United Nations Populations Fund, Level 6, Kadavu House, Suva. Private Mail Bag, Suva

For the supply and installation of Access Control System at UNFPA PSRO Suva office, Level 6 Kadavu House, 414 Victoria Parade, Suva Fiji.

Components of an access control system:

Software

Used to adjust all parameters of the system, control hardware, display events related to movement of users, alarms, and operation of hardware devices. The software is also used for storing all events in the database and generating reports based on requirements defined by an operator.

Electromechanical hardware

1. Electric locks
2. Release buttons for 6 doors

Electronic hardware

1. Controllers: receive settings from software and control the electromechanical hardware of the system.
2. Contactless readers: read unique numbers of identification cards/tags and forwards the numbers to controllers.
3. Facial & Fingerprint readers: scan facial and fingerprint images, compare them with the templates stored in the internal reader database (or on a smart card) and send the verification results to controllers.

System users

1. Operators: responsible for administrating the system, creating new users, issuing cards and performing other regular daily tasks.
2. Users: regular staff of the company, with permanent or long-term ID cards (or PINs), who use the system to gain access to certain door entry configured by operators.
3. Visitors: people that are not employed by the end-user company, but still have rights to access certain areas (contractors, visitors, delivery people, etc.).

Technical requirements:

1. ***Software***
    a. There shall be no limitations on the number of PC workstations, readers and alarm inputs.
    b. The number of cards/users shall be limited only by memory available in hardware.
    c. At least 2 active cards per user shall be supported.
    d. At least 8 access levels per user shall be supported.
    e. The software shall support at least 4000 holiday dates and have automatic holiday rescheduling feature.
    f. The software shall have the ability to perform scheduled automatic database maintenance and backup tasks at user selected intervals and ability to configure the amount of history stored in the active database.
    g. The software shall have the ability to produce the following report types:
        i. system and alarm event reports, user reports, hardware configuration settings, access level reports, employee time & attendance reports.
        ii. The reports shall be available in Adobe PDF and MS Excel formats.
        iii. Report filters must be convenient and user friendly: allow operator preview user photos, content of access levels, hardware settings and time zone configuration.
        iv. The software shall support at least 2 number of building floor plans.
        v. Floor plan viewing interface shall have convenient zoom in/out controls by mouse wheel.

vi. All configuration and user changes shall be sent to controller immediately. The software shall display the progress in percent as the changes are being downloaded. The downloading shall be done in background and not affect the normal use of the software in any way.
vii. The floor plans shall display real-time status of system hardware and allow operators to immediately see the effects caused by configuration changes.
viii. The software shall use an industry standard database engine released not earlier than 2020 and currently supported by the manufacturer.
ix. The software shall have the ability to automatically display photos and additional information about users as they enter/exit through doors.
x. The software shall have a modern interface, attractively designed and convenient to use.
xi. The software shall be adapted for operators who have not received any special training related to management of integrated security systems. Graphical user interface shall be intuitive. Introducing the system to a new operator shall not take more than 1 hour.
xii. In order to reduce the amount of work done by an operator, the software shall incorporate an option to copy objects: users, doors, floor plans, time schedules, access levels and holidays.
xiii. The software shall store information and provide reports about visitors and appointments.

2. ***Hardware***
   a. The hardware shall support all industry standard readers that output information in Wiegand or Clock/Data formats (up to 128 bits).
   b. There shall be at least 2 types of controllers: (a) for one door with an entry reader and an exit button and (b) for one door with two readers (entry and exit) or for two separate doors with entry readers and exit button.
   c. There shall be an IP-reader available. The IP-reader shall integrate a contactless card reader and controller in a single body, designed for surface mounting on a wall or a door frame eliminating the need for enclosures.
   d. Each controller and IP-reader shall have a standard RJ-45 network port for communication with software and other controllers.
   e. Controller and IP-reader shall support standard Ethernet 10/100BaseT network and TCP/IP communication protocol.
   f. Systems using Ethernet converters, adapters, or terminal servers that enable network connectivity for legacy controllers by tunneling RS-232/485 serial data over Ethernet shall not be acceptable.
   g. Single-door controller and IP-reader shall have at least 32Mb SDRAM operating memory and 8 MB Flash memory for database and events. Two-door controller shall have an option for expanding Flash memory to 32MB.
   h. All controllers and IP-readers shall use a 32 Bit 100 MHz RISC processor (or better) in order to enable fast execution of advanced functions.
   i. All system parameters including card numbers, PINs, access levels, time schedules, holidays and operations modes shall be stored in controller and IP-reader memory and not affected in case of a power loss.
   j. Single-door controller and IP-reader shall have enough memory to store at least 40,000 users. Two door controller shall have enough memory to store at least 250,000 users.
   k. In case communication with the host PC is interrupted, the controller and IP-reader must have enough memory to store at least 5000 latest events (FIFO buffer).

l. Operation of controller and IP-reader shall be completely independent of the PC or "Master controller". Should the PC or the communication link fail, the users should not be affected in any way and all functions should continue working.
m. IP-reader shall have the following inputs and outputs:
    i. Exit button input
    ii. Door contact input
    iii. Auxiliary alarm input
    iv. Inputs for monitoring AC power and backup battery state.
    v. Relay for controlling an electric lock.
    vi. One-door controller shall have the following inputs and outputs:
    1. Power output for the reader
    2. Outputs for controlling LEDs and beeper of the reader
    vii. Exit button input
    viii. Door contact input
    ix. Inputs for monitoring AC power and backup battery state. There should be an option to reconfigure these inputs to function as general purpose inputs.
    x. Relays of controllers and IP-readers should support two modes of operation:
    1. dry contact and
    2. powered mode, whereas power to the lock is provided via relay contacts this way simplifying wiring and eliminating the need for an additional power supply.
    xi. Controllers and IP-readers shall have a RJ45 or USB communication port that would act as a backup communication channel in case the network connection was interrupted.
    xii. Controllers and IP-readers shall have a built-in PoE capability, in order to reduce wiring and provide backup power effectively. PoE feature must comply with the 802.3af standard.
    xiii. Controllers and IP-readers shall be capable of supplying up to 600mA @ 12VDC to peripheral devices: readers, electric locks, sirens, detectors, etc. 22. Controllers and IP-readers shall accept the standard 12VDC power input in case an existing network infrastructure does not support PoE. 23. In case the main PC of the system fails, controllers and IP-readers shall accept a connection from a laptop in order to diagnose the problem, change settings or control peripheral devices.
n. The system shall support biometric IP-readers with the following or better specifications:
    i. min. 25,000 fingerprint template storage capacity
    ii. 1-to-many verification in less than 1 second (with the database of 3000 users)
    iii. 1-to-many verification with the database of 9000 users.
    iv. min. 500,000 event storage
    v. Built-in USB, RJ 45, LAN communication ports
    vi. Selectable operation modes:
    1. Facial, fingerprint, fingerprint + card, fingerprint + PIN
    vii. Door contact and exit button inputs

Additional Notes:

- The software to be owned by UNFPA
- UNFPA can obtain all inputs and records of using the card reader.
- Card Readers:
    - HID compatible, (HID Proximity)
    - Networkable; PoE, control panel installed and connected to a fixed workstation.
    - Card reader can open with a card, push button (see next) or a computer override.
- Exit Push Buttons.
- 7 Automated Locks:
    - Electromagnetic locks, strong enough to hold up to 280 Kg resistance
- Door Closers:
    - Heavy duty, open and close more than 100s times per day, well calibrated and easy to maintain.
- Cabling:
    - Outdoor weather resistant wiring (pipe) linear wiring between all 6 reader's locations and the control panel.
- Warranty and maintenance service assistance:
    - Minimum warranty should not be less than Five (5) Years starting the day of activation. The maintenance service shall include free of charge maintenance visit and free of charge spare parts and replacement.

High Level Diagram: