AUTEC
Gesellschaft für Automationstechnik mbH

XMP-BABYLON

OPERATING MANUAL

ACCESS CONTROL READERS

XMP-TMC22/23XX

MIRO® / Hitag® 1/2
MIFARE® Classic / MIFARE DESFire®
LEGIC® prime / LEGIC® advant
HID iClass® / Barcode

Version: 1.4

Date: July 15, 2016

File: EXMP-TMC22-23xx_CONFIG_V1.4

Issued by:
AUTEC Gesellschaft für Automationstechnik mbH
Bahnhofstr. 57 - 61B
D - 55234 Framersheim
e-mail: vk@autec-gmbh.de
Tel.: +49 (0)6733 9201-0
Fax: +49 (0)6733 9201-91
Internet: www.autec-gmbh.de
www.autec-security.com

Copyright © 2016 by AUTEC GmbH

All rights reserved. Errors and omissions excepted

CONTENTS

1 GENERAL NOTES 7
1.1 NOTES ON CE MARK 7
1.2 SAFETY REGULATIONS AND WARNINGS 7
1.3 LIABILITY 7
1.4 QUALIFICATION OF PERSONNEL 8
1.5 SCOPE OF THE MANUAL 8
1.6 COPYRIGHT 9
1.7 TECHNICAL SUPPORT 9
2 PREREQUISITES 10
2.1 SOFTWARE-VERSIONS 10
2.2 FIRMWARE-VERSION 10
2.3 USER-DEFINITION – USER RIGHTS 10
2.4 DOCUMENTATION REFERENCES 11
3 GENERAL FEATURES OF XMP-TMC22/23XX READERS 12
3.1 READER OVERVIEW 12
3.2 CONNECTION POSSIBILITIES 13
3.3 SETTING THE READER ADDRESSES 14
3.4 ACTIVATION OF THE BOOT LOADER PROGRAM 14
3.5 MEANING OF THE LEDS 15
4 GENERAL INFORMATION ON MIFARE® CARDS 16
4.1 MEMORY STRUCTURE OF MIFARE® CLASSIC 1K 16
4.2 MEMORY STRUCTURE OF MIFARE® CLASSIC 4K 17
4.3 THE MIFARE® CLASSIC BLOCK ADDRESSES 4K 18
4.4 MEMORY STRUCTURE MIFARE®-DESFIRE EV1 19
5 GENERAL INFORMATION ON LEGIC®-CARDS 20
5.1 LEGIC® PRIME CARDS 20
5.2 LEGIC® ADVANT CARDS 20
5.3 MEMORY LAYOUT OF A SEGMENTED LEGIC-CARD 20
6 W3PORT - MENU "XMP-K32/XMP-K12 PARAMETERS" 21
6.1 THE REGISTRY CARD "COMMUNICATION" 23
6.1.1 Reader Serial Protocols 23
6.1.2 Protocol variants and data formats 24
6.1.3 Connection reader with different protocols 24
6.1.4 Definition badge structure 25
6.1.5 Settings in W3ACPARM for checking the ID-number 27
6.1.5.1 Comparison W3ACPARM with the 6-digit card number 27
6.1.5.2 Comparison W3ACPARM with 14-digit Personal number 28
6.1.5.3 Comparison W3ACPARM with 14-digit card-number via AW146 29
6.1.5.4 W3K32P - Menu Attributes - Checking badge number 30

6.1.6 PIN-code structure definition in W3K32P ... 31
6.1.6.1 Application examples of the code structure ... 32
6.2 THE REGISTRY CARD "FLAGS/READERS" ... 33
6.3 THE REGISTRY CARD "PARAMETERS / READERS" ... 36
6.3.1 Examples of door control configurations ... 40
6.3.2 Door control with door frame and handle contact ... 41
6.3.3 Door control with pass through contact ... 42
6.3.4 Door control with push button and alarm signalling ... 43
6.3.5 Door control with In/out readers ... 44
6.4 THE REGISTRY CARD "INPUTS/OUTPUTS" ... 45
7 W3TM24P – CALL THE UTILITY PROGRAM ... 47
7.1 W3TM24P – DISPLAY READER STATUS ... 47
7.2 LOAD NEW FIRMWARE INTO THE READER ... 49
7.3 CHANGE OF ADDRESS WITH IP67-READERS ... 50
8 CONFIGURATION MIFARE® CLASSIC ... 51
8.1 W3TM24P - MEANING OF SYMBOLS OF THE TASK BAR ... 51
8.1.1 MIFARE® Classic reader features ... 52
8.1.2 Meaning of the reader features ... 53
8.2 READING THE MIFARE® CLASSIC DATA ... 56
8.2.1 Reading the MIFARE® Classic Serial Number (UID) ... 56
8.2.2 Reading the memory data of MIFARE® Classic (Sector/Block) ... 57
8.2.2.1 Key definition for the badge identification ... 58
8.2.2.2 Setting of block number for reading memory data ... 59
8.2.2.3 Download of the parameters into the reader ... 60
9 SPECIAL APPLICATIONS MIFARE®-CLASSIC ... 61
9.1 THE "ELOCK" APPLICATION WITH MIFARE® CLASSIC ... 62
9.1.1 General ... 62
9.1.2 Programming steps for Offline-eLocks and access readers ... 62
9.1.3 Key-Definition for eLock-application ... 63
9.1.3.1 The field "No" ... 63
9.1.3.2 The field "Application" ... 63
9.1.3.3 The fields "Key" and "Activate" ... 63
9.1.3.4 The fields "Parameter 1, 2, 3" of the eLock-application ... 64
9.1.4 MIFARE® Classic 4K – Address-assignment for eLock data ... 65
9.2 THE "FINGERPRINT ON CARD" APPLICATION WITH MIFARE® CLASSIC ... 66
9.2.1 The fields "Parameter 1, 2, 3" of the fingerprint application ... 66
9.2.2 Overview Fingerprint Start Block Addresses - MIFARE® Classic ... 67
9.3 THE "ILOCK ON CARD" APPLICATION ... 68
9.3.1 General ... 68
9.3.2 Meaning of W3TM24P for the Ilock on Card Application ... 68
9.3.3 Meaning of Parameter 1 ... 68
9.4 CONFIGURATION OF PARAMETER SETTING CARDS FOR MIFARE® CLASSIC READERS ... 69
10 MAD1-DATA MIFARE® CLASSIC ... 71

10.1 DEFINITION OF THE MAD-PARAMETERS 73
10.1.1 The field “No.“ 73
10.1.2 The field “AID” 73
10.1.3 The field “Key“ 74
10.1.4 The field “Key type” 74
10.1.5 The field “Block“ 74
10.1.6 The checkbox “Manual input of badge sector“ 74
10.1.7 The field “Format” for MAD 75
10.1.8 The fields “Start position” and “Length” 75
10.1.9 The checkbox “Deactivate MAD“ 75
11 READER SPECIFICATION MIFARE DESFIRE® EV1 76
11.1 W3TM24P - MEANING OF THE SYMBOLS OF THE TASK BAR 76
11.2 MIFARE DESFIRE® READER FEATURES 76
11.3 MIFARE DESFIRE® - MEANING OF THE READER FEATURES 77
11.4 MEANING OF THE MIFARE® DESFIRE PARAMETERS 80
11.4.1 The field “No.“ 80
11.4.2 The field “Application” 80
11.4.3 The field “Appl.-ID” 81
11.4.4 The field “File-ID“ 81
11.4.5 The field “Key-No” 82
11.4.6 The Field “HByte“ 82
11.4.7 The field “Length” and “Offset“ 83
11.4.8 The field “Security-Parameter” 84
11.4.9 The field “KDiv” 84
11.4.9.1 Objective of Key-Diversification 84
11.4.9.2 Requirements for Key-Diversification 85
11.4.9.3 Reading process by Key Diversification 85
11.4.10 The fields “Parameter 1 and 2” 86
11.4.11 The DESFire Key-Definition 86
12 MIFARE DESFIRE® APPLICATIONS 87
12.1 THE UID-APPLICATION 87
12.2 THE ACCESS CONTROL APPLICATION 87
12.3 THE ACCESS CONTROL APPLICATION WITH “KEY-DIVERSIFICATION” 88
12.3.1 Settings in Controller and W3PORT 88
12.4 THE ELOCK-KEY APPLICATION 89
12.4.1 General 89
12.4.2 Programming steps for Offline-eLocks and access readers 89
12.4.3 Settings in W3TM24P 90
12.4.4 The fields Length and Offset 90
12.4.5 Security-Parameter for eLock-Application 90
12.5 CONFIGURATION OF A MIFARE DESFIRE® PARAMETER CARD 91
13 READER SPECIFICATION HITAG® 92
13.1 MEANING OF THE SYMBOLS IN THE TASK BAR HITAG 92
13.2 HITAG® READER FEATURES 93

14 READER SPECIFICATION LEGIC® PRIME 94
14.1 GENERAL 94
14.2 LEGIC® READER FEATURES 94
14.3 MEANING OF SYMBOLS OF THE TASK BAR LEGIC 95
14.4 LEGIC® READER FEATURES 95
14.5 READER CONFIGURATION LEGIC® PRIME 97
14.6 DEFINITION OF THE LEGIC® SETUP PARAMETERS 98
14.7 LEGIC® PRIME APPLICATIONS 99
14.7.1 Reading badge number from segment X 99
14.7.2 Reading the badge number with Search string 99
14.7.3 Reading badge number with extended settings 100
14.8 DOWNLOAD OF LEGIC PRIME READER SETTINGS 100
15 READER SPECIFICATION LEGIC® ADVANT 101
15.1 ADDITIONAL HINT FOR LEGIC® CHIPS SM4200 AND SM4200M 101
15.1.1 SM4200 - LEGIC® prime & advant 101
15.1.2 SM4200M - LEGIC® prime & advant / MIFARE® classic & DESFire EV1 102
15.2 MEANING OF THE LEGIC® ADVANT PARAMETERS 103
15.3 READING THE LEGIC® ADVANT APPLICATION 106
15.3.1 Reading the UID-Application 106
15.3.2 Reading the Access Control-Application 106
15.3.3 Reading the Access Control-Application with CRC-Check 106
15.3.4 Reading the Access Control-Application with search string 107
15.4 DOWNLOAD OF LEGIC® ADVANT READER SETTINGS 107
16 READER SPECIFICATION HID ICLASS® (13.558MHZ) 108
16.1 MEANING OF THE SYMBOLS IN THE TOOL BAR HID 108
16.2 HID® READER FEATURES 108
17 READER SPECIFICATION 2D-SCANNER 109
17.1 2D-SCANNER READER FEATURES 109
18 FIRMWARE-UPDATE OF READERS 110
19 DATA POINTS AND ATTRIBUTES FOR READERS 111
20 DOCUMENTATION HISTORY 112

1 General Notes

1.1 Notes on CE Mark

EU directive

The following is applicable for the equipment described in this installation manual. The product fulfils the requirements of EU directive 2004/108/EC on “Electromagnetic compatibility” and EU directive 2006/95/EC, the “Low voltage directive”.

The EU Declarations of Conformity are kept available to the competent authorities at the following address:

AUTEC Gesellschaft für Automationstechnik mbH

Prod. Group: T/HE/SYS/D

Bahnhofstr. 57-61b

D - 55234 Framersheim

1.2 Safety regulations and warnings

The unit must only be used for the purpose intended by the manufacturer. The operating instructions must be kept to hand and made available to every user. Unauthorized changes and the use of spare parts and accessories which are not sold or recommended by the manufacturer of the unit could cause fire, electric shock or injury. Therefore, such measures will result in a renunciation of liability and the manufacturer will not accept any guarantee claims.

The manufacturer's guarantee terms in the version valid at the time of the sale are applicable to the unit. No liability will be accepted for unsuitably or incorrectly set parameters – whether automatic or manual – or for inappropriate use of the unit.

All repairs must be carried out by the manufacturer.

The user is responsible for ensuring that the unit is set up and connected in accordance with the recognized technical regulations in the country of installation and any other guidelines valid in the relevant region. Before opening the unit, always switch off the power supply and take measurements to ensure that there is no power to the unit.

1.3 Liability

We have checked that the content of this document agrees with the hardware described. However, it cannot be ruled out that there are discrepancies, so we cannot provide any guarantee that it agrees completely.

However, the information in this document is checked on a regular basis. Any corrections necessary are incorporated into subsequent editions. We are always happy to receive your comments and suggestions.

1.4 Qualification of personnel

With respect to the safety-related instructions in this manual or on the product itself, qualified personnel are persons who are familiar with the safety strategy of the access control systems and who have undergone training qualifying them to repair such access control mechanisms or who are authorized to work with electrical circuits and devices in accordance with the standards of safety engineering. This is especially the case when working with the door of the device open.

All electrical connections and work on the equipment/systems must only be carried out by persons and companies qualified to carry out such work.

Work on the equipment/systems by unqualified personnel or failure to observe the warnings detailed in this manual could result in severe physical injury or material damage.

1.5 Scope of the manual

This manual describes the parameterization of the reader family XMP-TMC22/23xx for reading HITAG® / MIFARE® / LEGIC®, HID® and barcode.

The RFID card readers XMP-TMC22/23xx are new proximity ID-Card readers with 125 KHz or 13.558MHz technology. The card readers are connected to the door controllers XMP-K32 / XMP-K12. The readers read either the unique serial number (UID) of proximity ID-Cards, or the personalized ID-number out of the card memory. The card number will be transmitted to the access control system via XMP-K12/XMP-K32-Controllers for processing.

After factory delivery the card readers always read the serial number of the corresponding card (UID). After having connected the readers to the door controllers, the definition and the parameterization of the readers at the connected door controller should be done via the XMP-BABYLON-Software.

The card readers of the type XMP-TMC22/23xx support the following RFID-Technologies:

MIRO® / Hitag®	125kHz proximity: MIRO (EM4102), Hitag 1, Hitag 2
MIFARE® Classic MIFARE DESFire®	13.558MHz proximity ISO14443A / ISO7816
LEGIC® prime / advant	13.558MHz proximity LEGIC® standard (prime) ISO14443A/ISO15693
HID iClass®	13.558 MHz
Barcode	1D und 2D

1.6 Copyright

Copyright AUTEC Gesellschaft für Automationstechnik mbH 2014. All rights reserved. This document and its content may not be passed on, reproduced, used or communicated in any way without explicit consent. Any contravention of this will result in a right to claim for damages.

All rights reserved.

1.7 Technical support

If you have any queries about the product or if you require technical support, please contact the following address:

AUTEC Gesellschaft für Automationstechnik mbH
Prod. Group: T/HE/SYS/D
Bahnhofstr. 57-61b
D - 55234 Framersheim

e-mail: helpdesk@autec-gmbh.de

Tel.: +49 6733 9201-0

2 Prerequisites

2.1 Software-versions

The documentation refers to the following program and firmware versions:

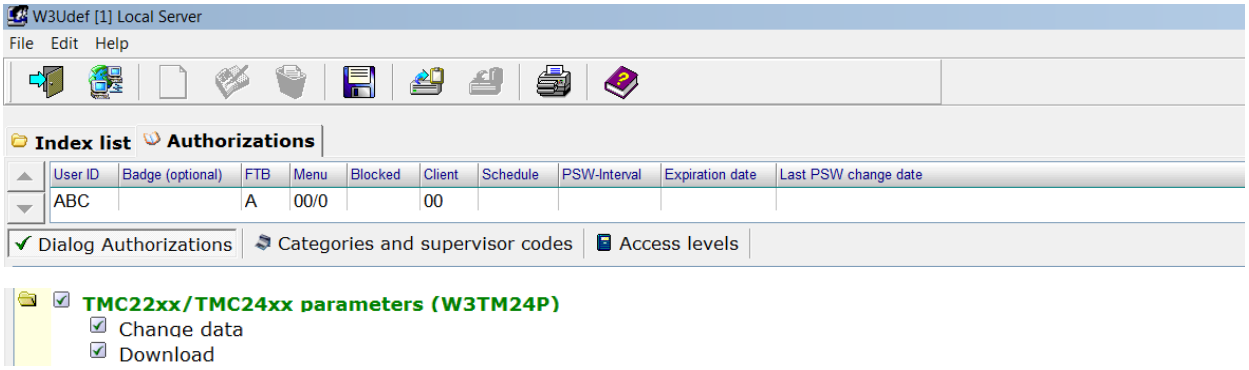
Programs	Versions
W3D	Version 3.9
N3.exe	Version 6.1.106
N3IBO	6.1.017
W3IP.DLL	Version dated June 11, 2013
W3TM24P	From version 1.2
W3K32P	From version 2.9

2.2 Firmware-Version

Device	Version
XMP-K32 Firmware	Version 4.4 dated July 26, 2010

2.3 User-definition – User rights

The authorization to call the program must be set in the user definition from the system administrator for each user.



You find a detailed description of the user definition („W3UDEF.EXE“) in the manual EW3UDEF_User-definition_Vx.x.

2.4 Documentation References

More details are available in the documentation:

- Software/XMP-BABYLON-IBO-Handbücher / E_TM24P_reader settings
- Door Controllers / XMP-K32 Information / XMP-K32 / XMP-K32sx / XMP-K32sx-19 Operating manual
- E-PIN-Code Configuration Manual

3 General Features of XMP-TMC22/23xx Readers

3.1 Reader Overview

The table gives a general overview of the currently available RFID-readers for access control with the relevant reader technologies.

x = available

Reader type	Keyboard	Miro / Hitag ®	MIFARE® Classic	MIFARE DESFire®	LEGIC® prime	LEGIC® advant	HID iCLASS®	Barcode 1D/2D
OEM Door frame reader								
XMP-TMC2210	x							
XMP-TMC2230		x						
XMP-TMC2240	x	x						
XMP-TMC2250			x	x				
XMP-TMC2260	x		x	x				
XMP-TMC2270					x	x		
XMP-TMC2280	x				x	x		
OEM Reader								
XMP-TMC2310	x							
XMP-TMC2330		x						
XMP-TMC2340	x	x						
XMP-TMC2350			x	x				
XMP-TMC2360	x		x	x				
XMP-TMC2370					x	x		
XMP-TMC2380	x				x	x		
XMP-TMC2390							x	
XMP-TMC2395	x						x	
Turnstile Reader								
XMP-TMC2450-TUR			x	x				
XMP-TMC2450-TUR-2D			x	x				x
Behnke Reader								
XMP-TMC2330-B*		x						
XMP-TMC2350-B*			x	x				
XMP-TMC2370-B*					x	x		
Siedle Reader								
XMP-TMC2310-S*	x							
XMP-TMC2330-S*		x						
XMP-TMC2340-S*	x	x						
XMP-TMC2350-S*			x	x				
XMP-TMC2360-S*	x		x	x				
XMP-TMC2370-S*					x	x		
XMP-TMC2380-S*	x				x	x		
Siedle Display Reader								
XMP-TMC2350-LCD-S*			x	x				
Flush-mounted Reader DIN 49073								
XMP-TMC2430-UP		x						
XMP-TMC2450-UP			x	x				
XMP-TMC2470-UP					x			
Explosion-proof Reader								
XMP-TMC2450-EX			x	x				

3.2 Connection possibilities

To connect the readers to the controller a star wiring, a bus-shaped or a mix of bus shaped and star-shaped wiring are possible.

a) star shaped b) bus shaped c) Mix star- bus shaped

If the card readers are supplied internally by the controller, the reader distance of respectively 100m at 12VDC and 200m at 24VDC should not be exceeded.

In the case of a mixed or bus wiring, the fuses for the readers must be adjusted (factory-500mA) with respect to the expected current flow!

3.3 Setting the reader addresses

Meaning of the DIP-Switches SW1

Switch	Meaning
1-3	For binary setting of reader addresses 0…7
4	Default OFF
5	Baud rate setting to XMP-K32/XMP-K12 OFF = 9600; ON = 19200 baud
6	On= UCI protocol active - Off= SecuCrypt® protocol active
7	Reserved
8	ON = Boot loader program activated

All card readers are issued with an individual address. Setting an address twice in one bus configuration will lead to address conflict and malfunction.

The reader address must be set using the micro switches 1-3 in binary way as follows:

DIP 1	DIP 2	DIP 3	Address
Off	Off	Off	0
On	Off	Off	1
Off	**On**	Off	2
On	**On**	Off	3
Off	Off	**On**	4
On	Off	**On**	5
Off	**On**	**On**	6
On	**On**	**On**	7

3.4 Activation of the boot loader program

In normal operation, there is no need to activate this switch. It can only be necessary if a firmware download to the reader is interrupted by switching off the power supply and then the application program in the reader cannot be restarted. For starting the boot loader program the switch 8 of SW1 is set to ON and the reader should be restarted.

The loading process is signaled at the reader by the alternating lighting of the yellow and red LED in 0.5 second intervals.

3.5 Meaning of the LEDs

The reader has three LEDs with the colors yellow, red and green.

LED Status	Meaning
Yellow on	Normal operation
Yellow flashing in 0.5 second cycle	No communication to the door control unit
Red on for time x	Access granted
Green on for time x	Access denied
Yellow and red flashing in 0.5 second cycle	Boot loading program activated
Yellow, red and green on	Reader blocked
Yellow on, red and green flashing in 0.5 second cycle	PIN-code input expected
Reverse side D4	Communication TXD
Reverse side D5	Communication RXD

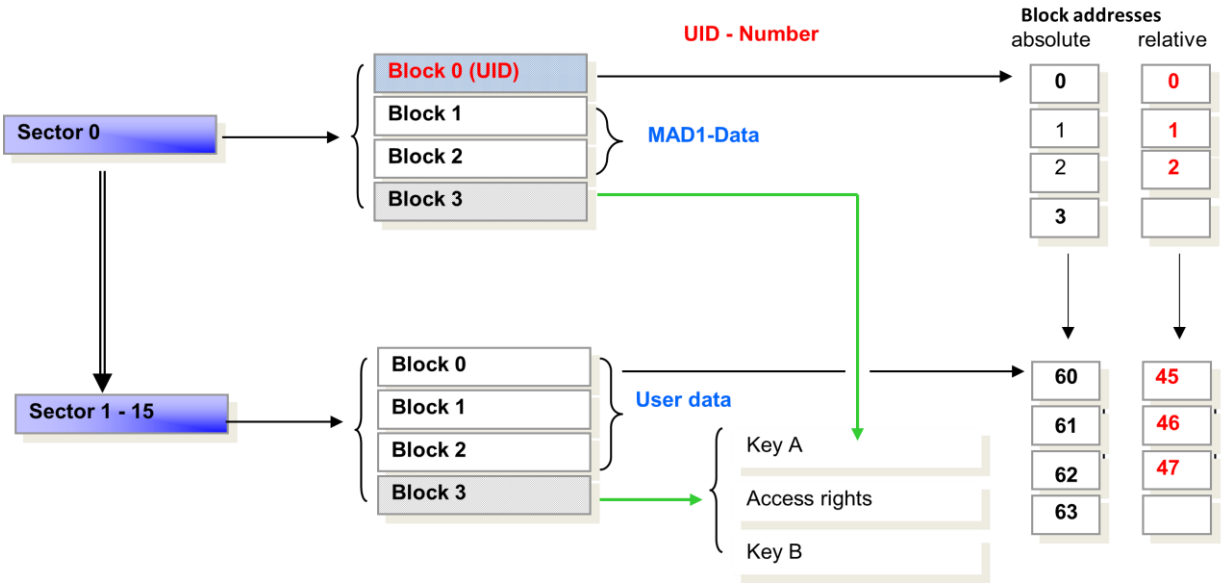
The times for activating the LEDs can be set in the XMP-BABYLON system through the attributes RC (Red Count), GC (Green Count) and RG (Red Green) of the system data point SY, card 2, channels 1-8.

4 General information on MIFARE® cards

4.1 Memory Structure of MIFARE® Classic 1K

The memory of Mifare 1K card is divided into 16 equal blocks of memory. The unique serial number of the chip is stored in sector 0 / block 0. In the sectors 1 to 15, the blocks 0, 1 and 2 contain user data.

The block 3 of the sectors includes the key and access rights and is not available as user data.

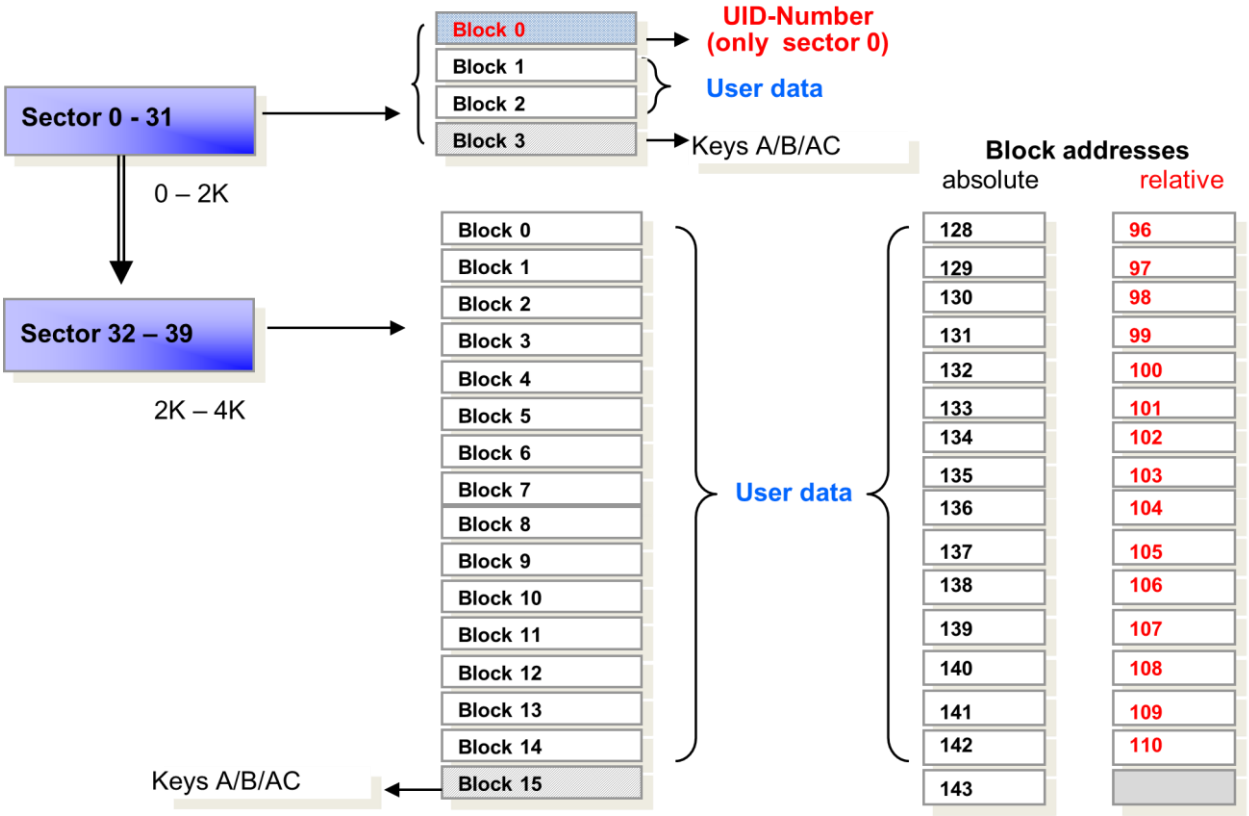


4.2 Memory structure of MIFARE® Classic 4K

The memory of Mifare 4K has in his first memory half (0K-2K), the same block structure as the 1K card (each sector contains 4 blocks), but the memory of 2K to 4K is divided into 8 sectors, each of 16 blocks. The unique serial number of the chip is stored in sector 0 / block 0.

The user data are available in blocks 0 to 2 in the sectors 1 to 31 and in blocks 0 to 14 in the sectors 32 to 39.

The keys A, B, and the access rights are in the respective sectors 3 (0K-2K) and 15 (2K-4K).



4.3 The Mifare® Classic Block addresses 4K

0-1K			
Adressen/Addresses			
Sec.	Blo.	abs.	rel.
0	0	0	0
	1	1	1
	2	2	2
	3	3	
1	0	4	3
	1	5	4
	2	6	5
	3	7	
2	0	8	6
	1	9	7
	2	10	8
	3	11	
3	0	12	9
	1	13	10
	2	14	11
	3	15	
4	0	16	12
	1	17	13
	2	18	14
	3	19	
5	0	20	15
	1	21	16
	2	22	17
	3	23	
6	0	24	18
	1	25	19
	2	26	20
	3	27	
7	0	28	21
	1	29	22
	2	30	23
	3	31	
8	0	32	24
	1	33	25
	2	34	26
	3	35	
9	0	36	27
	1	37	28
	2	38	29
	3	39	
10	0	40	30
	1	41	31
	2	42	32
	3	43	
11	0	44	33
	1	45	34
	2	46	35
	3	47	
12	0	48	36
	1	49	37
	2	50	38
	3	51	
13	0	52	39
	1	53	40
	2	54	41
	3	55	
14	0	56	42
	1	57	43
	2	58	44
	3	59	
15	0	60	45
	1	61	46
	2	62	47
	3	63	

1-2K			
Adressen/Addresses			
Sec.	Blo.	abs.	rel.
16	0	64	48
	1	65	49
	2	66	50
	3	67	
17	0	68	51
	1	69	52
	2	70	53
	3	71	
18	0	72	54
	1	73	55
	2	74	56
	3	75	
19	0	76	57
	1	77	58
	2	78	59
	3	79	
20	0	80	60
	1	81	61
	2	82	62
	3	83	
21	0	84	63
	1	85	64
	2	86	65
	3	87	
22	0	88	66
	1	89	67
	2	90	68
	3	91	
23	0	92	69
	1	93	70
	2	94	71
	3	95	
24	0	96	72
	1	97	73
	2	98	74
	3	99	
25	0	100	75
	1	101	76
	2	102	77
	3	103	
26	0	104	78
	1	105	79
	2	106	80
	3	107	
27	0	108	81
	1	109	82
	2	110	83
	3	111	
28	0	112	84
	1	113	85
	2	114	86
	3	115	
29	0	116	87
	1	117	88
	2	118	89
	3	119	
30	0	120	90
	1	121	91
	2	122	92
	3	123	
31	0	124	93
	1	125	94
	2	126	95
	3	127	

2-3K			
Adressen/Addresses			
Sec	Blo.	abs.	rel.
32	0	128	96
	1	129	97
	2	130	98
	3	131	99
	4	132	100
	5	133	101
	6	134	102
	7	135	103
	8	136	104
	9	137	105
	10	138	106
	11	139	107
	12	140	108
	13	141	109
	14	142	110
	15	143	
33	0	144	111
	1	145	112
	2	146	113
	3	147	114
	4	148	115
	5	149	116
	6	150	117
	7	151	118
	8	152	119
	9	153	120
	10	154	121
	11	155	122
	12	156	123
	13	157	124
	14	158	125
	15	159	
34	0	160	126
	1	161	127
	2	162	128
	3	163	129
	4	164	130
	5	165	131
	6	166	132
	7	167	133
	8	168	134
	9	169	135
	10	170	136
	11	171	137
	12	172	138
	13	173	139
	14	174	140
	15	175	
35	0	176	141
	1	177	142
	2	178	143
	3	179	144
	4	180	145
	5	181	146
	6	182	147
	7	183	148
	8	184	149
	9	185	150
	10	186	151
	11	187	152
	12	188	153
	13	189	154
	14	190	155
	15	191	

3-4K			
Adressen/Addresses			
Sec.	blo.	abs.	rel.
36	0	192	156
	1	193	157
	2	194	158
	3	195	159
	4	196	160
	5	197	161
	6	198	162
	7	199	163
	8	200	164
	9	201	165
	10	202	166
	11	203	167
	12	204	168
	13	205	169
	14	206	170
	15	207	
37	0	208	171
	1	209	172
	2	210	173
	3	211	174
	4	212	175
	5	213	176
	6	214	177
	7	215	178
	8	216	179
	9	217	180
	10	218	181
	11	219	182
	12	220	183
	13	221	184
	14	222	185
	15	223	
38	0	224	186
	1	225	187
	2	226	188
	3	227	189
	4	228	190
	5	229	191
	6	230	192
	7	231	193
	8	232	194
	9	233	195
	10	234	196
	11	235	197
	12	236	198
	13	237	199
	14	238	200
	15	239	
39	0	240	201
	1	241	202
	2	242	203
	3	243	204
	4	244	205
	5	245	206
	6	246	207
	7	247	208
	8	248	209
	9	249	210
	10	250	211
	11	251	212
	12	252	213
	13	253	214
	14	254	215
	15	255	

Abs. = absolute Adresse
rel. = relative Adresse

Sec. = Sektor Nr.
Blo. = Block Nr.

Sektor/Trailer Blöcke
Sector/Trailer blocks

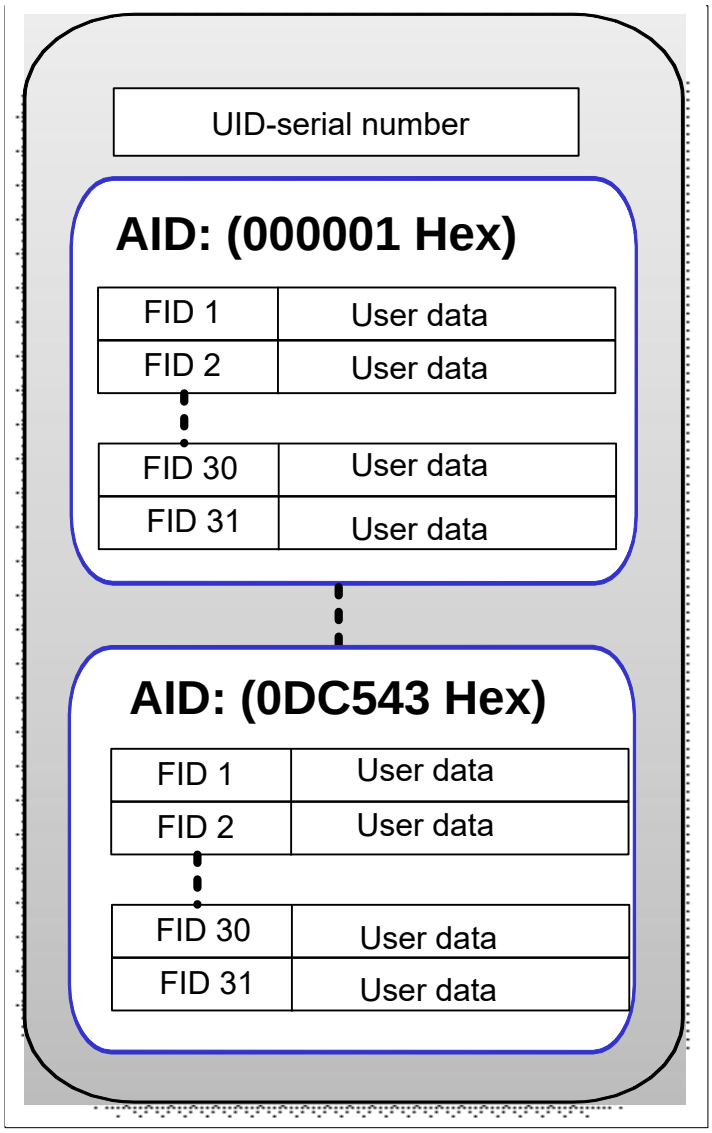
4.4 Memory structure Mifare®-DESFire EV1

MIFARE Desfire® EV1-cards are available in versions with 2k, 4k and 8k (2048, 4096 or 8192 bytes). Unlike the Mifare Classic, there is no fixed number of segments with a fixed size.

MIFARE Desfire® cards must be encoded before first use and initialized. First, the individual applications must be defined in detail and then stored in the file system of the cards.

The algorithms DES, 3DES and AES (Advanced Encryption Standard) are available, but the company AUTEC uses the AES-algorithm.

In the memory of Mifare DESFire EV1 chip up to 28 applications can be defined. Each application can be created with up to 32 files. Each file has its own AID (Application IDentifier).



5 General information on LEGIC®-Cards

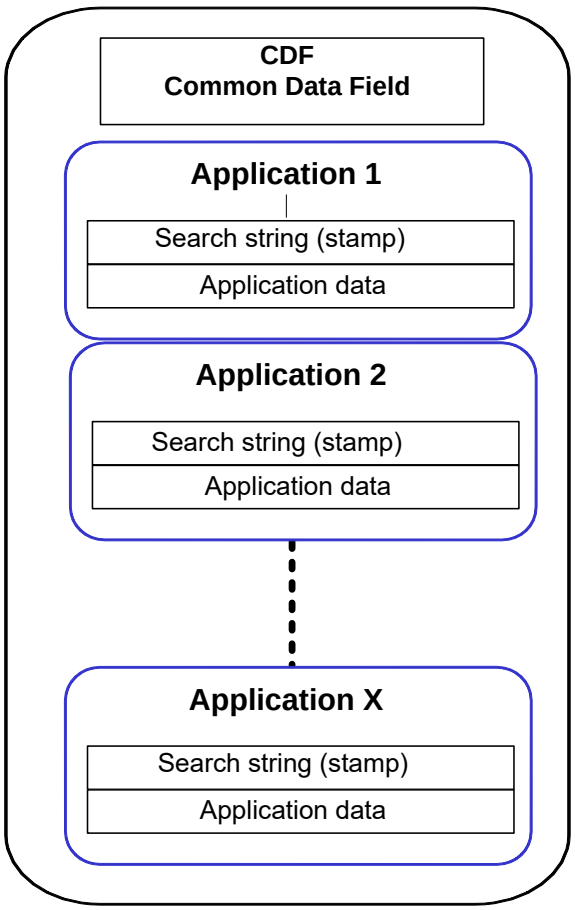
5.1 LEGIC® prime Cards

These cards have a maximum storage capacity of 1024 bytes and can operate up to 127 applications in one card. The unique serial number (UID) or memory data can be read in the LEGIC cards.

5.2 LEGIC® advant Cards

LEGIC® advant cards are compatible with ISO standards 15693 and 14443 A. Up to 127 applications can be defined. The size of an application is not limited. Unlike LEGIC® prime the read/write speed of LEGIC® advant is more efficiently. To encrypt the communication channels the readers XMP-TMC22/23xx use the AES-128 bit encryption.

5.3 Memory layout of a segmented Legic-card



Common Data Field (CDF)

MCD = License number of the chip 1 Byte

MSN = Serial number of the chip 3 Byte

MCC = Check sum of MCD and MCC 1 Byte

DCF = Encoded type of card

And the organization level 2 Byte

Security function WRite Protected WRP

- WRite Conditional WRC
- Read Disable RD 1 Byte

SSC = License number of system supplier

6 W3PORT - Menu “XMP-K32/XMP-K12 Parameters“

Left mouse-click on the menu button

in W3Port activates the program **W3K32p.exe**.

The meaning of the symbols in the top-line menu is as follows:

Exit program

Reboots the XMP-K32/ DS32

XMP-K32 data/ parameters will be load from a file on the central computer.

XMP-K32 data/ parameters will be saved into a file on the central computer.

Upload of data/ parameters from XMP-K32/ DS32

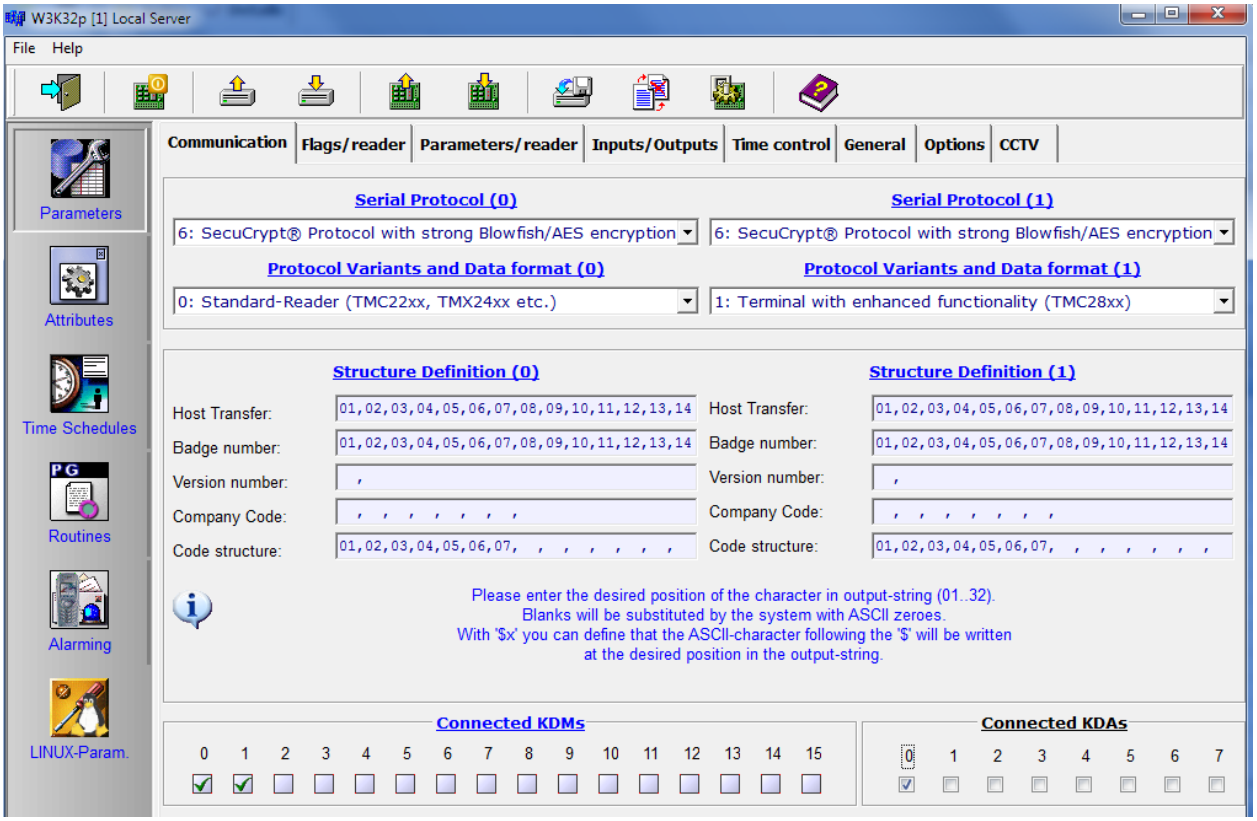
Download of data/ parameters into the XMP-K32/ DS32.

Data/ parameters of another XMP-K32/ DS32 can be imported.

The current data/ parameters will be overwritten by default values.

A sub-menu with utility functions opens.

Overview W3K32P



There are further menu buttons on the left range of the window: ***Attributes***, ***Time-Schedules, Routines, Alarming and LINUX-Parameters***.

The menu ***Parameters*** consists of different registry cards. So it is possible to specify further properties of the controller as well as peripheral units which are connected to it.

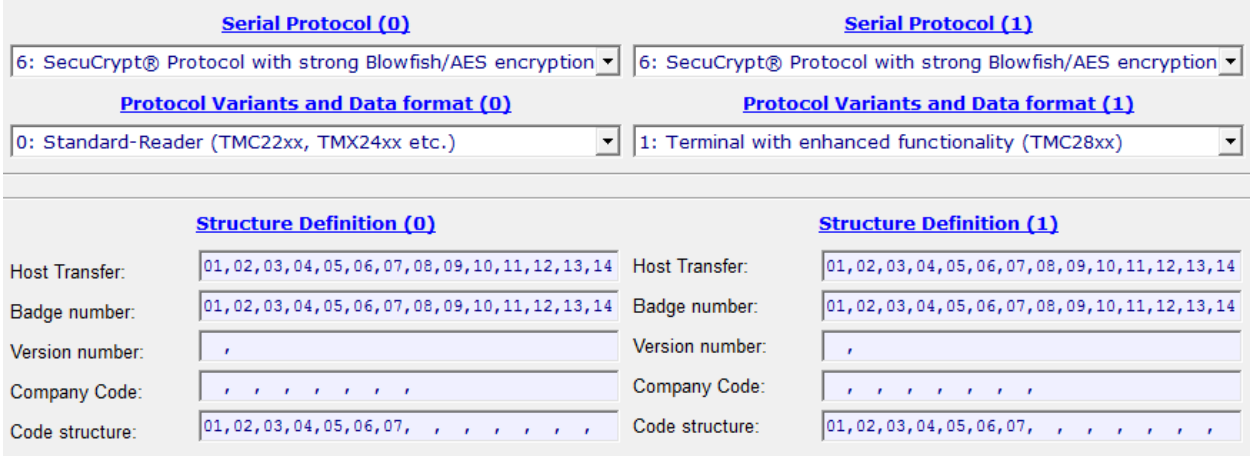
Peripheral units are e.g. card readers, door locks, extension modules (XMP-KDM-16, XMP-KDA-24), alarm contacts, etc…

Furthermore, for the XMP-K32 must be specified e.g. communication protocols, data structures or response times, too.

The registry cards of the menu program ***Parameters*** are described in the following.

6.1 The registry card "Communication"

In the registry card ***Communication*** the definitions are specified for the data communication between XMP-K32 and the card readers connected to it as well as for the evaluation of the card identification data.

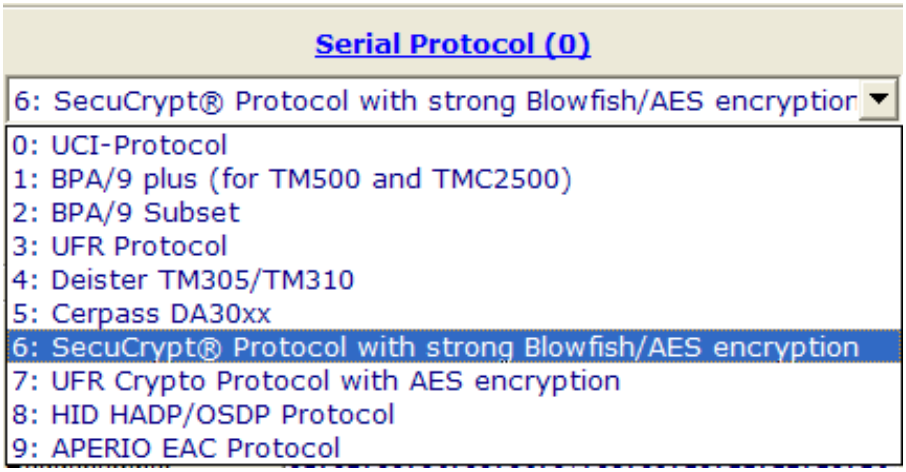


The following settings can be defined:

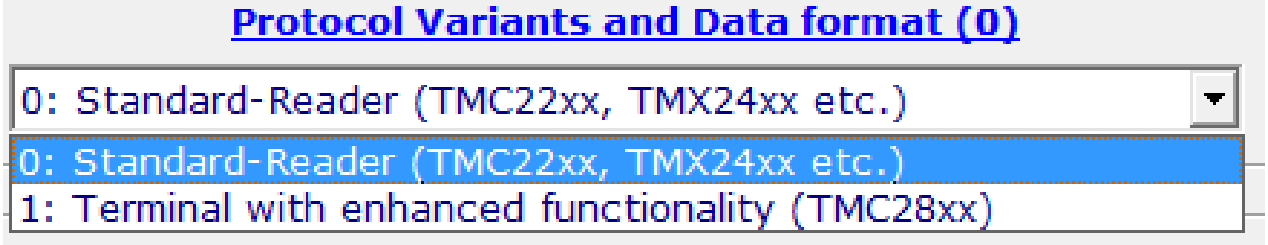
- Serial Protocol (0 or 1)
- Protocol and data format (0 or 1)
- Structure Definition (0 or 1)

6.1.1 Reader Serial Protocols

The following serial protocols can be selected:



6.1.2 Protocol variants and data formats

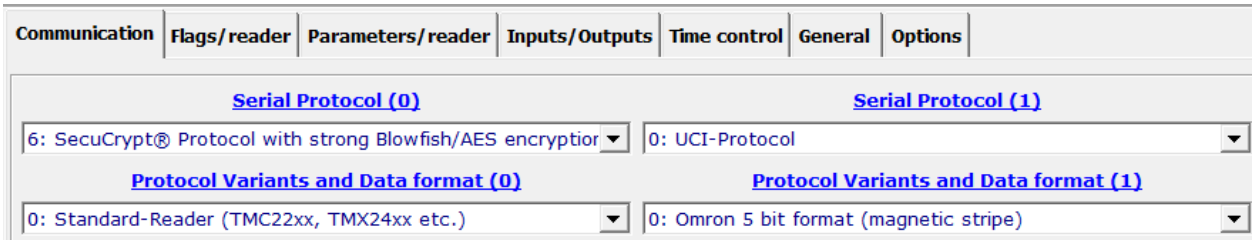


Here you can select the protocol variant and data format between access control and time management readers.

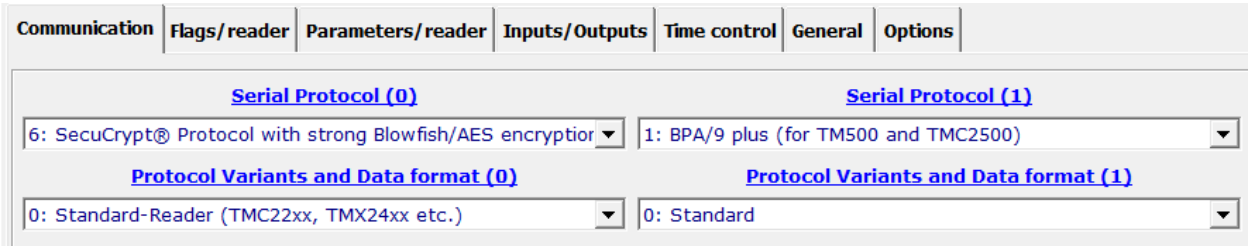
6.1.3 Connection reader with different protocols

AUTEC-readers (no other readers) can be connected with Secucrypt-Protocol and UCI or BPA9 protocol on the same controller.

SecuCrypt and UCI



SecuCrypt and BPA9



For all other foreign readers or communication protocols, AUTEC cannot accept any liability.

6.1.4 Definition badge structure

W3K32P

Structure Definition (0)

Host Transfer:	01,02,03,04,05,06,07,08,09,10,11,12,13,14	Online	→ Interface to reader
Badge number:	01,02,03,04,05,06,07,08,09,10,11,12,13,14	Offline	→ Definition badge number
Version number:	,	Offline	
Company Code:	, , , , , , ,	Offline + Online	
Code structure:	, ,01,02,03,04,$0, , , , , , ,	Offline + Online	

W3ACPARM

Badge-number		
01,02,03,04,05,06,07,08,09,10,11,12,13,14	Online	→ Definition badge number

Host Transfer:

Up to 32 characters of card information can be read. However, the XMP-K32 always transmits 14 characters of identification card information to the master computer.

The sequence of the 14 characters which are transmitted to the master computer is defined here as a selection from the maximum 32 characters [01-32] received from the reader.

Example: (01,02,03,04,05,06,07,08,09,10,11,12,13,14)

Blanks (empty fields) are replaced by ASCII zeros from the system.

An input of the form „$x “(x = ASCII character) causes the appearance of the ASCII character that follows after the $ character at the appropriate position of the output string.

Badge number:

By entering data positions into these fields (assuming from the data positions transmitted by the reader) the sequence of the card identification number for offline mode is defined here.

Example: (,09,10,11,12,13, , , , , , , ,)

The sequence of the example corresponds to a 6 digit card number with leading zero.

Version number:

By entering data positions into these two fields (assuming from the data positions transmitted by the reader) a version number can be defined.

This number will be checked in off-line mode.

Example: (,08)

The input indicated in the example corresponds to a version number with two digits with leading zero.

The off-line check of the version number can be suppressed by setting flag 4 in register card **Options**.

Company Code

By entering data positions into these fields (assuming from the data positions transmitted by the reader) the sequence of a company code for the online and offline mode is defined.

In the online case the company code is always checked in connection with the card identification number.

Example: (01, 02, 03, 04, ,) There is also the possibility of checking only the company code.

Code structure:

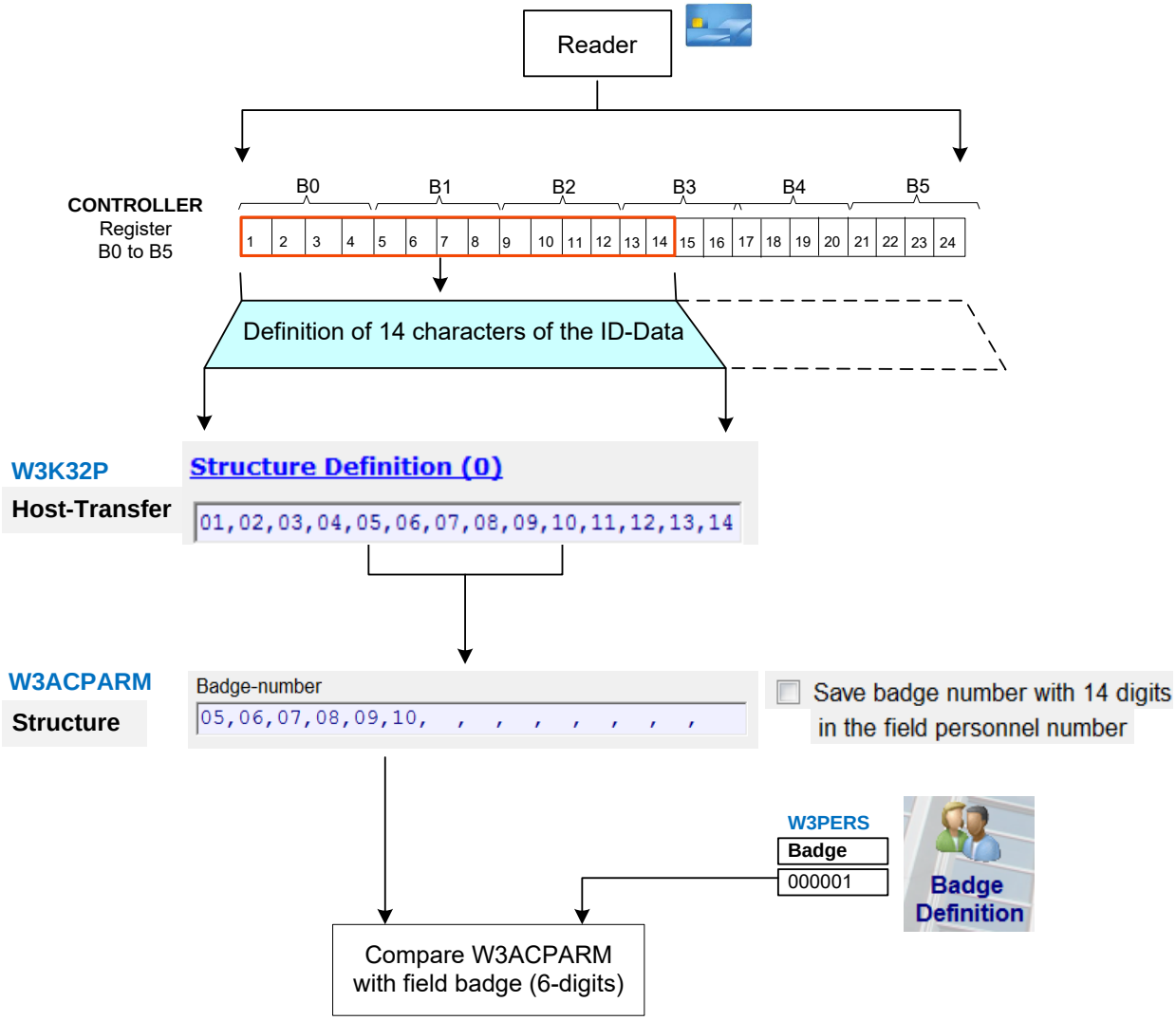
By entering the pin code data positions into these fields (assuming from the pin code data positions transmitted by the reader) the sequence for the pin code evaluation is defined for the system.

Example: (01,02,03,04,05,06,07, , , , , , ,)

6.1.5 Settings in W3ACPARM for checking the ID-number

6.1.5.1 Comparison W3ACPARM with the 6-digit card number

In the program W3ACPARM, The digits representing the card number in the field “Host-transfer” are entered in the field “badge number” of W3ACPARM. This value will be compared with the field **Badge** in the personnel database (W3PERS).



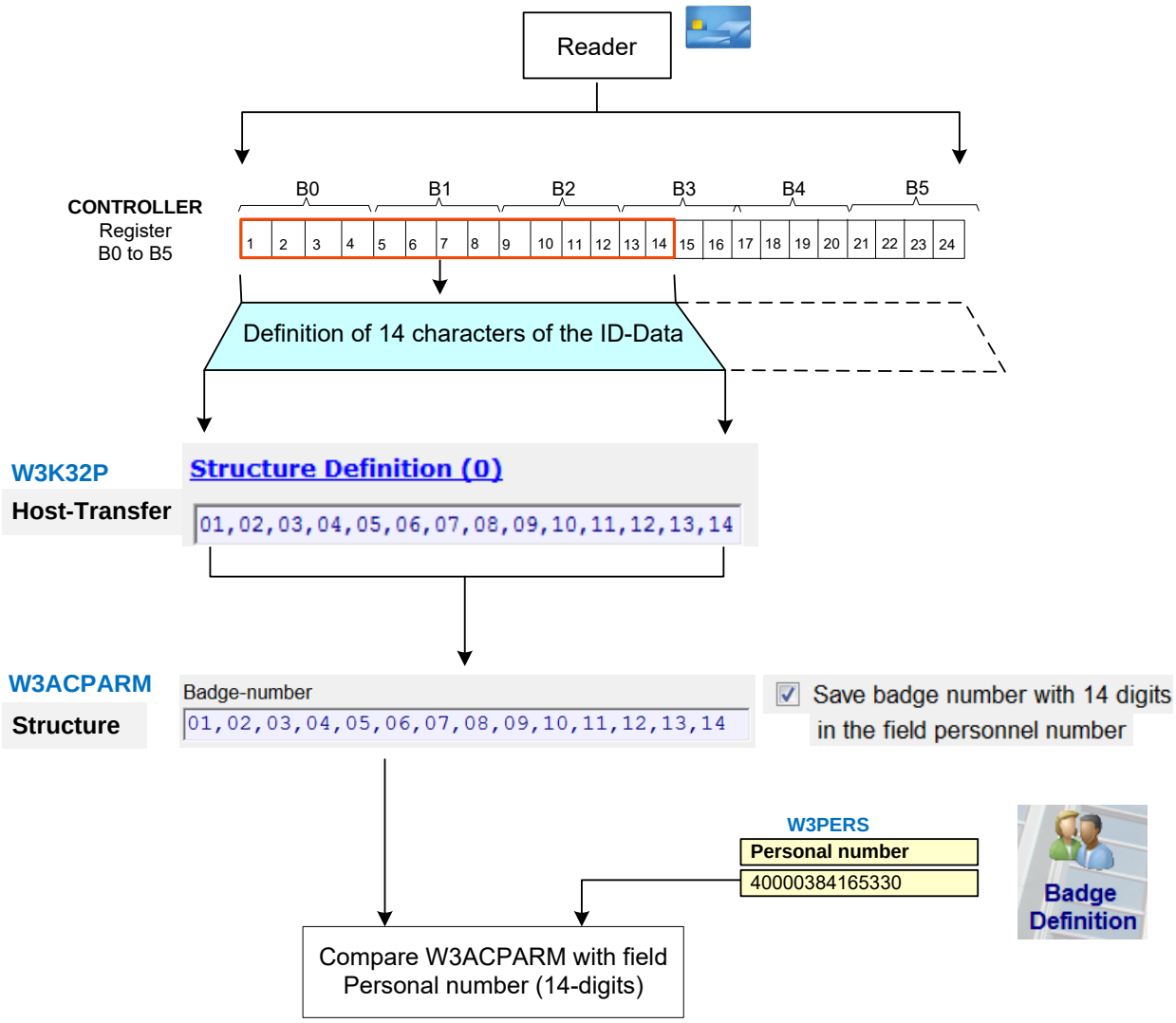
The positions 5 to 10, representing the 6-digit card number in Host-transfer, will be entered in W3ACPARM as badge number for online check.

6.1.5.2 Comparison W3ACPARM with 14-digit Personal number

In the program W3ACPARM, The digits representing the card number in the field “Host-transfer” are entered in the field “badge number” of W3ACPARM. This value will be compared with the field **Personal number** in the personnel database (W3PERS).

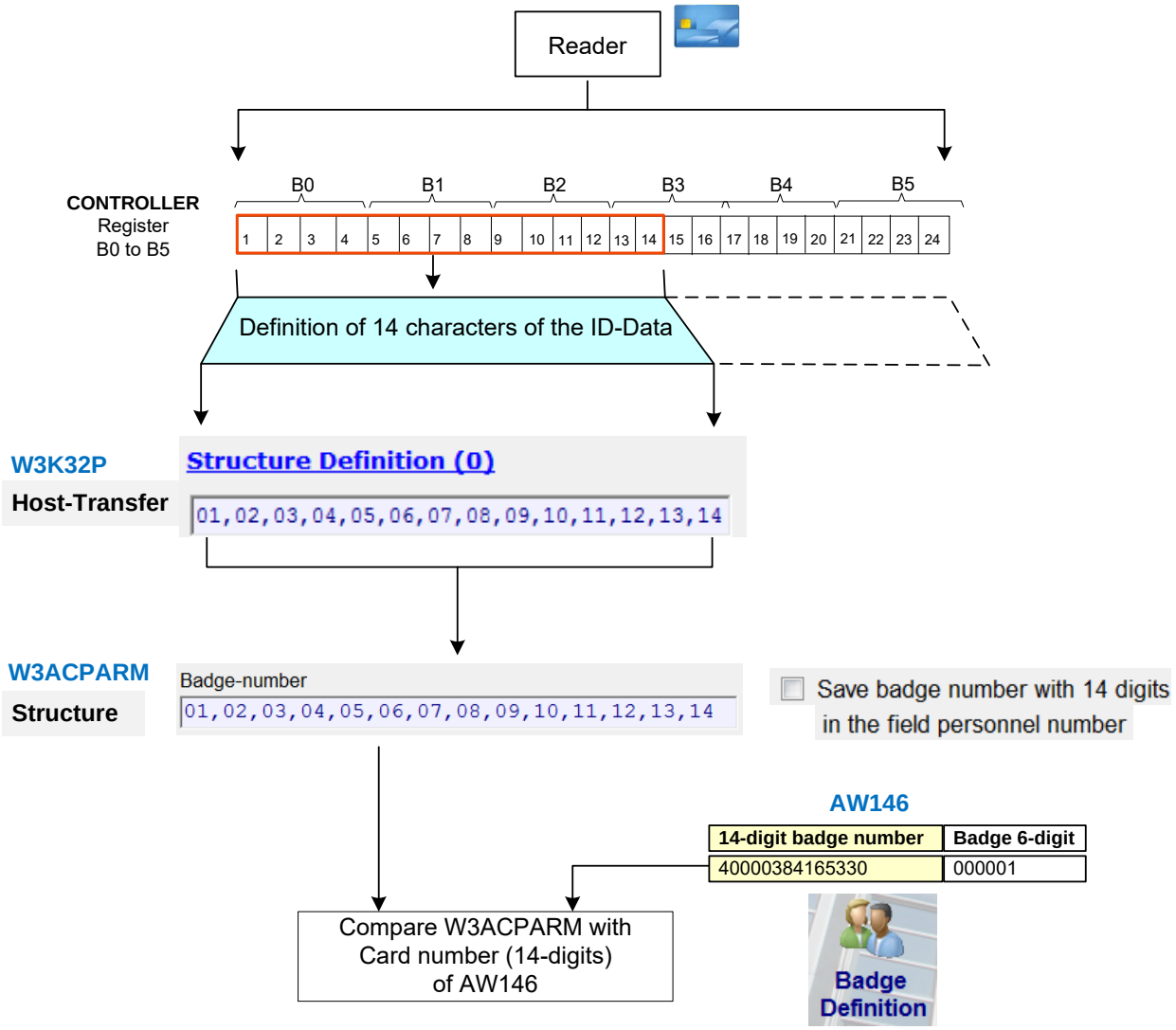
The function “Save badge number..” must be activated.

☑ Save badge number with 14 digits in the field personnel number



6.1.5.3 Comparison W3ACPARM with 14-digit card-number via AW146

If a 14-digit badge number is required, the XMP-BABYLON system uses the translation table AW146 for checking access. This database contents the 14-digit badge numbers of all employees and their corresponding 6-digit badge numbers. After booking, the 14-digit number is searched in AW146 and, if found, the access profile of the associated 6-digit badge number is checked.



The 14-digit card numbers are not displayed in the personnel database.

6.1.5.4 W3K32P - Menu Attributes - Checking badge number

In the menu ATTRIBUTES the badge number can be checked under System Data point SY / Card 3 / Channel 1.

Meaning of the attributes

BL = Length of the badge number

B0 to B5 = show the read badge number

D0 to D3 = show the badge number transferred in the server after the code structure transformation.

Example: The 13 digits badge number „**4002056159180**“ is transferred without modification to the host.

As always 14 digits should be transmitted, the position 14 is set to 0.

D0 = 4002 Pos. 1 to 4

D1 = 0561 Pos. 5 to 8

D2 = 5918 Pos. 9 to 12

D3 = 00 Pos. 13 to 14

0	BL	14	
136	B0	34 30 30 32	(HEX)
136	B1	30 35 36 31	(HEX)
136	B2	35 37 39 31	(HEX)
136	B3	38 30 30 30	(HEX)
136	B4	30 30 30 30	(HEX)
136	B5	30 30 30 30	(HEX)
136	D0	34 30 30 32	(HEX)
136	D1	30 35 36 31	(HEX)
136	D2	35 37 39 31	(HEX)
136	D3	38 30 00 00	(HEX)

Attribute Type SY - Card 3 - Channel 1

Badge	Name	Personal number
000001	Smith, Mike	40020561579180

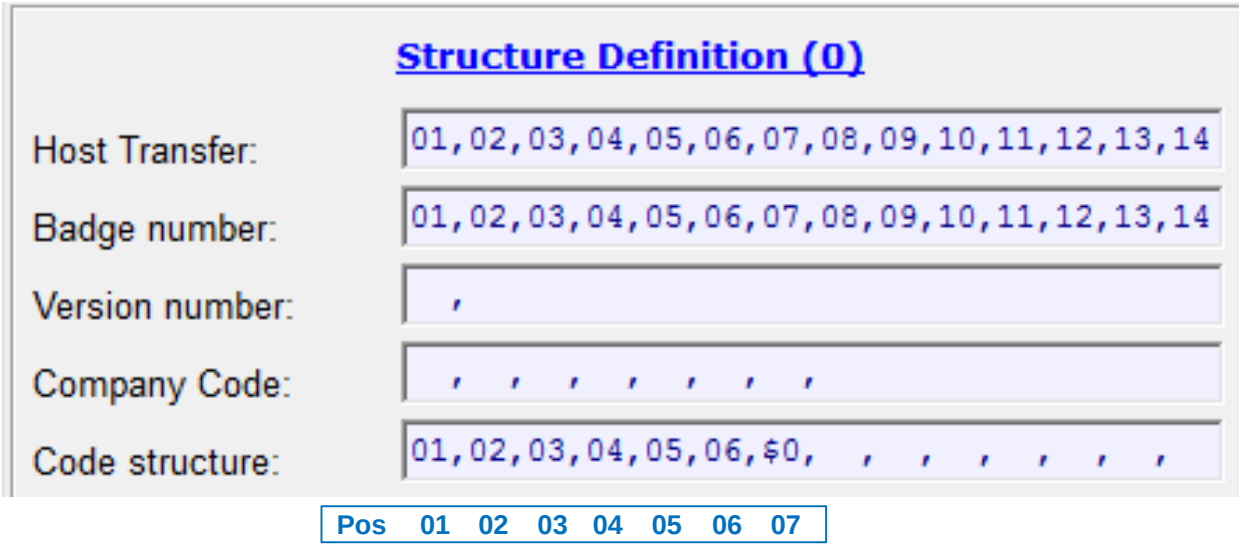
Structure-Definition (0)

Host-Transfer:	01,02,03,04,05,06,07,08,09,10,11,12,13,14
Badgenumber:	01,02,03,04,05,06,07,08,09,10,11,12,13,14

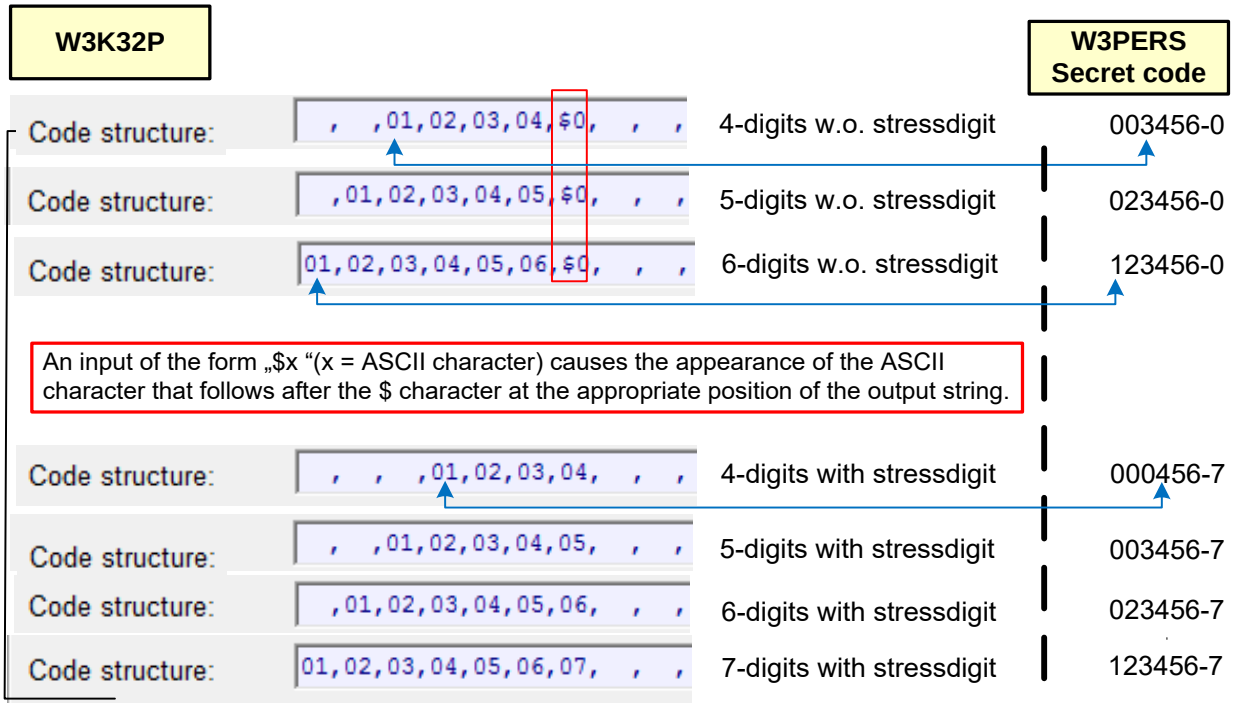
6.1.6 PIN-code structure definition in W3K32P

The target of the field “code structure” is to adjust the entered PIN-code on the reader with the “Secret code” in the personnel database.

Code structure in W3K32P



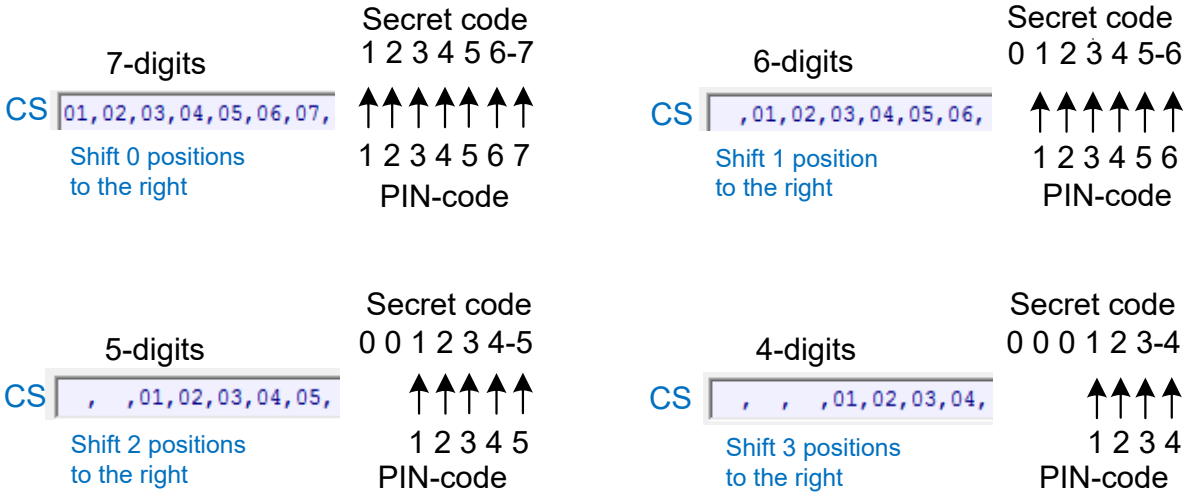
The field secret code of the personal database is always right-aligned in the 6 available places. The seventh digit is the stress digit. For a 6-digit PIN-code the code structure in W3K32P is identical with the secret code. But with a 5-digit PIN-code the first position is left blank in the code structure or in case of a 4-digit PIN-code 2 positions are left blank. With this shifting to the right, the adjustment with the secret code is reached.



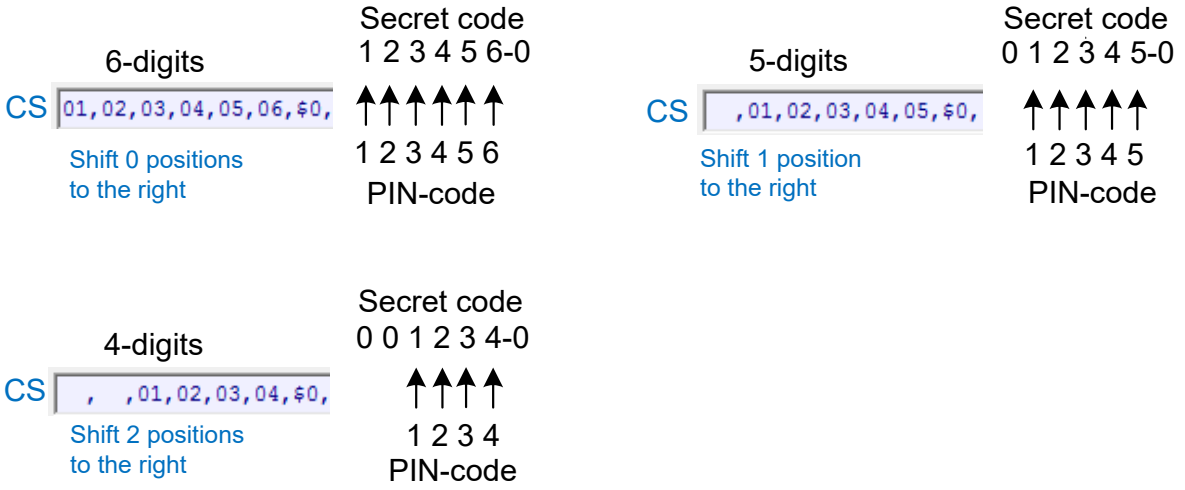
6.1.6.1 Application examples of the code structure

In the secret code (PIN-code) the unused positions are filled with zeros. In order to compare the structure of the secret code with the entered PIN-code the following examples show the required adjustment in W3K32P.

WITH STRESSDIGIT

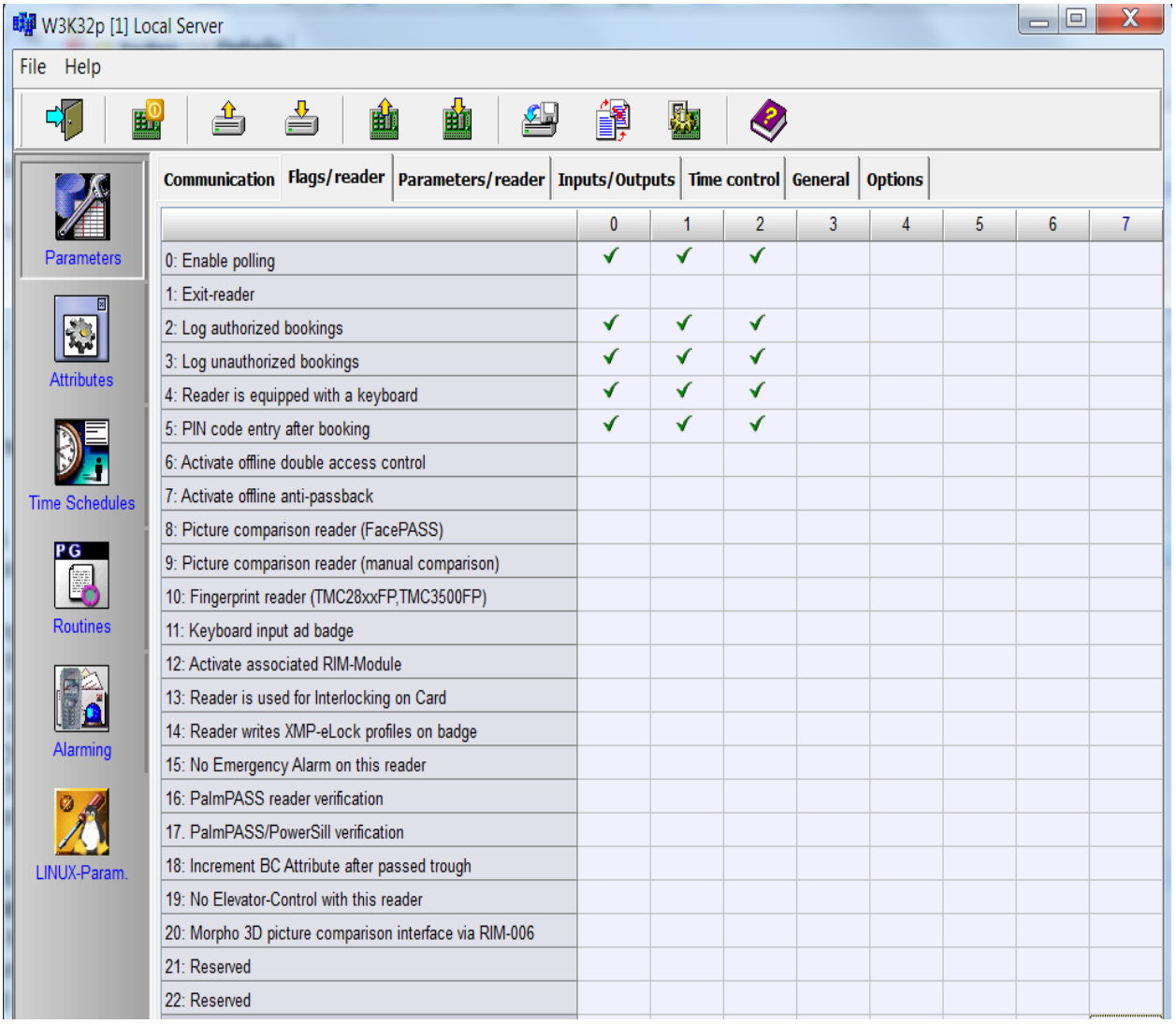


WITHOUT STRESSDIGIT



6.2 The registry card “Flags/Readers”

In the registry card ***Flags/reader*** general and special functional properties of the connected card readers are specified.



	0	1	2	3	4	5	6	7
0: Enable polling	✓	✓	✓					
1: Exit-reader								
2: Log authorized bookings	✓	✓	✓					
3: Log unauthorized bookings	✓	✓	✓					
4: Reader is equipped with a keyboard	✓	✓	✓					
5: PIN code entry after booking	✓	✓	✓					
6: Activate offline double access control								
7: Activate offline anti-passback								
8: Picture comparison reader (FacePASS)								
9: Picture comparison reader (manual comparison)								
10: Fingerprint reader (TMC28xxFP,TMC3500FP)								
11: Keyboard input ad badge								
12: Activate associated RIM-Module								
13: Reader is used for Interlocking on Card								
14: Reader writes XMP-eLock profiles on badge								
15: No Emergency Alarm on this reader								
16: PalmPASS reader verification								
17. PalmPASS/PowerSill verification								
18: Increment BC Attribute after passed trough								
19: No Elevator-Control with this reader								
20: Morpho 3D picture comparison interface via RIM-006								
21: Reserved								
22: Reserved								

Depending of the type of controller, the flags for the readers are set in the column 0 to 7.

Meaning of the input fields of the registry card *Flags / reader*

0	**Enable polling** Setting the flag activates the polling to the reader after the next XMP-K32 parameter download. The flag should be set only, if the reader with the appropriate address is connected to the XMP-K32.
1	**Exit-reader** Setting of this flag defines the inside reader of a reader pair for anti pass back operation (reader 1 and reader 2, reader 3 and reader 4). The first („even”) reader of such a pair always must be set as exit or inside reader). In this situation two readers influence the same door control periphery (door opener, door contacts). For this reason only the data points for the outside reader is set. Furthermore the settings for the room balancing must be executed (e.g. (from 1 to 2) and (from 2 to 1) or (from 3 to 4) and (from 4 to 3).
2	**Save authorized bookings** Authorized bookings at this card reader are stored into the XMP-K32 in offline mode.
3	**Save unauthorized bookings** Unauthorized bookings at this card reader are stored into the XMP-K32 in offline-mode.
4	**Reader is equipped with a keyboard** The connected card reader is equipped with a keyboard for PIN-code input.
5	**PIN-Code-entry after booking** By setting this flag, the order of "First card then PIN-code" is set. This option only works with the reader types XMP-TMC22/23xx.
6	**Activate offline double access control** The double access control in offline mode is activated for this reader. The time for this double access control is specified in the registry card General in the field ‚Number of seconds for double access control'.
7	**Activate offline anti pass back** The anti pass back is activated also for the offline mode.
8	**Picture comparison reader (FacePASS)** After a booking on this reader, the image of the person is detected at the FacePASS-Face recognition system and checked. The access result is sent to the controller.
9	**Picture comparison reader (manual comparison)** The door release after booking is coupled to an additional manual release by a picture comparison system. A booking at the reader locks the reader first for more card bookings. If the picture comparison is positive, then the door is released from the supervisory staff and the reader is unlocked after activation of the passage contact. Otherwise, the blocking of the reader is canceled after the expiration of the passage monitoring time.

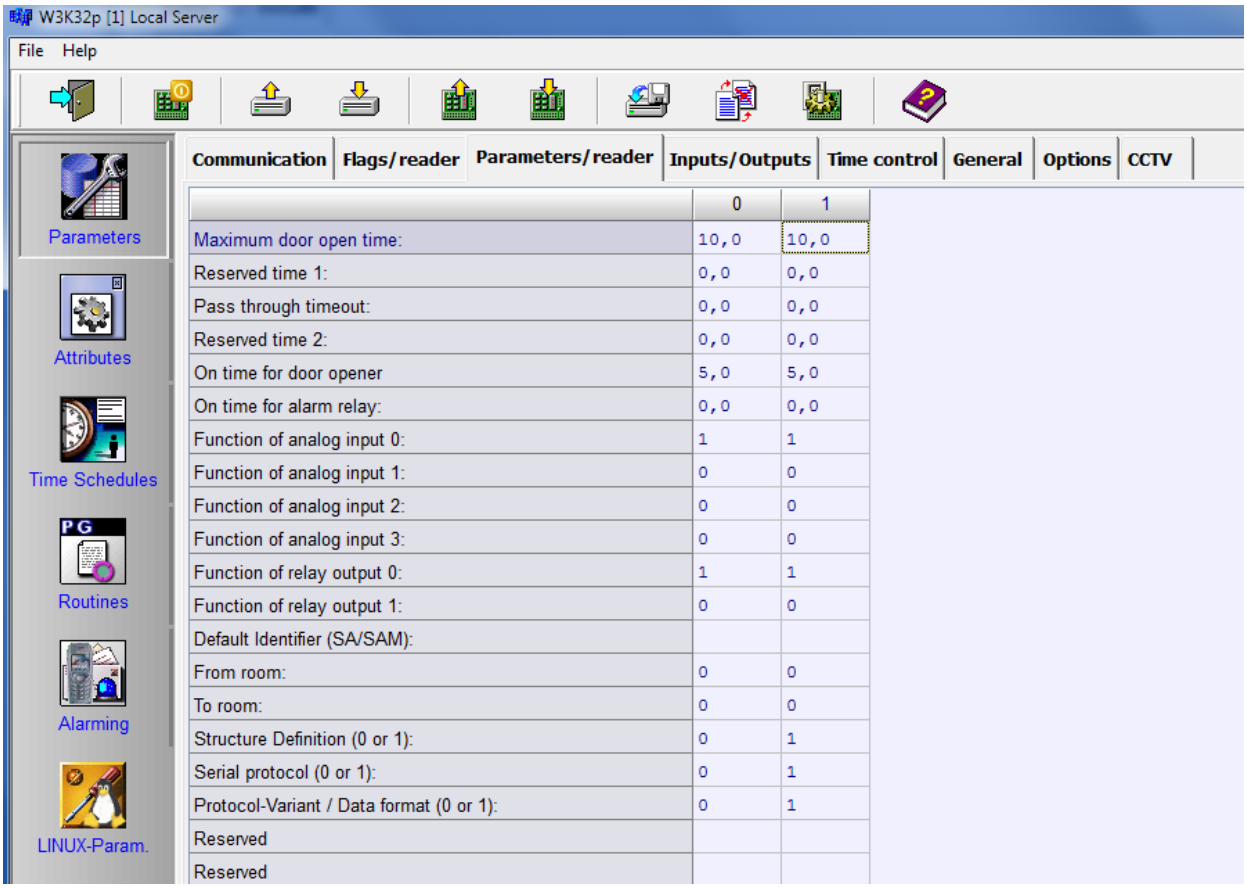
Meaning of the input fields of the registry card *Flags / reader*

10	**Fingerprint-reader** The door release is activated after a card booking and a biometric check.
11	**Keyboard input as badge number** Special solution. The standard solution is to set the flag 2 in W3TM24P.
12	**Activate associated XMP-RIM-Module** This flag activates the communication of the reader with the associated XMP-RIM module.
13	**Reader is used for Interlocking on Card** With this function, the access to different areas is denied for a predefined time when a person has been contaminated by a chemical, bacteriological or radioactive area (cross-contamination). See also the documentation W3ContTI
14	**Reader writes XMP-eLock access profiles on badge** The reader writes access rights on the ID-card for doors with electronic door cylinders.
15	**No emergency alarm on this reader** Special solution
16	**PalmPASS reader verification** Connecting a XMP-Palm-001/002 controller. (Old Version)
17	**Palm-Controller/PowerSill-Plus Verification** Connecting an XMP Palm-003 controller (New Version)
18	**Increment BC Attribute after pass through** The BC-attribute (Booking counter) increments only in case of bookings with successful passage (Input) on this reader (Type SY, Card 2, channel 1-8).
19	**No elevator control with this reader** This reader is a normal access reader and is not used for elevator control. Thus elevator readers and access control reader can be mixed on a controller.
20 to 23	Reserved for future applications

6.3 The registry card “Parameters / readers”

Into the registry card **Parameters/readers** the following settings are made:

- definition of the control and supervision times for relay outputs and analog inputs, respectively for the door control
- activation of the functions for relay outputs and analog inputs
- definition of a default identifier (SA/SAM) for the appropriate card reader
- setting of room numbers
- definition of the structure type for the identification number, the serial interface and the protocol or the data format (according to the definitions in the registry card *Communication*)



	0	1
Maximum door open time:	10,0	10,0
Reserved time 1:	0,0	0,0
Pass through timeout:	0,0	0,0
Reserved time 2:	0,0	0,0
On time for door opener	5,0	5,0
On time for alarm relay:	0,0	0,0
Function of analog input 0:	1	1
Function of analog input 1:	0	0
Function of analog input 2:	0	0
Function of analog input 3:	0	0
Function of relay output 0:	1	1
Function of relay output 1:	0	0
Default Identifier (SA/SAM):		
From room:	0	0
To room:	0	0
Structure Definition (0 or 1):	0	1
Serial protocol (0 or 1):	0	1
Protocol-Variant / Data format (0 or 1):	0	1
Reserved		
Reserved		

Meaning of the input fields of the registry card “Parameters/ reader”

Maximum door open time:	The maximum door open time in seconds is specified here. This is the maximum time, which may pass between opening and closing the door, before an alarm will be released.
Reserved time 1:	Reserved time. Not used at the moment.
Pass through timeout:	This is the maximum time interval, which may pass between a booking and pass through (activation or release of the pass through contact). During this time, the reader is blocked and the message “Terminal blocked” will appear on the reader display.
Reserved time 2:	Reserved time. Not used at the moment.
On-time for door opener:	The maximum effective period (on-time) for the first door relay of the respective card reader is entered here.
On-time for alarm-relay:	The maximum effective period (on-time) for the second relay is entered here, if this is set as alarm output (function of the relay output 1 = 2). Otherwise the max. door opening time is valid.
Function of analog input 0:	0: Disabled 1: Doorframe contact active 2: Reader handles door frame contact With this reader (with BPA/9 protocol) the door supervision is controlled externally. This function is important for integration of older reader installations based of BPA/9 protocol and integrated door supervision. The door supervision and/or door control is carried out directly by the reader. The alarms resulting from it are registered and processed by the XMP-K32 as if it would concern supervision and control contacts of the XMP-K32 itself. With this function no supervision times may be activated.
Function of analog input 1:	0: Disabled 1: Push button connected (For opening with alarm bridging) 2: Handle contact connected

Meaning of the input fields of the registry card “Parameters/ reader

Function of analog input 2:	0: Disabled 1: Pass through contact active
Function of analog input 3:	0: Disabled 1: Reader blocking input active 2: Pass through reset contact
Function of analog output 0:	0: Disabled For the parameter setting of an anti pass back system the inside reader should be an „even reader“ (address 0, 2, 4 or 6) and the outside reader an „odd reader” (address 1, 3, 5, 7). If the readers 0 and 1 work as anti pass back reader pair, the function for the output relay of reader 0 should be set on „0“ and for reader 1 this function should be set on „1“. By this constellation an authorized booking at reader 0 as well as at reader 1 activates the same door opener relay (BO2). 1: Door striker active 2: Door striker is reset when door opens (according to VDS) 3: Door striker is reset when door opens and pass through contact activated
Function of analog output 1:	0: Disabled 1: ON while door opening is allowed (external alarm system is bridged) 2: Alarm output (badge related alarms, e.g. *Badge not valid*) with → On time of alarm relay.
Default-Identifier (SA/SAM):	Each reader can get its own default identifier (e.g. A0 = access, B1 = coming, B2 = going) by entering this identifier into this field. After a booking this identifier (together with the card information) is send to the control system. If this field remains free, then the identifier of the reader (e.g. XMP-TMC2503) is send. The card readers identifier is determined, e.g. on basis of a key action at the reader (*coming* or *going*). With readers, which do not sent an own identifier (e.g. XMP-TMC450N) the identifier type A0 will be send to the control system automatically.

Meaning of the input fields of the registry card “Parameters/ reader

From room:	Virtual room numbers can be entered here. These numbers are used for anti pass back in offline mode (also global!). Values from 0 to 254 are allowed. A special case is the room number –1, which marks an undefined room. If a person is in room –1 the anti pass back is deactivated temporarily, i.e. the person can go into every other room. After restarting the XMP-K32, first, all persons are set as are being in room –1 (to prevent problems). It is recommended, however, not necessary absolutely, to use the same room numbers for the control system and for the XMP-K32. This function can be activated with systems up to 255 rooms. The assignment of the room names is realized in the menu option Rooms (W3ROOM.EXE) of the parameter set for the door control units. The anti pass back option is only possible with an inside/outside reader pair.
To room:	
Structure-Definition (0 or 1)	The code number (0 or 1) for the structure definition of the card reader must be entered here (see registry card ***Communication***).
Serial protocol (0 or 1)	The code number (0 or 1) for the serial protocol of the card reader must be entered here (see registry card ***Communication***).
Protocol variant/ Data format (0 or 1)	The code number (0 or 1) for the protocol variant and/or the data format of the card reader must be entered here (see registry card *Communication*).

6.3.1 Examples of door control configurations

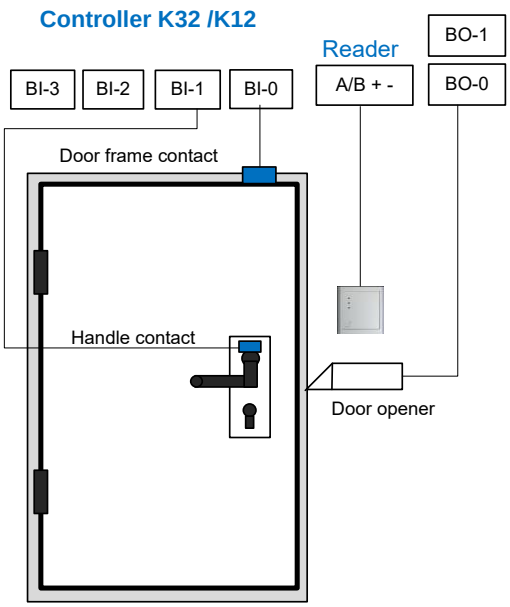
At the inputs of the controller XMP-K32/XMP-K12, different wiring configurations of the doors can be parameterized. We define e.g. if the door is wired to a door frame contact, a door push button, a pass-through contact, a lock with a handle contact or an alarm device.

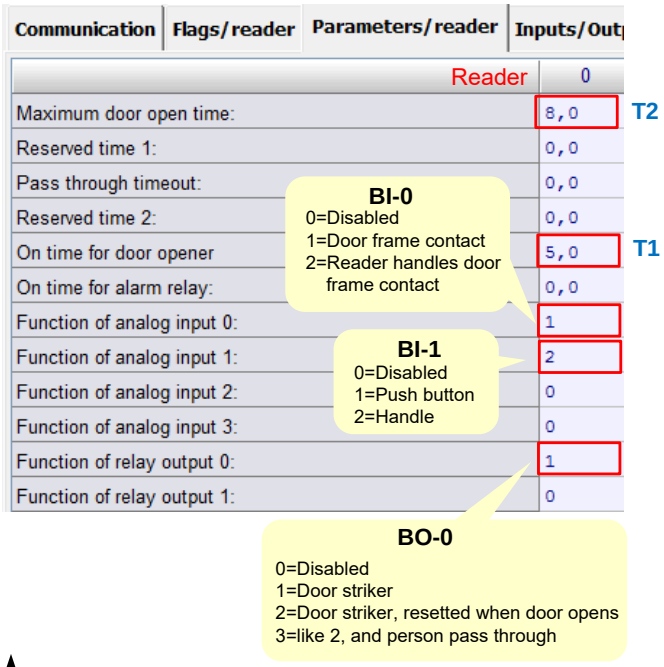
The following examples describe different door configuration options that have an influence on the inputs and outputs parameterization.

Controller I/O	Reader Nr.	
Input BI-0	0	0=Disabled 1=Doorframe contact active 2=Reader handles door frame contact
Input BI-1	0	0=Disabled 1=Pushbutton connected (For opening with alarm bridging) 2=Handle contact connected
Input BI-2	0	0=disabled 1=Pass through contact active
Input BI-3	0	0=Disabled 1=Reader blocking input active 2=Pass through reset contact
Relay Output BO-0	0	0=Disabled 1=Door striker active 2=Door striker is reset when door opens 3=Door striker is reset when door opens and pass-through contact activated
Relay Output BO-1	0	0=Disabled 1=ON while door opening is allowed (external alarm system is bridged) 2=On time of alarm relay

6.3.2 Door control with door frame and handle contact

The input BI-0 of the controller is wired to the door frame contact and the BI-1 input is connected with the door handle contact. The relay output BO-0 controls the door strike. When leaving the room by activating the handle contact, no alarm is generated.





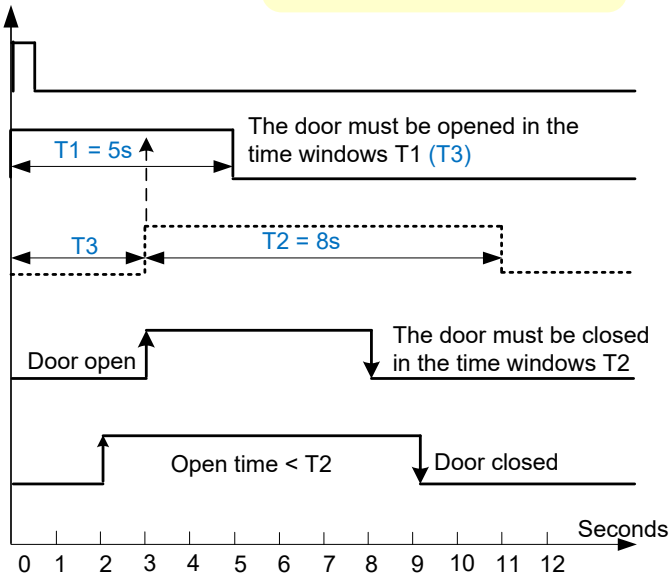
Booking on reader OK

ON time for door opener **(T1)**
Relay output BO-0=1 — **5s**

Maximum door open time **(T2)** — **8s**

Door opening with reader supervised with door frame contact BI-0

Door opening from inside supervised by handle contact BI-1

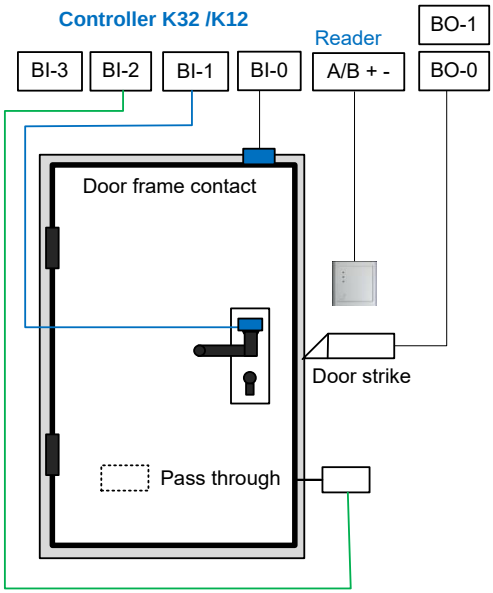


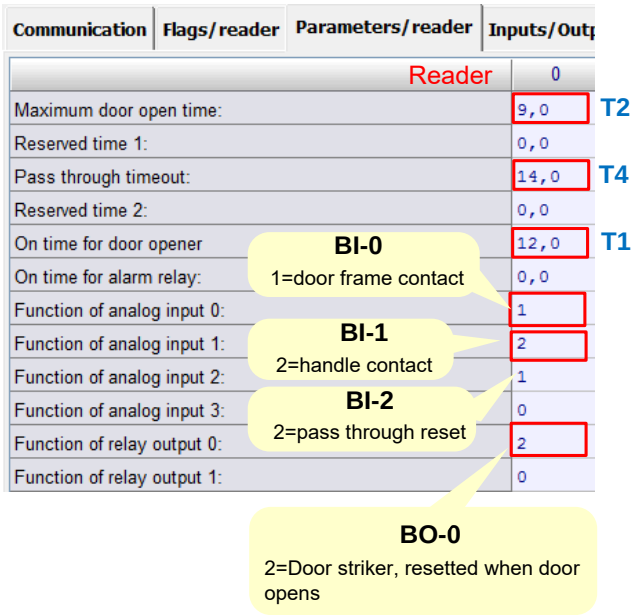
T3 is the time that elapses between booking (door release) and door opening.

The door must be closed within the time **T2**, otherwise an alarm is generated

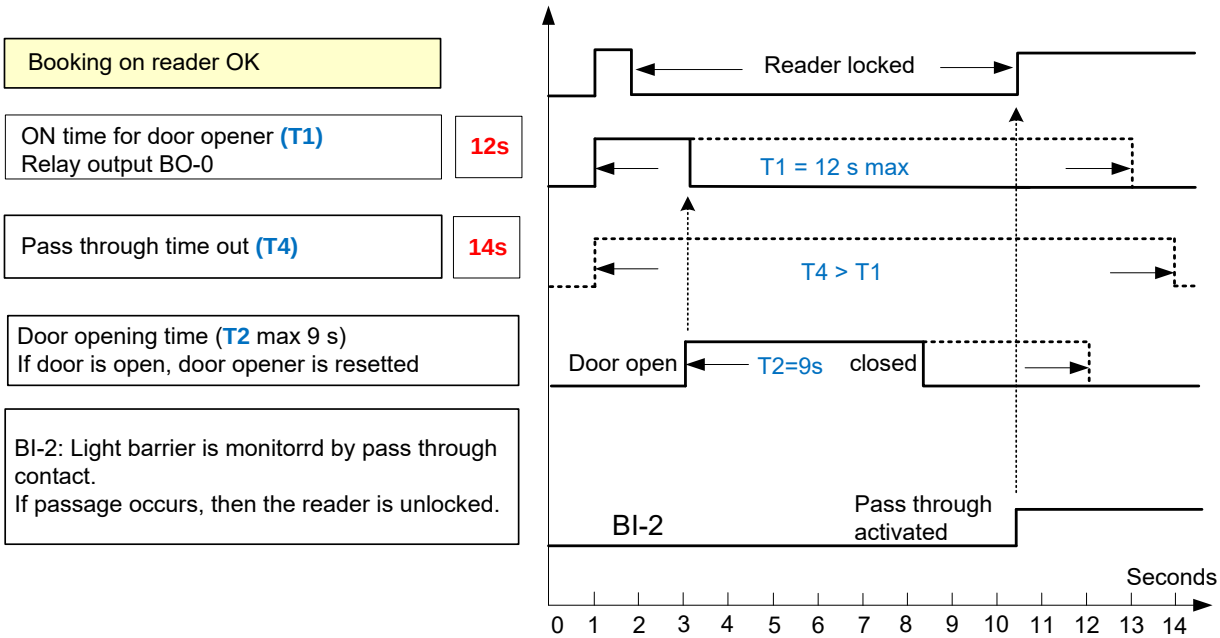
6.3.3 Door control with pass through contact

The inputs BI-0 and BI-1 of the controller will be wired to the door frame- and handle contact. The input BI-3 monitors the pass through contact (e.g. light barrier). The relay output BO-0 controls the door strike.



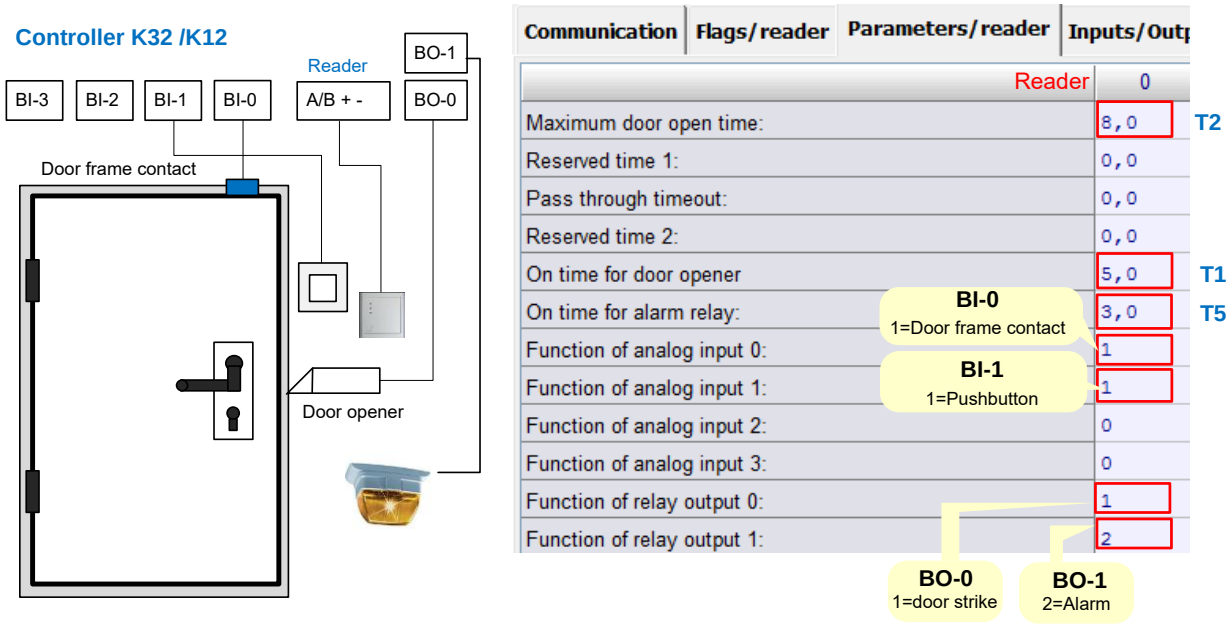


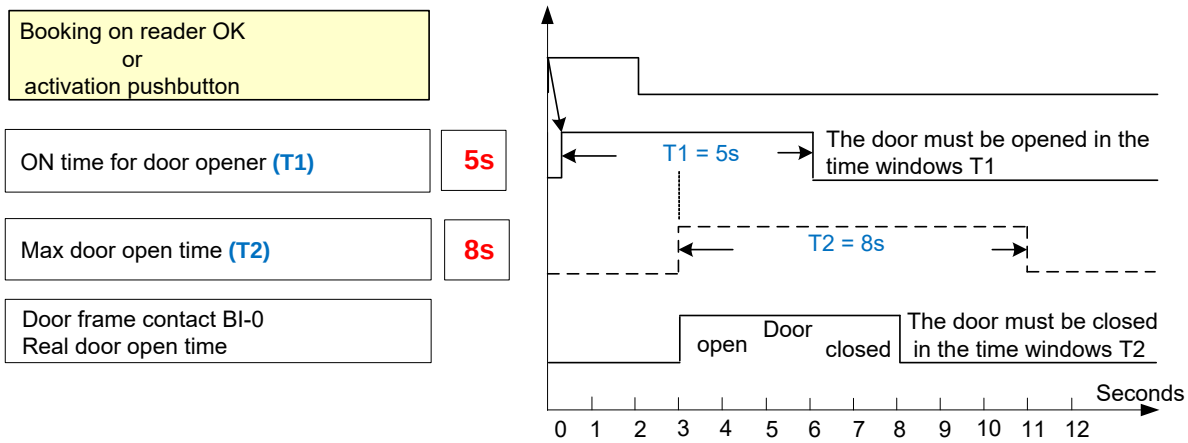
By booking on the reader the door open time and the “pass through time out” are initiated. The pass through monitoring time is the maximum time that can elapse between booking and activation of the light barrier. During this period, the reader is disabled.

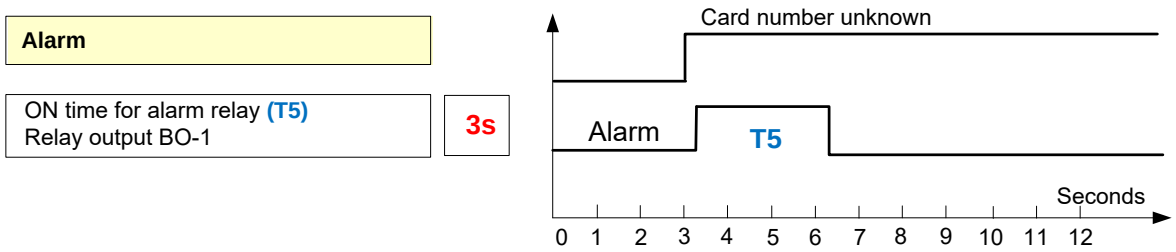


6.3.4 Door control with push button and alarm signalling

The BI-0 input of the controller is wired to the door frame contact. The input BI-1 is connected to the door push button which must be pressed to leave the room. The relay output BO-0 controls the strike and the relay output BO-1 is used to trigger an alarm device. The duration of the alarm output (ID-related alarms, e.g. invalid card) is set with the parameter "ON time for alarm relay".

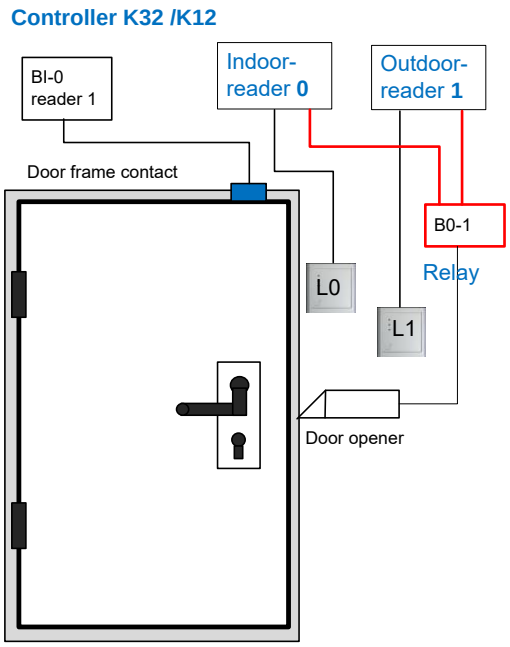


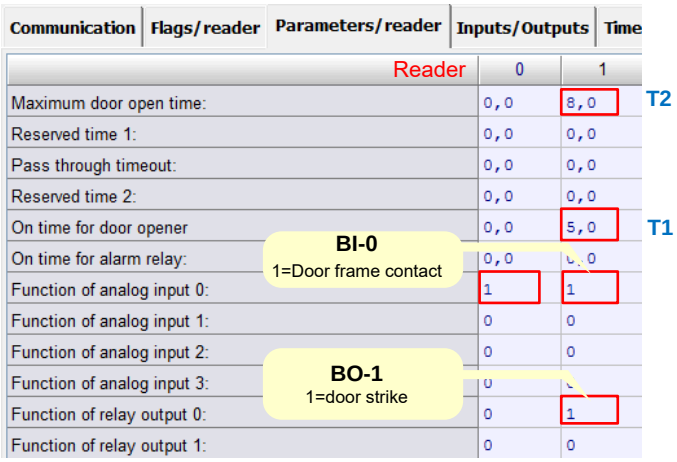


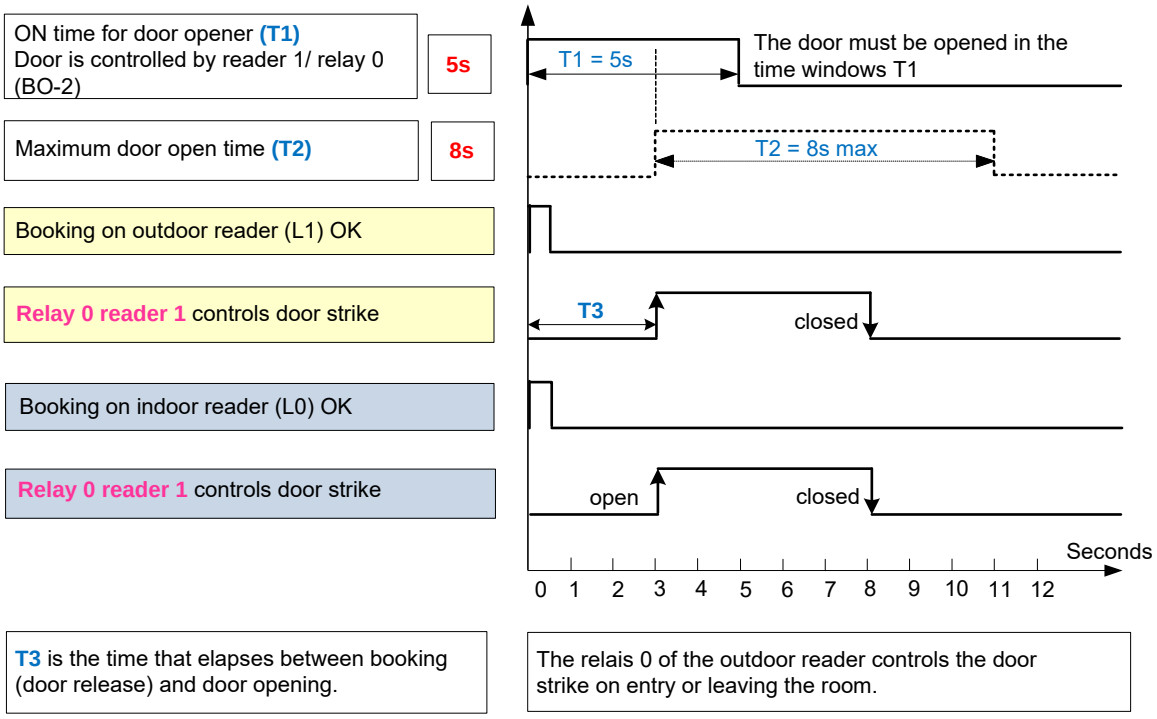


6.3.5 Door control with In/out readers

For the parameter settings of an IN/OUT control the inside reader should be an „even reader“ (address 0, 2, 4 or 6) and the outside reader an „odd reader” (address 1, 3, 5, 7). If the readers 0 and 1 work as a reader pair, all settings for both readers will be performed in the column for reader 1, *excepted analog input 0* which must be also set to 1. By this constellation an authorized booking at reader 0 as well as at reader 1 activates the same door opener relay (BO-2).





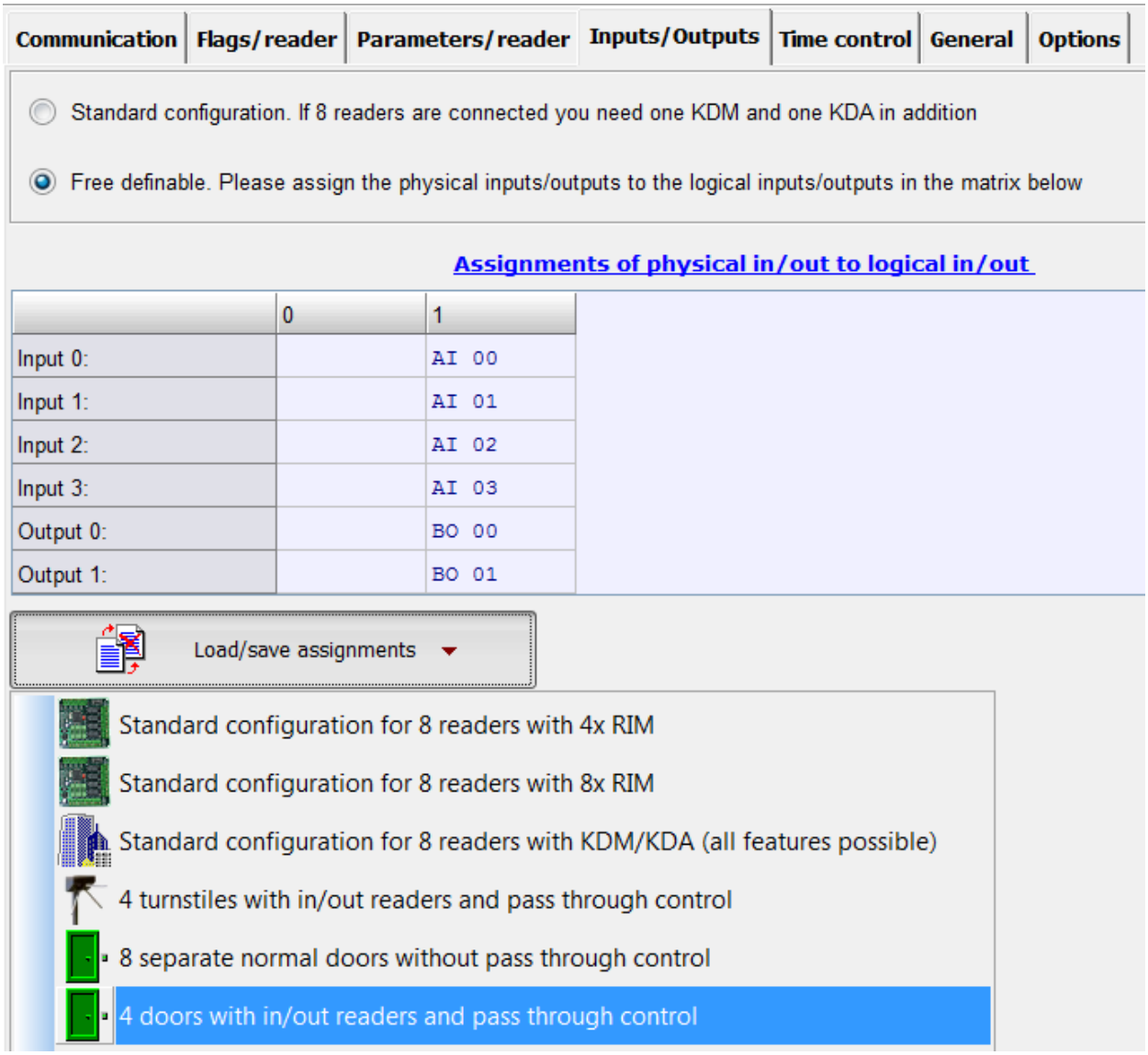


T3 is the time that elapses between booking (door release) and door opening.

The relais 0 of the outdoor reader controls the door strike on entry or leaving the room.

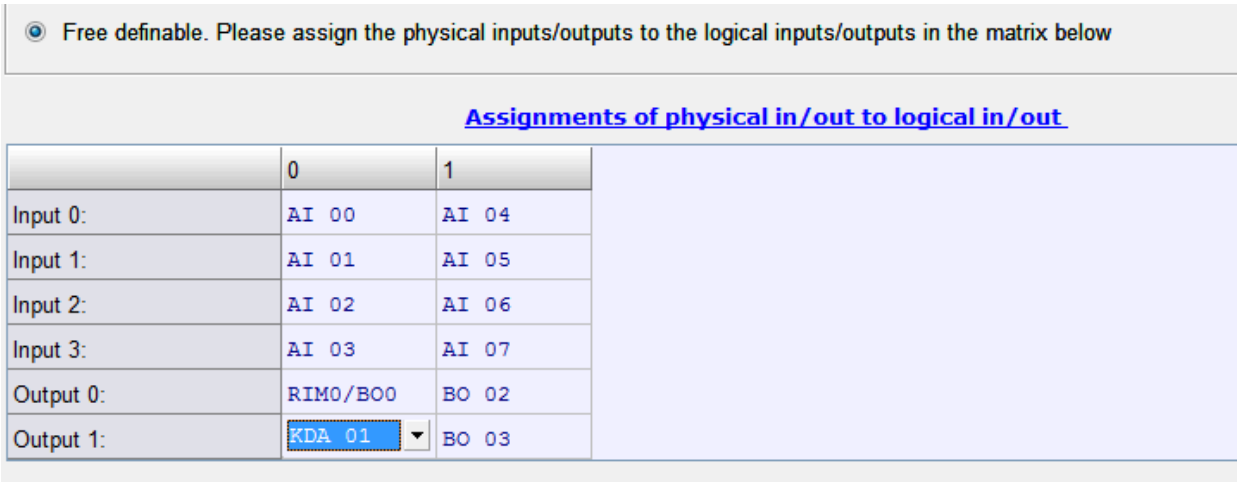
6.4 The registry card “Inputs/outputs”

In the anti pass back configuration of the input and output reader, the door is always controlled by the input reader (odd address). This feature is enabled in the system by selecting the function “Four doors with in/out readers and pass through control” in the registry *“inputs / outputs”.*



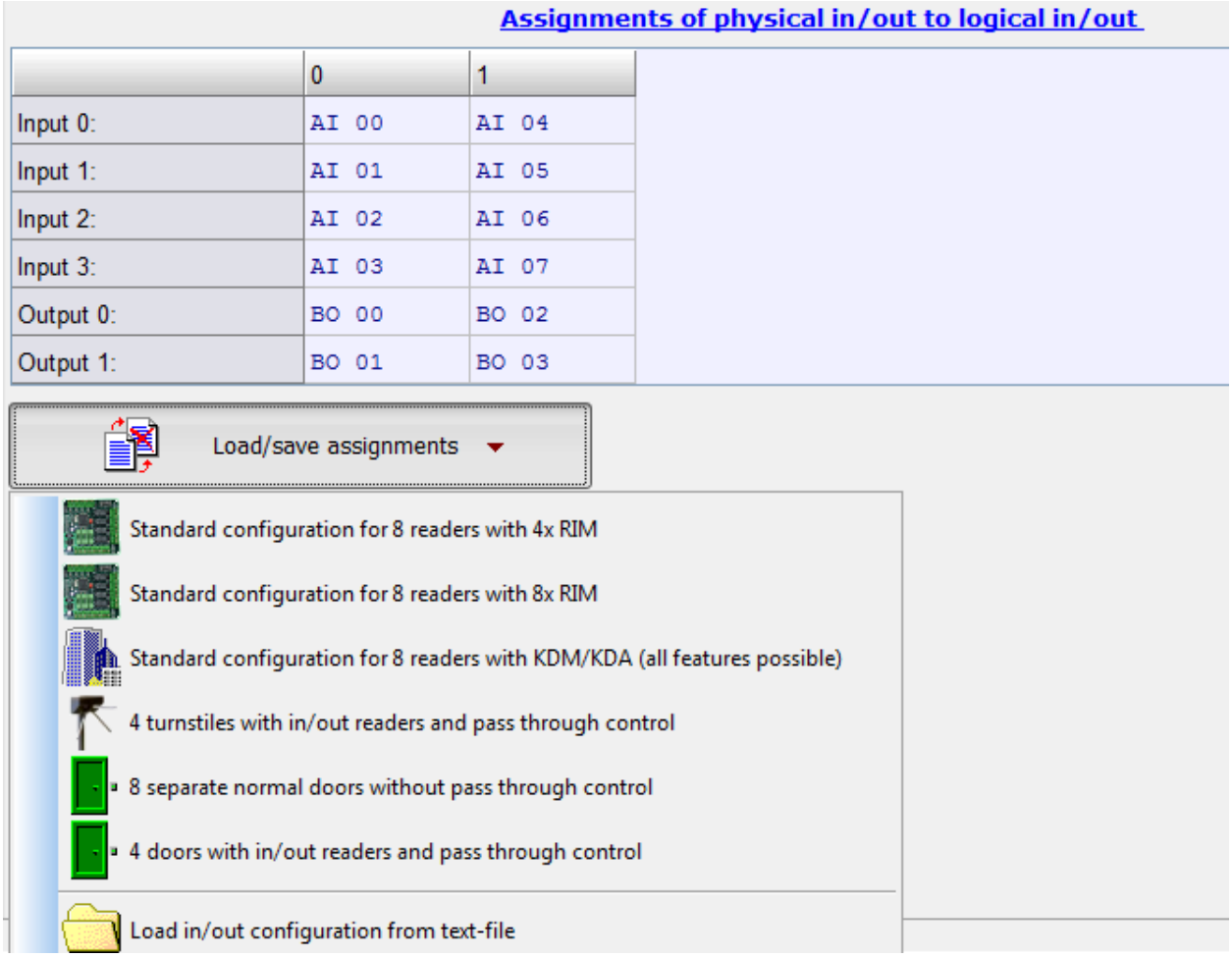
Free definable:

By selecting this option it is possible to assign outputs and inputs for the reader on individual way. To do this the operator can use the scroll down menus in the matrix.



Load/save assignments

With this selection menu it is possible to load or save frequently realized standard and own input/output configurations.

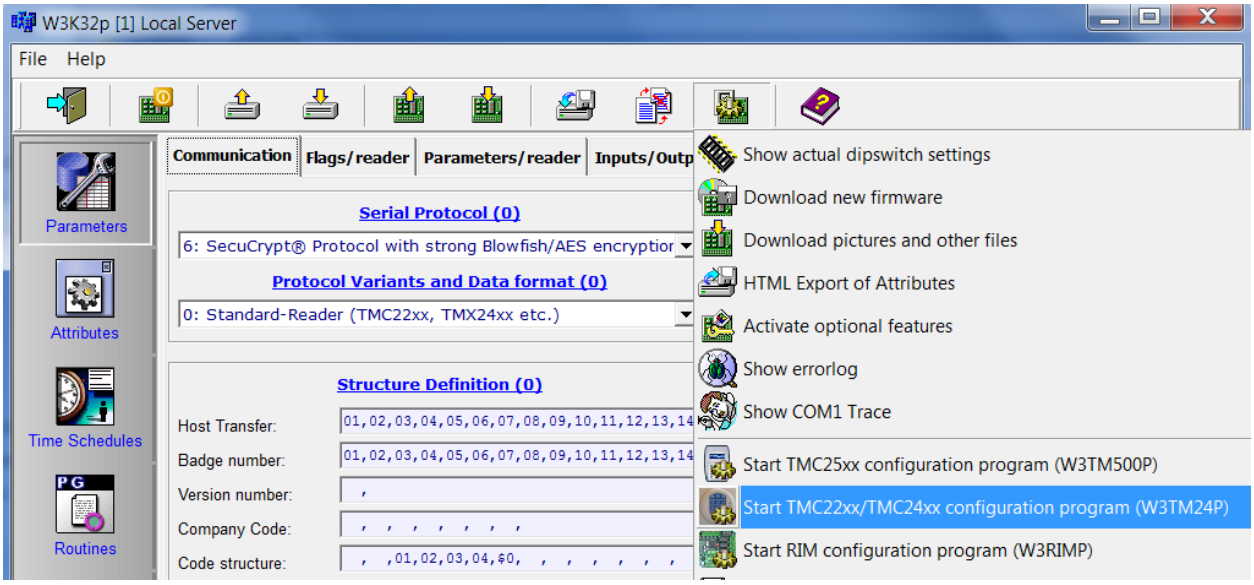


7 W3TM24P – Call the utility program

With the program W3TM24P all necessary parameters to read the data from the readers are set. This program also serves to update the reader firmware.

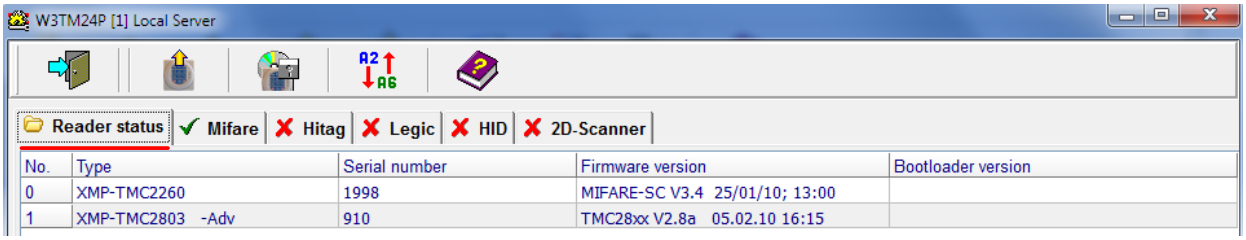
The program W3TM24P will be started under the following path:

Network administration / W3Port / K32/K12 Parameters /W3K32p / Utility functions / start menu W3TM24P.



7.1 W3TM24P – Display Reader Status

In the registry-card “Reader status“, those card readers, which are connected via SecuCrypt® protocol to the corresponding controller, can be shown. The card readers will be displayed with address, type, serial number and firmware version. In the column "Bootloader version" the version of the bootloader appears. For older readers, this function may not be given. The bootloader is reader specifically responsible for downloading new firmware versions.



After a successfully upload of parameters from the readers, the recognized reader technology will be quit with ✓ MIFARE

Meaning of symbols of the task bar

Leave program

Parameters upload from card reader

The upload of the card reader parameters is started by activating the symbol *"Parameter upload from card reader".*

Card readers which are connected via UCI or BPA9 protocol to the XMP-K32 will not be displayed.

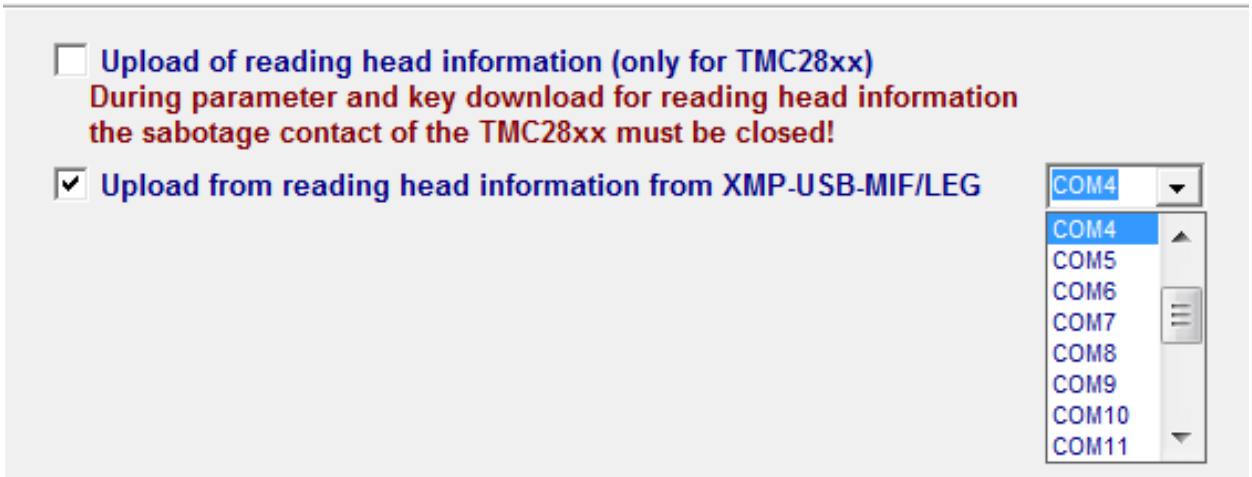
Options

- Upload of reading header information (for XMP-TMC28xx)

  Enabling this option allows you to read the firmware version installed in a XMP-TMC28xx reading head. When downloading reader parameters in the reader head (e.g. security keys), make sure that the tamper contact of XMP-TMC28xx is closed!

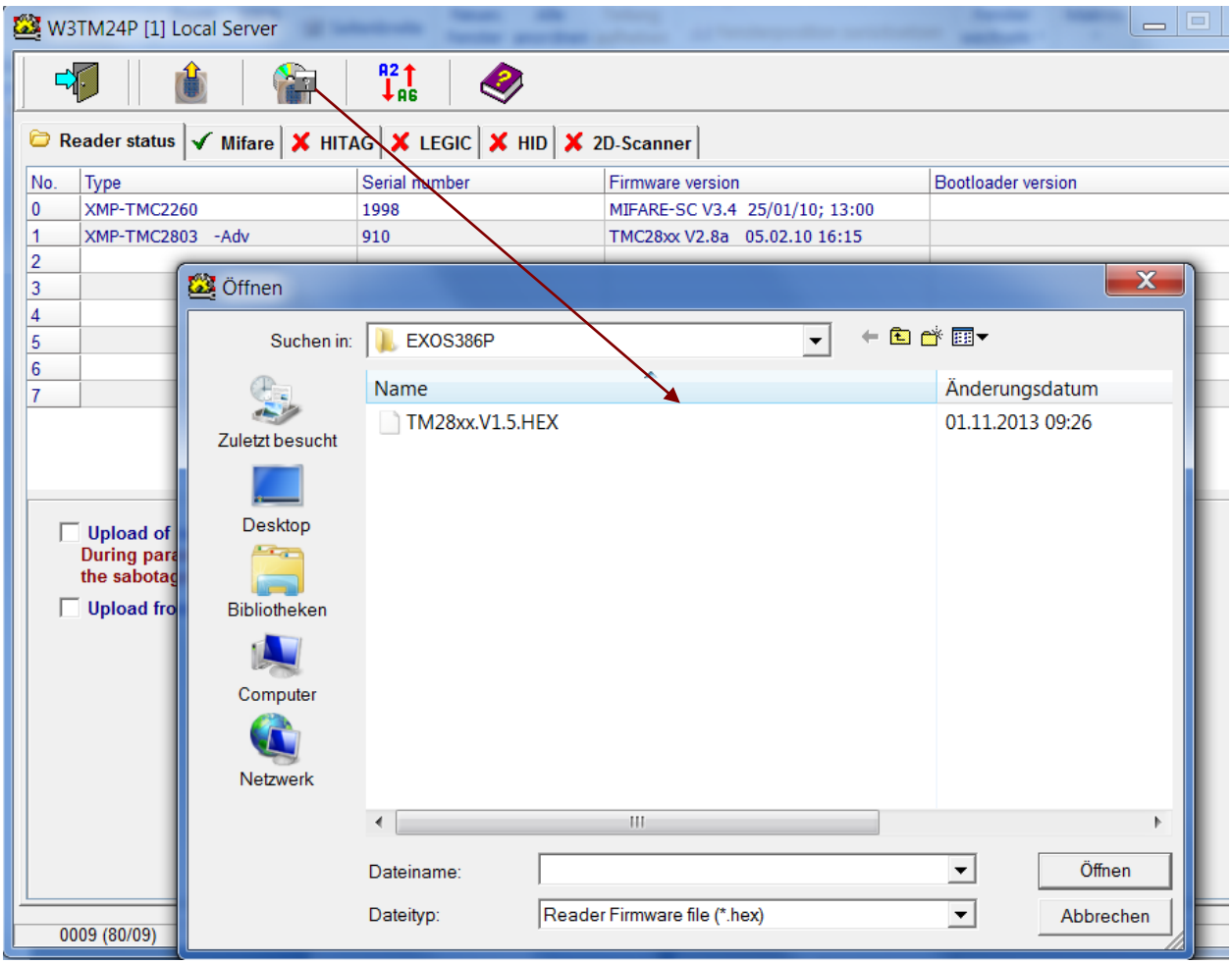
- Upload from reading head information from XMP-USB-MIF/LEG

  With this option, information from reading head connected to a particular COM-port can be read. The appropriate COM-port must be selected first.



7.2 Load new firmware into the reader

If the SecuCrypt® communication is active, it is possible to execute a firmware update for the card reader with the symbol "*Reader firmware download* " of the reader configuration program *W3TM24P*.



The firmware must be available as "TM24xxVxy.hex" file and can be downloaded into the selected card reader.

In case of an active firmware download, the yellow, green and red LEDs will flash in subsequent way.

7.3 Change of address with IP67-readers

Conditioned by their design, IP67-readers have no DIP-switches for addressing. After delivery all IP67-readers are set to address 0. To change the address, open the window with the icon

and enter the old and new address before sending it to the reader.

It should be take into account that during an initial installation, the readers must be individually connected to the controller and provided immediately with the new reader address.

8 Configuration MIFARE® Classic

8.1 W3TM24P - Meaning of symbols of the task bar

Leave program

Read parameters from file

Save parameters into file

Parameter upload from card reader

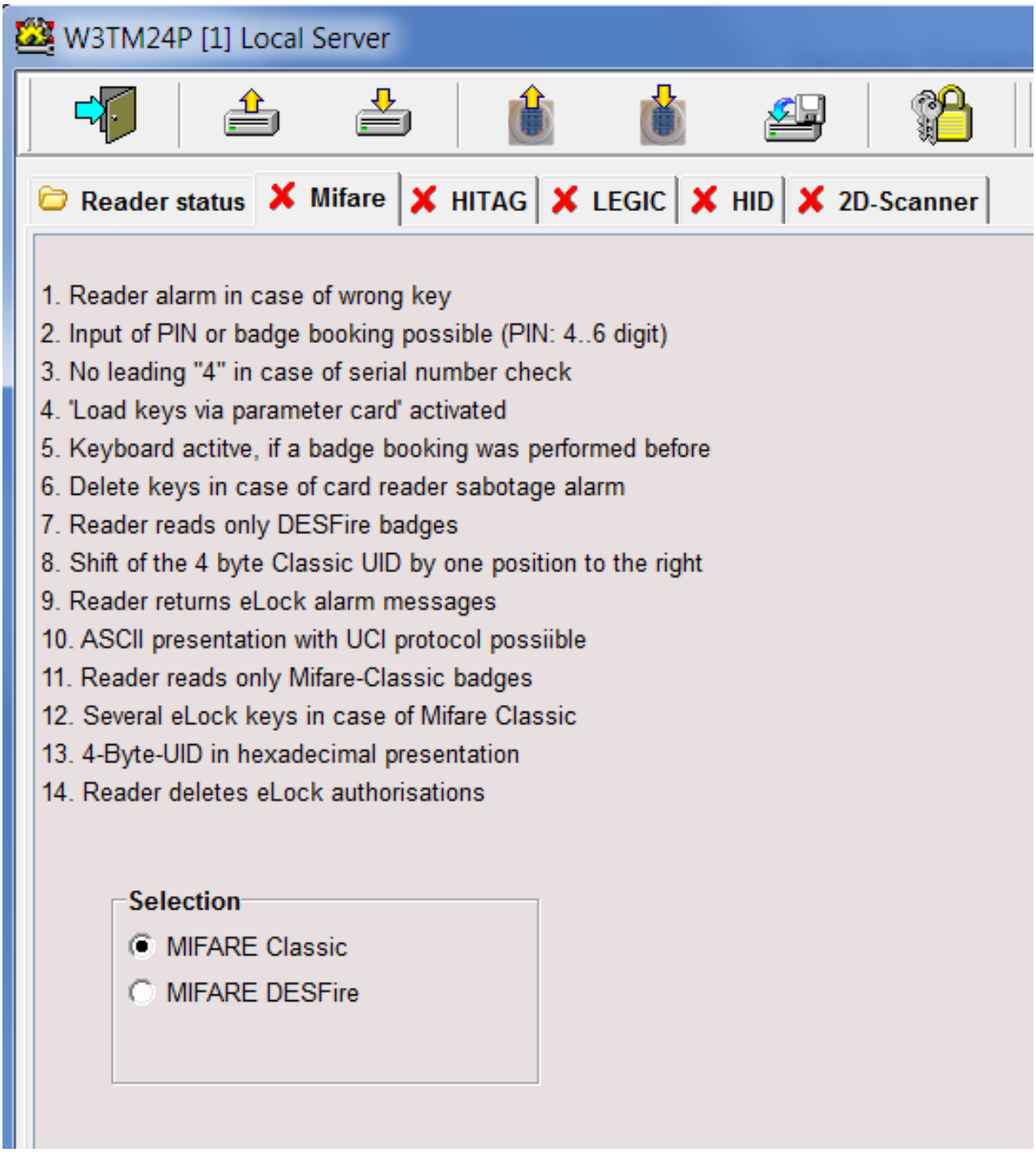
Parameter download into card reader

Import data/parameters from another file

Special reader definitions

8.1.1 MIFARE® Classic reader features

With the registry card “MIFARE“, specific settings for MIFARE-cards can be executed. A required card reader property will be activated by setting a checkmark into the desired field and a subsequent parameter download with the program symbol “Parameter download into the card reader”.



8.1.2 Meaning of the reader features

FLAG	DESCRIPTION
1	Reader alarm in case of wrong key This alarm is generated by the card reader, if the current badge does not match the required card reader key during reading of sector block information. This is a reader internal alarm which is not forwarded to the XMP-K32 or to the host computer. This option should not be used if the pass through supervision (XMP-K32 input I-2) is activated or the card reader is used for writing parameter cards.
2	Input of PIN or badge booking possible (PIN: 4-6 digit) Instead of a badge booking it is also possible to insert the corresponding badge number directly via PIN-code. For this special case the badge number check must be realized as 4-6 digit check (not 14 digits). This number has nothing to do with the secret code, which is normally entered under “Badge Definition” in the personal database. **Hint:** The use of this option reduces the security
3	No leading "4" in case of serial number check For historical reasons, MIFARE card readers of the TMC-family send always a leading „4“ by reading a 14-digit serial number. Normally this 4 not belongs to the serial number of the badge. By activating this option the leading „4“ will not be generated. STANDARD PRESENTATION CLASSIC (4 BYTES) 40034908539740 Fading out the leading 4 CLASSIC (4 BYTES) 00034908539740
4	“Load keys via parameter card” activated Beside the possibility to load the MIFARE-key with the program W3TM24P into the MIFARE-readers XMP-TMC2250/2260, it is also possible to load the key by using a special parameter card (XMP-MIF-PARA-CARD) for reading the sector-block. By setting this flag, the reader is prepared for reading the key information from the parameter card. After reader configuration, the flag will be automatically deleted to avoid a modification of configuration. This flag is not stored into the reader, that means, after power-off the flag must be set again if necessary.

Meaning of the reader features

5	Keyboard active, if a badge booking was performed first If the reader is set so that the PIN will be entered after booking (W3Port -> Flag 24, W3K32P -> “Reader / Flags” -> Flag5), with this option the reader keyboard will be deactivated. After a new card booking the keyboard is again active for about 10 seconds.
6	Delete keys in case of sabotage alarm at the reader If a tamper alarm occurs at the reader, the security keys will be deleted. The keys must be reloaded into the reader after power-on.
7	Reader reads only DESFire badges If this flag is set, the reader reads only DESFire badges. Classic cards are ignored. After completing a migration from Classic to DESFire, this flag can be set to improve project safety.
8	Shift of the 4 byte UID-Classic by one position to the right With this flag, the four byte of a UID-number from a MIFARE® Classic card is shifted by one position to the right, to ensure the simultaneous use of MIFARE® Classic and DESFire cards. 40033672387420 → Flag 8 deactivated 40003367238742 → Flag 8 activated
9	Reader returns eLock alarm messages By setting this flag and with appropriate XMP-eLock configuration, the reader looks first for alarm messages in the eLock alarm memory of the ID-card and then starts with the reading of the badge data. 04/04/13 18:12:55 99 ? Door 1 elock elo_test Battery too low
10	ASCII presentation with UCI-protocol possible With this flag the reader sends the badge data to the XMP-K32 in a format which will match with the UCI-protocol from the controller and allows the data to be forwarded as ASCII-data. (K32→Serial Protocol = 0: UCI Protocol, Protocol Variants and Data format 4: ASCII-data)

Meaning of the reader features

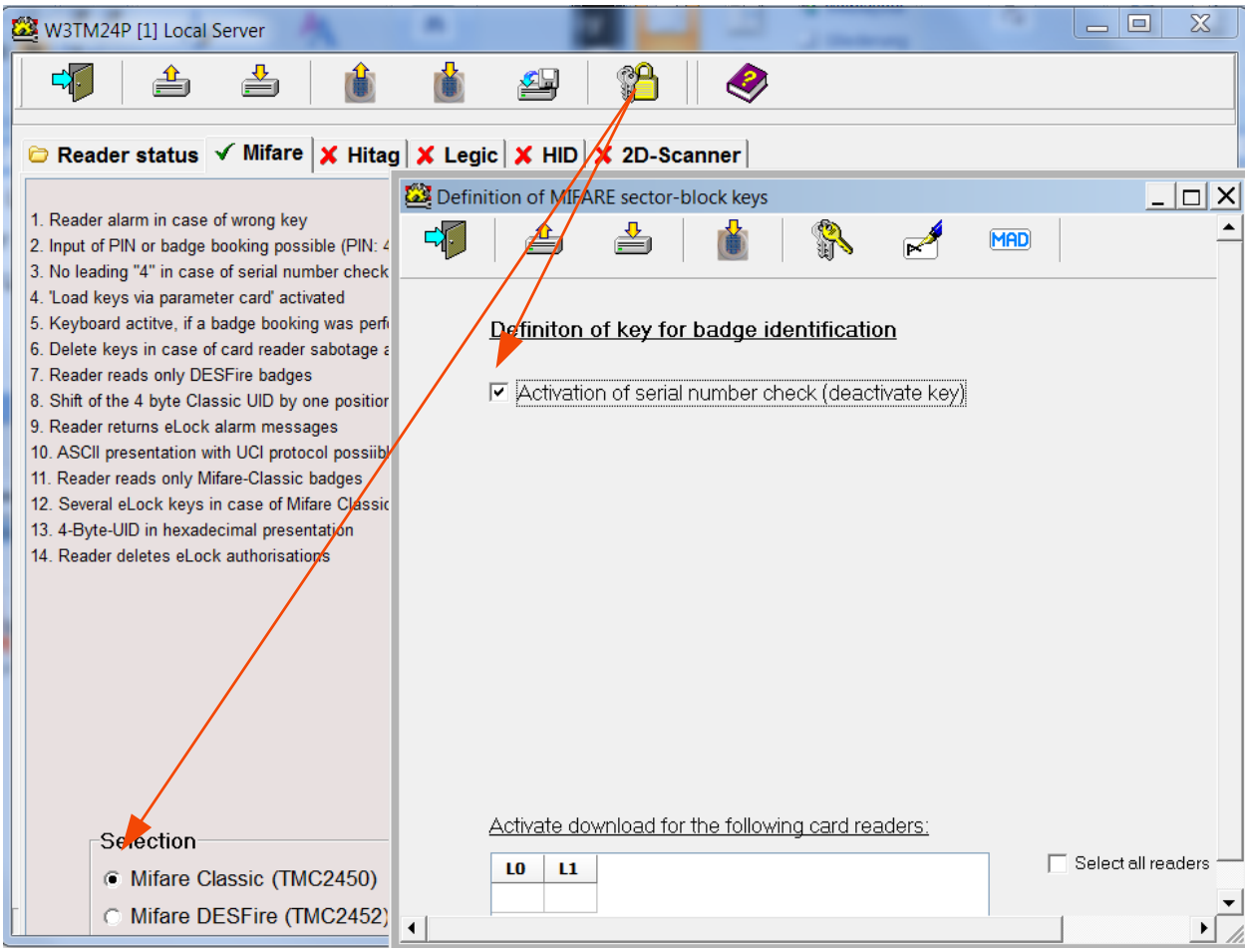
11	Reader reads only MIFARE If this flag is set, the reader reads only MIFARE® Classic badges. DESFire badges are ignored.
12	Several eLock keys in case of MIFARE® Classic Normally the memory space of the MIFARE® Classic cards reserved for XMP- eLock data is encrypted for all sectors with the same key. With this flag the reader can be set for reading a maximum of 4 consecutive card sectors with a different key for each sector.
13	4-Byte-UID in hexadecimal presentation By default, the serial number (UID – 14 digits) of the card is sent in decimal format. When this flag is set, the transmission is done in hexadecimal format.
14	Reader deletes eLock-authorizations With this flag, the access authorization at electronic offline door locks is deleted.

8.2 Reading the MIFARE® Classic Data

8.2.1 Reading the MIFARE® Classic Serial Number (UID)

In the selection box the reader MIFARE® Classic or MIFARE DESFire® can be selected. By clicking on the button "Specific definitions", depending on the selection Classic or DESFire, the configuration page is opened.

In many applications, the 4-byte UID (Unique Identifier = serial number) of the RFID identity cards is used.



After the selection of the MIFARE-Classic and the function a window opens with the function to activate the serial number check.

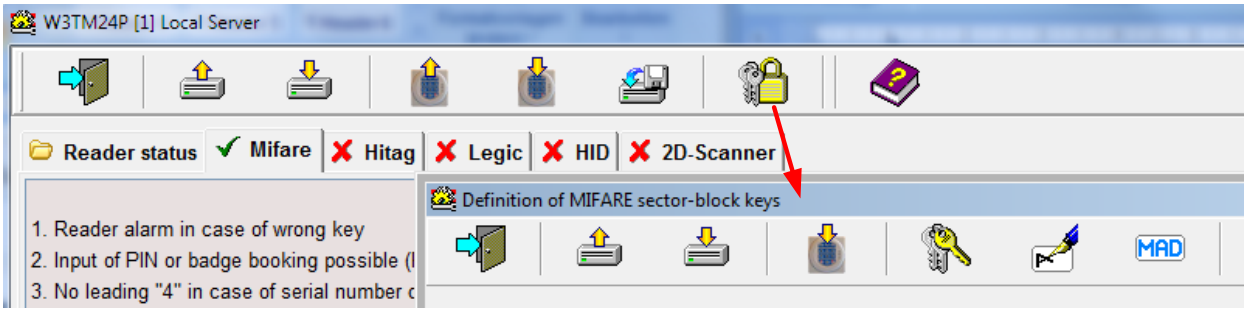
After downloading the settings with , the reader is ready to read the serial number of the MIFARE card.

Field	Description
Activation of serial number check	If activated and downloaded the card reader will read the serial number of the badge again. All other fields will be faded out.

8.2.2 Reading the memory data of MIFARE® Classic (Sector/Block)

In various applications, the card number is read from the card memory. To read the desired information from the memory (1K or 4K) the reader needs a security key and the sector/block address. In addition, the reader must know, in which data format, the 16 bytes may be sent to the system. With the program W3TM24P, these settings will be defined and sent to the selected reader(s).

With the icon “Special definitions” , you open the window "Definition of MIFARE Sector Block Keys".

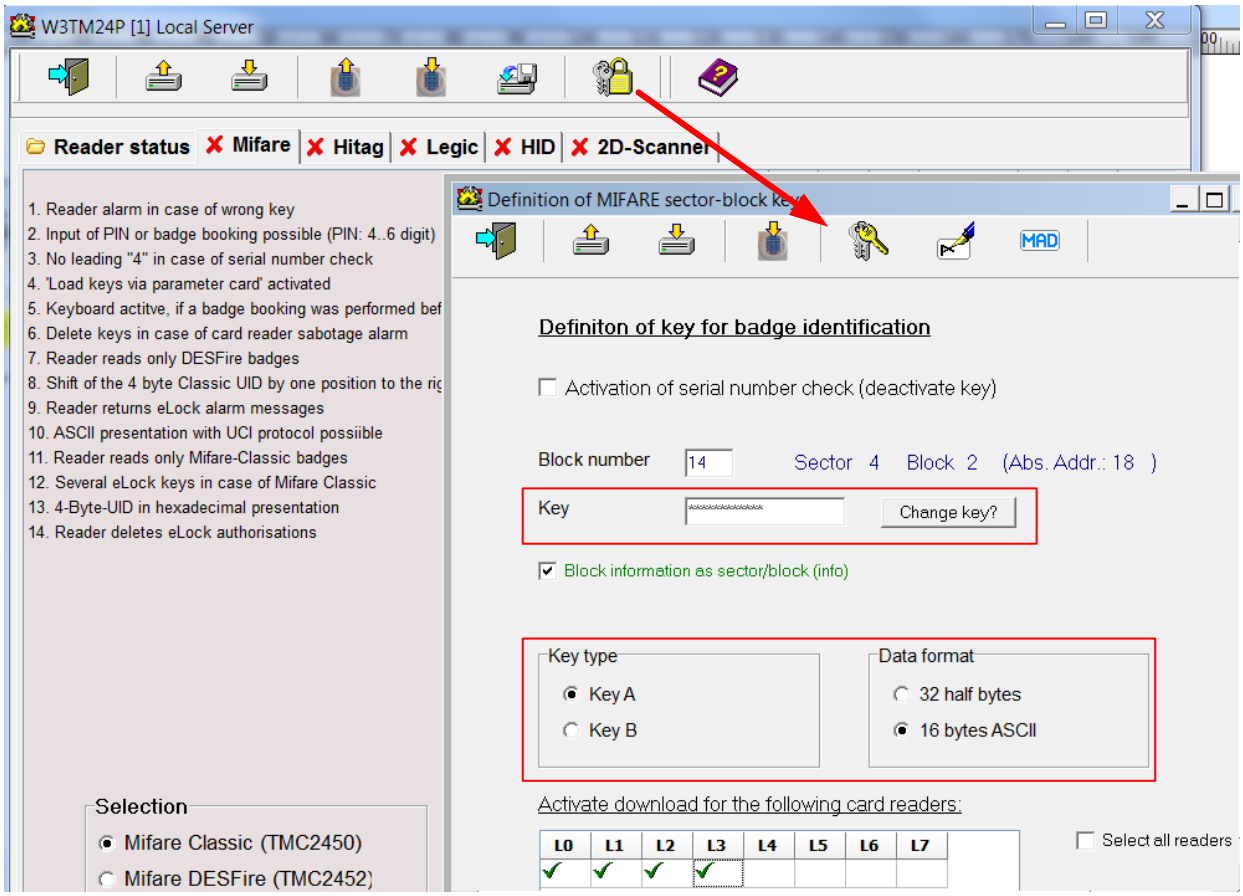


Meaning of the icons in the definition of MIFARE-keys

- Leave program
- Read parameters from file
- Save parameters into file
- Key download for marked card readers
- Key definition for special applications
- Prepare parameter card
- MAD definition

8.2.2.1 Key definition for the badge identification

The entry of keys (Key A or B) or the modification of a key (12 characters) is hidden and followed by a verification. The characters must be entered in hexadecimal format (0..F) and in uppercase for the letters.



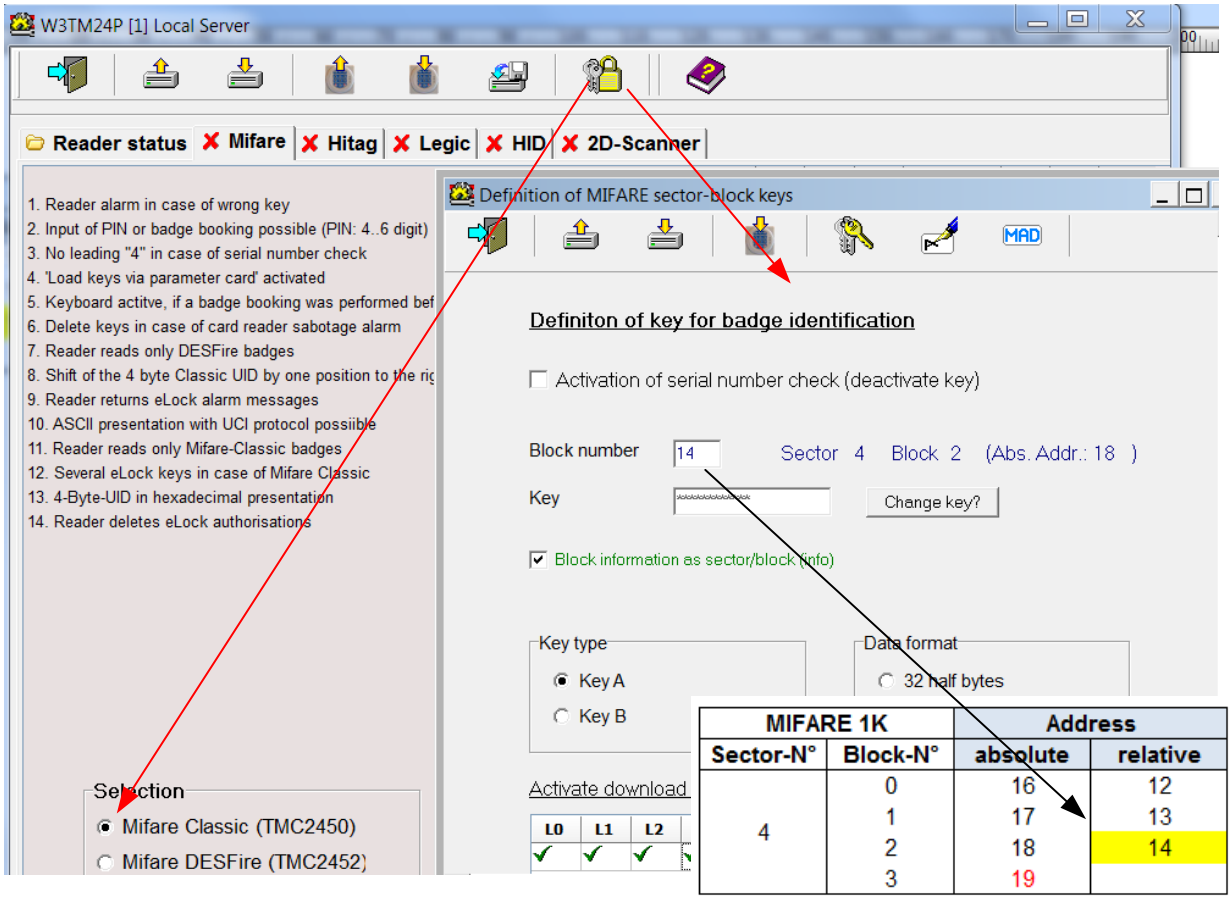
Field	Description
Key	6 byte key (12 characters**)** (invisible input) FFFFFFFFFFFF = transport key Use capital letters for the characters A to F!
Key-Type	A- or B-Key
Data format	Sending data as 32 half bytes e.g. 54657374617573776569732054455354 or interpretation of the 16 byte memory information as ASCII characters e.g. Test card TEST

8.2.2.2 Setting of block number for reading memory data

For this task the following settings may be done:

- Enter the relative block address
- Select reader for data download
- Activate the block info field to check the sector/block address

In the picture below *sector* 4 block 2 and relative address 14 is set.



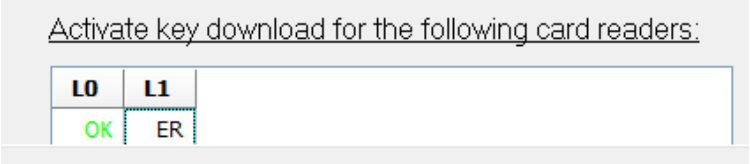
For specifying the starting address to be read in the card, the relative block address must always be entered in the field “Block number”.

The parameters created on this page can be stored on encrypted way into the file $$FES.386 (DB No. 251) into directory *EXOS386P>* or *ACL32>*. The used password must be the same for all applications!

8.2.2.3 Download of the parameters into the reader

The download of the key data – defined on this way – will be activated for the marked card reader by clicking the symbol *‚Key-Download for marked card readers'*

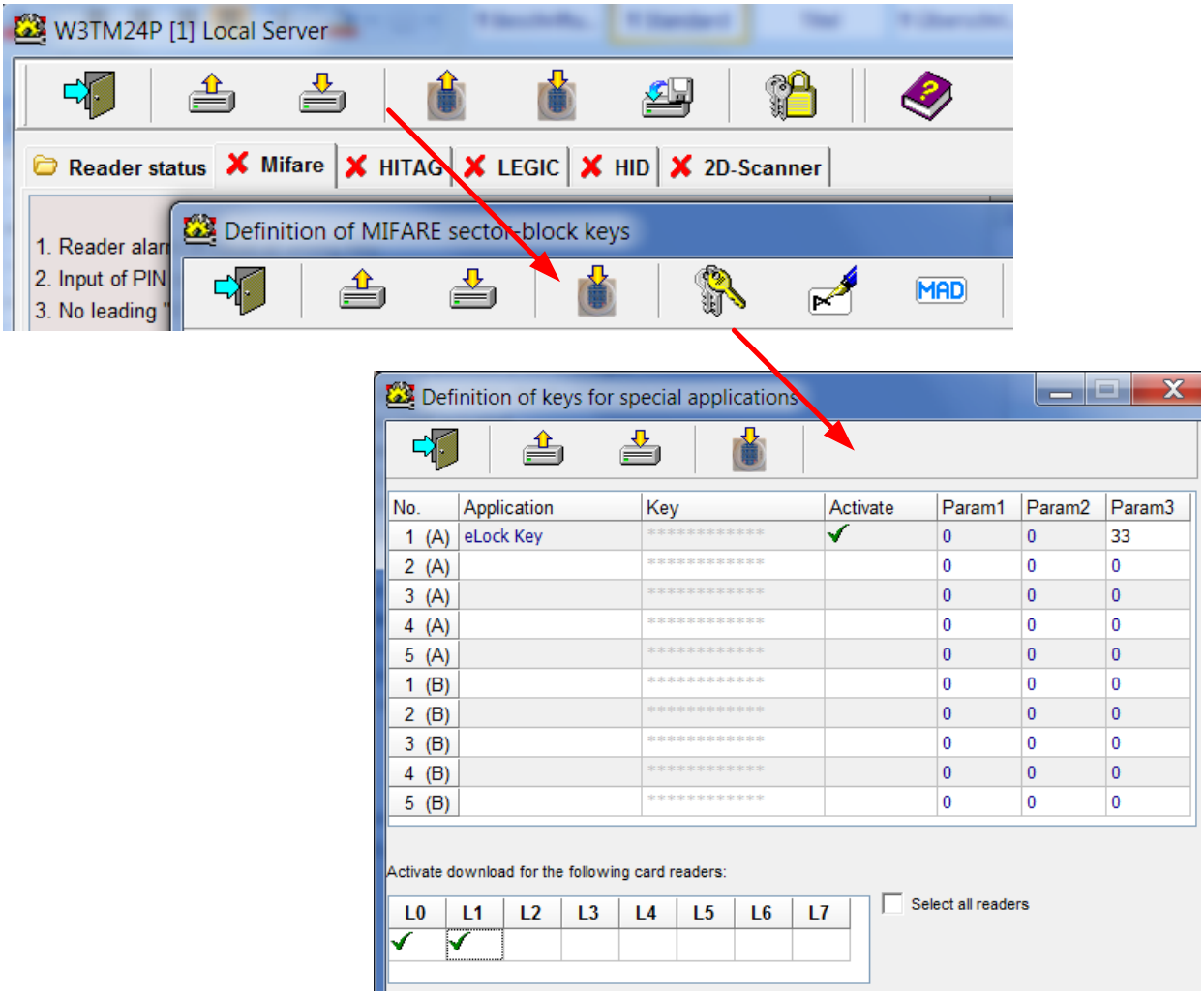
The corresponding card readers will acknowledge the download with an acoustical signal and the message OK or error (ER).



The defined key data can be saved by the symbol ‚Save current key definition' into a file and be loaded again from file by the symbol ‚Get last defined key definition' at later times.

9 Special Applications MIFARE®-Classic

With the icon the "Definition of keys for special applications" window appears. In these fields are entered the key, and the parameters for MIFARE® Classic applications. These data will then be loaded into the defined reader(s).



<u>Meaning of symbols of the task bar</u>

Leave program item

Get parameters from file

Save new defined parameters into file

Parameter download into the marked card readers

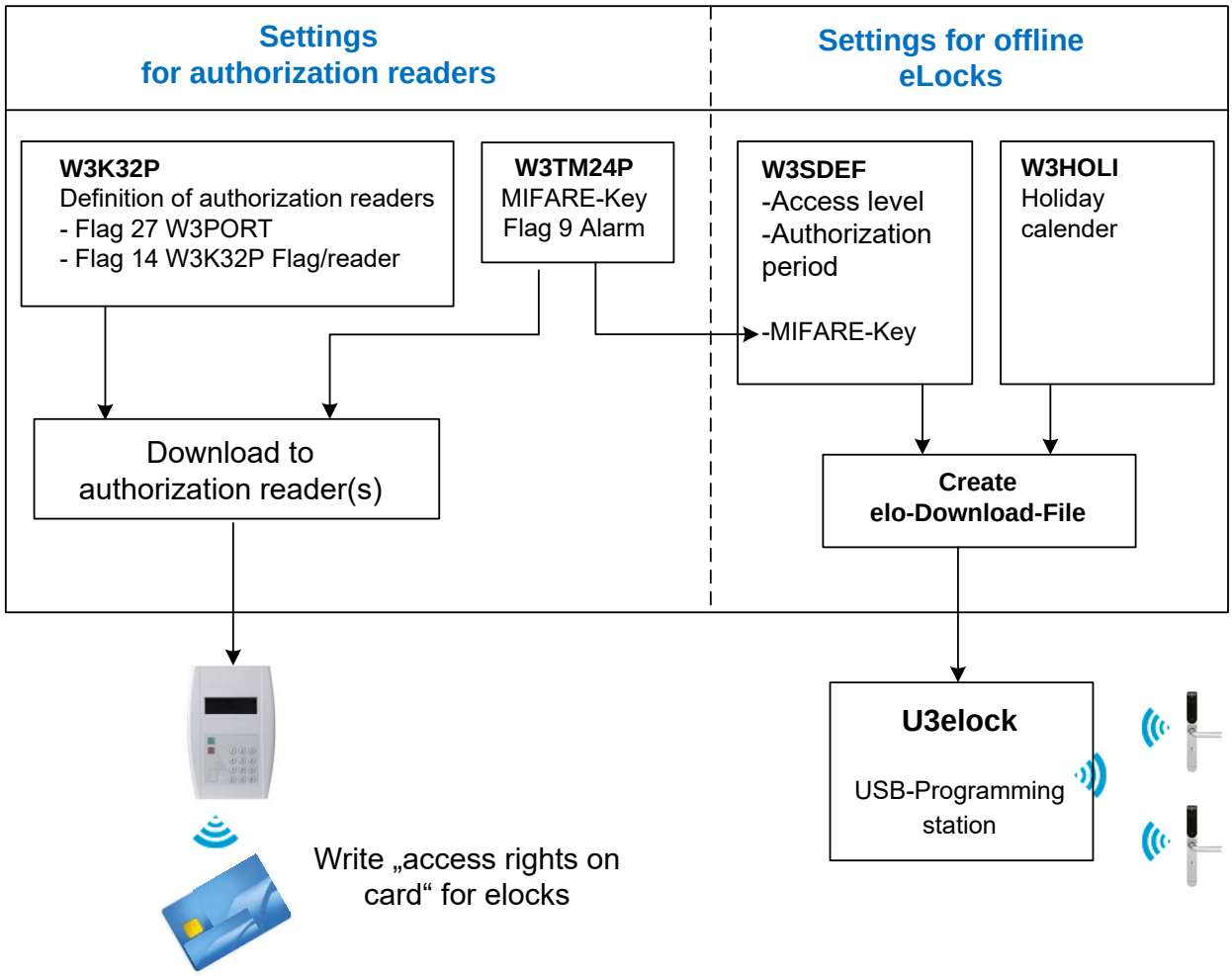
9.1 The “eLock” application with MIFARE® Classic

9.1.1 General

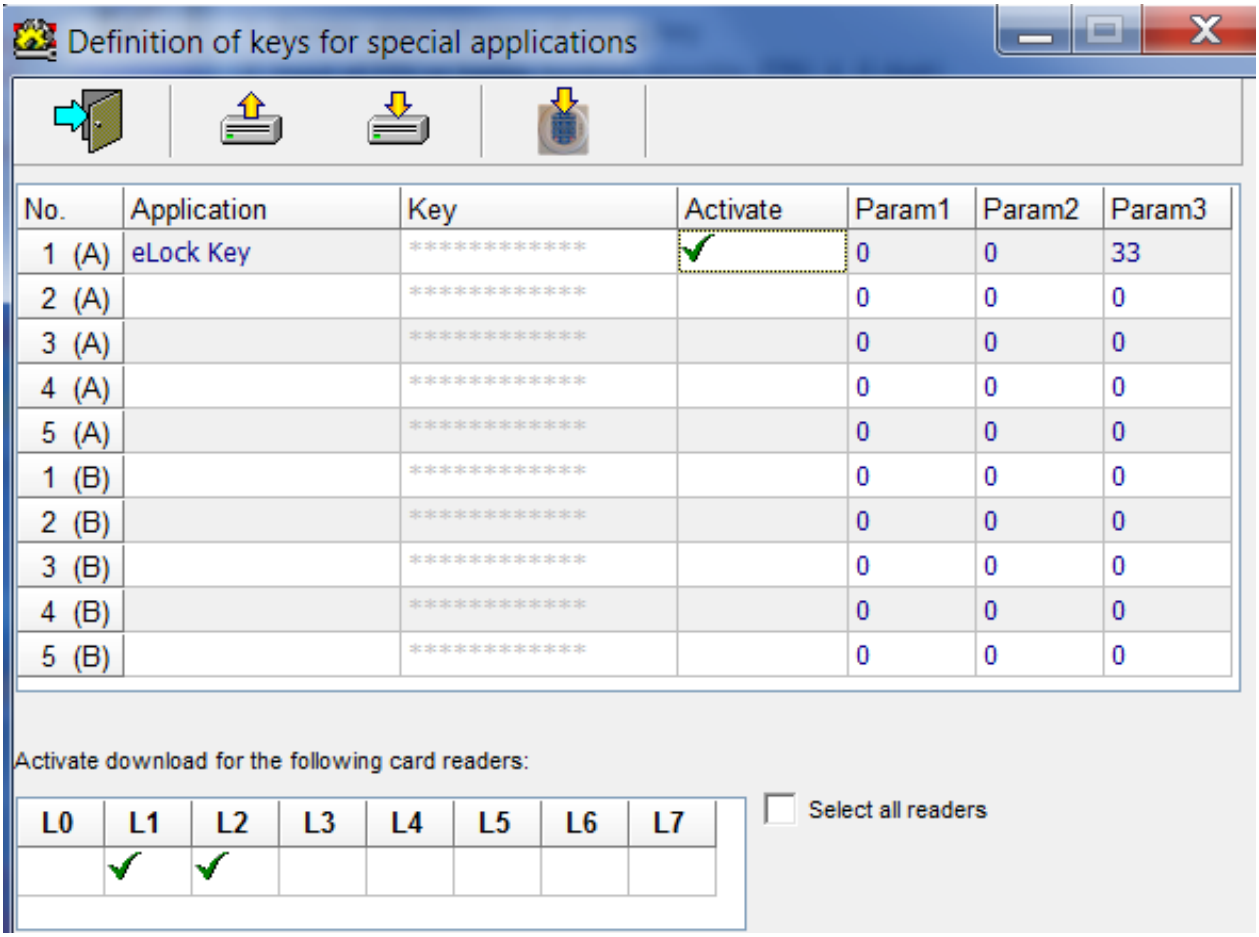
XMP-BABYLON enables the management of the access authorizations of electronic door cylinders or door locks. These electronic locks (eLocks) are equipped with MIFARE® Classic or DESFire reader-heads and will be programmed wireless via a programming tool with appropriate parameters (access levels, authorization times, holiday calendar and MIFARE® security keys). Then the eLocks work in an offline mode without direct connection to the XMP-BABYLON Host computer.

9.1.2 Programming steps for Offline-eLocks and access readers

To get access to an offline door lock, the access rights must be written in the employee-ID with dedicated readers. This is done daily. The access data for offline locks are defined in XMP-BABYLON.



9.1.3 Key-Definition for eLock-application



9.1.3.1 The field "No"

These fields define the number and the key-type of the selected applications.

9.1.3.2 The field “Application“

In this field the application type is entered.

9.1.3.3 The fields “Key” and “Activate“

The corresponding MIFARE-Keys will be entered or changed with verification.

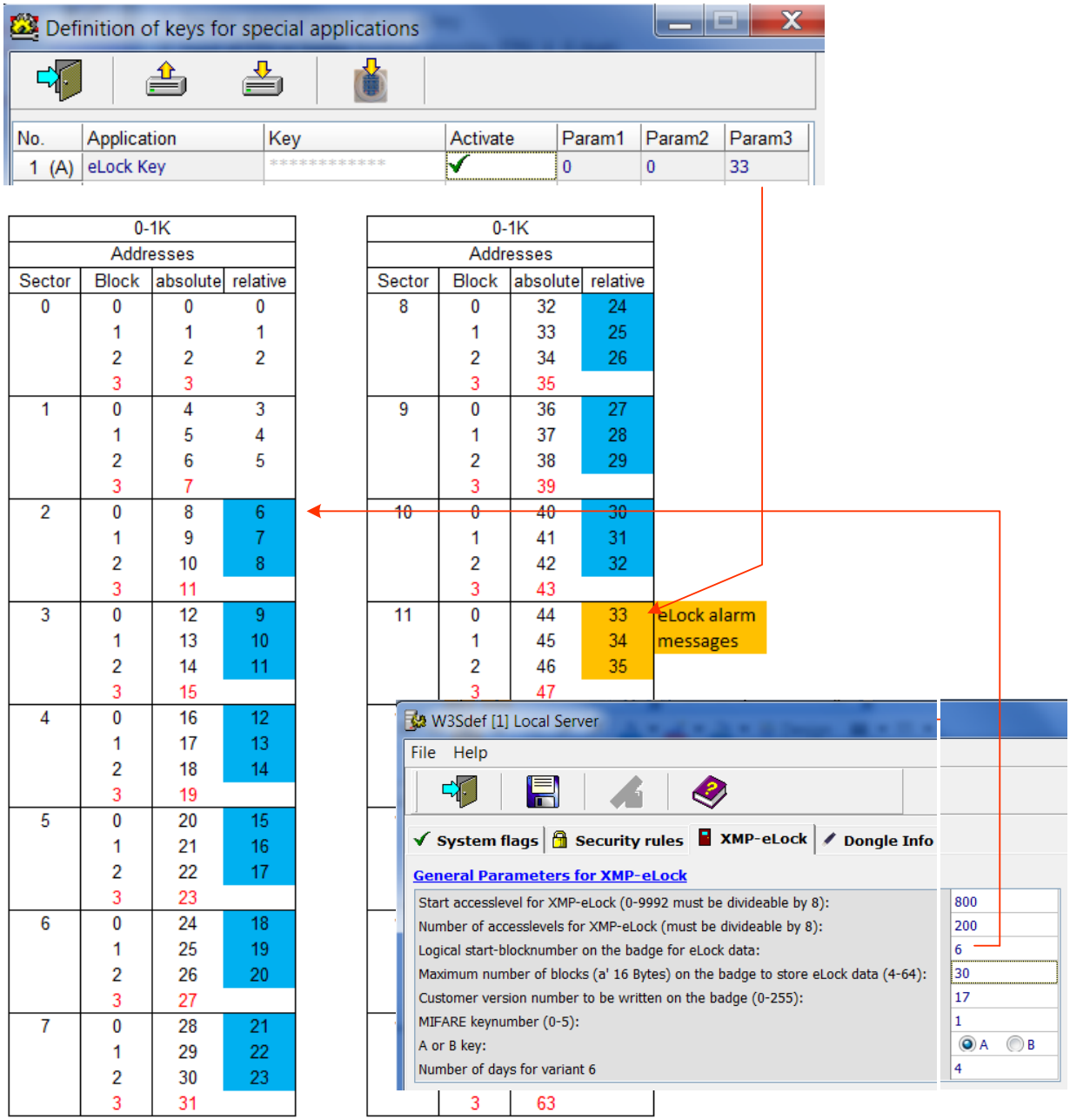
If a field is blue-backgrounded then this field already contains a key which is different from the virgin key = „FFFFFFFFFFFF“.

As a standard the fields are predefined with the key „FFFFFFFFFFFF” and have no coloured background.

In the field “Activate” the application will be activated with a check mark.

9.1.3.4 The fields “Parameter 1, 2, 3“ of the eLock-application

- Parameters 1 and 2 are not used for eLock application
- Parameter 3 can be used for entering the block address starting from which alarm messages of the eLock will be saved (for example “Battery to low”). This relative block address is specified in the W3TM24P program.



9.1.4 MIFARE® Classic 4K – Address-assignment for eLock data

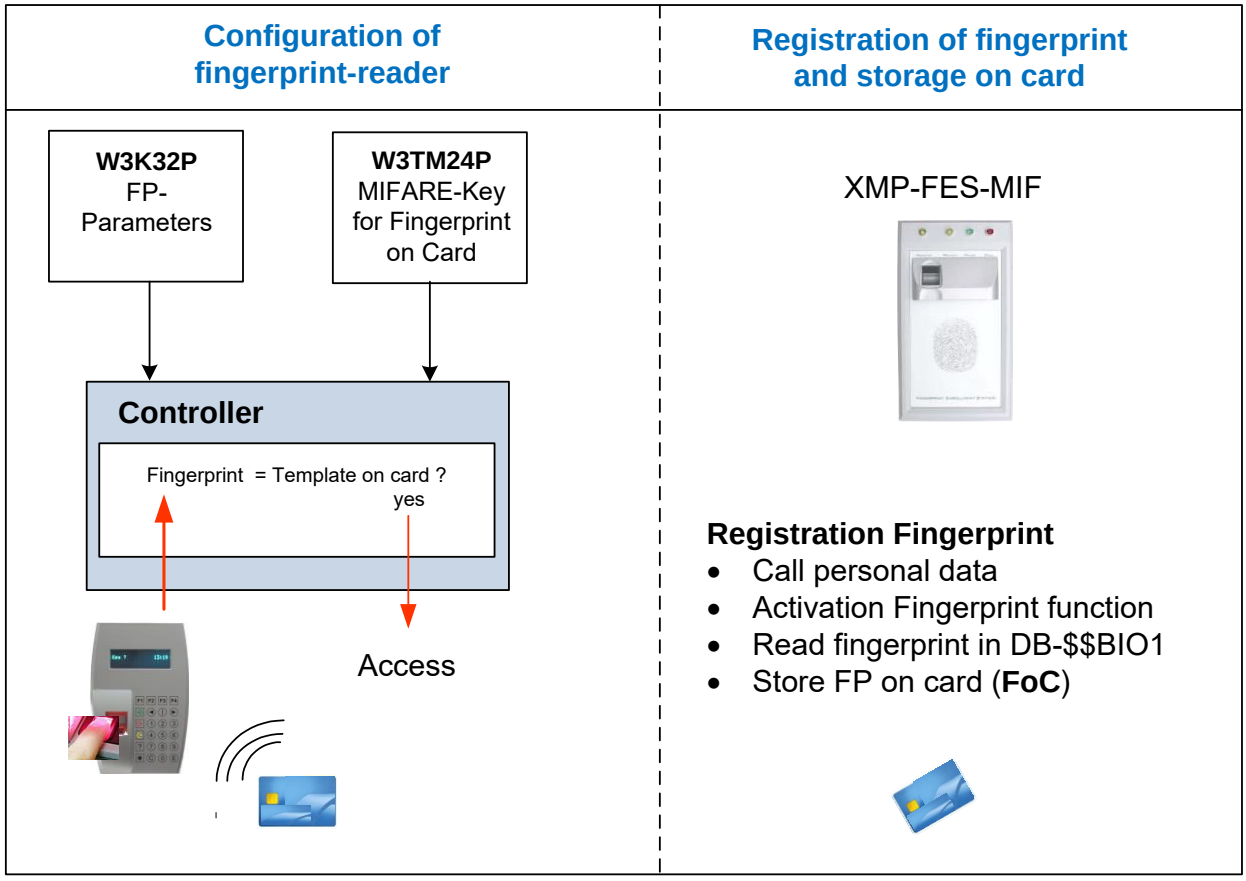
The eLock memory space can be defined between 4 and 64 blocks long. In this table the eLock space starts at relative address 9 and has a length of 27 blocks.

0-1K				1-2K				2-3K				3-4K			
Adressen/Addresses				Adressen/Addresses				Adressen/Addresses				Adressen/Addresses			
Sec.	Blo.	abs.	rel.	Sec.	Blo.	abs.	rel.	Sec	Blo.	abs.	rel.	Sec.	blo.	abs.	rel.
0	0	0	0	16	0	64	48	32	0	128	96	36	0	192	156
	1	1	1		1	65	49		1	129	97		1	193	157
	2	2	2		2	66	50		2	130	98		2	194	158
	3	3			3	67			3	131	99		3	195	159
1	0	4	3	17	0	68	51		4	132	100		4	196	160
	1	5	4		1	69	52		5	133	101		5	197	161
	2	6	5		2	70	53		6	134	102		6	198	162
	3	7			3	71			7	135	103		7	199	163
2	0	8	6	18	0	72	54		8	136	104		8	200	164
	1	9	7		1	73	55		9	137	105		9	201	165
	2	10	8		2	74	56		10	138	106		10	202	166
	3	11			3	75			11	139	107		11	203	167
3	0	12	9	19	0	76	57		12	140	108		12	204	168
	1	13	10		1	77	58		13	141	109		13	205	169
	2	14	11		2	78	59		14	142	110		14	206	170
	3	15			3	79			15	143			15	207	
4	0	16	12	20	0	80	60	33	0	144	111	37	0	208	171
	1	17	13		1	81	61		1	145	112		1	209	172
	2	18	14		2	82	62		2	146	113		2	210	173
	3	19			3	83			3	147	114		3	211	174
5	0	20	15	21	0	84	63		4	148	115		4	212	175
	1	21	16		1	85	64		5	149	116		5	213	176
	2	22	17		2	86	65		6	150	117		6	214	177
	3	23			3	87			7	151	118		7	215	178
6	0	24	18	22	0	88	66		8	152	119		8	216	179
	1	25	19		1	89	67		9	153	120		9	217	180
	2	26	20		2	90	68		10	154	121		10	218	181
	3	27			3	91			11	155	122		11	219	182
7	0	28	21	23	0	92	69		12	156	123		12	220	183
	1	29	22		1	93	70		13	157	124		13	221	184
	2	30	23		2	94	71		14	158	125		14	222	185
	3	31			3	95			15	159			15	223	
8	0	32	24	24	0	96	72	34	0	160	126	38	0	224	186
	1	33	25		1	97	73		1	161	127		1	225	187
	2	34	26		2	98	74		2	162	128		2	226	188
	3	35			3	99			3	163	129		3	227	189
9	0	36	27	25	0	100	75		4	164	130		4	228	190
	1	37	28		1	101	76		5	165	131		5	229	191
	2	38	29		2	102	77		6	166	132		6	230	192
	3	39			3	103			7	167	133		7	231	193
10	0	40	30	26	0	104	78		8	168	134		8	232	194
	1	41	31		1	105	79		9	169	135		9	233	195
	2	42	32		2	106	80		10	170	136		10	234	196
	3	43			3	107			11	171	137		11	235	197
11	0	44	33	27	0	108	81		12	172	138		12	236	198
	1	45	34		1	109	82		13	173	139		13	237	199
	2	46	35		2	110	83		14	174	140		14	238	200
	3	47			3	111			15	175			15	239	
12	0	48	36	28	0	112	84	35	0	176	141	39	0	240	201
	1	49	37		1	113	85		1	177	142		1	241	202
	2	50	38		2	114	86		2	178	143		2	242	203
	3	51			3	115			3	179	144		3	243	204
13	0	52	39	29	0	116	87		4	180	145		4	244	205
	1	53	40		1	117	88		5	181	146		5	245	206
	2	54	41		2	118	89		6	182	147		6	246	207
	3	55			3	119			7	183	148		7	247	208
14	0	56	42	30	0	120	90		8	184	149		8	248	209
	1	57	43		1	121	91		9	185	150		9	249	210
	2	58	44		2	122	92		10	186	151		10	250	211
	3	59			3	123			11	187	152		11	251	212
15	0	60	45	31	0	124	93		12	188	153		12	252	213
	1	61	46		1	125	94		13	189	154		13	253	214
	2	62	47		2	126	95		14	190	155		14	254	215
	3	63			3	127			15	191			15	255	

9.2 The “Fingerprint on Card“ Application with MIFARE® Classic

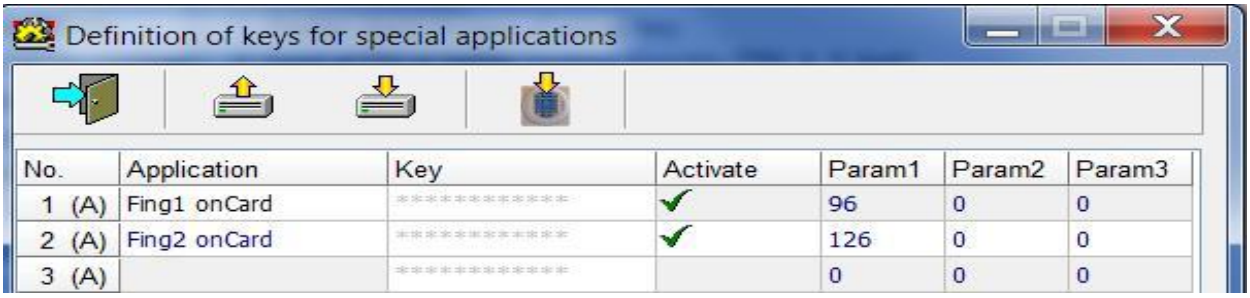
The access with the function “fingerprint on card” is granted by reading first the ID-Card and then by checking the fingerprint. The read fingerprint is transmitted in encrypted form to the controller and compared with the fingerprint-template from the ID-card.

With the program W3TM24P the security keys are transmitted to the readers.



9.2.1 The fields “Parameter 1, 2, 3“ of the fingerprint application

For "Fingerprint on card" the starting block address must be entered in the field Param1 as a relative block address. The number of blocks to be read has a constant size of 24 blocks (384 bytes), and therefore must not be entered as the second parameter. The function "fingerprint on card" is only possible in conjunction with a XMP-TMC28xx-FP reader.



No.	Application	Key	Activate	Param1	Param2	Param3
1 (A)	Fing1 onCard	**********	✓	96	0	0
2 (A)	Fing2 onCard	**********	✓	126	0	0
3 (A)		**********		0	0	0

9.2.2 Overview Fingerprint Start Block Addresses - MIFARE® Classic

0-1K			
Adressen/Addresses			
Sec.	Blo.	abs.	rel.
0	0	0	0
	1	1	1
	2	2	2
	3	3	
1	0	4	3
	1	5	4
	2	6	5
	3	7	
2	0	8	6
	1	9	7
	2	10	8
	3	11	
3	0	12	9
	1	13	10
	2	14	11
	3	15	
4	0	16	12
	1	17	13
	2	18	14
	3	19	
5	0	20	15
	1	21	16
	2	22	17
	3	23	
6	0	24	18
	1	25	19
	2	26	20
	3	27	
7	0	28	21
	1	29	22
	2	30	23
	3	31	
8	0	32	24
	1	33	25
	2	34	26
	3	35	
9	0	36	27
	1	37	28
	2	38	29
	3	39	
10	0	40	30
	1	41	31
	2	42	32
	3	43	
11	0	44	33
	1	45	34
	2	46	35
	3	47	
12	0	48	36
	1	49	37
	2	50	38
	3	51	
13	0	52	39
	1	53	40
	2	54	41
	3	55	
14	0	56	42
	1	57	43
	2	58	44
	3	59	
15	0	60	45
	1	61	46
	2	62	47
	3	63	

1-2K			
Adressen/Addresses			
Sec.	Blo.	abs.	rel.
16	0	64	48
	1	65	49
	2	66	50
	3	67	
17	0	68	51
	1	69	52
	2	70	53
	3	71	
18	0	72	54
	1	73	55
	2	74	56
	3	75	
19	0	76	57
	1	77	58
	2	78	59
	3	79	
20	0	80	60
	1	81	61
	2	82	62
	3	83	
21	0	84	63
	1	85	64
	2	86	65
	3	87	
22	0	88	66
	1	89	67
	2	90	68
	3	91	
23	0	92	69
	1	93	70
	2	94	71
	3	95	
24	0	96	72
	1	97	73
	2	98	74
	3	99	
25	0	100	75
	1	101	76
	2	102	77
	3	103	
26	0	104	78
	1	105	79
	2	106	80
	3	107	
27	0	108	81
	1	109	82
	2	110	83
	3	111	
28	0	112	84
	1	113	85
	2	114	86
	3	115	
29	0	116	87
	1	117	88
	2	118	89
	3	119	
30	0	120	90
	1	121	91
	2	122	92
	3	123	
31	0	124	93
	1	125	94
	2	126	95
	3	127	

2-3K				
Adressen/Addresses				
Sec	Blo.	abs.	rel.	
32	0	128	96	Fingerprint 1
	1	129	97	
	2	130	98	
	3	131	99	
	4	132	100	
	5	133	101	
	6	134	102	
	7	135	103	
	8	136	104	
	9	137	105	
	10	138	106	
	11	139	107	
	12	140	108	
	13	141	109	
	14	142	110	
	15	143		
33	0	144	111	
	1	145	112	
	2	146	113	
	3	147	114	
	4	148	115	
	5	149	116	
	6	150	117	
	7	151	118	
	8	152	119	
	9	153	120	
	10	154	121	
	11	155	122	
	12	156	123	
	13	157	124	
	14	158	125	
	15	159		
34	0	160	126	Fingerprint 2
	1	161	127	
	2	162	128	
	3	163	129	
	4	164	130	
	5	165	131	
	6	166	132	
	7	167	133	
	8	168	134	
	9	169	135	
	10	170	136	
	11	171	137	
	12	172	138	
	13	173	139	
	14	174	140	
	15	175		
35	0	176	141	
	1	177	142	
	2	178	143	
	3	179	144	
	4	180	145	
	5	181	146	
	6	182	147	
	7	183	148	
	8	184	149	
	9	185	150	
	10	186	151	
	11	187	152	
	12	188	153	
	13	189	154	
	14	190	155	
	15	191		

3-4K			
Adressen			
Sec.	blo.	abs.	rel.
36	0	192	156
	1	193	157
	2	194	158
	3	195	159
	4	196	160
	5	197	161
	6	198	162
	7	199	163
	8	200	164
	9	201	165
	10	202	166
	11	203	167
	12	204	168
	13	205	169
	14	206	170
	15	207	
37	0	208	171
	1	209	172
	2	210	173
	3	211	174
	4	212	175
	5	213	176
	6	214	177
	7	215	178
	8	216	179
	9	217	180
	10	218	181
	11	219	182
	12	220	183
	13	221	184
	14	222	185
	15	223	
38	0	224	186
	1	225	187
	2	226	188
	3	227	189
	4	228	190
	5	229	191
	6	230	192
	7	231	193
	8	232	194
	9	233	195
	10	234	196
	11	235	197
	12	236	198
	13	237	199
	14	238	200
	15	239	
39	0	240	201
	1	241	202
	2	242	203
	3	243	204
	4	244	205
	5	245	206
	6	246	207
	7	247	208
	8	248	209
	9	249	210
	10	250	211
	11	251	212
	12	252	213
	13	253	214
	14	254	215
	15	255	

9.3 The “ILock on Card“ Application

9.3.1 General

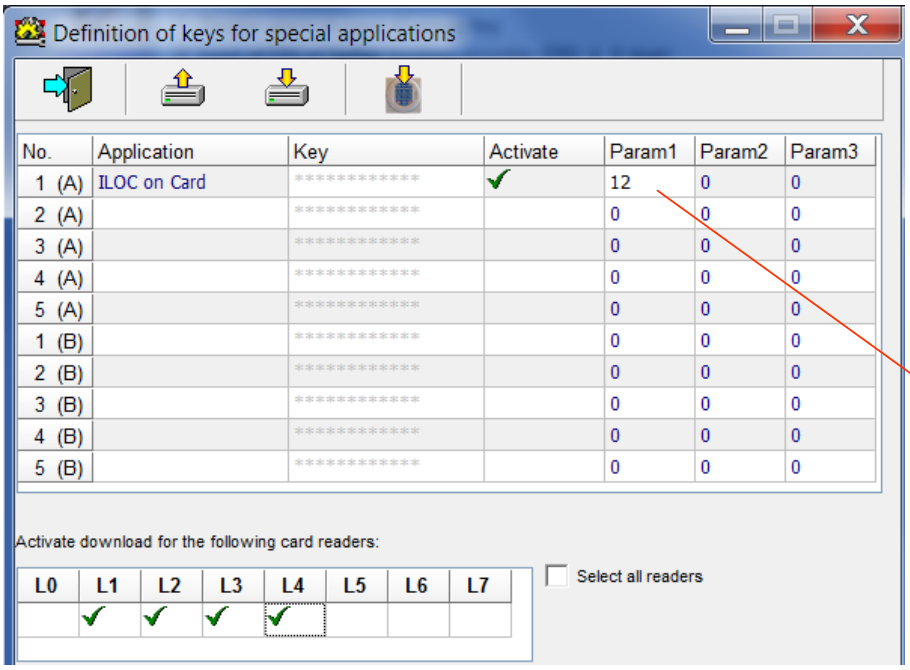
It should be ensured by the system, that people who have been contaminated in a pharmaceutical sector (chemical, bacteriological, radioactive, etc.), have no access for a predefined time to certain other rooms. The application “Interlocking on card” fulfills these requirements.

9.3.2 Meaning of W3TM24P for the Ilock on Card Application

The program W3TM24P writes only the security keys and parameters in the readers of the monitored interlocking rooms. All other settings are made in the programs W3K32P and W3CONTTI.

9.3.3 Meaning of Parameter 1

Parameter 1 indicates the relative block address from which the locking times will be written on the Mifare-card (Example: rel. block address 12).

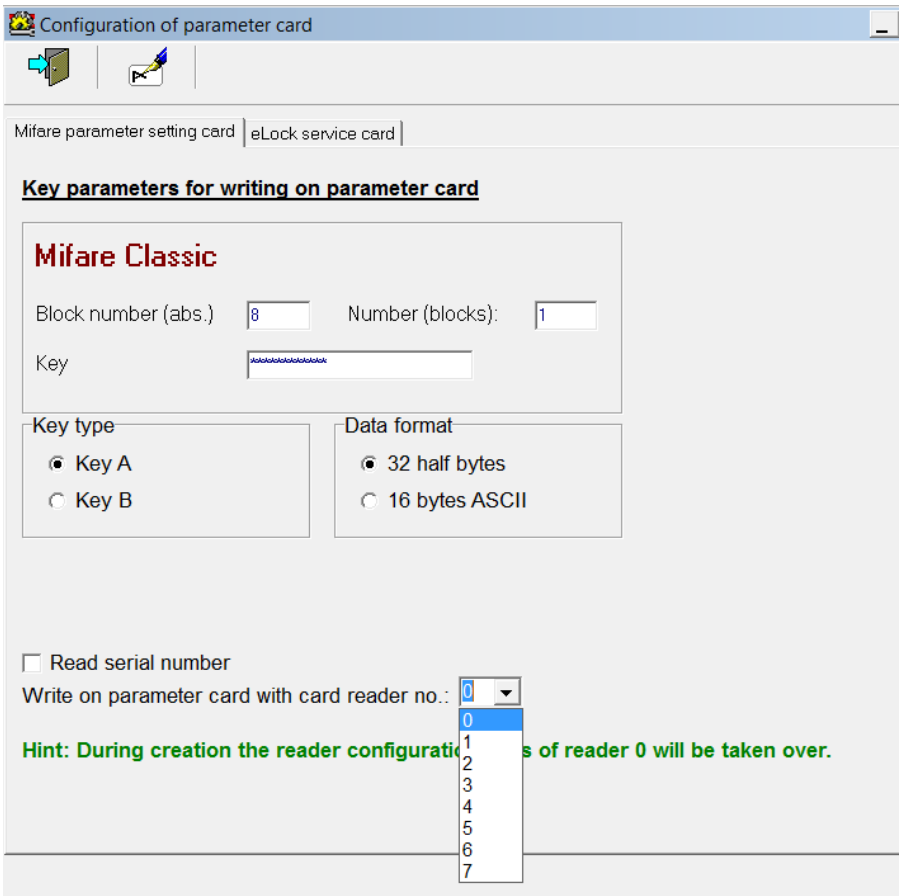


0-1K			
Addresses			
Sec.	Blo.	abs.	rel.
0	0	0	0
	1	1	1
	2	2	2
	3	3	
1	0	4	3
	1	5	4
	2	6	5
	3	7	
2	0	8	6
	1	9	7
	2	10	8
	3	11	
3	0	12	9
	1	13	10
	2	14	11
	3	15	
4	0	16	12
	1	17	13
	2	18	14
	3	19	

The function Interlocking on card is described in detail in the documentation GCONTII.

9.4 Configuration of parameter setting cards for MIFARE® Classic readers

In order to use MIFARE® Classic readers, key-parameters must be written in the readers. This will be done with a MIFARE-parameter card which will be configured in W3TM24P with the icon "Prepare parameter card ". In the window „Configuration of parameter card" the application data from the window „MIFARE sector block keys" are taken over. These data can be new defined or simply changed.



Now the defined key-parameters can be written on the parameter card via the selected reader address by clicking the symbol *"Write current parameters on parameter card* ".

Within the next 2.5 seconds, after sending the data, the parameter card must be hold into the card reader field. After expiring of this time frame, the data will be dismissed.

Special card reader properties should be deactivated during this operation.

Meaning of the field Number (Blocks)

The input field "*Number (blocks)"* is only used for the reader XMP-TMC28xx and the special solution "Access on Card". If the MIFARE-reading-head of the XMP-TMC28xx should read several subsequent blocks in the ID-card and send it by clock-data interface to the reader, the number of blocks (max 9) will be entered in this field for programming the parameter card.

Settings:

- Data format: 32 half bytes
- XMP-TMC280x→SW3: mode 15
- XMP-TM500 parameters→Time/Coding→Badge encoding 02/00), Flags→Flag 22
- General chip parameters→ Insert level for AOC)

Special feature for XMP-TMC28xx

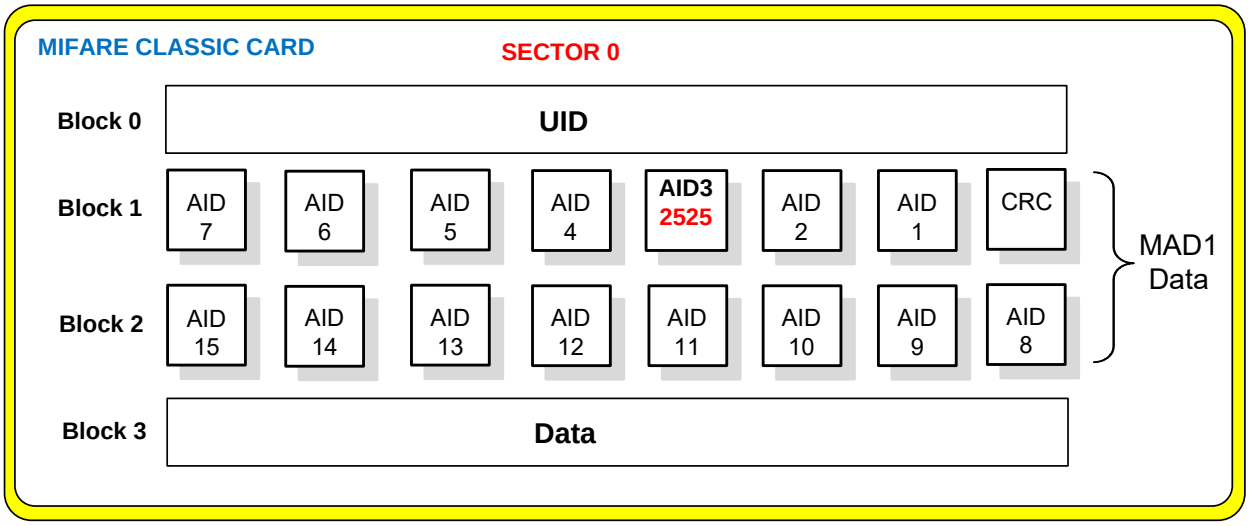
If a XMP-TMC28xx or XMP-TMC26xx should read the block content in ASCII-format, the data format for the parameter card must nevertheless be set on "32 half bytes". The card data received by the XMP-TMC28xx (after parameter setting of the reading head with this parameter card) will be converted in the reader into ASCII format. In this case you have to enter the value 00/04 into the TM500-Parameters →Time/ Coding →Badge encoding.

The parameter card can only be used to write parameters for reading the card-ID from the card memory! Further application parameters, e.g. for Fingerprint On Card or XMP-eLock cannot be written on the parameter card.

10 MAD1-Data MIFARE® Classic

In the standard reading process, the reader contents the block address to be read out of the MIFARE-card memory. When using the MAD1-reading method, the reader contents the name of the application (AID) and not the sector/block memory address. The reader sends the AID-No. to the card. The card looks in the MAD1-data for this AID-No. from AID-1 to AID-15. When the searched AID-number is found, the stored sector / block address is read out and sent to the reader.

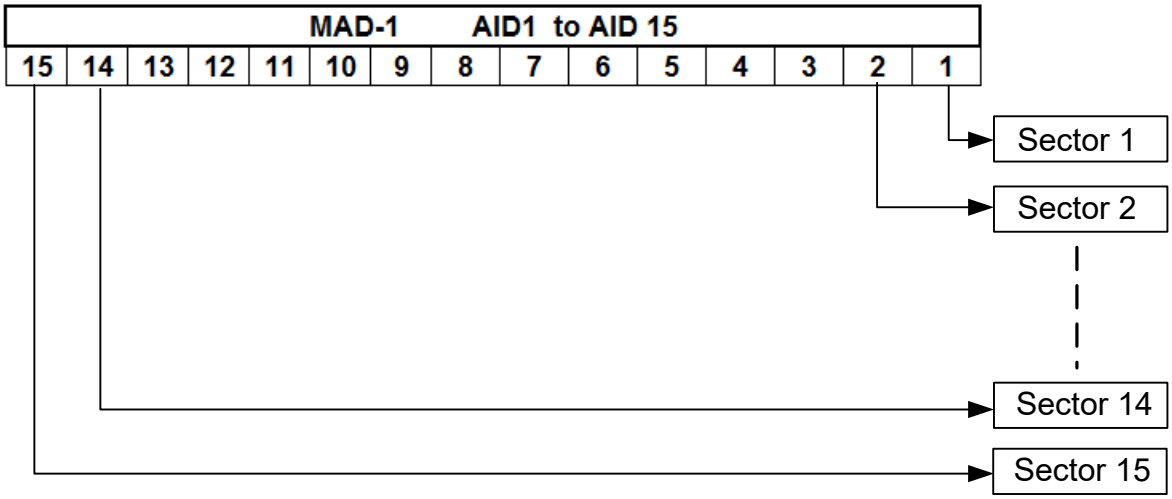
The MAD1-data are stored in the MIFARE 1K-chip in Sector 0 / block1 and 2.



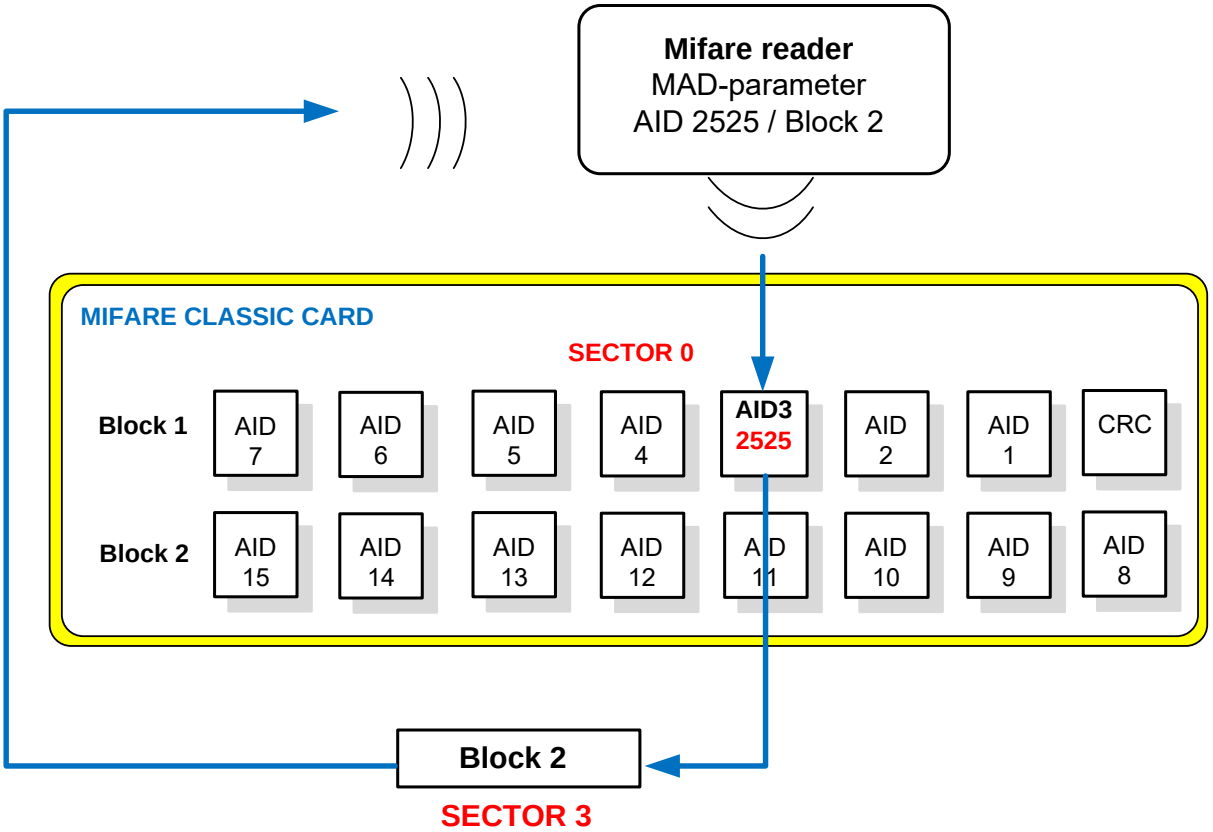
Advantage of the MAD-Function

If for example the access control application cannot be stored for all company employees in the same sector of the card, because this position is already assigned to another application, reference is made to the MAD-addressing method. In the MAD-memory the applications are defined with names and serve as pointer to the sectors. If the name of the application is found in the MAD-structure, the card number will be read out of the respective sector number.

Assignment AID to sectors

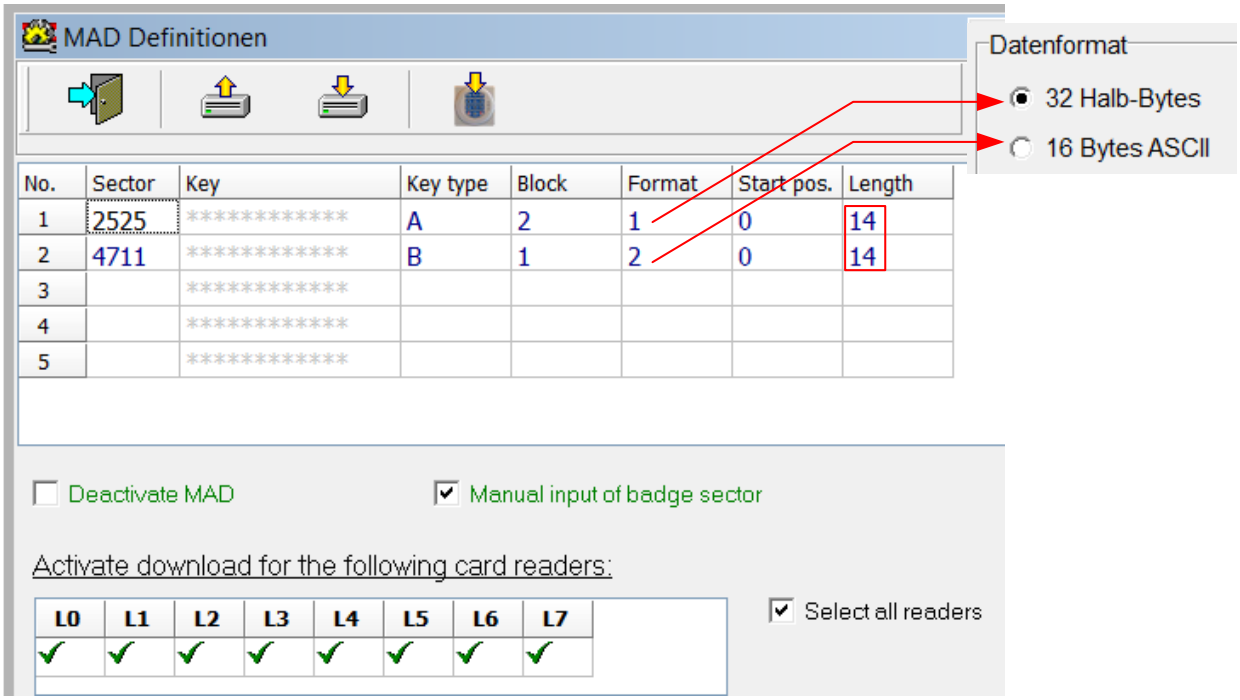


Example: The reader tries to find the AID-2525 in the MAD-blocks 1 and 2 of the card. If the AID-Number is found, in our example, the MIFARE-card reads the sector 3, block 2, and transmits the data to the reader. The AID-Nos. are directly attributable to the sector numbers i.e. AID3 = sector 3. If the AID2525 has been found in AID14, the card would read the data from sector 14 / block 2.



10.1 Definition of the MAD-Parameters

With symbol MAD *‚MAD definition'* of the window „Definition of MIFARE sector block keys“, the window for configuring the necessary MAD-parameters will open.



The required information is read on the basis of the input application identifier (AID), the 12-digit keys, the key type (A, B) and the block number of the card sector. The format type indicates whether the information in half byte format (type 1, 32 half bytes) or in ASCII format (type 2, 16 bytes) should be interpreted. Furthermore, the information to be transmitted can be defined by starting position and length.

10.1.1 The field “No.“

The number (No.) of the line corresponds to the MAD-application.

10.1.2 The field “AID”

The application identifier (AID) consists of a two byte-information, which defines the address of the searched card sector by their position within blocks 1 and 2 of card sector 0 of the MIFARE-badge.

The sequence of defined keys defines the priority of the information to read at the same time, too. If already the first reading attempt with key 1 would be successful, a reading attempt for the following key would be stopped, i.e. these keys will not be evaluated for this badge.

10.1.3 The field “Key“

The sequence in which the keys have been defined, defines also the priority of the information to be read. If already the first reading attempt with key 1 has been successful, a reading attempt for the following keys would be stopped, i.e. these keys will not be evaluated for this badge. The data input of keys are hidden on the display and verified after seizure.

A blue highlighted field corresponds to a key that is not the Virgin-Key = "FFFFFFFFFFFF".

The sequence of defined keys defines the priority of the information to read at the same time, too.

As a standard the fields are predefined with this key „FFFFFFFFFFFF” and have no coloured background. For the characters A to F capital letters should be used.

No.	Sector	Key	Key type	Block	Format	Start pos.	Length
1	2525	**********	A	2	1	0	14
2	4711	**********	B	1	2	0	14

10.1.4 The field “Key type”

It can be selected between key type A or B.

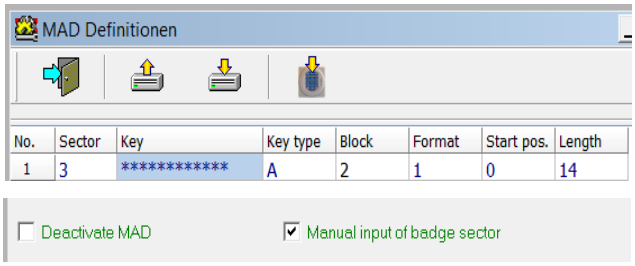
10.1.5 The field “Block“

In this field the block number is entered, which is read from the sector addressed by the matching AID-Number. This field can only be entered a block number from 0 to 2, therefore no absolute or relative block address.

No.	Sector	Key	Key type	Block	Format	Start pos.	Length
1	2525	**********	A	2	1	0	14

10.1.6 The checkbox “Manual input of badge sector“

With the checkbox “*Manual input of badge sector”* the possibility exists to assign the card sector information belonging to the key by direct input. Then the MAD is without effect.



Mifare Classic			
Addresses			
Sector	Block	absolute	relative
3	0	12	9
	1	13	10
	2	14	11
	3	15	

10.1.7 The field “Format” for MAD

The format type indicates if the information will be interpreted as half bytes (type 1, 32 half-bytes) or as ASCII-format (type 2, 16 bytes).

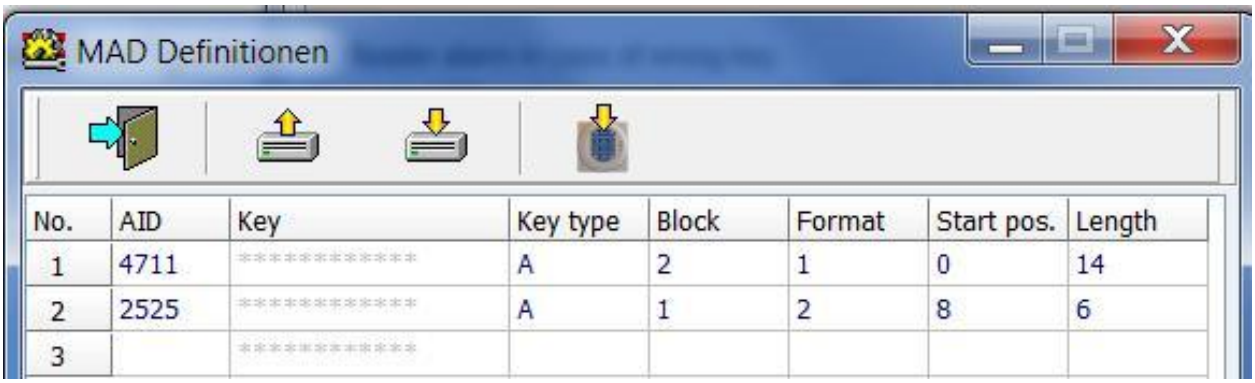
Example: The 14-digit ID-number is stored in hex format in the memory of the card.

The following table shows the value in ASCII and half bytes.

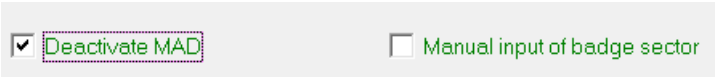
Hex	56	49	53	49	54	4F	52	20	43	41	52	44	30	31
Halbbytes	56	49	53	49	54	4F	52	20	43	41	52	44	30	31
ASCII	V	I	S	I	T	O	R		C	A	R	D	0	1
Start Position	**0**	1	2	3	4	5	6	7	**8**	9	10	11	12	13

10.1.8 The fields “Start position” and “Length”

The information to be transmitted from the card to the reader is defined with start position and length. The length is always specified in bytes, and the total of the value of length and start position may not exceed the number 16.



10.1.9 The checkbox “Deactivate MAD“



Activating the checkbox *‚Deactivate MAD’* ifollowing by a corresponding download will deactivate all keys. The card reader will then read the serial number of the MIFARE-badge again.

Currently, the AUTEC-readers support only MIFARE 1K with MAD1-data.

11 Reader Specification MIFARE DESFire® EV1

The readers can read DESFire EV1 cards (2K, 4K, 8K) with AES-128 bit encryption. Other DESFire cards can be read “PLAIN”.

11.1 W3TM24P - Meaning of the symbols of the task bar

Leave program

Read parameters from file

Save parameters into file

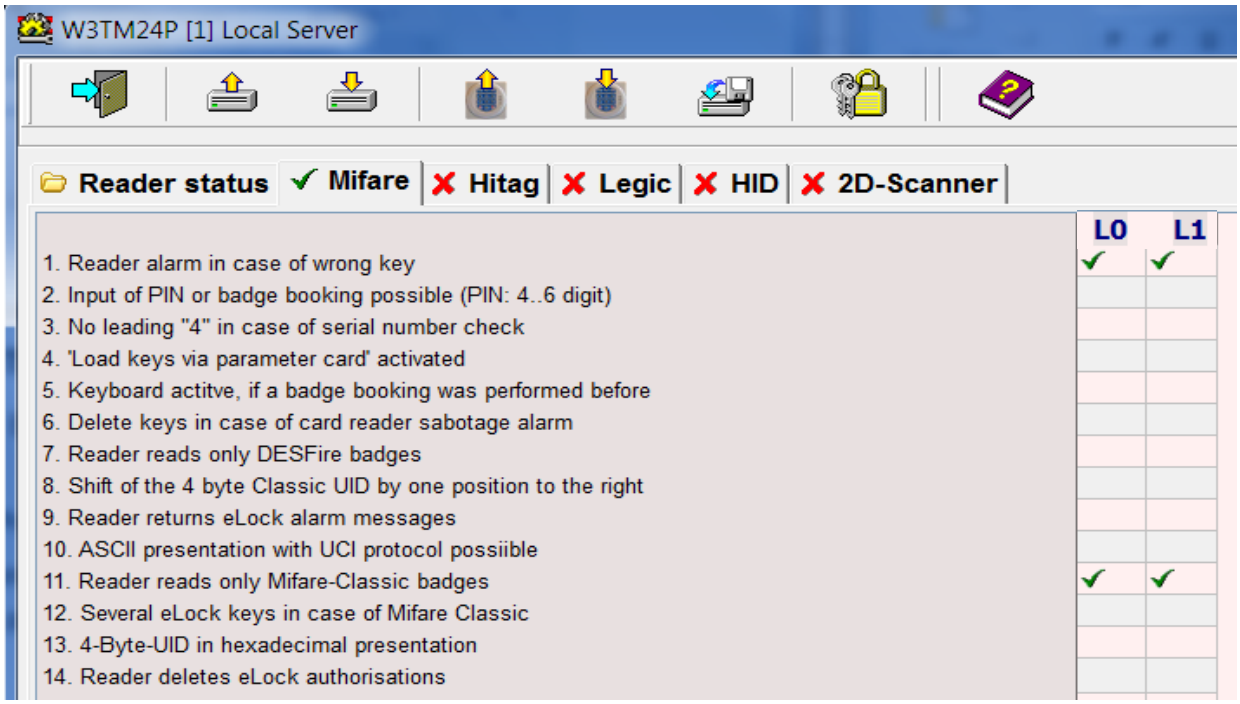
Parameter upload from card reader

Parameter download into card reader

Import data/parameters from another XMP-K32 (KTMCppuu.386)

Special reader definitions

11.2 MIFARE DESFire® Reader Features



11.3 MIFARE DESFire® - Meaning of the Reader Features

The current reader settings can be made visible with the icon , “Upload parameters from the reader”. The desired feature is activated by placing a check mark in the appropriate field and then by downloading the parameters into the readers.

FLAG	DESCRIPTION
1	Reader alarm in case of wrong key This alarm is generated by the card reader, if the current badge does not match the required card reader key during reading of sector block information. This is a reader internal alarm which is not forwarded to the XMP-K32 or to the host computer. This option should not be used if the pass through supervision (XMP-K32 input I-2) is activated or the card reader is used for writing parameter cards.
2	Input of PIN or badge booking possible (PIN: 4-6 digit) Instead of a badge booking it is also possible to insert the corresponding badge number directly via PIN-code. For this special case the badge number check must be realized as 4-6 digit check (not 14 digits). This number has nothing to do with the secret code, which is normally entered under “Badge Definition” in the personal database. **Hint:** The use of this option reduces the security
3	No leading "4" in case of serial number check For historical reasons, MIFARE card readers of the TMC-family send always a leading „4“ by reading a 14-digit serial number. Normally this 4 not belongs to the serial number of the badge. By activating this option the leading „4“ will not be generated. STANDARD PRESENTATION CLASSIC (4 BYTES) 40034908539740 Fading out the leading 4 Classic (4 Bytes) 00034908539740
4	“Load keys via parameter card” activated Beside the possibility to load the MIFARE-key with the program W3TM24P into the MIFARE-readers XMP-TMC2250/2260, it is also possible to load the key by using a special parameter card (XMP-MIF-PARA-CARD) for reading the sector-block. By setting this flag, the reader is prepared for reading the key information from the parameter card. After reader configuration, the flag will be automatically deleted to avoid a modification of configuration. This flag is not stored into the reader, that means, after power-off the flag must be set again if necessary.

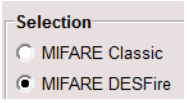
Meaning of the Reader Features

5	Keyboard active, if a badge booking was performed first If the reader is set so that the PIN will be entered after booking (W3Port -> Flag 24, W3K32P -> “Reader / Flags” -> Flag5), with this option the reader keyboard will be deactivated. After a new card booking the keyboard is again active for about 10 seconds.
6	Delete keys in case of sabotage alarm at the reader If a tamper alarm occurs at the reader, the security keys will be deleted. The keys must be reloaded into the reader after power-on.
7	Reader reads only DESFire badges If this flag is set, the reader reads only DESFire badges. Classic cards are ignored. After completing a migration from Classic to DESFire, this flag can be set to improve project safety.
8	Shift of the 4 byte UID-Classic by one position to the right With this flag, the four byte of a UID-number from a MIFARE® Classic card is shifted by one position to the right, to ensure the simultaneous use of MIFARE® Classic and DESFire cards. 40033672387420 → Flag 8 deactivated 40003367238742 → Flag 8 activated
9	Reader returns eLock alarm messages By setting this flag and with appropriate XMP-eLock configuration, the reader looks first for alarm messages in the eLock alarm memory of the ID-card and then starts with the reading of the badge data. 04/04/13 18:12:55 99 ? Door 1 elock elo_test Battery too low
10	ASCII presentation with UCI-protocol possible With this flag the reader sends the badge data to the XMP-K32 in a format which will match with the UCI-protocol from the controller and allows the data to be forwarded as ASCII-data. (K32→Serial Protocol = 0: UCI Protocol, Protocol Variants and Data format 4: ASCII-data)
11	Reader reads only MIFARE If this flag is set, the reader reads only MIFARE® Classic badges. DESFire badges are ignored.

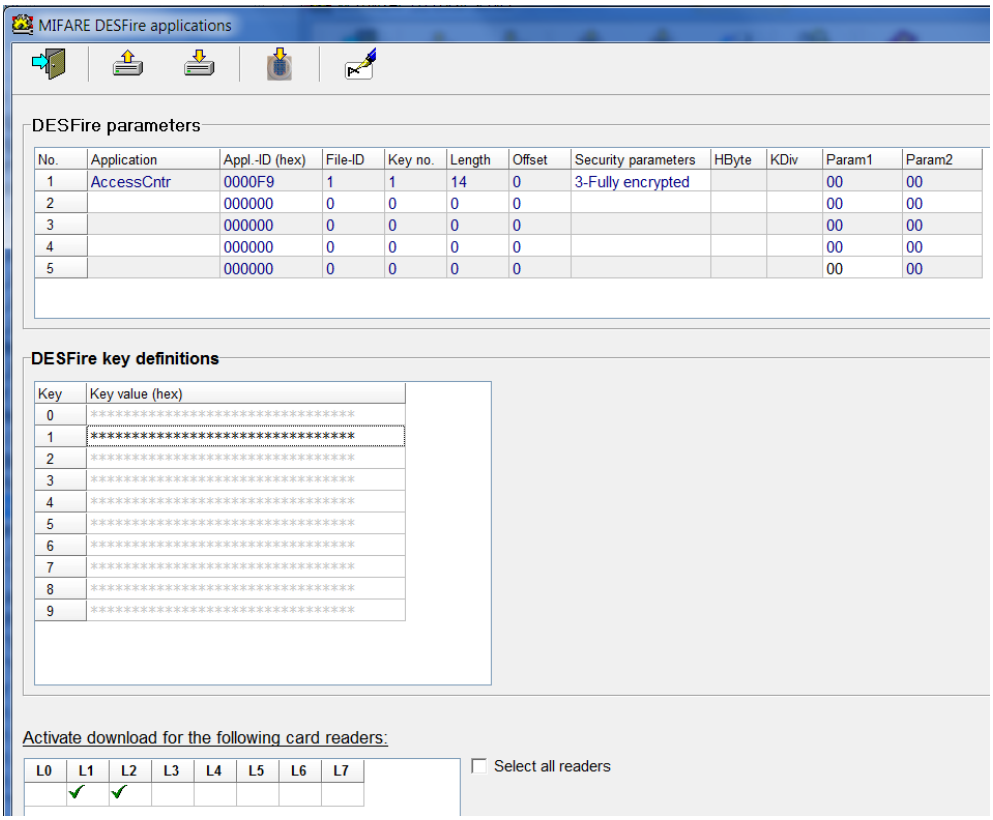
Meaning of the Reader Features

12	Several eLock keys in case of MIFARE® Classic Normally the memory space of the MIFARE® Classic cards reserved for XMP- eLock data is encrypted for all sectors with the same key. With this flag the reader can be set for reading a maximum of 4 consecutive card sectors with a different key for each sector.
13	4-Byte-UID in hexadecimal presentation By default, the serial number (UID – 14 digits) of the card is sent in decimal format. When this flag is set, the transmission is done in hexadecimal format.
14	Reader deletes eLock-authorizations With this flag, the access authorization at electronic offline door locks is deleted.

11.4 Meaning of the MIFARE® DESFire Parameters

By using the selection box 

the reader MIFARE DESFire® is selected. By clicking on the button "Specific definitions", the configuration page is opened.



11.4.1 The field “No.“

This is the numbering of the 5 possible applications which can be downloaded in the readers.

11.4.2 The field “Application”

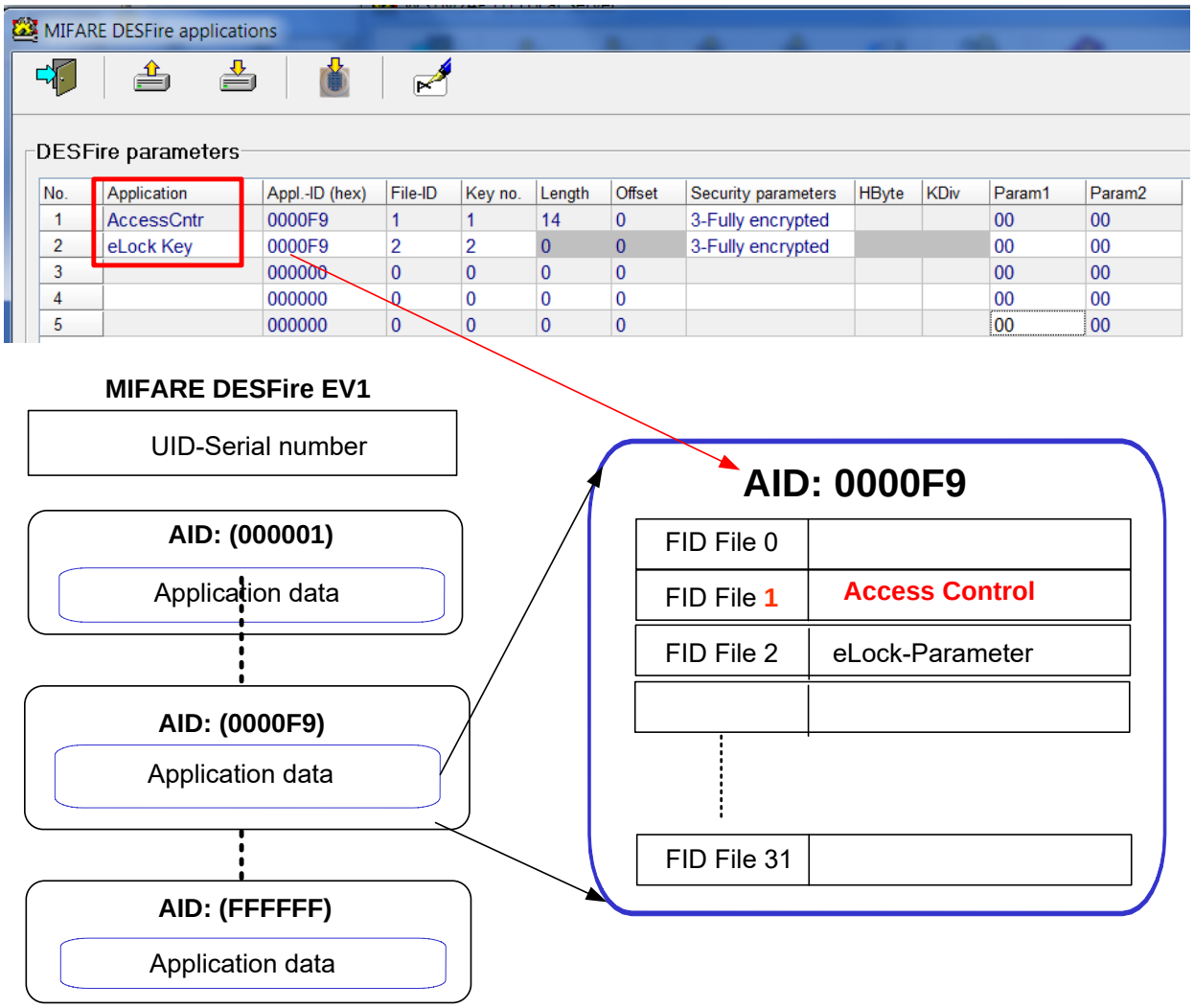
All application parameters setting in the fields will be downloaded into the selected readers.

- **UID** = The serial number is read from the MIFARE DESFire® card
- **AccessCntr** = Setting parameters for access control application
- **Fing1 on Card** = Setting parameters for reading Finger template 1 on ID-Card
- **eLock Key** = Parameters to download in reader for read/write eLocks

The application No.1 should always contain the parameters for the card number (UID or AccessCntr)

11.4.3 The field “Appl.-ID”

In the memory of the MIFARE®-DESFire EV1-chip, up to a total of FFFFFF (hex) Applications (AID) may be defined, depending on the memory capacity.

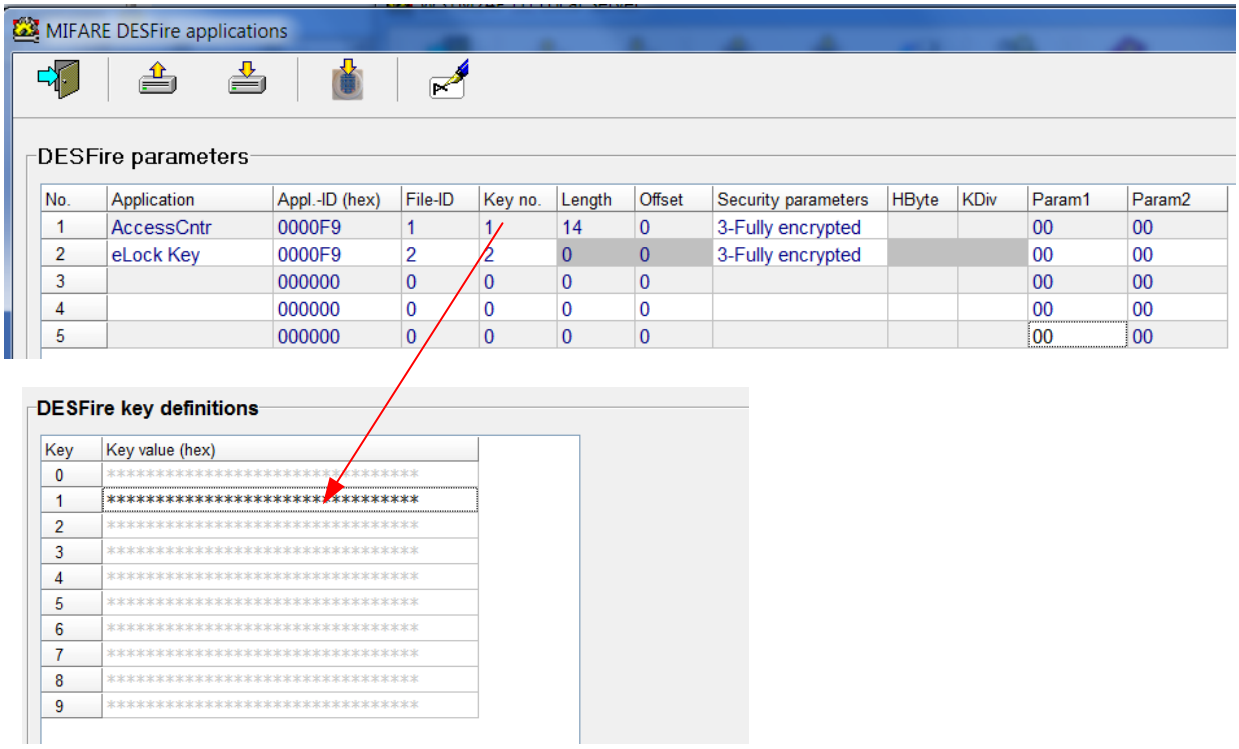


11.4.4 The field “File-ID“

In each application up to 32 files can be created (0 to 31 dec. / 00-1F Hex) which are addressable via their FID (File Application Identifier).

11.4.5 The field “Key-No”

The key number, registered in this field, must be the key used by the reader for decoding.



The key must match with the key which was used for the encoding of the application on the ID-card.

11.4.6 The Field “HByte“

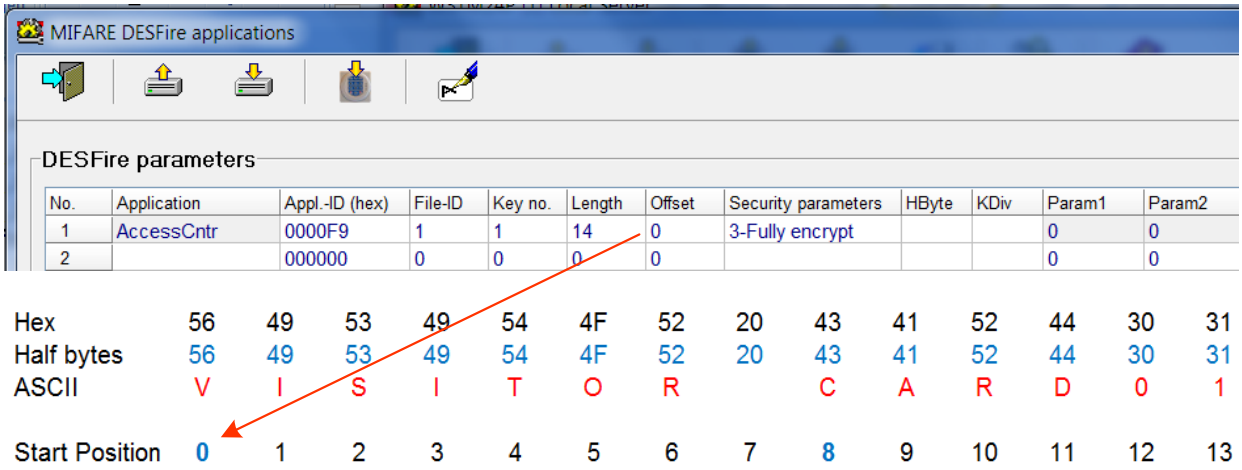
If the check box “HByte” is marked, the reader sends the card data in half bytes and not in ASCII-format.

11.4.7 The field “Length” and “Offset“

The field "Length" contents the number of bytes which the ID-card sends back to the reader. The length must not exceed a total of 16 bytes including the offset. If this value exceeds the encoded length, the reader gives no information back to the system. In the dark gray-shaded fields no entries are possible. The field “Offset” specifies the byte number from which the ID-number defined in the field Length is read.

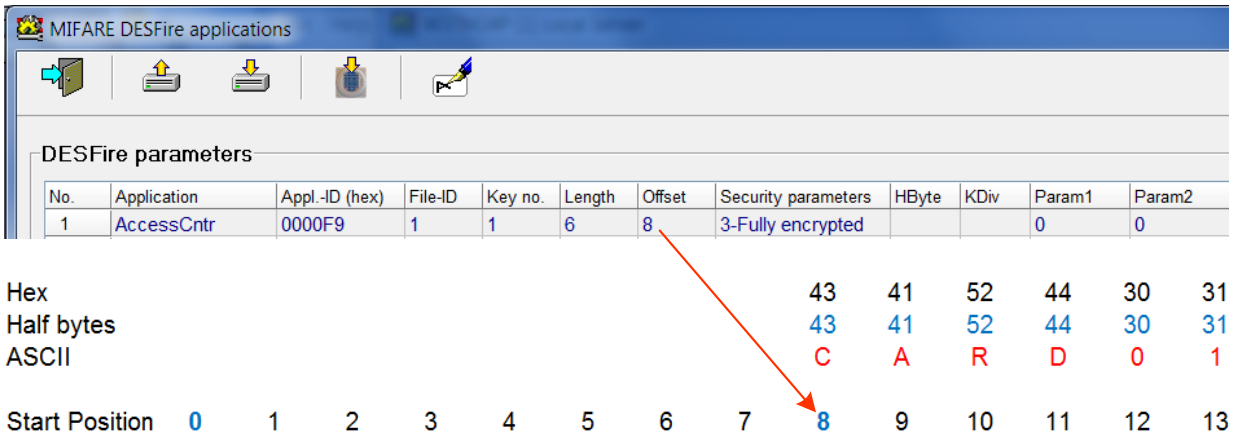
Example with offset = 0:

Format: 16 Bytes (ASCII)
Length: 14 Bytes
Offset: 0 → Read ID-Number: VISITOR CARD01



Example with offset = 8:

Format: 16 Bytes (ASCII)
Length: 6 Bytes
Offset: 8 → Read ID-Number: CARD01



11.4.8 The field “Security-Parameter”

This field defines the type of transfer (encryption, data integrity) for the air interface.

1- Plain, without key: no authentication required by the application.

2- Fully encrypted: access to the application only possible with authentication (128-bit AES key). The read data are sent fully encrypted with checksum to the reader. The decryption takes place in the reader.

MIFARE DESFire® has currently the following security levels:

➢ Plain without Key
➢ Plain with Key
➢ MACed
➢ Fully encrypted
➢ Fully encrypted with key-diversification

11.4.9 The field “KDiv”

11.4.9.1 Objective of Key-Diversification

The special feature of the Key-diversification is that the badge data of each card in a project are read with an individual key. This option protects the total project from a security attack in terms of unauthorized knowledge of project-Keys. If security Keys of some cards are known from unauthorized persons, only these cards must be disabled in the system, but not the total cards of the project.

A further advantage of this procedure is that the security keys are not loaded in the reader, but stay in the door controller and are transmitted encrypted to the reader for each booking. The diversified (derived) key is calculated from the door control unit on the basis of the badge UID and the project Master Key. The Master Key is saved on a dongle which is required for setting the option Key-diversification. After set up the system, this dongle can be stored in the safe of the customer. Only if using the security dongle, the customer assigned project master key can be loaded in the door control units or in XMP-TMC3500-terminals.

11.4.9.2 Requirements for Key-Diversification

The use of KDIV requires the following technical preconditions:

- License for Dongle Master-Key XMP-NT-141
- Door control units of type: XMP-K32/K12 or XMP-TMC3500.

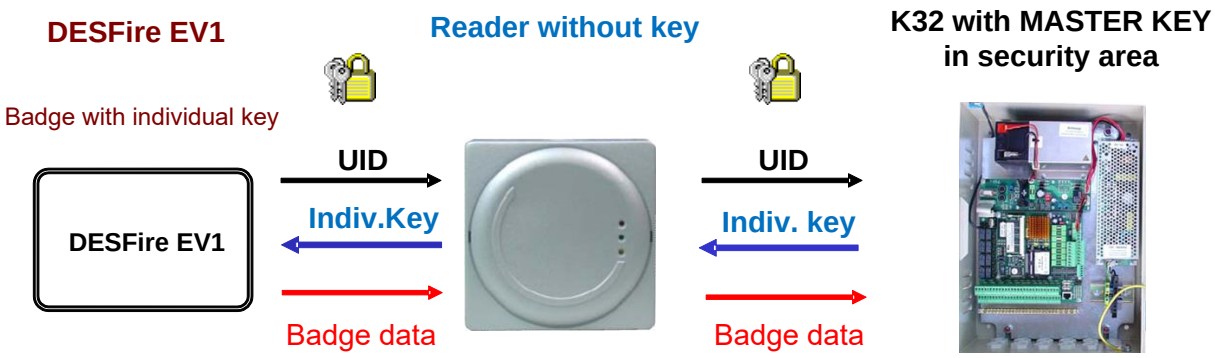
  (Version 4.6, BD = 07.09.2012) "Enable Key-diversification" with option 13
- Use of access control readers of the family MIFARE-DESFire® (version V4.4)
- Use of cards DESFire-EV1 (AES128-bit encryption) with appropriate encoding of cards

11.4.9.3 Reading process by Key Diversification

1- After placing the card in the reading field, the reader sends the UID with the needed parameters- defined in W3TM24P - to the XMP-K32.

2- The XMP-K32 calculates for this card the KDIV based on the UID and the project master key and sends it back to the reader.

3- If the key-authentication-process between reader and card is successful, the data will be read from the card and are sent to the XMP-K32 for further evaluation.



Please note:

The card encoding should be performed on the basis of the project master key. This may be done with the program W3DESFire, the encoding station XMP-USB-MIF and an appropriate XMP-K32 controller. The encoding process can also be realized by an authorized card manufacturer.

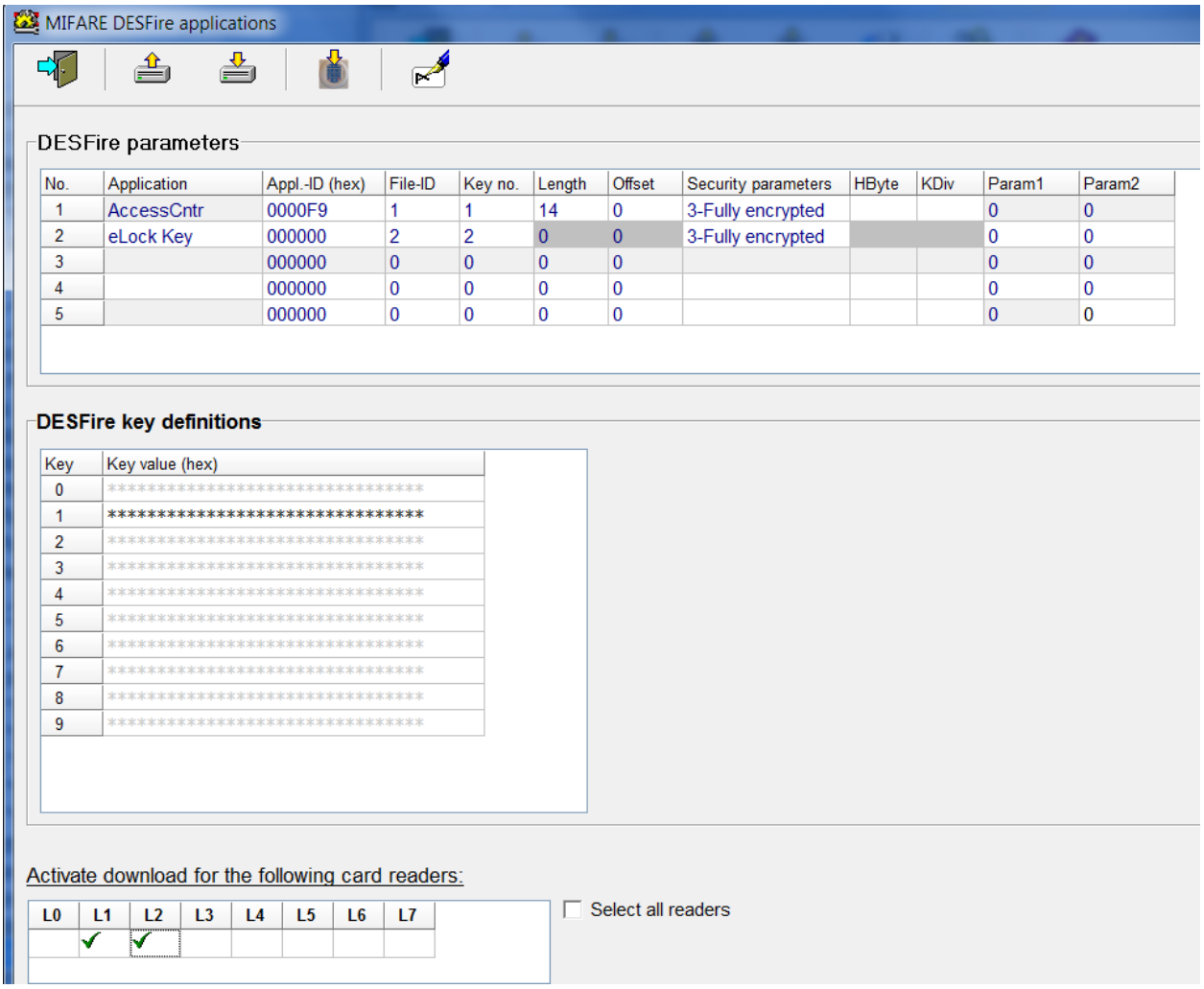
11.4.10 The fields “Parameter 1 and 2”

It depends on the application whether a value must be entered or not in the fields “Param1 and Param2”.

11.4.11 The DESFire Key-Definition

Up to 10 keys (128-bit AES keys) can be loaded into the reader and assigned to the appropriate applications. A key is a 32-character string with the value 0 to 9, and A to F.

Example: „*A0A1A2A3A4A5A6A7A8A9AAABACADAEAF*



12 MIFARE DESFire® Applications

12.1 The UID-Application

The application No.1 should always include the parameters with the badge-ID!

When the UID-function (serial number 7 bytes) is enabled in the field “application”, all other fields are then without signification.

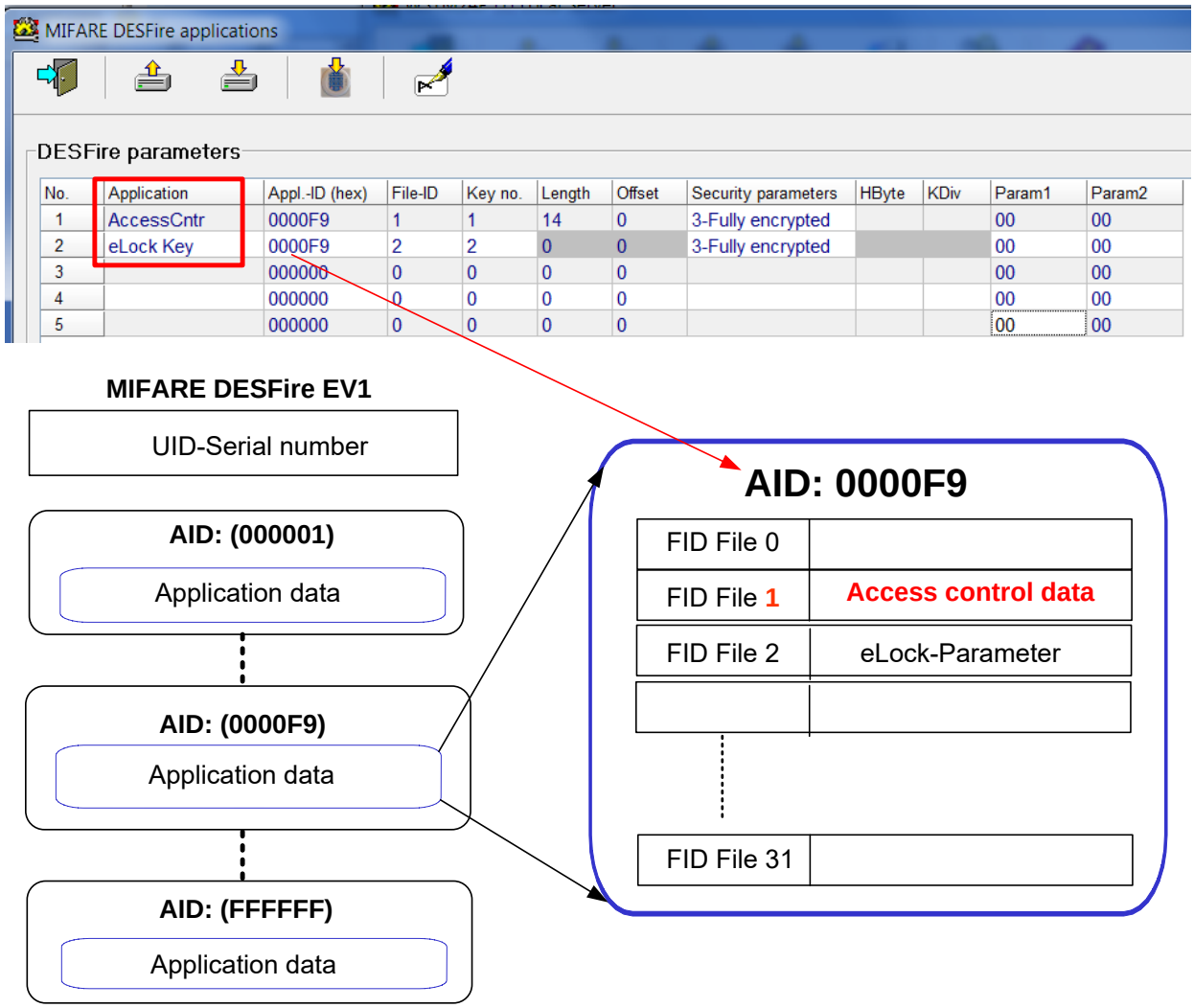
This entry ensures that the card number (also called ID-number) will be read from the UID-sector and not from the card memory.

DESFire parameters

No.	Application	Appl.-ID (hex)	File-ID	Key no.	Length	Offset	Security parameters	HByte	KDiv	Param1	Param2
1	UID	000000	0	0	0	0				00	00

12.2 The Access Control Application

The badge ID-number is read from the card memory (application = AccessCntr) with corresponding access parameters. In the following figure, the ID-number is read from the application-ID 0000F9, in file-ID 1, and with Key No. 1.



12.3 The Access Control Application with “Key-Diversification”

The Key diversification can only be used with the application "AccessCntr". For this function no reader-Key is required.

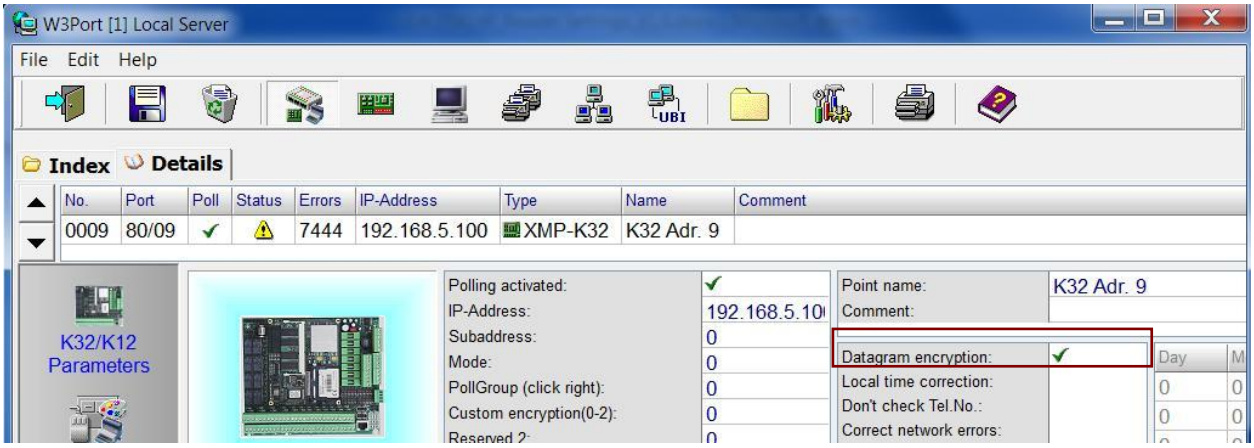
DESFire parameters

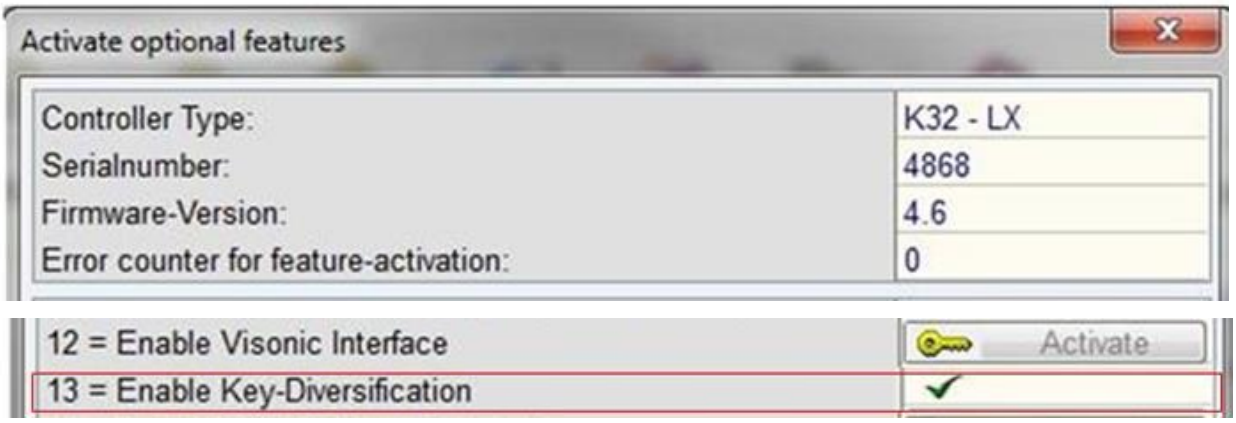
No.	Application	Appl.-ID (hex)	File-ID	Key no.	Length	Offset	Security parameters	HByte	KDiv	Param1	Param2
1	AccessCntr	0000F9	1	1	14	0	3-Fully encrypted		✓	0	0

12.3.1 Settings in Controller and W3PORT

Before downloading a project master key in the controller with the utility program W3SMKEY, the communication between the controller and XMP-BABYLON must be encrypted with the following settings:

- In the controller: DIP switch block 3 → switch 7 to ON
- In the software: W3Port → activate datagram encryption.
- In the software: XMP-K32 → Dongle Flag 13 must be enabled





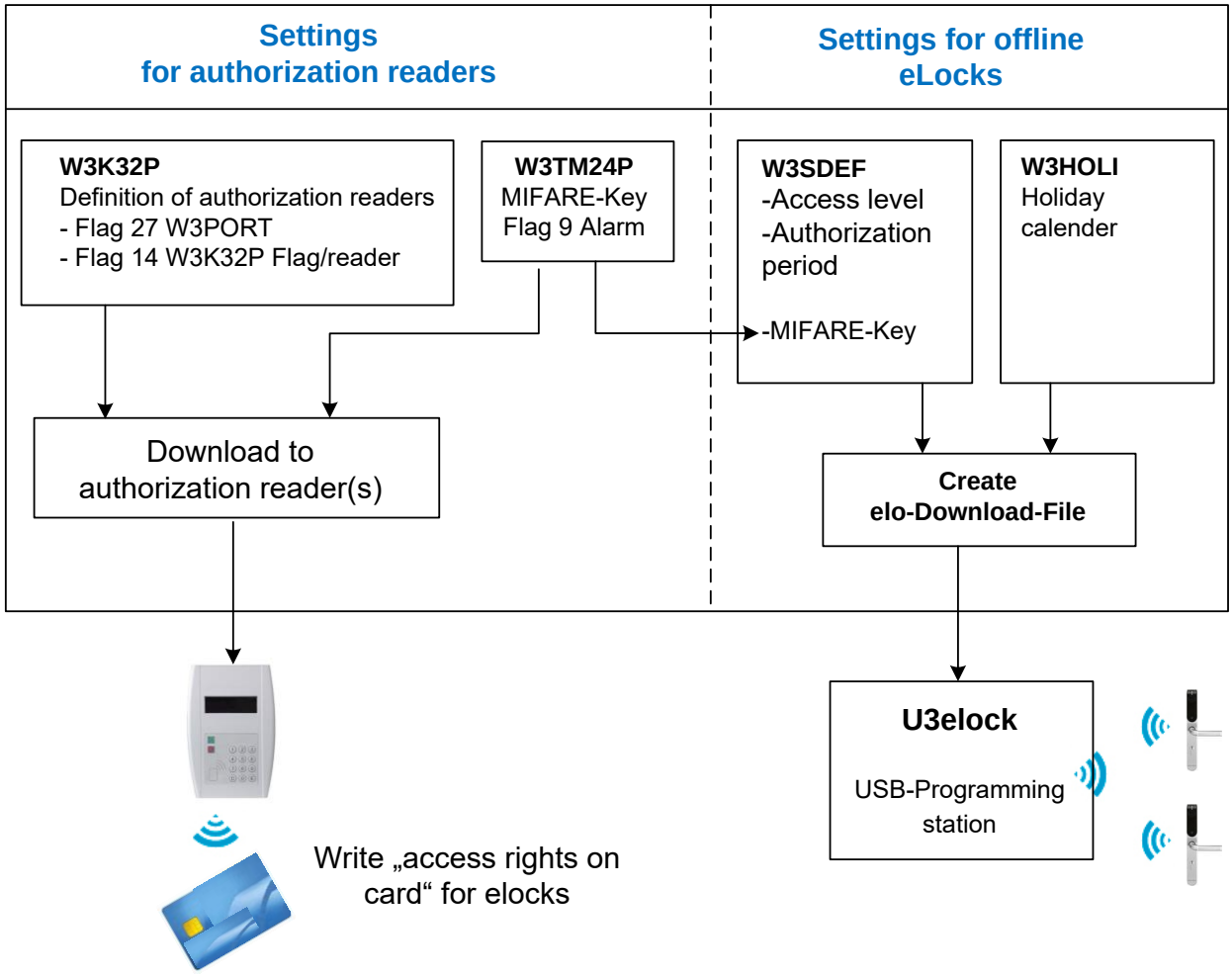
12.4 The eLock-Key Application

12.4.1 General

XMP-BABYLON enables the management of the access authorizations of electronic door locks. These eLocks are equipped with MIFARE DESFire® reader-heads and will be programmed wireless via a programming tool with appropriate parameters (access levels, authorization period, holiday calendar and MIFARE®-security keys). Then the eLocks work in an offline mode without direct connection to the XMP-BABYLON host computer.

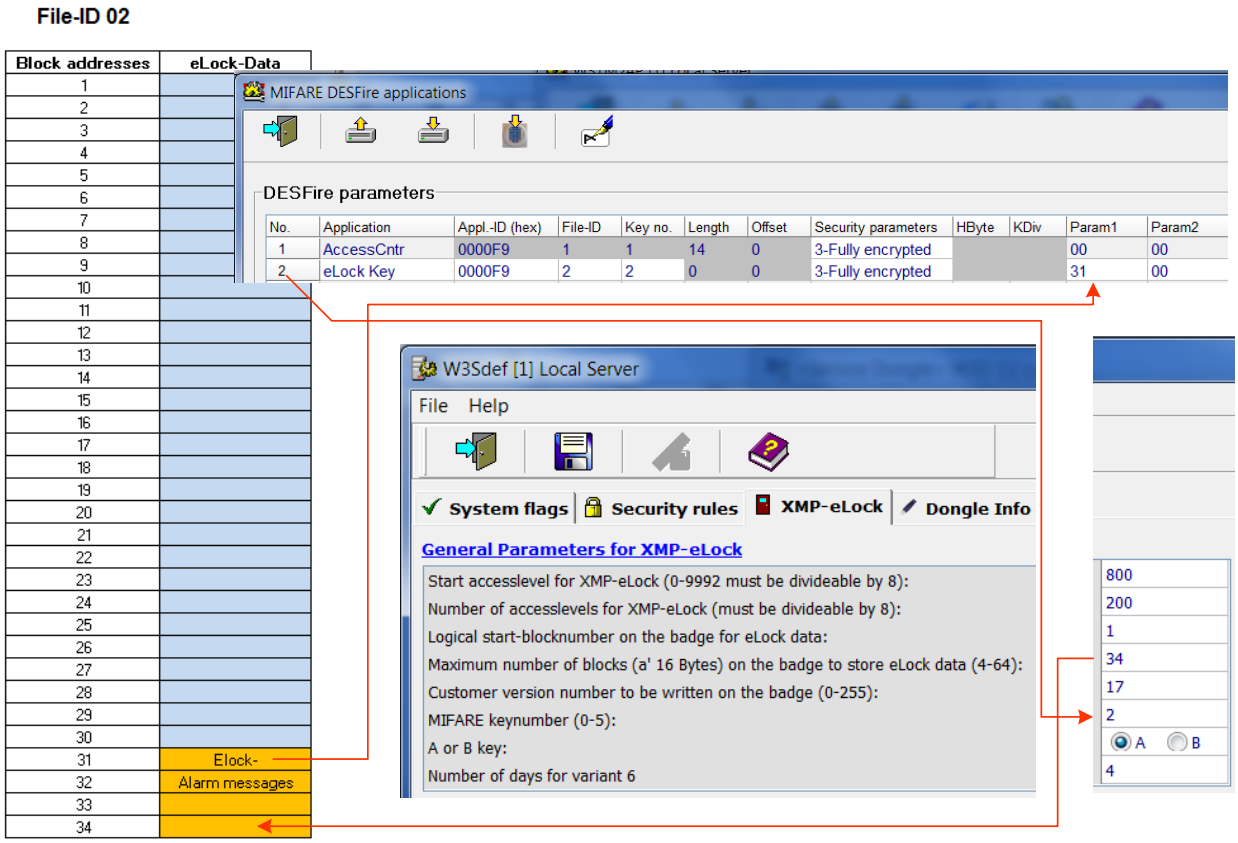
12.4.2 Programming steps for Offline-eLocks and access readers

To get access to an offline door lock, the access rights must be written in the employee-ID with dedicated readers. This is done daily. The access data for offline locks are defined in XMP-BABYLON.



12.4.3 Settings in W3TM24P

In parameter 1, the start address is entered for writing back alarms from the eLock to the ID-card.



12.4.4 The fields Length and Offset

The entries for the offset and length parameters are set internally by the application.

12.4.5 Security-Parameter for eLock-Application

Depending on the used DESFire EV1 card type (e.g. ISO standard), it may occur that the eLock data cannot be read in the communication mode "full encrypted" from the door cylinder. In this case, the communication mode "Plain" must be used. Furthermore, this type of door cylinder can neither read the ID-card number "fully encrypted", then the data stored in the logbook will be either the UID (7 bytes) or depending of the settings, the card number read from a “PLAIN” encrypted memory space.

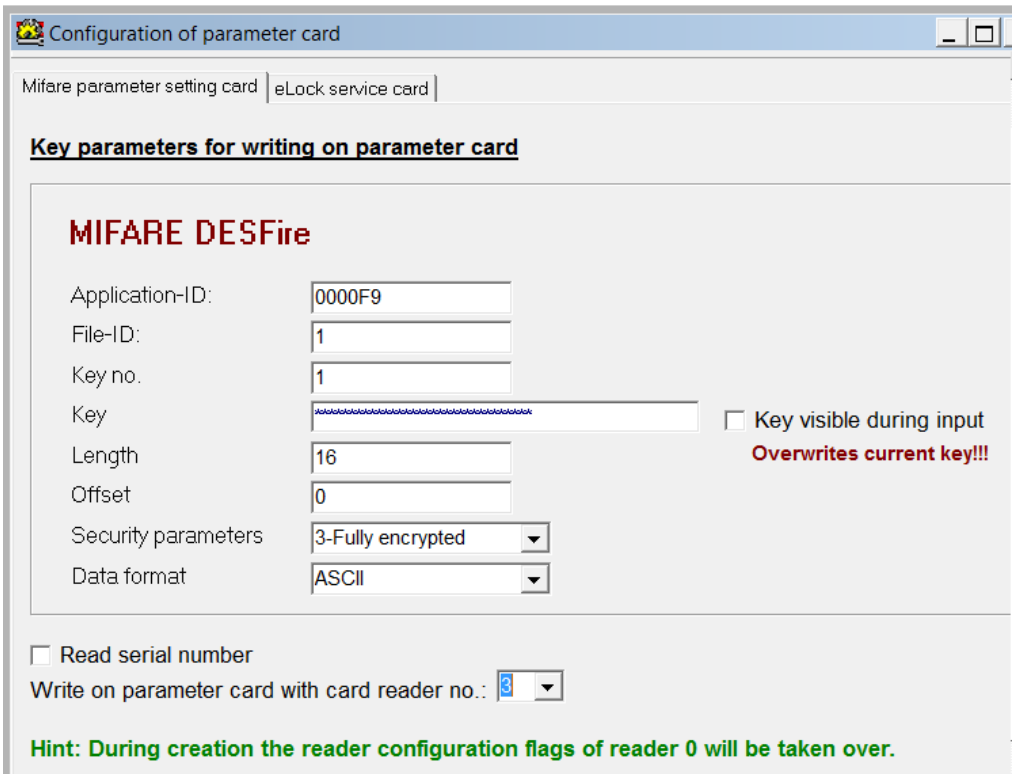
More details are available in the documentation:

Card readers / Offline Card readers eLock / Documentation/ eLock Program description

12.5 Configuration of a MIFARE DESFire® parameter card

This function enables the programming of cards to configure the card reader with key-parameters.

With the symbol *‚Prepare parameter card'* of the window „MIFARE DESFire® applications“, the window „Configuration of parameter card“ will open. The application data from the window „MIFARE DESFire® applications“ are taken over. But the data can be new defined or simply changed.



Now the defined key-parameters can be written on the parameter card via the selected reader address by clicking the symbol “*Write current parameters on parameter card”* .

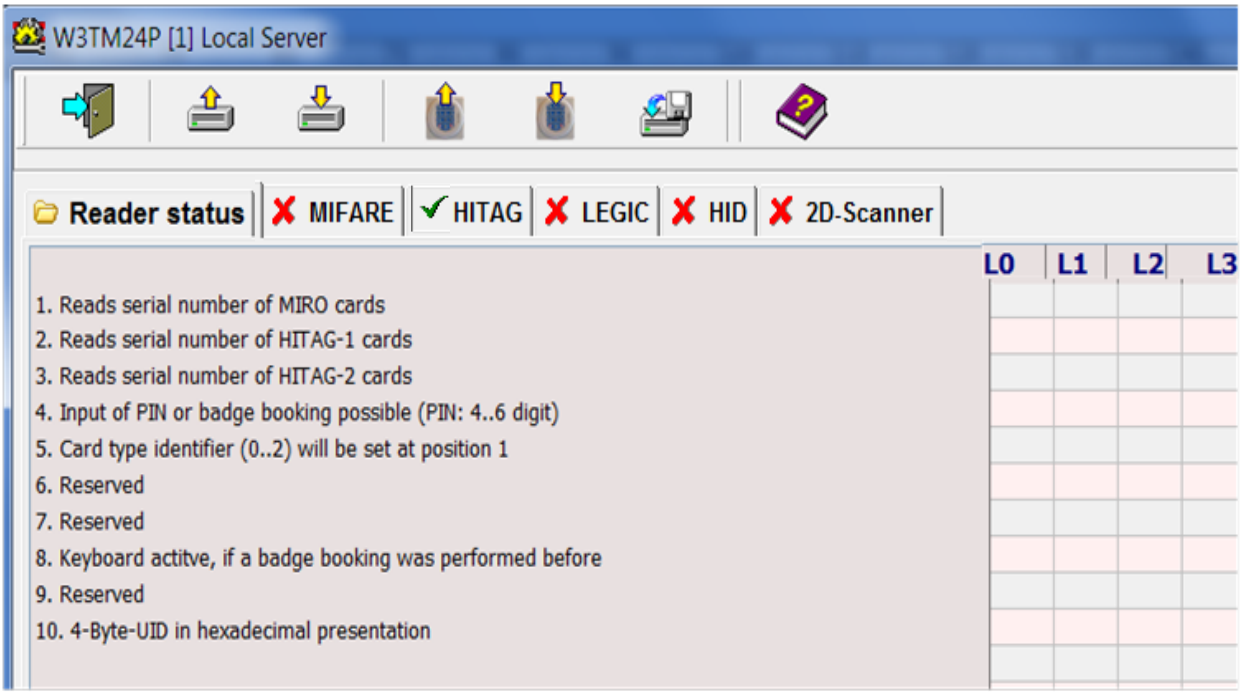
Within the next 2.5 seconds after transmitting the data, the parameter card must be hold into the card reader field. After expiring of this time frame, the data will be dismissed.

Special card reader properties should be deactivated during this operation.

13 Reader specification Hitag®

With the registry card „Hitag“, it is possible to configure specific settings for card readers of types XMP-TMC2230 and XMP-TMC2330. These readers work in the low frequency range of 125 KHz and always read the serial number (UID) of the card. The current reader parameters can be displayed with the program symbol , *“Parameter upload from card reader”*.

The necessary card reader features are activated by setting a checkmark into the corresponding field and a download in the reader with the symbol .



13.1 Meaning of the symbols in the task bar Hitag

Leave program

Read parameters from file

Save parameters into file

Parameter upload from card reader

Parameter download into card reader

Import data/parameters from another controller

13.2 Hitag® Reader Features

1	Reads serial number of MIRO badges
2	Reads serial number of Hitag®1 badges
3	Reads serial number of Hitag®2 badges
4	Input of PIN or badge booking possible (PIN: 4-6 digit) Instead of a badge booking it is also possible to insert the corresponding badge number directly via PIN code keyboard of the card reader. For this special case the badge number check must be realized as 6 digit (not 14 digits) check. This number has nothing to do with the secret code, which normally is entered in the personal database “Badge Definition”. Hint: The use of this option reduces the security
5	CARD TYPE identity (0..2) setting to Position 1 To ensure compatibility with 3rd party readers, the card type identity can be moved from position 14 to position 1. (0 = Miro, 1 = Hitag®1, 2 = Hitag®2). 10002774591265: ID card unknown Flag activated (Hitag® 1 on Pos. 1) 00027745912651: ID card unknown Flag deactivated (Hitag® 1 on Pos. 14) All combinations of reading methods are possible.
6	reserved
7	reserved
8	Keyboard active, if a badge booking was performed first If the reader is set in this way that the PIN input can also be executed if a Badge booking was executed first (W3Port→Flag 24, W3K32P→tab. ‚Reader/Flags’→Flag 5) – with this option the reader keyboard can be deactivated for the time without preceded badge booking. After badge booking the keyboard will be active for approximately 10 seconds.
9	Reserved
10	4 Byte-UID in hexadecimal presentation By default, the serial number (UID, 14 digits) of the card is sent from the reader in the decimal format. When this flag is set, the transmission is done in hexadecimal format.

14 Reader specification LEGIC® prime

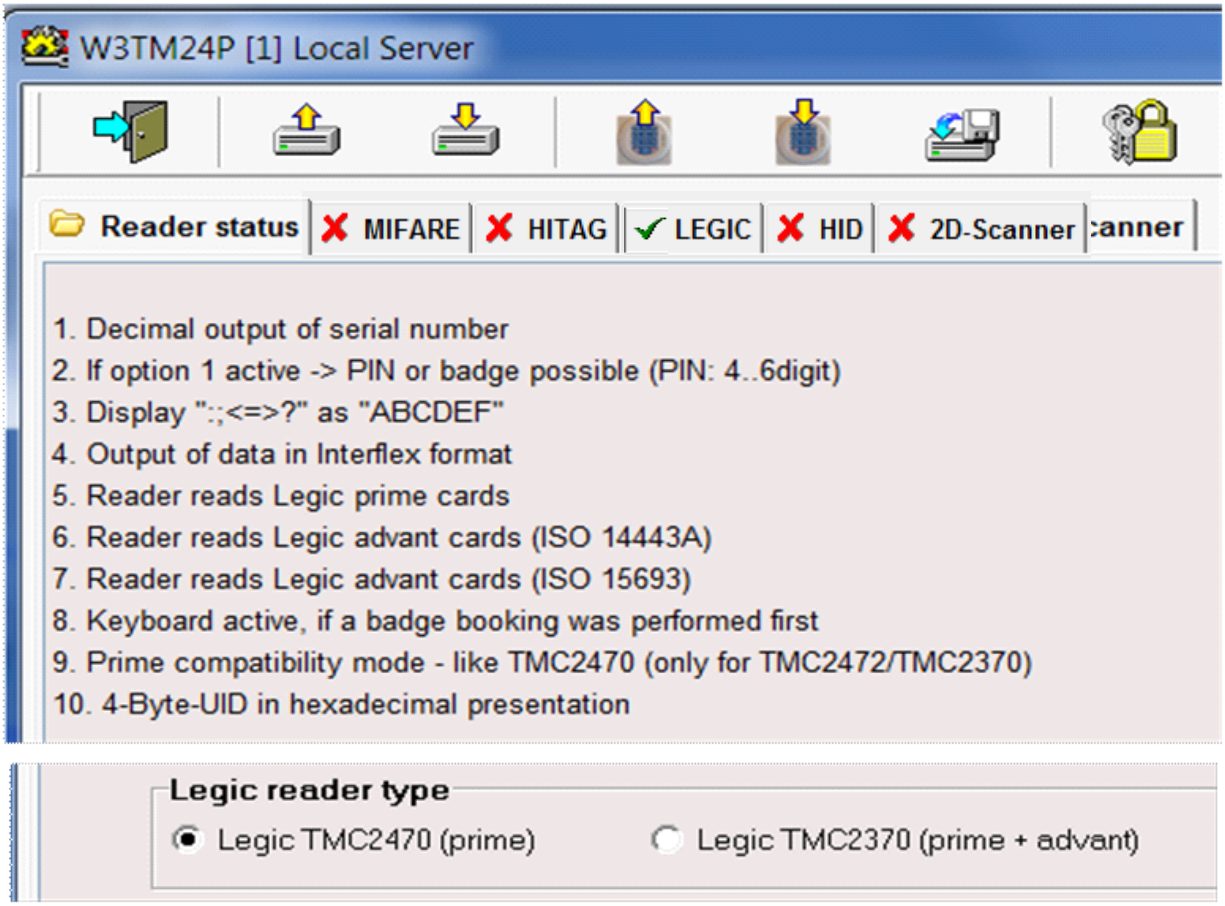
14.1 General

The following data can be read from the Legic prime ID-cards:

- 6-digit ID-number
- 14-digit ID-number
- Serial number (UID)
- Data from Segment
- Data from segment with search string (Stamp max. 7 bytes)

14.2 LEGIC® Reader Features

With the registry card „LEGIC“, it is possible to configure specific settings for card readers (LEGIC® prime and advant) of types XMP-TMC2270/2280 and XMP-TMC-2370/2380. These readers work in the frequency range 13.558 MHz. The current reader parameters can be displayed with the program symbol , “*Parameter upload from card reader”*.
The necessary card reader features are activated by setting a checkmark into the corresponding field and a download in the reader with the symbol .



14.3 Meaning of symbols of the task bar LEGIC

Leave program

Read parameters from file

Save parameters into file

Parameter-upload from card reader

Parameter-download into card reader

Import data/parameters from another controller

Special definitions (reader type dependent)

14.4 LEGIC® Reader Features

1	Decimal output of the serial number The hexadecimal serial number of a LEGIC-card is converted in the reader to a decimal value and is sent to the door control unit in positions 1 to 14. The LEGIC chip must be configured accordingly (see icon special definitions).
2	If option 1 active → Input of PIN or badge booking possible (PIN: 4..6 digit) Instead of a badge booking, it is also possible to insert the corresponding badge number directly via PIN-code keyboard of the card reader. For this special case the badge number check must be realized as 4-6 digit check (not 14 digits). This number has nothing to do with the secret code, which normally is entered in “Badge Definition”. Attention: This option should only be used if the option 1 (decimal output of the serial number) is activated. The use of this option reduces the security
3	Display „.;<>?“ as „ABCDEF“ Character conversion
4	Output of data in the format InterFlex The Interflex memory data, encoded in the hexadecimal format, are converted and sent by the reader in decimal.
5	Reader reads LEGIC® prime badges Operative only with LEGIC® advant readers

LEGIC® Reader Features

6	Reader reads LEGIC® advant badges (ISO14443A) Operative only with LEGIC® advant readers
7	Reader reads LEGIC® advant badges (ISO15693) Operative only with LEGIC® advant readers
8	Keyboard active, if a badge booking was performed first With this option the reader keyboard will be deactivated. The PIN-code input can only be executed if a badge booking was executed first. After badge booking the keyboard will be released for approximately 10 seconds (W3Port→Flag 24, W3K32P→tab. ‚Reader/Flags'→Flag 5).
9	Conversion of Prime UID as XMP-TMC2470 (for TMC2472/TMC2370) The hexadecimal serial number (UID) of the LEGIC® prime card is interpreted differently in the LEGIC® advant chip as in the LEGIC® prime chip. To be compatible in projects, the UID can be adjusted with this flag. Example: Result with LEGIC® prime-reader: 1484973202 (E4 58 82 92 hex) Result with LEGIC® advant reader TMC2370: 1486021762 (58 92 E4 82 hex) The setting of the flag allows to adapt the reader results between prime and advant when reading the UID-number as identification.
10	4 Byte-UID in hexadecimal presentation By default, the serial number (UID, 14 digits) of the card is sent from the reader in the decimal format. When this flag is set, the transmission is done in hexadecimal format.

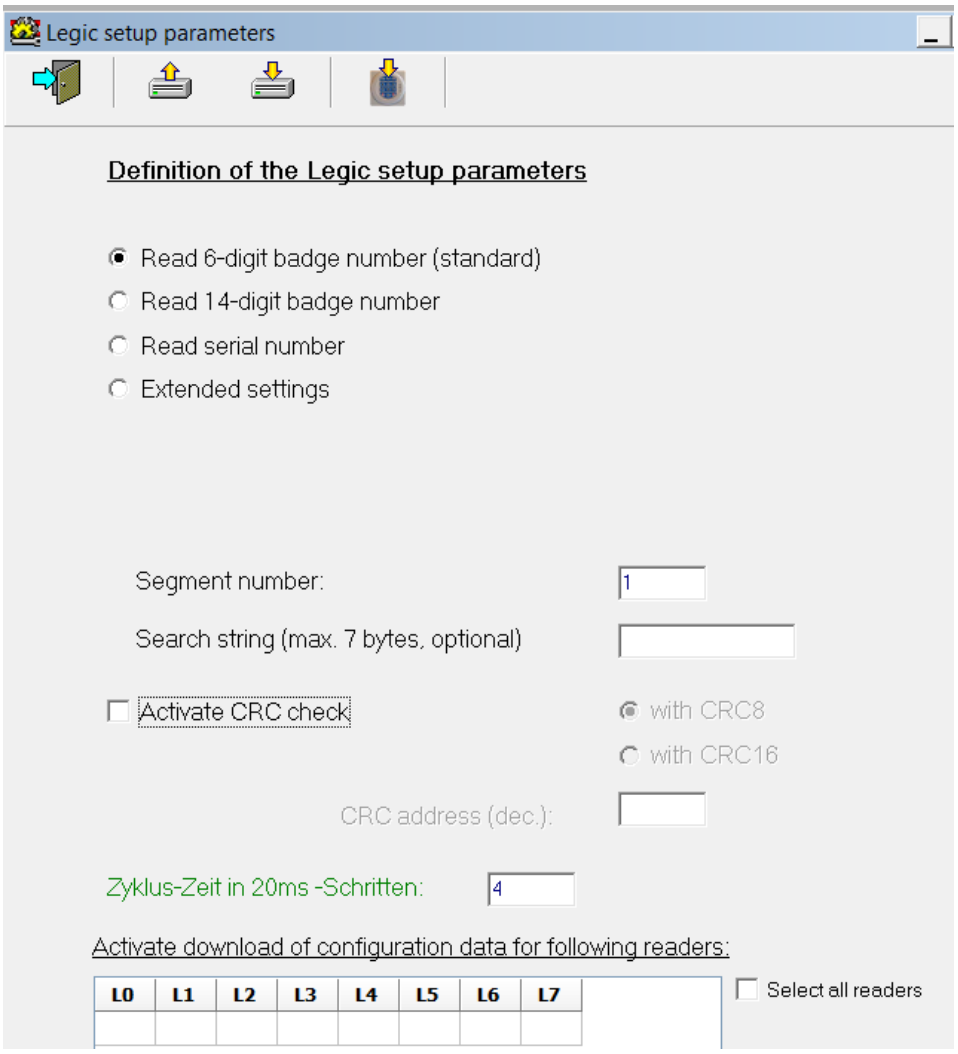
14.5 Reader configuration LEGIC® prime

These cards are suitable for multi-applications and have a programmable segment length. Up to 127 applications can be stored in max. 1Kbytes. The serial number (UID) or segment memory data can be read from the LEGIC® prime cards.

By using the selection box

the reader LEGIC® prime will be selected. By clicking on the button "Specific definitions", the configuration page is opened.

Depending of the Legic badge organization (segment settings), it is necessary to define the position of the data and the security features in the badge. These parameters will be downloaded in the readers.



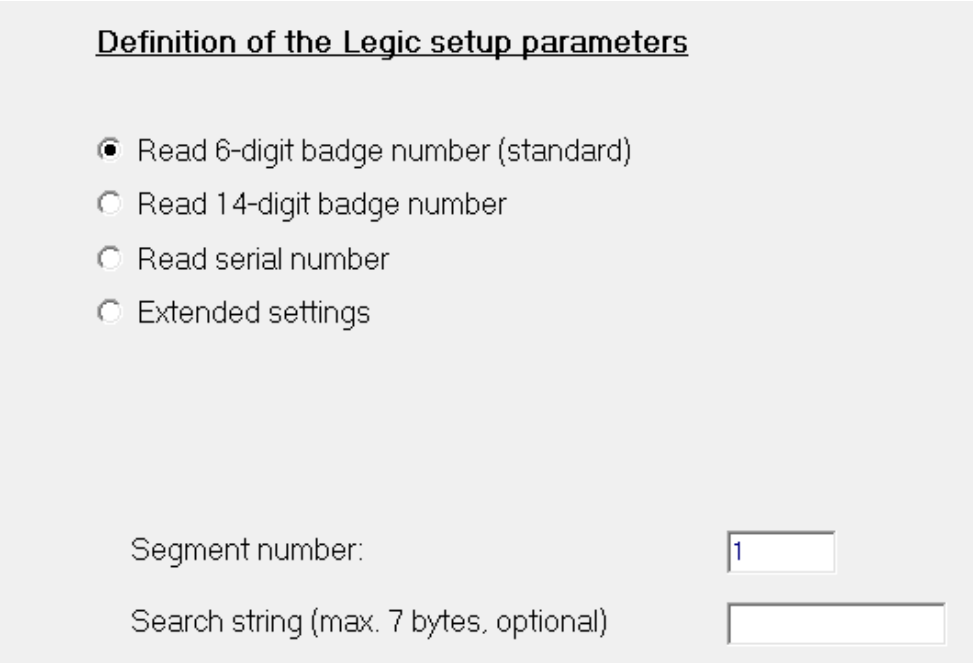
14.6 Definition of the LEGIC® Setup Parameters

Field	Description
Read 6-digit badge number (Standard)	Standard parameters for transmitting the 6 digit badge number are set. (Start pos. 14 →16 bytes)
Read 14-digit badge number	Standard parameters for transmitting the 14 digit badge number are set. (Start pos. 18 →16 bytes)
Read serial number	Standard parameters for transmitting the serial number of a Legic badge are set. All input fields not necessary for this setting are faded off.
Extended settings	All settings necessary for reading the required information from the Legic badge can be performed by the user. All input fields are faded in.
Number of bytes to read	Number of bytes that must be read starting from start address. One byte badge information consists of a two half byte information, which will be transmitted separate to the door control unit. Example: 11 bytes = 22 data to the system
Start address (dec.)	Relative start address (in decimal) in corresponding segment. Starting from here the information must be read.
Segment number	Number of segment, from which the information must be read. In connection with the search string (see Search string) it defines the segment start number.
Activate CRC check	Activates an additional security step within the Legic chip. It causes, that a CRC check (CRC8 or CRC16) via the read data will be performed and compared with a CRC value stored at defined memory position. In case that the CRC check fails no data will be transmitted.
Search string (optionally)	A maximum 7 bytes search string can be entered here. In connection with the field ‘Segment number’ (has to be considered as start segment for searching) the card information is read from this segment where the search string – entered here - was found.
CRC-Address	Specification of CRC-Address in segment
Cycle time in 20 ms steps	Special application

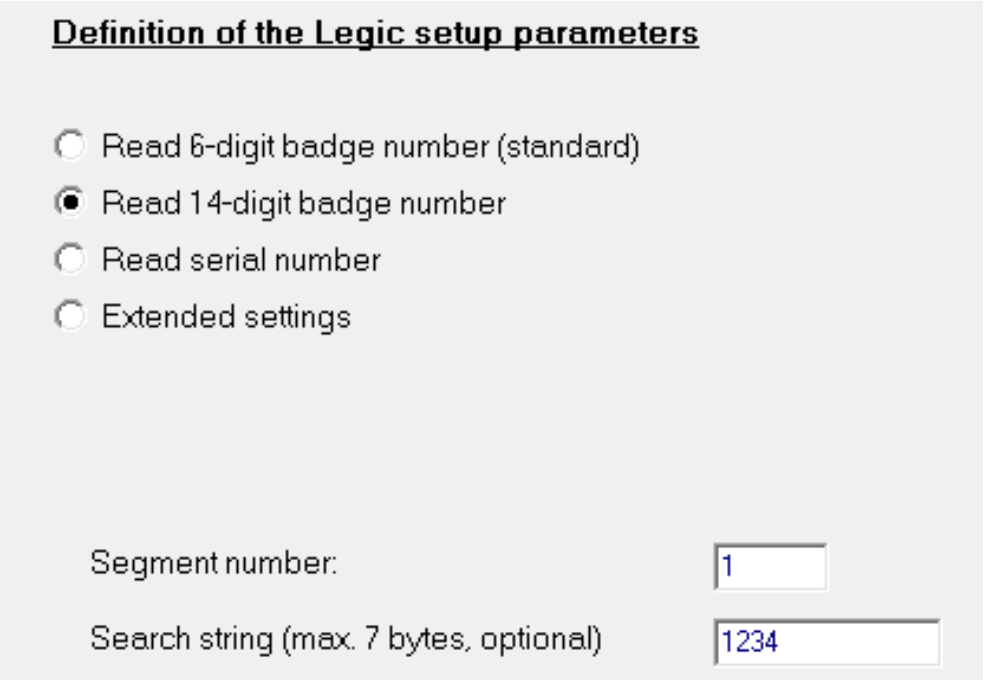
14.7 LEGIC® Prime Applications

14.7.1 Reading badge number from segment X

The card number can be reader as 6-digit or 14-digit from the specified segment.



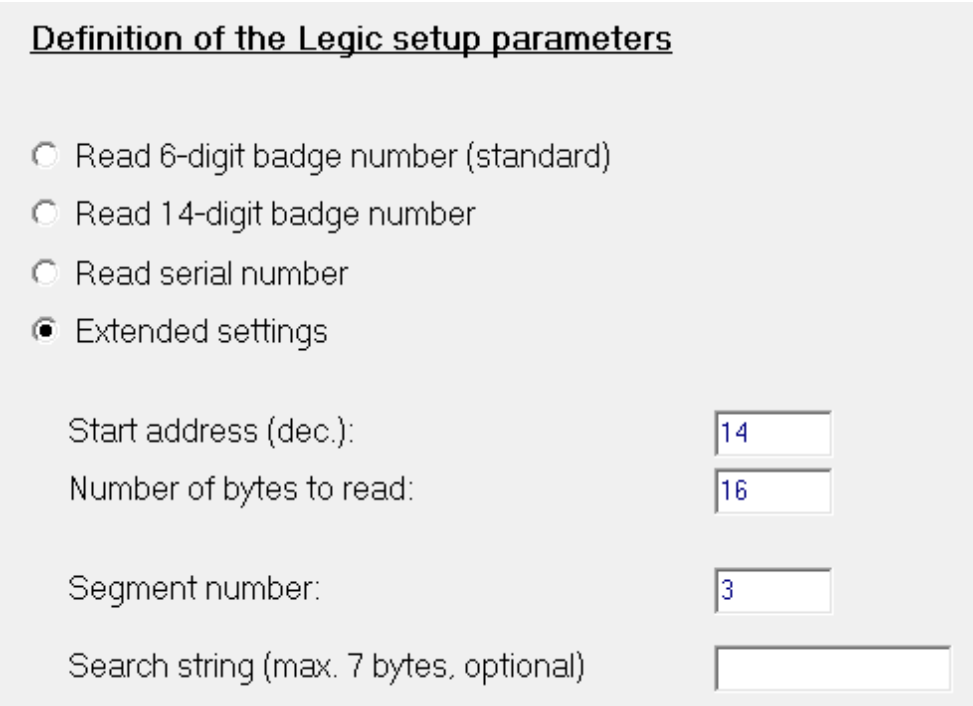
14.7.2 Reading the badge number with Search string



The badge number is read from the segment where the search string (Stamp=1234) was found. The search starts from segment 5. If the specified search string does not exist, no data will be sent back.

14.7.3 Reading badge number with extended settings

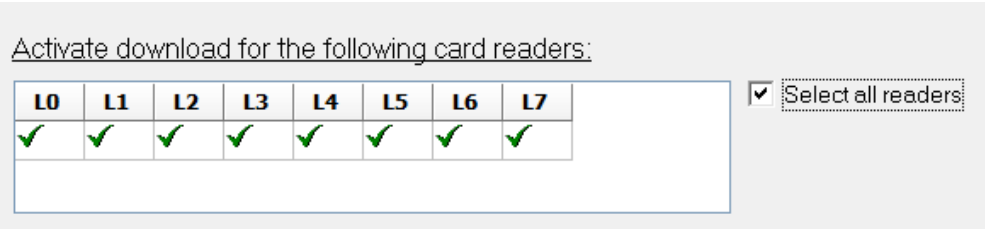
Here it is possible to define the beginning and the length of the data to be read.



14.8 Download of LEGIC Prime reader settings

The download of the Legic configuration data in the card reader is realized with the symbol *‚Parameter download into the readers'*.

The card reader acknowledges the download with an optical and acoustical signal.



The parameters created on this page can be stored on encrypted way into the file $$FES.386 into directory *EXOS386P>* or *ACL32>*, with (*„Save current Legic parameters"*) and can also be uploaded from there (*„Get last defined Legic parameters"*).

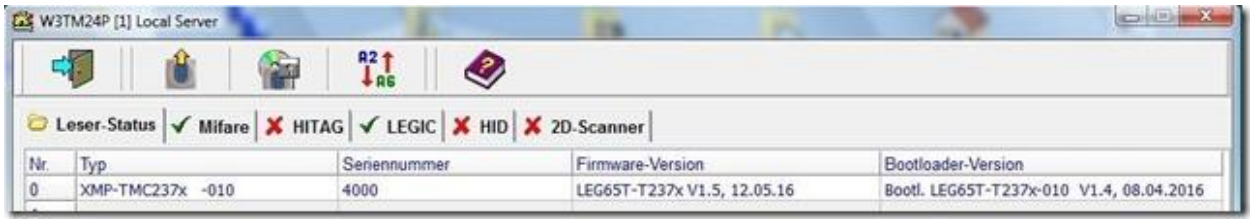
15 Reader specification LEGIC® advant

LEGIC® advant cards are compatible with the ISO standards 15693 and 14443A. Here, up to 127 applications (segments) in max. 4K-bytes can be stored.

15.1 Additional hint for LEGIC® chips SM4200 and SM4200M

15.1.1 SM4200 - LEGIC® prime & advant

In W3TM24P (beginning with Version 3.1s) the readers XMP-TMC2370/80 (SM4200) shows a „-010“ under „Type“ und „Bootloader version”.

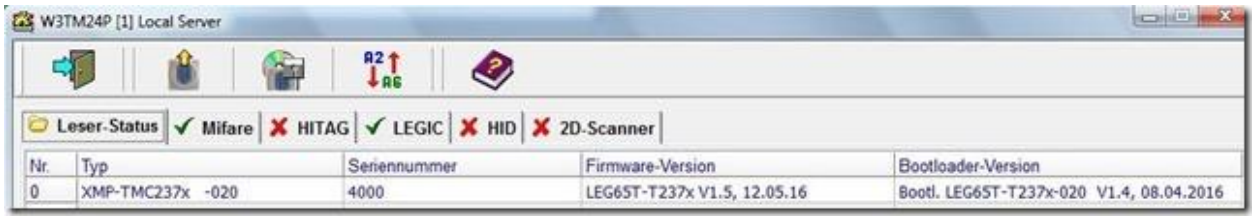


010 = LEGIC® prime & advant → UID and memory

The segment no. for LEGIC® prime & advant begins with “0”. The older version TMC2370/80 (SM2570) begins with “1”.

15.1.2 SM4200M - LEGIC® prime & advant / MIFARE® classic & DESFire EV1

In W3TM24P (beginning with Version 3.1s) the readers XMP-TMC2370/80 (SM4200) shows a „-020“ under „Type“ und „Bootloader version”.



020 = LEGIC® prime & advant → UID and memory / MIFARE® classic & DESFire EV1 → UID and memory

The segment no. for LEGIC® prime & advant begins with “0”. The older version TMC2370/80 (SM2570) begins with “1”.

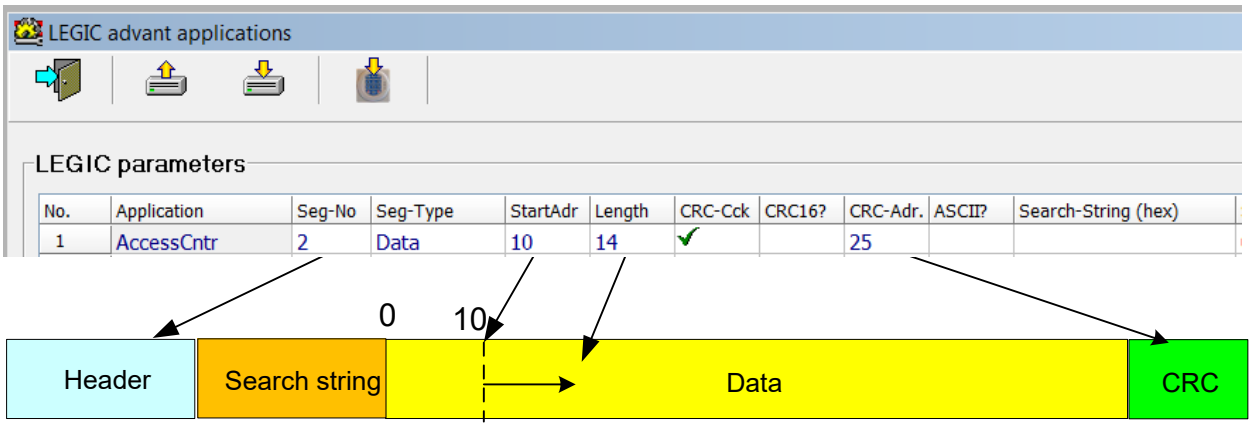
15.2 Meaning of the LEGIC® advant Parameters

By using the selection box

the LEGIC® advant reader is selected. By clicking on the button "Specific definitions", the configuration page is opened.

It needed to inform the LEGIC chip, exactly where and with what security features are required to read the card data.

The LEGIC-Chip in the badge has to known the start address, the length and the security features of the data to be read.



Advant Segment No. 2 (schematic)

Meaning of the LEGIC® Parameters

Function	Description
No.	Number of the application
Application	Name of the application: AccessCntr = Access control by using memory data UID = reading serial number of LEGIC® card
Seg-No.	Number of the segment from which the data will be read.
Seg-Type	Selectable are data segment (standard) or LEGIC® access segment
StartAdr	Start address in the relevant segment from which the information must be read (in decimal format).
Length	Length in bytes of the return. If this value exceeds the real encoded length, the reader will not return any information to the system.
CRC-Cck	If the flag is set, a comparison is done between the redundancy check of the specified data on the card during the card encoding and the value in the field "CRC addr.". If both data match, the badge data are sent - otherwise not. By default, a CRC8 calculation is performed. If the badge encoding has been realized with a CRC16 calculation, the flag in the field “CRC16” must be set too. At Prime-cards (only for Prime-cards!) the CRC-calculation could integrate security functions and/or the stamp. Depending on these settings, the flags for CkStmp and/or CkWR must be set.
CRC16	The CRC check is performed as CRC16, and not as CRC8.
CRC-Adr.	The CRC8 or CRC16-value is written in this address.
ASCII	The encoded user data are interpreted by the reader as ASCII-data. e.g.: 31 32 33 34 35 36 37 38 = „12345678..“ as ASCII-data otherwise „3132333435363738..“ as half bytes

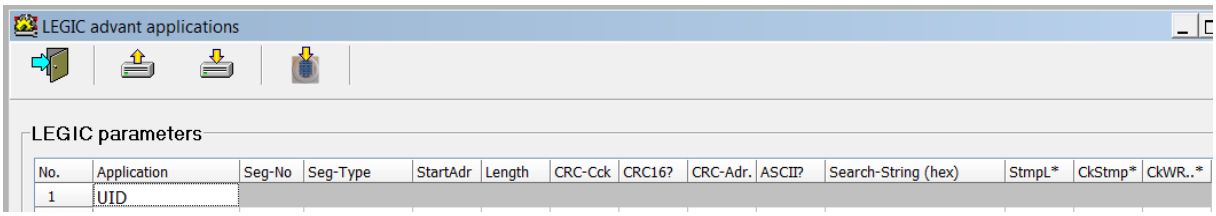
Meaning of the LEGIC® Parameters

Function	Description
SearchString	A maximum of 7 bytes search string can be entered here. In connection with the field ‘Segment number’ (has to be considered as start segment for searching) the card information is read from this segment where the search string is found.
StampL*	**Only prime!!** In the “advant Philosophy” the stamp does not belong to the utilizable data of the segment. An entry of a stamp length accomplished here takes the Stamp information off from the data information. e.g.: Stamp + user data **BC00A01**112345678901111 input StampL = 4: → data = „12345678901111“ else StampL = 0 → Data = „BC00A01112345678901111“
CkStmp*	**Only prime!!** Stamp data were involved during the coding of the card to the CRC calculation.
CkWR.*	**Only prime!!** Protection features (WRP/WRC/RD) were involved during the coding of the card to the CRC calculation.

15.3 Reading the LEGIC® advant Application

15.3.1 Reading the UID-Application

The UID-function (serial number, 7 bytes) is activated in the field “Application”. All other fields are meaningsless.



15.3.2 Reading the Access Control-Application

The badge number is read from the memory of the card (application = AccessCntr) with corresponding access parameters. In the following parameters the badge number is read of segment 1, start address 0, length 14 bytes, no CRC-check and no Search-String.

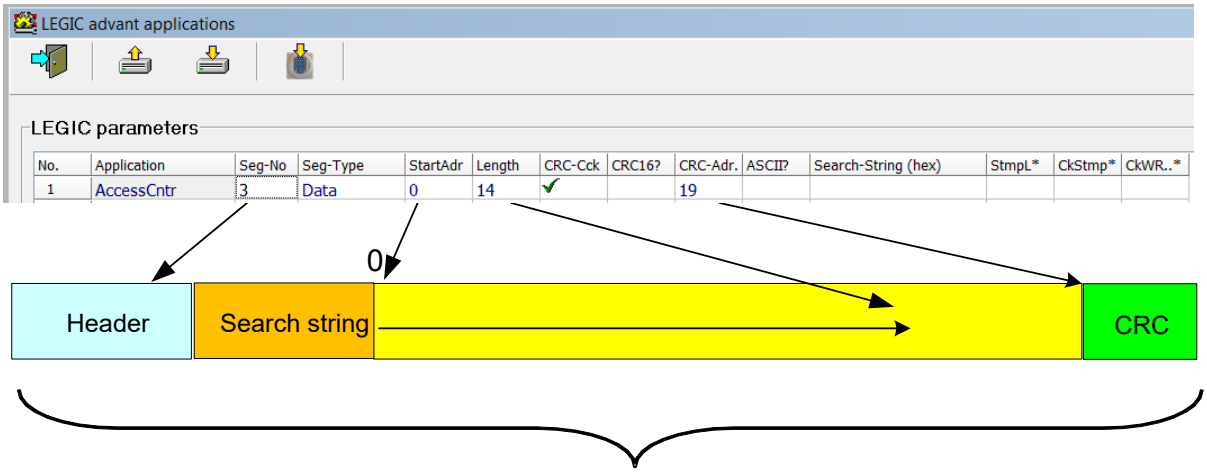
LEGIC parameters

No.	Application	Seg-No	Seg-Type	StartAdr	Length	CRC-Cck	CRC16?	CRC-Adr.	ASCII?	Search-String (hex)	StmpL*	CkStmp*	CkWR..*
1	AccessCntr	1	Data	0	14								

*For LEGIC prime cards only - if required.

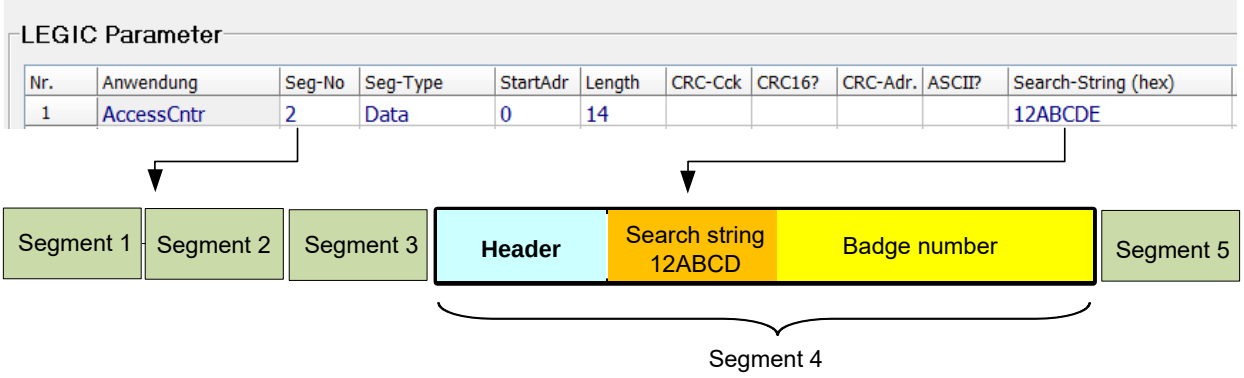
15.3.3 Reading the Access Control-Application with CRC-Check

The badge number is read from the memory of the card (application = AccessCntr) with corresponding access parameters. In the following parameters the badge number is read of segment 3, start address 0, length 14 bytes, CRC-check, CRC-Value stored in address 19 (decimal), and no search-string.



15.3.4 Reading the Access Control-Application with search string

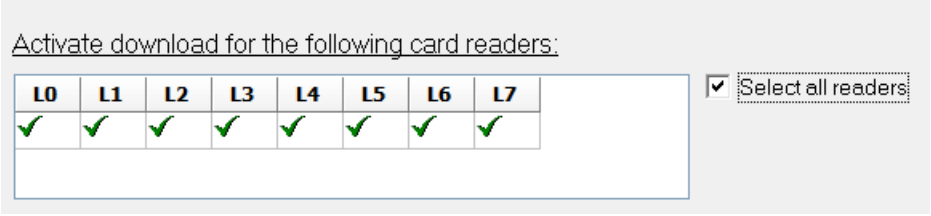
As search string with an up to 7-byte value (Hex) can be specified. In connection with the field “segment number”, whose value gives the start of the search (segm.2), the data are read from the segment in which the search string will be found (segment 4).



15.4 Download of LEGIC® advant reader settings

The download of the LEGIC® configuration data in the card reader is realized with the symbol *‚Parameter download into the readers‘*.

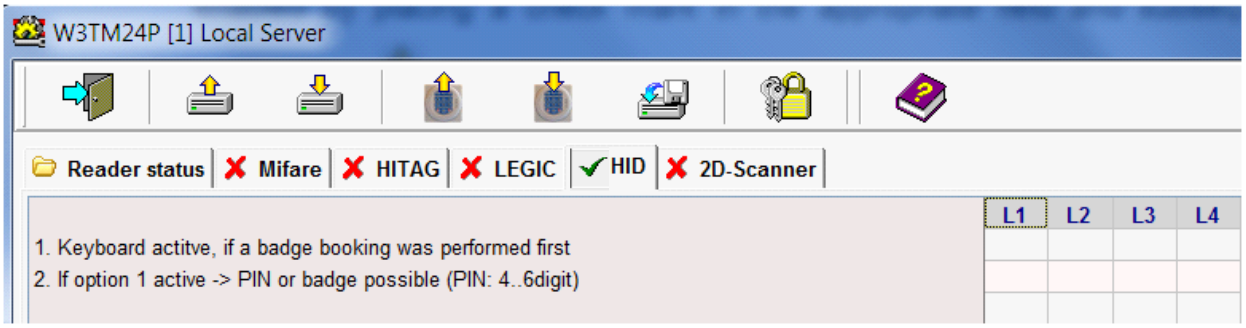
The card reader acknowledges the download with an optical and acoustical signal.



The parameters created on this page can be stored on encrypted way into the file ***legk.FIL*** into directory *EXOS386P>* or *ACL32>*, with (*„Save current LEGIC® parameters“*) and can also be uploaded from there (*„Get last defined LEGIC® parameters“*).

16 Reader specification HID iClass® (13.558 MHz)

The TMC2390/2395 reads HID iClass® ID cards with 14-digit card number and the formats H10301 (26 bits) and Corporate 1000 (35 bits). The reader parameters can be displayed with the icon . The reader properties will be enabled by placing a check mark in the appropriate field and subsequent download of the parameters).



16.1 Meaning of the symbols in the tool bar HID

- Leave program
- Read parameters from file
- Save parameters into file
- Parameter-upload from card reader
- Parameter-download into card reader
- Import data/parameters from another controller
- Special reader definitions

16.2 HID® Reader Features

At time the following settings are available:

1	Keyboard active, if a badge booking was performed first With this option the reader keyboard will be deactivated. The PIN-input can only be executed if a badge booking was executed first. After badge booking the keyboard will be released for approximately 10 seconds (W3Port→Flag 24, W3K32P→tab. ‚Reader/Flags'→Flag 5).
2	If option 1 active → Input of PIN or badge booking possible (PIN: 4..6 digits) Instead of a badge booking, it is also possible to insert the corresponding badge number directly via PIN-code. For this special case the badge number check must be realized as a 6-digit check (not 14 digits). This number has nothing to do with the secret code, which is entered under "Badge Definition".

17 Reader specification 2D-Scanner

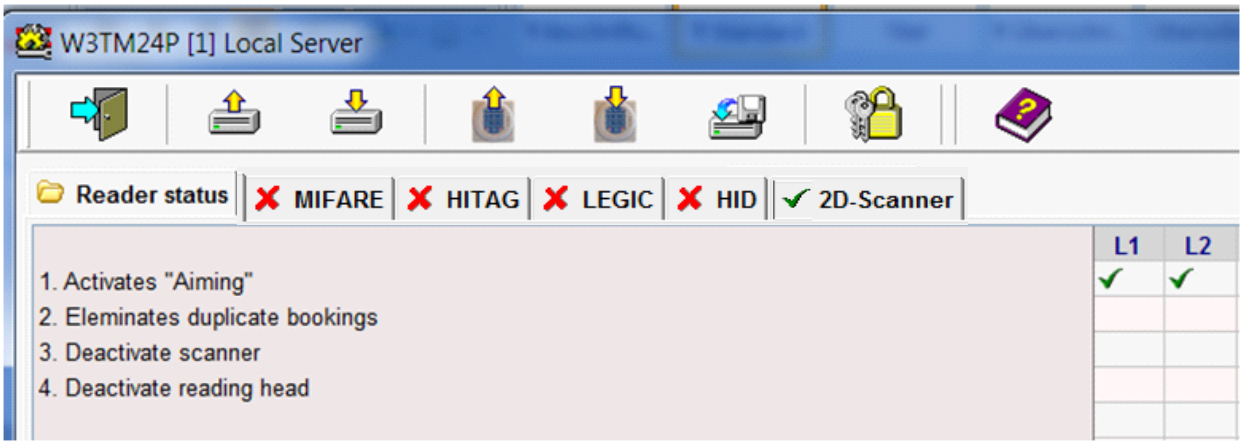
The reader XMP-TMC2450-TUR-2D is a dual reader capable to read 1D/2D barcodes or MIFARE® classic & DESFire® cards. The reader settings for MIFARE® are performed in the registry “MIFARE” and the barcode settings in the registry "2D Scanner".

The communication protocol “Secucrypt” is required for these readers.

The current reader parameters can be displayed with the icon , “upload parameters from the reader”. The reader properties will be enabled by placing a check mark in the appropriate field and subsequent download of the parameters).

17.1 2D-Scanner reader features

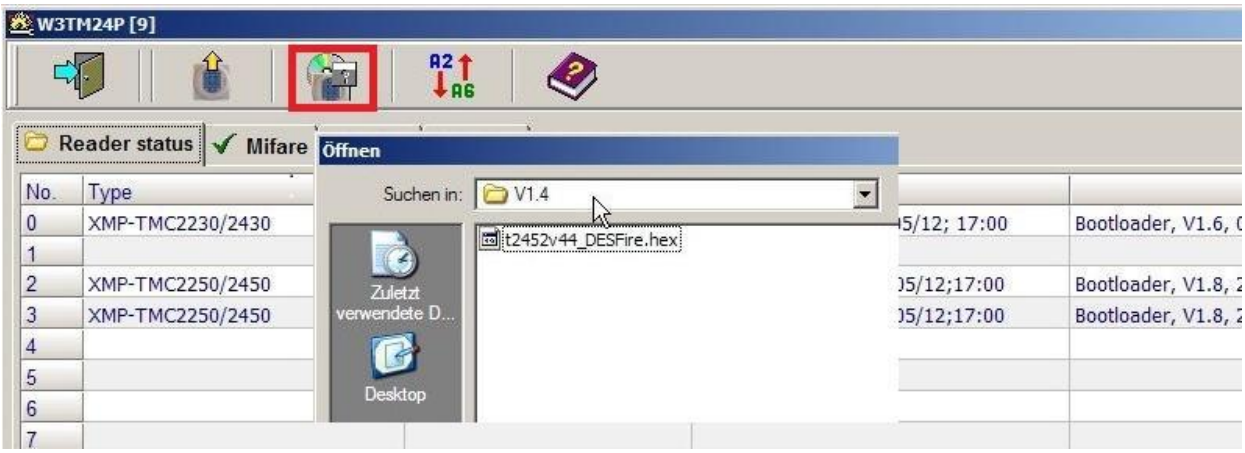
At time the following settings are available:



1	Activate „Aiming“
2	Eliminate duplicate bookings
3	Deactivate scanner
4	Deactivate reading head

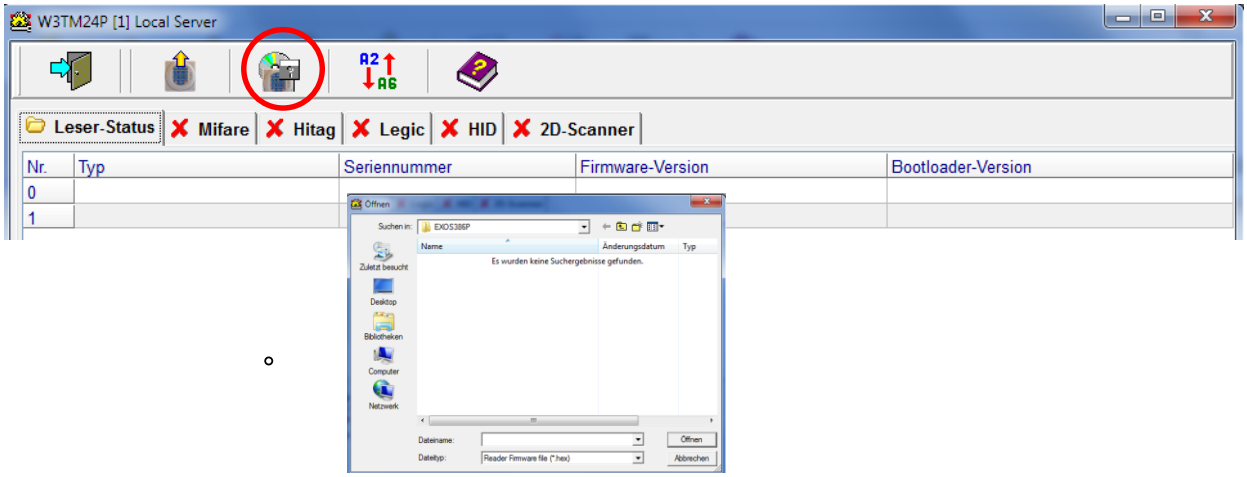
18 Firmware-Update of readers

If the SecuCrypt® communication is active, it is possible to execute a firmware update for the card readers with the symbol *"Reader firmware download"* of the reader configuration program W3TM24P.



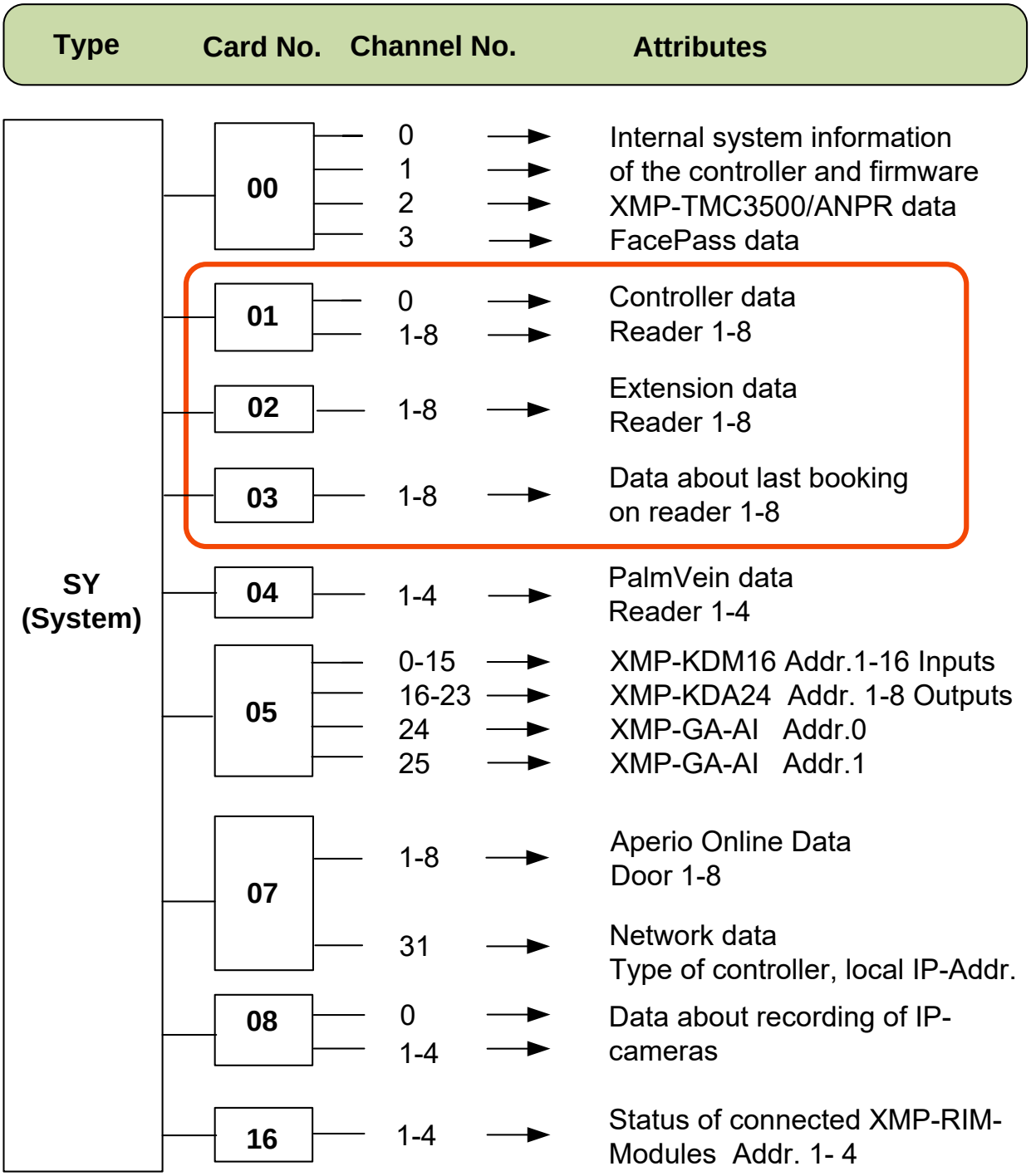
The firmware must be available as „TM23xxVxy.hex" file for being downloaded into the selected card readers.

In case of a successful firmware download, the yellow, green and red LEDs will flash in subsequent way.



19 Data points and attributes for readers

The status of the reader is given with the data point attribute values of type SY, Card 1, 2 and 3. More information about data points, attributes and routines are available in the data point documentation "GW3POIN".



20 Documentation History

Version	Date	Reason
V1.0	02.02.2012	First issue
V1.1	02.04.2013	New release
V1.2	03.26.2014	New release
V1.3	06.01.2016	Update for SM4200
V1.4	15.07.2016	Update/Correction SM4200

COPYRIGHT © AUTEC GMBH 2016

AUTEC Gesellschaft für Automationstechnik mbH
Bahnhofstraße 57-61b
D-55234 Framersheim
Germany

Tel.: +49 (0)6733-9201-0
Fax: +49 (0)6733-9201-91
e-mail: vk@autec-gmbh.de
Internet: www.autec-gmbh.de

www.autec-security.com

FEDERAL COMMUNICATIONS COMMISSION INTERFERENCE STATEMENT
This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.
This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.
If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
-Reorient or relocate the receiving antenna.
-Increase the separation between the equipment and receiver.
-Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
-Consult the dealer or an experienced radio/ TV technician for help.

CAUTION:
Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.
This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

RF exposure warning
This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provide with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.

FCC ID:2A6AAXMP2357

Copyright © 2016 AUTEC Gesellschaft für Automationstechnik mbH - All rights reserved

Revision: July 2016 - This issue replaces all previous issues. Availability, errors and specifications are subject to change without notice.

The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions and typographical errors.

Transmitting as well as copying of this document, utilization and communication of its contents are not permitted, if not explicitly allowed. Contravention obliges for compensation. All rights reserved for the case of patent allocation or registered design registration.

The list of information in this manual occurs according to best knowledge and conscience. AUTEC gives no guarantee for the correctness and completeness of information in this manual. In particular, AUTEC cannot be made liable for consequential damages, which are due to erroneous or incomplete information.

Since mistakes - in spite of all efforts - cannot be avoided completely, we appreciate hints at any time.

The installation recommendations gained in this manual presume the most favorable general conditions. AUTEC gives no guarantee for the perfect function of an installation in system foreign environments.

AUTEC gives no guarantee that the information of this document is free from other industrial property rights. With this document AUTEC grants no licenses for own or other patents or other industrial property rights.