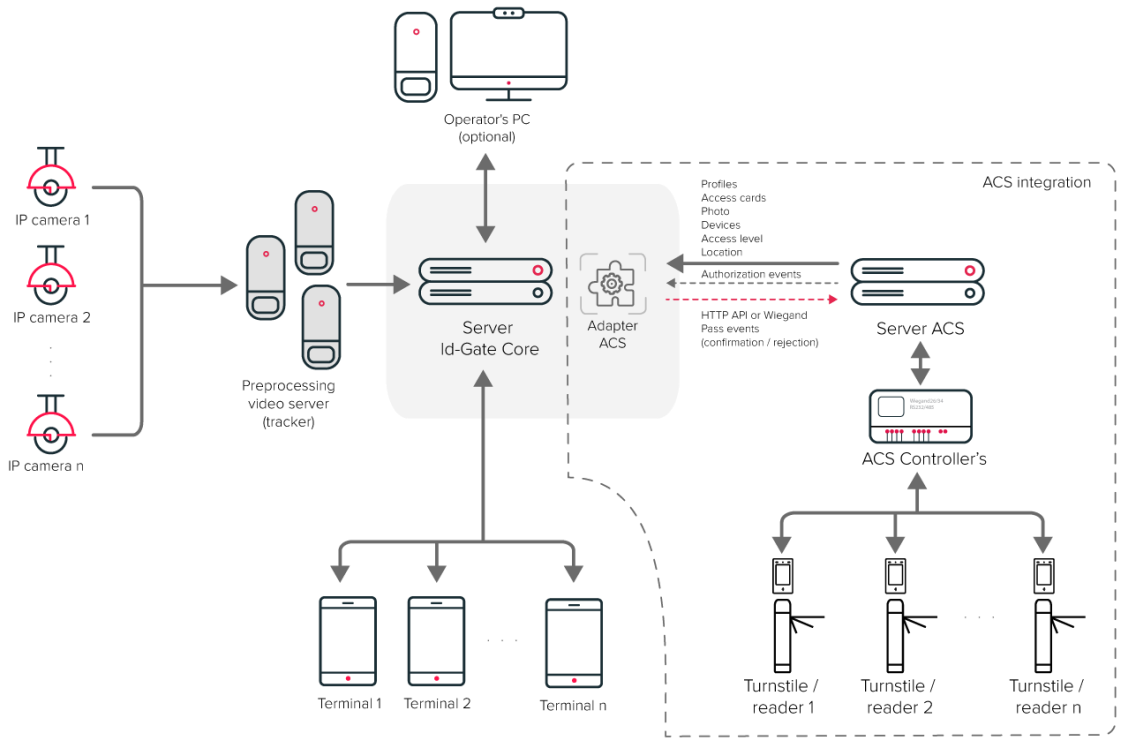

Figure 2. Id-Gate and external system integration scheme in Master mode

The ACS side maintains the database of employees and visitors with photos and identification cards, information on the locations of the actuation devices, access levels, as well as data on the readers and controllers. As a result of periodic synchronization, information from the ACS goes to Id-Gate, updating the information about the devices, locations of the executive devices, profiles and access levels.

The Id-Gate side processes real-time streams from CCTV cameras connected to the System, as well as from terminals. Based on the results of the biometrics subsystem, all detected persons are identified using the profile database synchronized with the ACS. The arising identification events are checked according to the set of configured rules, access levels by devices, and as a result of the processing, the events are formed and sent to the ACS. Depending on the settings, these can be commands via HTTP API or commands for Wiegand to open access devices (turnstiles, doors, barriers) that are connected to the ACS.

2.3.2 EXTERNAL SYSTEM IN SLAVE MODE

For cases where Id-Gate is the source of master data about profiles, access cards and profile pictures, the integrated external system is enabled in the **Slave** mode. For such an integration, a bilateral data exchange between the systems is performed. The scheme of such a solution is shown below (**Figure 3**).

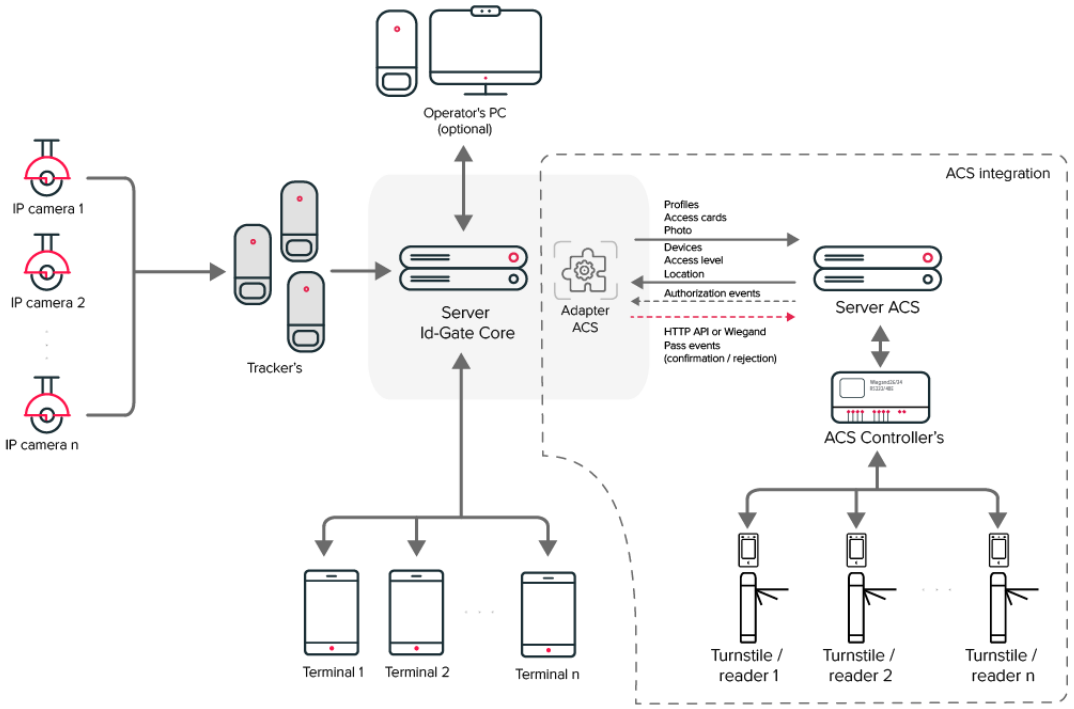

Figure 3. Id-Gate and external system integration scheme in Slave mode

The Id-Gate side maintains a database of profiles with photos and access cards. The streams from CCTV cameras connected to the System, as well as from terminals, are processed in real time. Based on the results of the biometrics subsystem, all detected persons are identified.

On the ACS side the information about the devices (controllers, readers, actuators), locations of the actuators and access levels is entered. As a result of periodic synchronization, the information about access rights and devices is delivered to the Id-Gate and must be applied to form the rules of identification event processing.

Identification events arising on the Id-Gate side or authorization events received from the external system are checked according to the set of configured rules, access levels by devices and as a result of their processing the commands are formed to grant or deny access, which are sent to the external system. Depending on the settings it can be commands via HTTP API or commands for Wiegand to open access devices (turnstiles, doors, barriers) that are connected to the external system.

ATTENTION! Before configuring the external system in the Slave mode, it is necessary to make a full backup of the connected ACS. The Id-Gate system operating in Master mode automatically replaces all data in the connected system at the first synchronization.

2.4 TECHNOLOGIES

The system is developed with the use of the following programming languages:

- Golang
- C#
- AngularJS
- RabbitMQ
- Nginx
- PostgreSQL
- Redis

2.5 LIST OF ID-GATE CORE SERVICES

Id-Gate Core includes the following services:

Table 1. Id-Gate Core services description

Service	Description	Port
Nginx	A web server and mail proxy server	80, 443, 23231
PostgreSQL	Free and open-source relational database management system (RDBMS)	5432
RabbitMQ	Service providing work with data queues	5672, 15672
Redis	Open-source software for managing NoSQL databases	6379
mkvz-tracker	Service for preprocessing video stream (tracker)	8001
mkvz-launcher	Service for managing client applications	8876
mkv-server-report	Service for generating reports: includes reports by gender, age, visits, etc.	11084
mu-server-api	Notification service	11090
support-server-api	Service for system maintenance	11091
mkv-server-url-shortener	URL shortening service	11092
mas-server-api	Management service, which provides API for processing data about devices, applications, cameras	11101
mas-server-settings	Service for storing configuration settings and sending them to the modules	11102
mpdn-secret-vault-api	Service for storing personal data	11204
mdc-server-api	Service for working with dynamic classifiers	11205
mfs-server-api	Service for storing and working with images	11300
mfs-server-thumbnail	Service for working with thumbnails of the file storage	11301
fs-server-api	File storage service	11302
mi-sender-email	Service for sending e-mail notifications	11400
mi-sender-http	Service for sending notifications by http (push)	11401
mi-sender-smsmodem	Service for sending SMS with a USB gsm modem	11402
mi-server-api	Service for implementing API functions to work with services	11403
mi-sender-telegram	Service for sending SMS to Telegram	11404

mi-controller-acs	Service for integration with external systems and request routing between them	11406
mi-adapter-acs-biostar2	Service of integration adapter with Biostar 2 ACS	11413
mi-adapter-acs-moxa	Service of integration adapter with Moxa 1214 ACS	11414
mi-adapter-acs-suprema-fs2	Service of integration adapter with Suprema Facestation 2 ACS	11415
mi-adapter-acs-honeywell-pro-watch	Service of integration adapter with Honeywell Pro Watch ACS	11416
mi-adapter-acs-bosch	Service of integration adapter with Bosch BIS ACS	11417
mi-adapter-acs-se	Service of integration adapter with Security Expert ACS	11418
mi-adapter-acs-exos	Service of integration adapter with Dormakaba EXOS ACS	11421
mi-adapter-acs-onguard	Service of integration adapter with Lenel OnGuard ACS	11422
mkv-server-admin	User interface for the System administration module	11500
mkv-server-api	The service contains API methods to work with the main functionality of the System	11501
mkv-server-auth	Service for authorization in the System by entering a username and password	11502
mkv-server-ws	Application back-end for working with the client via WebSocket	11503
backup-client-server-api	System data backup service	11506
logging-server-api	Service is used to get logs from services	11509
event-configuration-api	Service for simplifying working with event storage, so that a single request creates a pool of necessary entries in the dictionaries for event processing	11510
event-storage-server-api	Service for processing System events and performing various actions depending on the type of event	11511
mkv-client-profiles-import	Service for importing profiles into the System	11514
mas-meta-server-api	Meta information service	11515
monitoring-server-api	Services for monitoring statuses of the running services	11517
statistics-server-api	Service for recording statistics on the System operation	11518
audit-server-api	Auditing and logging service	11521
mkv-server-auth-ldap	Service for authorization in the System via LDAP/AD	11522
mkvz-onvif-cameras	Service for searching and connecting cameras supporting ONVIF protocol	11550
discovery-server-api	Service for mobile app searching with DNS-SD	11551
adb-server-api	Service for managing mobile apps with ADB protocol	11552
mas-server-report	Report service for MAS	11553
medical-server-api	Medical control service	11554
mie-export-api	Service for exporting customized data sets from CSV	11555
mie-import-api	Service for importing customized data sets to CSV	11556
logging-server-siem	Service for SIEM logging	11557
mmpd	Service for managing detecting processes	11600
mobile-service-api	API for working with mobile apps	11601
gate-server-api	Service for managing access control	11602

compromise-server-api	Service for compromise control	11605
modi-image-worker	Service for processing photos (crop, resize, etc.)	11700
modi-server-api	Service for processing discrete images	11701
modi-ubda-tevian-[01-04]	Service for processing photos: searching faces and creating biometric templates	11710 y [01], 11711 y [02], 11712 y [03], 11713 y [04]
modi-ubda-tevian-alg1	Service for processing photos	11714
mrp-server-api	Service that provides API for processing data during working with the streaming video	11800
mrp-server-ubt-broker	Service for UBT proxying to other systems	11801
mrp-matching-tevian-go	Matching service for the Tevian engine	11806
mrp-server-broker	Service managing a request queue to the matching algorithms	11821
mrp-server-image-broker	Service for image distribution among trackers	11822
ms-server-filecache	Service providing file caching	11900
mkv-scheduler-api	Service that implements working with scheduled tasks	11910
video-restreamer-server	Server for video restreaming	40000, 40001

One of the server requirements for installing the Id-Gate Core software package is the absence on the server of the software specified in the table above and the presence of free ports indicated in the table.

3 REQUIREMENTS FOR CORRECT WORK

3.1 ID-GATE SERVER

It is recommended to install the Id-Gate Core on the server. Server characteristics directly depend on the number of cameras processed by the System. An approximate calculation for the most common values is presented in the table below.

Table 2. Server requirements

Number of cameras	CPU (Core)	RAM (GB)	HDD (GB)	SSD (GB)
1	5	16	600	240
2	6	16	700	240
3	8	16	700	240
5	10	32	800	240
7	14	32	900	240
10	18	64	1000	240

Operating System: Windows 10 Pro (2004 and later, according to the end date of the operating system support), Windows Server 2016/2019 and later. If you have the “Windows 10 Pro N” OS edition installed, you have to additionally install the “Media Feature Pack” component. The account (login/password) (including for a remote user) must remain unchanged throughout the installation. The account (login/password) must allow upgrading privileges to Administrator if necessary.

The following components **must not** be pre-installed on the server:

- PostgreSQL
- RabbitMQ
- Redis
- Web server that uses ports 80 and 443

3.2 EQUIPMENT INSTALLATION

3.2.1 RECOMMENDATIONS ON TERMINAL INSTALLATION

When installing the terminals indoors, place the device at least 2 meters away from the light source (to eliminate illumination and glare) and at least 0.3–0.5 meters away from a window or door (**Figure 4**).

When installing the terminal, avoid the following:

- Strong back illumination
- Direct sunlight on the terminal
- Close proximity to bright light sources

The mounting surface must withstand loads of up to twice the equipment weight.

Recommended installation height of the terminal: 1.45–1.55 m from the floor level to the module with cameras built into the terminal. The specified height of the terminal installation is recommended and can be changed according to your needs.

During installation, it is necessary to ensure the safety of the equipment and installation tools used.

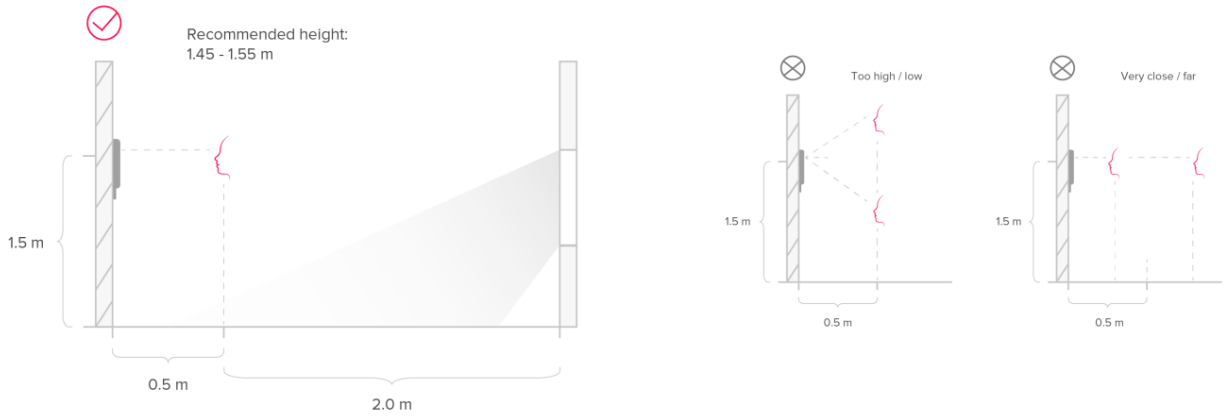

Figure 4. Terminal installation recommendations

3.2.2 RECOMMENDATIONS ON CAMERA INSTALLATION

- The camera must be fixed using the special bracket supplied to minimize the blurring caused by the movement of the camera. It is allowed to mount the camera on a tripod; the camera installation height is from 1.5 to 2 m.
- The recommended camera placement: a person looks at the camera and moves towards it or across the camera's line of sight.
- Screens, interactive kiosks, boards, banners should not block a person moving.
- For recognition and identification purposes, it is required to use cameras with varifocal lenses.
- The lens focal length must be in the range from 9 to 40 mm.

- The camera tilt at the end of the face detection area should be within 15 deg.
- The optimal camera height above the floor is 2.2 m, it is desirable that the beginning of the face detection area is located further than 8.0–8.5 m.
- If cameras are mounted indoors, uniform and constant level of illumination must be provided. For proper facial recognition, indirect lighting must provide such conditions, when visitors' faces have uniform illumination without shadows or glare. The recommended light intensity is about 300 Lux (minimum 150 Lux, maximum 600 Lux).
- At the beginning of the process of facial recognition, it is required to mount and configure a camera so that the size of an adult's face is about 160x160 pixels (the line of sight is more than 2 meters in width — a little wider than the width of outstretched arms).

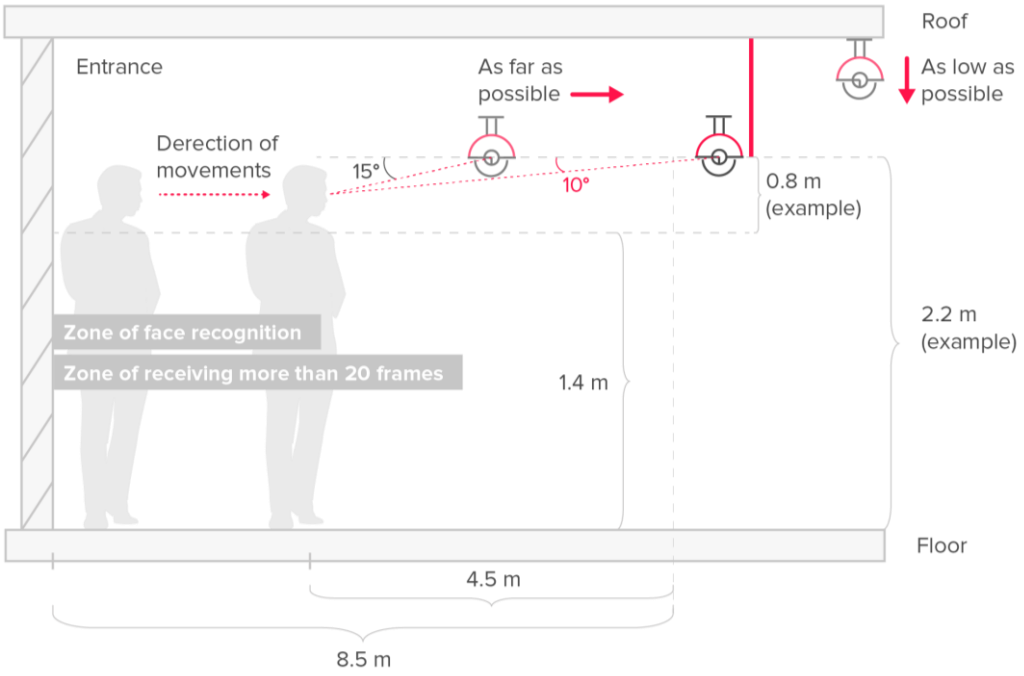

Figure 5. Camera placement recommendations

4 LANGUAGE SUPPORT

The Id-Gate software is a multilingual solution that allows you to choose from the following language options:

- English (by default)
- Spanish

The list of available languages can be expanded upon request.

5 DOCUMENTATION LIST

- Id-Gate Administrator's Guide
- Id-Gate Operator's Guide
- Id-Gate Terminal Android App User Guide

6 SOFTWARE MANUFACTURER

RecFaces FZ-LLC

Address: Dubai Internet City Building 3, Dubai, UAE

Telephone: +971 4 8368339

E-mail:

- General questions: in@recfaces.com
- License and partner policy: sales@recfaces.com
- Technical support: id-gate@recfaces.com