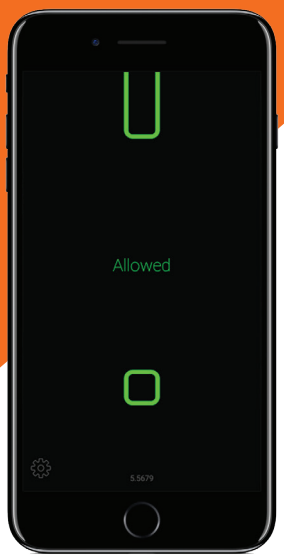
Prox-T ID

DIGITAL PERSONAL MOBILE CREDENTIALS

FOR NEW GENERATION OF READERS

Prox-T SmartLine

- **now the phone works as an access card**
- **convinient and safe**
- **security level is same as Mifare Plus SL3**
- **one identifier for doors and barriers**
- **NFC and 2.4 GHz radio as transmission technology**
- **can not be copied and moved to another smartphone**
- **works with any access control system**



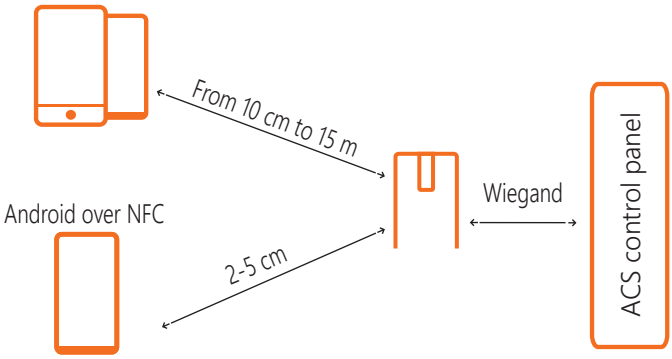
Digital personal mobile credential. It is processed and stored in the user's smartphone using the Prox-T Mobile ID application. It can be transferred over NFC and/or 2.4 GHz radio between the reader and the smartphone.

Prox-T Mobile ID

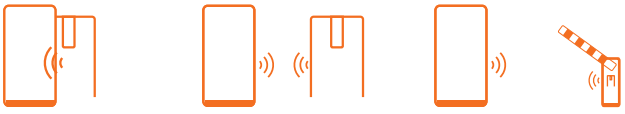
Free mobile application Prox-T Mobile ID receives, stores and transmits mobile credentials Prox-T ID between the reader and the smartphone.

How it works

iOS and Android over 2.4 GHz radio



2.4 GHz radio operating modes



Proximity-Door
Reader activates by the presence sensor. Read range 5-10 cm

Door
Reader is always active. Read range 50-60 cm

Gate/Barrier
Reader is always active. Read range 1 - 15 m

How to user receive Prox-T ID

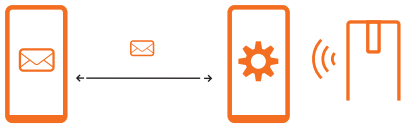
By QR code

The user reads a one-time QR code or loads it from a graphic file to Prox-T Mobile ID application.
Using the information (link) from this QR-code, the application gets a unique mobile credential from the bank of credentials on the cloud server.

From Prox-T Desktop over 2.4 GHz radio

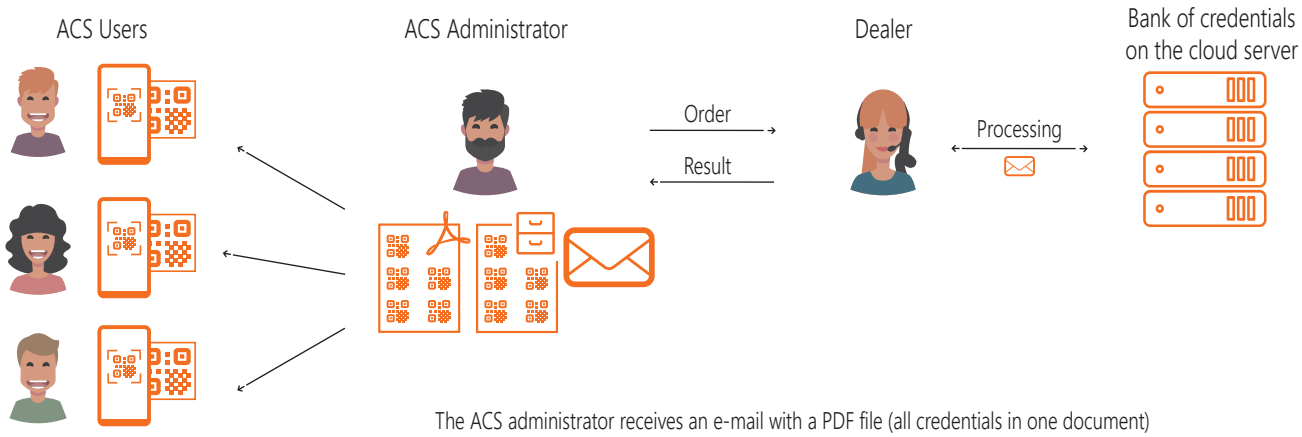
1. The system administrator switches Prox-T Desktop into "issure mobile credentials" mode.
2. The user runs the Prox-T Mobile ID app, clicks "Get ID from Prox-T Desktop" and brings the smartphone to Prox-T Desktop.
3. Desktop issues a unique mobile credential and marks it as issued.

From Prox-T Desktop by E-Mail



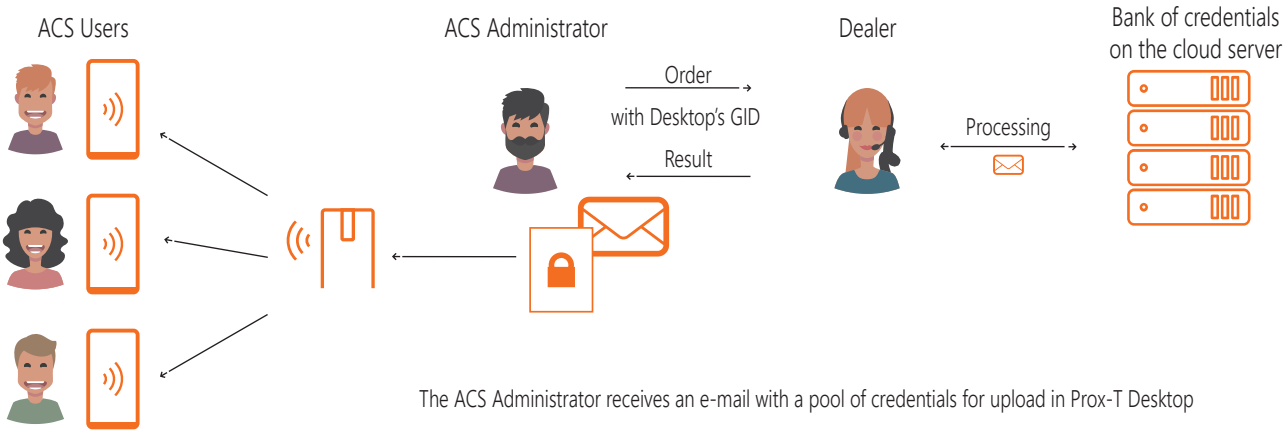
1. User from Prox-T Mobile sends an e-mail request to receive Prox-T ID to ACS administrator. A special link will be created in the text.
2. Administrator receives the letter, then clicks this link in the e-mail and loads the request data into its engineering application.
3. Next, the administrator takes Prox-T Desktop into the "issure mobile credentials" and connects to it with engineering applications.
4. Administrator processes the request, obtains credential from Prox-T Desktop and sends it by e-mail to user in the engineering application.
5. User opens the link from the e-mail with Prox-T Mobile ID app and obtain mobile credential Prox-T ID.

Distribution of mobile credentials. QR codes



The ACS administrator receives an e-mail with a PDF file (all credentials in one document) and ZIP-archive (credentilas separately)

Distribution of mobile credentials for Prox-T Desktop



The ACS Administrator receives an e-mail with a pool of credentials for upload in Prox-T Desktop

Mobile credentials' security

Binding to the device
When receiving, mobile credential binds to UGID of app installed on the device

Secure storage
Mobile credential is stored in a container encrypted with a 256-bit key.

Secure remote issuing
One-time links into e-mail, one-time QR codes for mobile credential's activation

Can not be copied
Unable to copy or clone mobile credentials

Secure transfer
The container with mobile credential is transmitted via 2.4 GHz radio or NFC with a crypto- and imitation-resistant protocol

Life cycle
After uninstalling the application or resetting the smartphone to factory settings, mobile credential will be removed