

TIDOMAT smartONE

version 2

- System description -

Copyright information

© 2008 Tidomat AB. All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form by any means, electronic, mechanical, recording or otherwise, without the prior written permission of Tidomat AB.

The content of this publication is furnished for informational use only. Data subject to change without notice and should not be construed as a commitment by Tidomat AB.

TIDOMAT, the TIDOMAT logo, smartONE and the smartONE logo are registered trademarks of Tidomat AB. All other trademarks are the property of their respective owners.

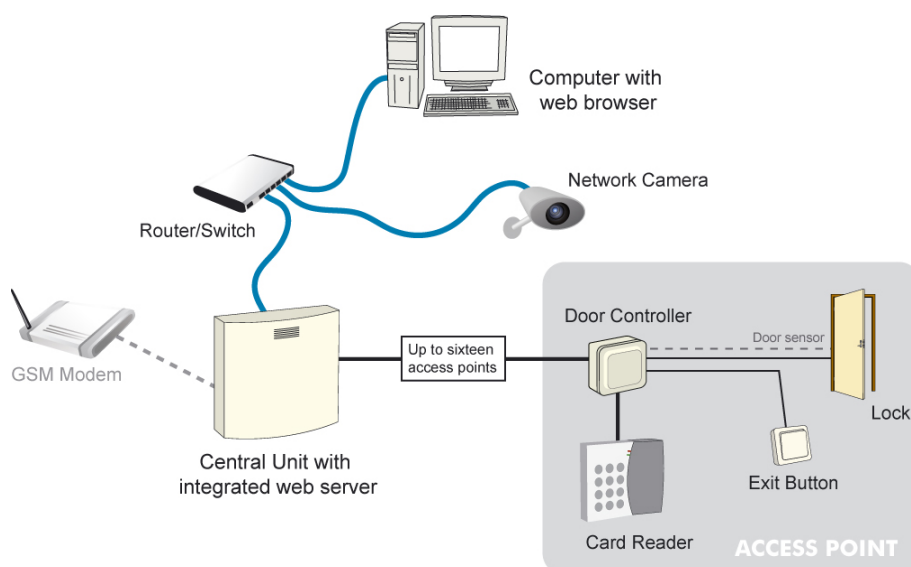
www.tidomat.se
info@tidomat.se
doc.no. 01080009-0837
© 2008 Tidomat AB

Content

Copyright information	2
About smartONE	4
Security on different levels	4
Security by individual user rights	5
A personal system for both the Administrator and the Cardholder.....	5
Controlling the Access Points with Time Channels, Schedules and Cards.....	5
Schedules for convenient administration of time spans	6
Communication to and from the system	6
Flexible Help- and Language files	6
Comprehensive overview with the Log and the Reports.....	6
Overview of smartONE	7
Technical data	7
Performance of smartONE	8
Accessories	8
System Functions.....	9

About smartONE

The security system smartONE controls up to sixteen Access Points and is administrated through the web. The doors are configured in the so called Central Unit. The Central Unit communicates with the Access Points, which is where the Card Reader, Exit buttons and Electric Locks are assembled. There is no need to install any software, since smartONE is ready to be used as soon as the doors are configured to the Access Points.



Security on different levels

The security system smartONE controls up to sixteen Access Points, of which eight are configured to the Connectors in the Door Central. Eight additional Access Points may be configured to an Expansion Card, which is connected to the Central Unit. The settings of the Access Points are programmed in the System-layer in the user interface. The Access Points can be programmed to be unlocked by using a Door code; a Card + PIN; a Card only. The Relay Functions are connected to the Access Points and can be used in a variety of ways, for example as Alarm by pass, Motor Operated Lock and Automatic Door. The Relay Functions can also control the light in a room or a roll up shutter door.

Each Access Point connected to the system has a window in the user interface. This window displays the events from the Access Point in real time. Symbols and captions decipher how an Access Point has been entered and if divergences has occurred, such as incorrect PIN entered. When Cards are used for granted access, a brief text states which Cardholder has entered the Access Point and at what time. The symbols also indicate the status of the Access Points, whether it is locked, unlocked, blocked or off-line.

The security can be enhanced by connecting Network Cameras to the Access Points. When a Network Camera is operating, a symbol is displayed in the window of the Access Point. By clicking on the symbol, still images from the Network Camera are displayed in the user interface.

Security by individual user rights

The security system smartONE is implemented in two layers, the System- and the Admin-layer. The hardware and the Access Points are configured in the System-layer. The everyday use and administration of the program is carried out in the Admin-layer. A further eight users can use smartONE. Each user is given a personal User-name and a Password. The Users are granted user rights and can operate on three different levels. The user interface of the system is dynamic, thus adapting to every User's individual rights.

A personal system for both the Administrator and the Cardholder

The security system smartONE is conveniently adapted to every Administrator's need. The designation of the system may be changed to a personal name. All the designations related to the object Cardholder may be edited. The designations may refer to data such as First name and Surname, or be changed to for example Building, Flat, Flat owner and so on. Should personal data already be stored in a data base, the system may import this data with CSV-files. Once the personal data is uploaded in the system, the Administrator can issue cards and create Access Plans to the Cardholders. An Access Plan is a detailed plan of the Access Points which a Cardholder is granted access to, including during which hours and days.

Controlling the Access Points with Time Channels, Schedules and Cards

A Time Channel or a Schedule may be connected to an Access Point, thus ensuring that the Access Point for the specified times is either unlocked; requests Card+PIN to grant access; activates a Relay Function or blocks the door.

The security system smartONE can also activate a Time Channel when a specified Cardholder enters a specified Access Point. This function may be useful in a reception, if the Entrance is to be locked until the receptionist has entered the premises. The Access Point remains unlocked until the receptionist displays the Card to the Card Reader. The Time Channel prompts the Access Point to unlock. When the manual time settings or the Schedule are set to 08.00-17.00, the Access Point is unlocked between those hours, even if the receptionist should enter the premises earlier. Should the receptionist enter the premises later than 08.00, the Access Point remains unlocked until the Card is displayed to the Card Reader. Should the receptionist not enter the premises at all, the Access Point remains unlocked unless it is edited in the user interface.

Schedules for convenient administration of time spans

The Schedules specify time spans and can be connected to various functions in smartONE. A Calendar enables Special days to be included, such as education days and public holidays. The Schedules can be connected to Cardholders, Time Channels and Triggers.

Communication to and from the system

The security system smartONE sends messages as E-mail, Text-message, IP-notify or HTTP-request, should stated events in the system occur. The Contact Lists enables the communication to run smoothly, since several receivers are notified when the system starts up, an Access Point goes off-line or an Access Point is forced. The events may be limited to for example Access Point forced or Access Point off-line during manually specified hours or according to a Schedule. The HTTP request is sent by the method POST. The IP notify is sent URL-style. The messages may be programmed with smartONE variables, or else remain a standard message stating information about the event, the day and what time it took place.

The Access Point can also be unlocked using the telephone. Should a GSM modem be configured to the system, an authorized Cardholder can call the phone number of the modem. The mobile number of the Cardholder is identified and the Access Point is thus unlocked.

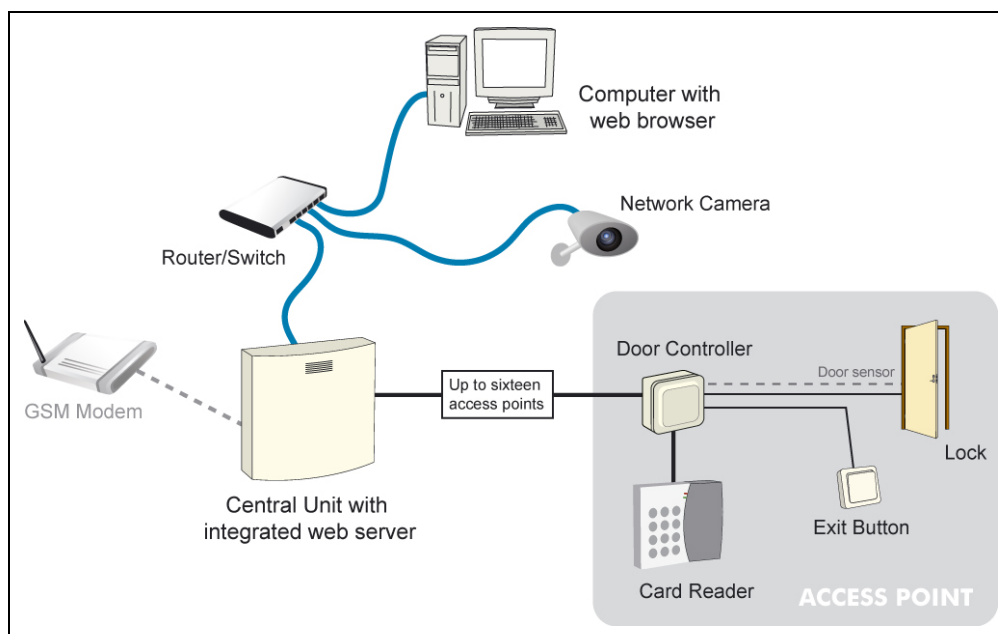
Flexible Help- and Language files

The security system smartONE can be used in different languages, for example English and Swedish. The Language files can be uploaded in the system, and the System designations as well as the Help files are changed to the selected language. The Help files are also adaptable to the functions every user activates. Should specific functions be activated, the Help files shows help and instructions for those functions. The information is thus adapted to the need of every user.

Comprehensive overview with the Log and the Reports

The security system smartONE keeps a Log which provides the Administrator with a comprehensive overview of the events in the Access Points. Information regarding the Access Points, Cardholders, Events, Date and Time is compiled in a list. The Reports can be created with both general and detailed information. The system also keeps a Journal of all the administrative events in the security system smartONE.

Overview of smartONE



Technical data

Data integritet	Confidential data in the data base is encrypted. HTTPS encryption (SLL certificate) between the Central Unit and the web browser. Data encryption between the Central Unit and the Card Reader.
Protocol	IPv4, HTTP, HTTPS, SSL/TLS, TCP, ICMP, UDP, SMTP, FTP, DHCP, UPnP, ARP, NTP, DNS, XMLAPI, NetBIOS.
Web browsers	Internet Explorer 5, 6+ och 7+, Firefox 2+ och 3+, Opera 7+, 8+ och 9+, Safari 3+.
Power Supply	24 VDC regulated voltage.
Current Consumption	Central Unit: 200 mA Door Control Unit: 50 mA Card Readers: 50 mA – 100 mA (depending on the model) Electric lock: 60 mA – 500 mA
The Card Reader	smartONE- Reader, OEM-Reader (clock & data, ABA track 2). Proximity cards: Mifare® 13,56 MHz ISO 14443A/B or 125 kHz EM4102

Performance of smartONE

Access Points	Up to 16 Access Points, 8 connected to the Door Central SO-3008 and 8 additional to the expansion card SO-3016. The expansion card is connected to the Central Unit.
Door codes	2 Door codes for each Access Point.
Cardholders	Up to 2 500.
Cards	Up to 2 500.
Time Channels	Up to 50.
Triggers	Up to 50.
Schedules	Up to 50.
Schedule items	Up to 200 items, spanning over all the created Schedules.
Special days in the Calendar	Up to 50.
Contact lists	Up to 10.
Users	Up to 10.
Departements	Up to 100.
Network Cameras	Up to 16, one for each Access Point.
Log	Up to 10 000 events.

Accessories

GSM modem	In order to send text-messages and open the Access Points using the telephone, a separate GSM modem is required.
------------------	--

System Functions

Time Channels

- Manual time spans or schedules which can activate an Access Point to be either: locked/unlocked; request Card + PIN; block Door codes.

Triggers

- E-mail, text messages, IP notify and HTTP request notifies one or several recipients when selected events in the system occur.
- Events related to the Access Points, the Cardholders or divergences may be included or excluded.
- The Triggers may be active during manual time spans or Schedules.

Schedules

- Time spans for days and hours.
- Calendar with Special days.

Cards and Cardholders

- A Cardholder may have more than one Card.
- The Access Plans may be individual for each Cardholder.
- Personal Data may be imported to the system using CSV-files and used to register data.
- The so called Show card twice function, when the Access Point is controlled to respond in certain ways after a Card/tag has been displayed to the Card Reader twice.
- An Access Point may have a so called PIN cod timer, a function which controls the Access Point in a way which makes the Card Reader memorise the PIN for a set time when a Card + PIN is presented, thus unlocking the door by recognising the Card only.
- The Card holder may be granted a specified number of accesses. When the number of accesses has been counted for, the Card holder is to return the Card to the administrator.

Dynamic System designations and Help- and Language files

- The designation of the security system smartONE and the System designations may be changed to a personal preference.
- Different languages, such as English and Swedish may be uploaded by using the Language files of the system.
- Help files for each language.
- Dynamic Help files, which as well as giving help and instructions for the static functions are activated simultaneously as the optional functions.

Relay functions

- Motor Operated Lock
- Alarm by pass
- Automatic door
- Manual control via the Card Reader and/or Exit button.

Door codes

- 2 Door codes for each Access Point. The Door codes may be blocked separately or simultaneously.

Optional times for Access Points

- Unlocked door function
- Delay between Door Strike and Relay
- Block duration after incorrect Door code
- A Number of incorrect digits before the Card Reader blocks.

Overview of Log, Report and Journal

- A comprehensive overview of the Access Points and the administrative events of the system.

Network Camera

- One Network Camera for each Access Point may be connected to the system.
- Still images are displayed in the user interface.

Door bell

- By pressing the button * (star) on the Card Reader, a signal is sent to the computer. A signal indicates that somebody has pressed the button. A pop up window shows from which Access Point the signal comes, and the Access Point may be unlocked from the user interface.

Data base

- Saves backup copies of data and settings.
- Imports and Exports data.