Description

The desktop reader for mobile identifiers (U-PROX ID) and contactless identifiers is designed for entering identifier codes into an access control and management system.

It can work with mobile identifiers (U-PROX ID), RF-ID 125 kHz (ASK/FSK), and with Mifare® ISO14443A 13.56 MHz (read and write operations).

It supports a personalization mode (setting an additional encryption mode) for mobile identifiers and Mifare® identifiers, which provides protection against cloning. Additionally, during Mifare® personalization, an internal (secret) user card number can be set.

An additional feature is the distribution of U-PROX ID mobile identifiers to users' mobile devices.

For integrating the device into other systems, an open text protocol can be used.

> It is not recommended to install the reader on a metal surface, as this reduces the reading distance.

Reading Distance

The reader is capable of reading a contactless identifier’s code from a distance of 10–80 mm (depending on the type of identifier and operating conditions).

Connection

The reader comes with a USB cable that is used to connect it to the access control system.

1. The reader can be connected to existing or new access control systems.
2. Install the reader in a location convenient for card reading and connect it to a PC.
3. Install the device driver from the u-prox.systems website.
4. After that, an additional virtual COM port will appear on the computer.

Reader Operation

The reader has a tri-color indicator and a built-in buzzer. In its default mode, the red LED lights up, indicating that power is present.

When an identifier is brought near, the code is read. A correct reading is indicated by the built-in buzzer and the activation of the green LED.

When the card is held within the reading field, the green LED remains lit.

The next identifier can be read 0.5 seconds after the previous identifier has been removed from the reader's active zone.

Personalization Mode (Encryption)

To enhance protection against cloning, readers with a specific user-defined secret encryption key are used.

In personalization mode, the readers only read the codes of identifiers that have been encrypted with a known encryption key set during programming.

The U-PROX Desktop reader provides the ability to prepare such identifiers: for Mifare® – encrypting data sectors and setting a user card number, and for U-PROX ID – setting the encryption key.

Configuration

Using the free mobile app U-Prox Config, the reader is fully configured, including encryption modes.

Download and install the U-PROX Config mobile software on your smartphone.

Put the reader into programming mode – place the master card on the reader.

> The reader is supplied without a master card. You can add it during the reader's first programming.

Launch U-PROX Config, press the "Search" button, and device scanning will begin.

After scanning, select the desktop reader from the list and press the "Connect" button – the configuration will be read.

After successful reading, the main menu will be available, through which you can configure the desktop reader, update the list of mobile identifiers, save or restore its configuration (template)

for further programming, update the reader's firmware, and replace the master card.

In the "Configuration" section, you can view the device's serial number and firmware version, the remaining mobile identifiers, set which types of identifiers the desktop reader works with, etc.

You can also enable personalization mode by setting an encryption password for Mifare Classic, Mifare Plus cards, and mobile identifiers.

After configuring the desktop reader, a "Write to Device" option will be available in the main menu. After pressing it, the configuration will be written to the device.

> Firmware updates for the reader are possible only using an Android smartphone with NFC support.

Mobile Identification

The reader supports reading U-PROX ID mobile identifiers and is also used for issuing identifiers from a preloaded list of mobile identifiers.

Procedure for Local Issuance of a New U-PROX ID Identifier

1. The system administrator puts the desktop reader into programming mode – places the master card on the reader.
2. The user brings their smartphone to the U-PROX Desktop, and in the U-PROX ID app settings presses the "Get from Desktop" button – the app connects to the desktop reader and retrieves a mobile identifier from the list.
3. The code of the obtained mobile identifier is issued to the access control system, etc.

U-PROX ID App

The free mobile app U-Prox Mobile ID is designed for receiving, storing, and transmitting the U-Prox ID mobile identifier between a smartphone and the reader.

How to Obtain Mobile Identifiers

You can purchase mobile identifiers from our dealers.

125 kHz Identifiers

The reader supports 125 kHz cards with amplitude modulation (ASK – EmMarine, etc.) and frequency modulation (FSK – Temik, etc.).

> These cards do not have protection against cloning, but they are very popular due to their low cost.

Mifare® Identifiers

The reader supports working with Mifare® cards, reading and writing encrypted identifiers with a user-assigned card number, using either a static or diversified encryption key.

Mifare®Classic

The least secure series of cards, vulnerable to the Crypto 1 encryption algorithm (SL1).

When in use, it is recommended to encrypt all card sectors with a diversified encryption key.

Mifare®Plus

The reader supports reading and writing in SL1 and SL3 modes for Mifare®Plus. It is recommended to use SL3 mode, as it offers the highest protection and uses the AES encryption algorithm.

Mifare®Desfire

The reader works with Mifare DESFire EV1, EV2, and EV3 cards. AES encryption is supported.

Procedure for Encrypting a New Mifare® Identifier

1. Put the desktop reader into programming mode – place the master card on the reader.
2. Launch U-PROX Config, press the "Search" button, and device scanning will begin. After scanning, select the desktop reader from the list and press the "Connect" button – the configuration will be read.
3. In the app menu, press "Next" and select "Card Issuance".
4. Choose the type of encryption according to your card – Mifare Classic (SL1) or Mifare Plus (SL3).
5. Place an empty card on the reader and wait for the issuance process to complete.
6. The code of the obtained mobile identifier is issued to the access control system, etc.

Integration Protocols

For integrating the device into other systems, an open text protocol can be used.
Possible integration options include: directly via the virtual COM port created when the reader is connected to a computer, and through a special software module that allows working with the reader in JSON format.

Warranty

The warranty period for U-PROX devices (excluding power sources) is 2 years from the date of purchase. If the device does not operate properly, please contact support@u-prox.systems first, as the issue may be resolved remotely.