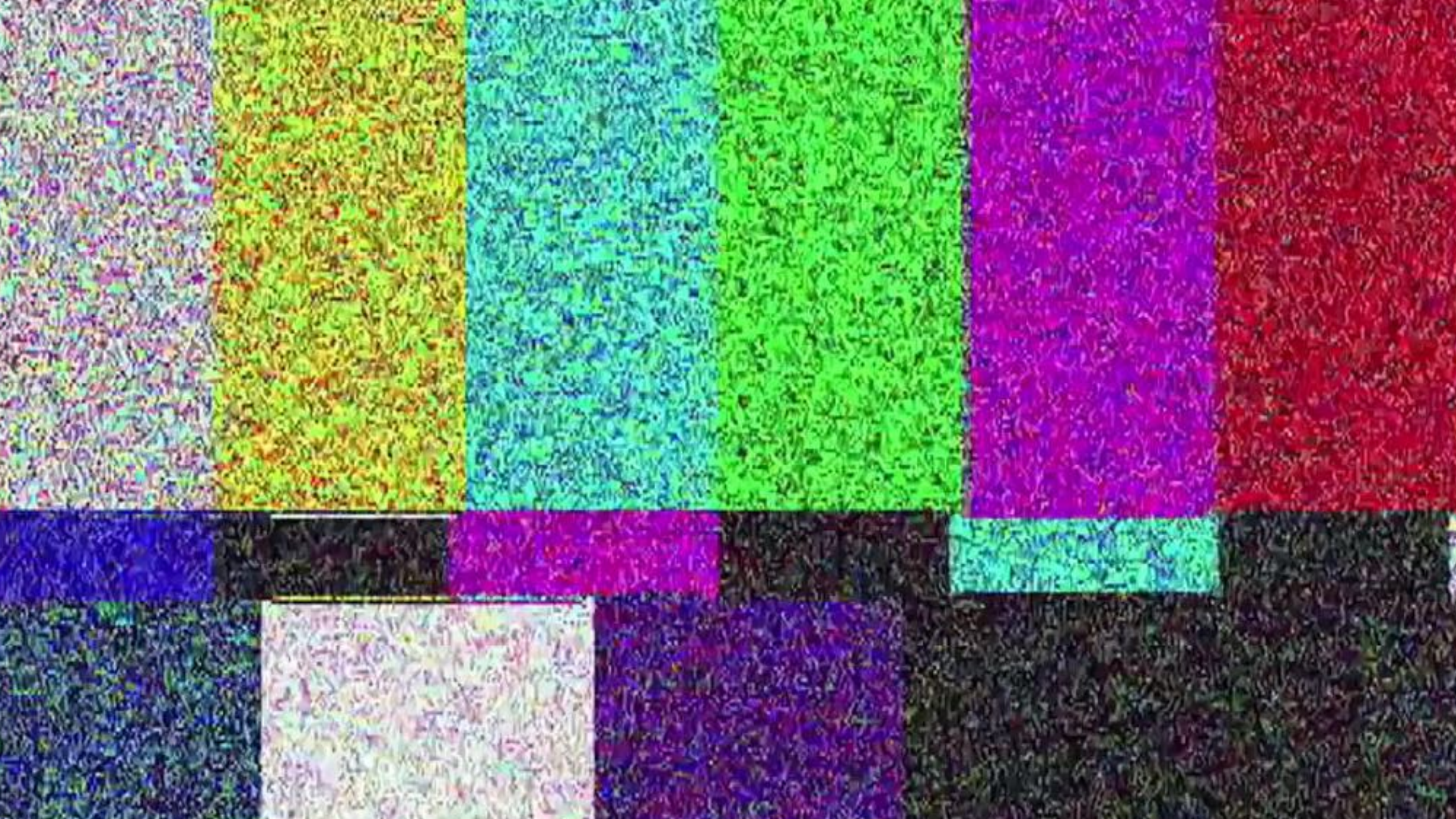

GHOST IN THE LOCKS
OWNING ELECTRONIC LOCKS WITHOUT LEAVING A TRACE
F-Secure

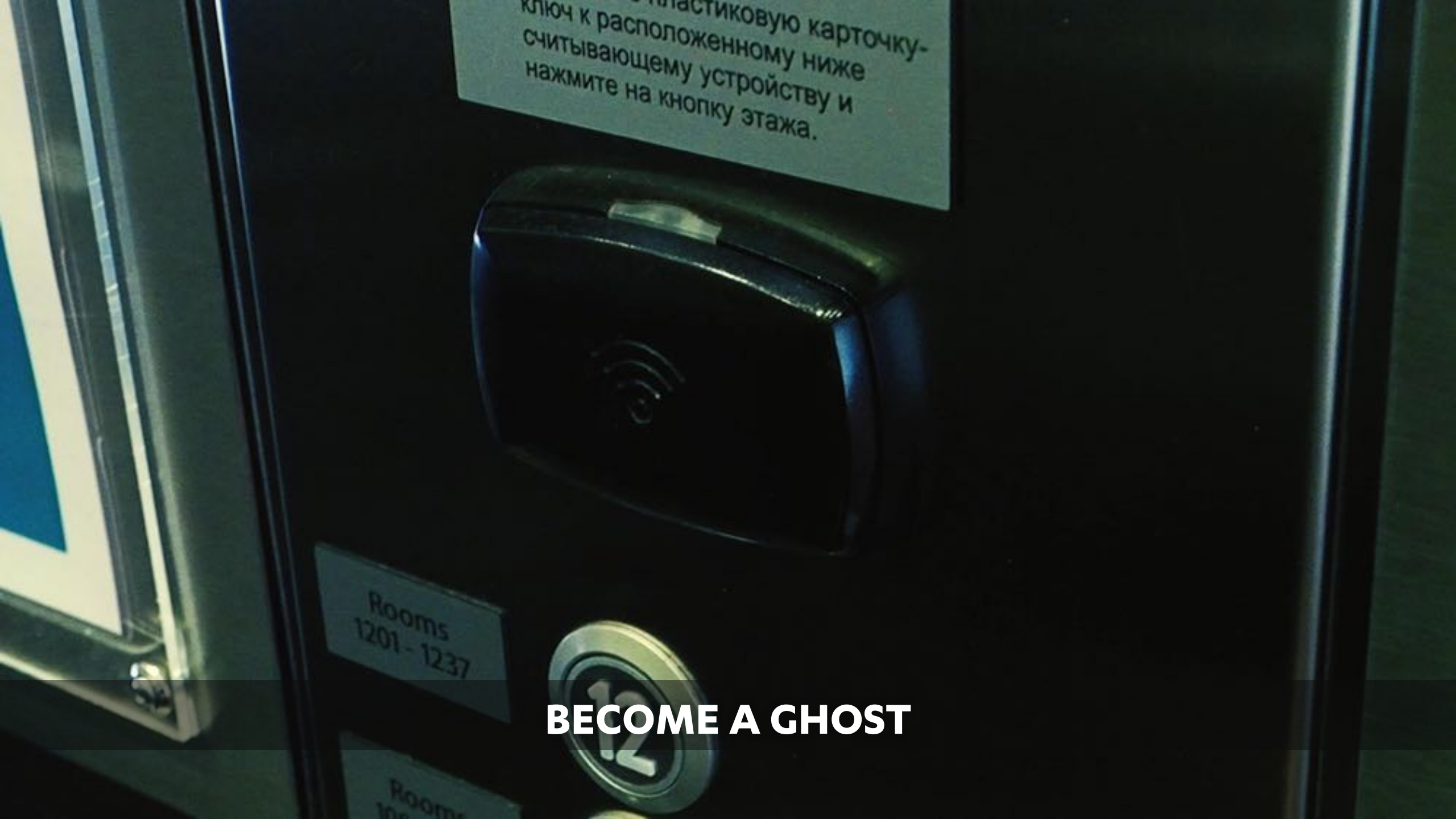
ASSA ABLOY



One Card to rule them all

READ ANY CURRENT OR EXPIRED KEY


ELEVATE TO FACILITY MASTER KEY



BECOME A GHOST

IMPACT

source: https://www.assaabloyhospitality.com/

Case Studies and References from Hospitality Providers

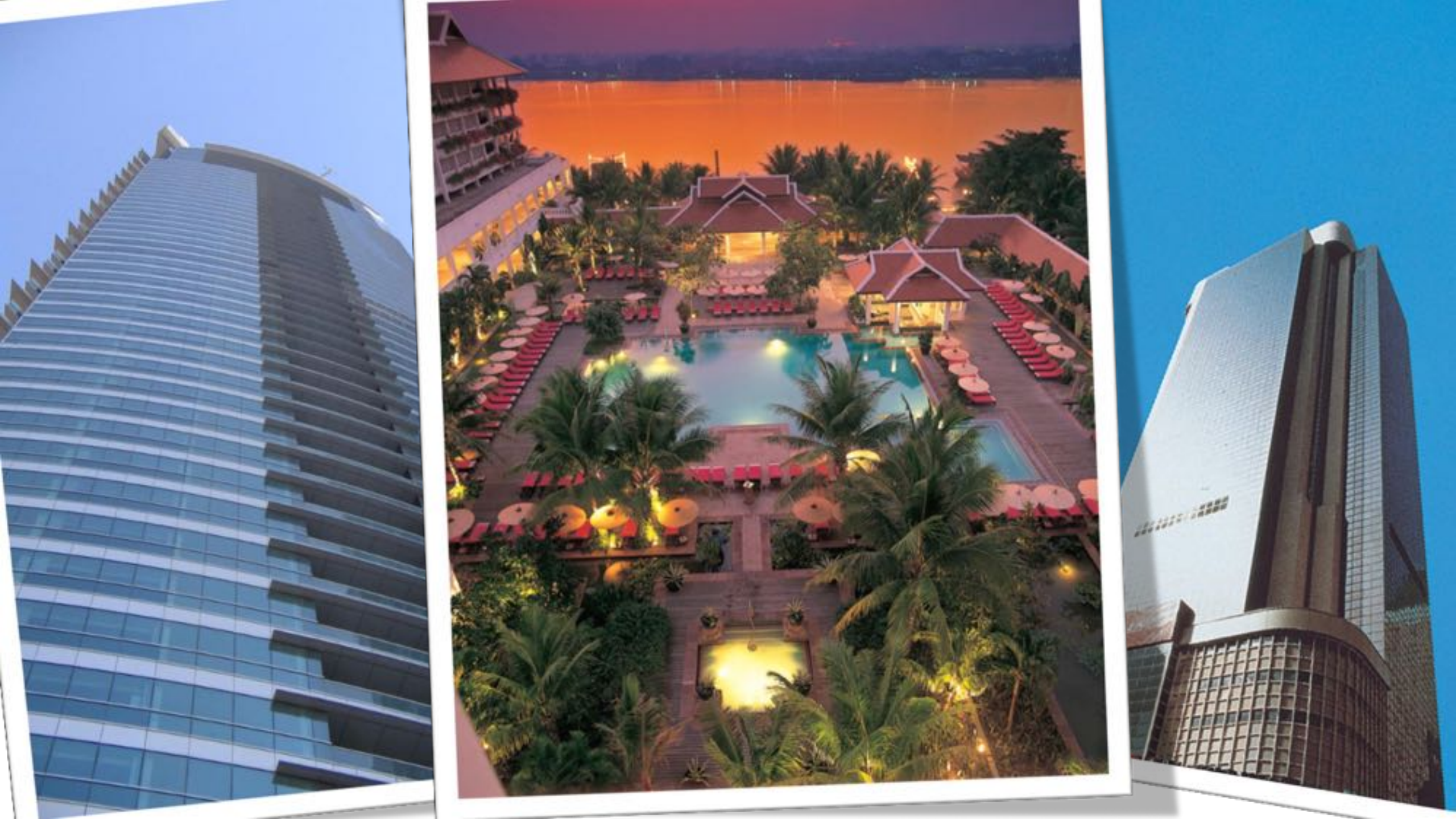
ASSA ABLOY Hospitality has provided solutions to a range of Hotels and Hospitality providers worldwide. Click on any of the Hotel Logos below to see how our solutions and products have changed the way hotels interact with their customers.

InterContinental. Toronto Centre

Renaissance® Toronto Downtown Hotel

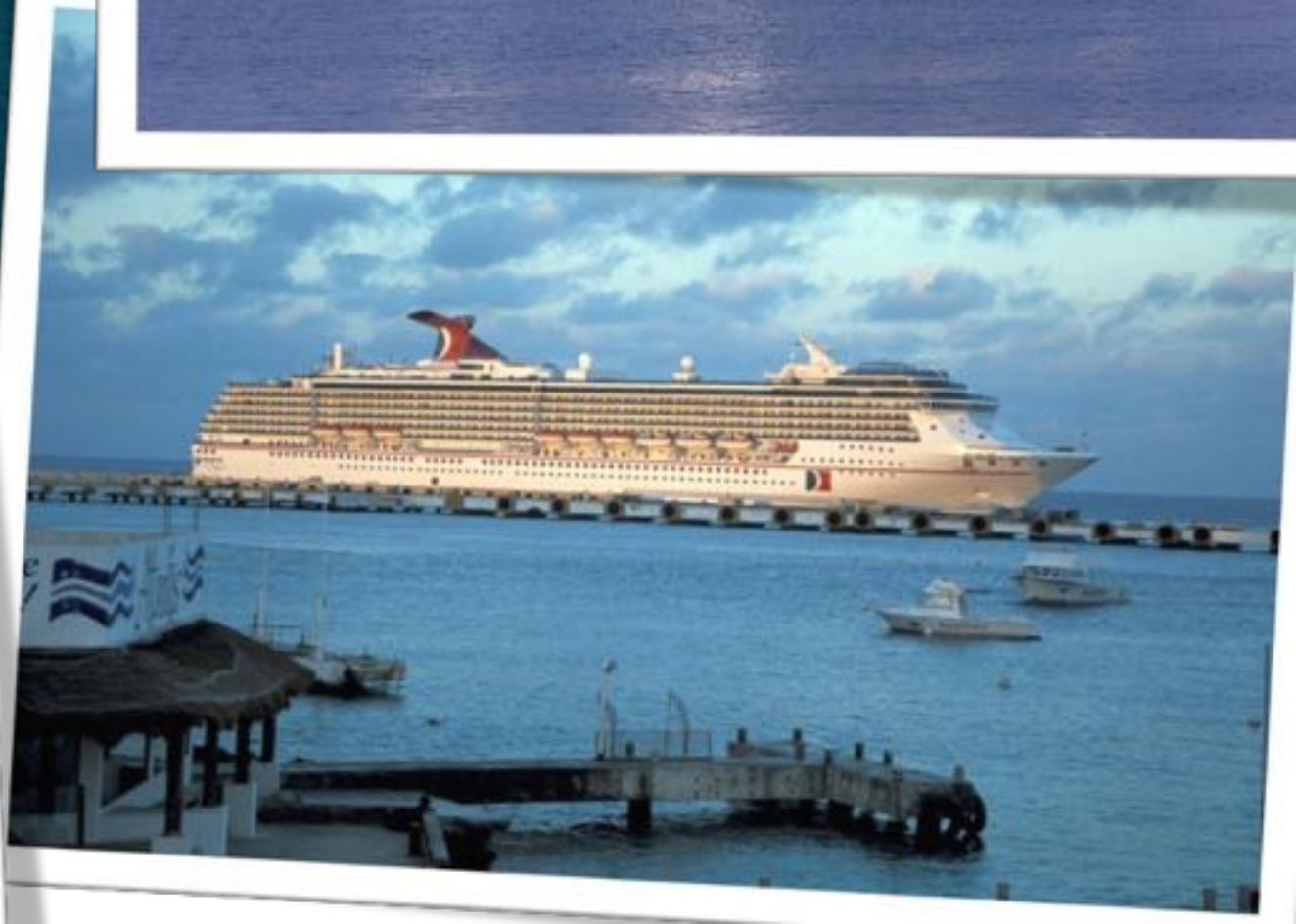
Radisson RED

ULTRA Hotel




Holland America Line


SEA LAUNCH




Carmel


Starlight

Timo Hirvonen

@TimoHirvonen

Senior security consultant @FSecure. Passionate about keeping the good guys safe by studying the latest tricks the bad guys use.

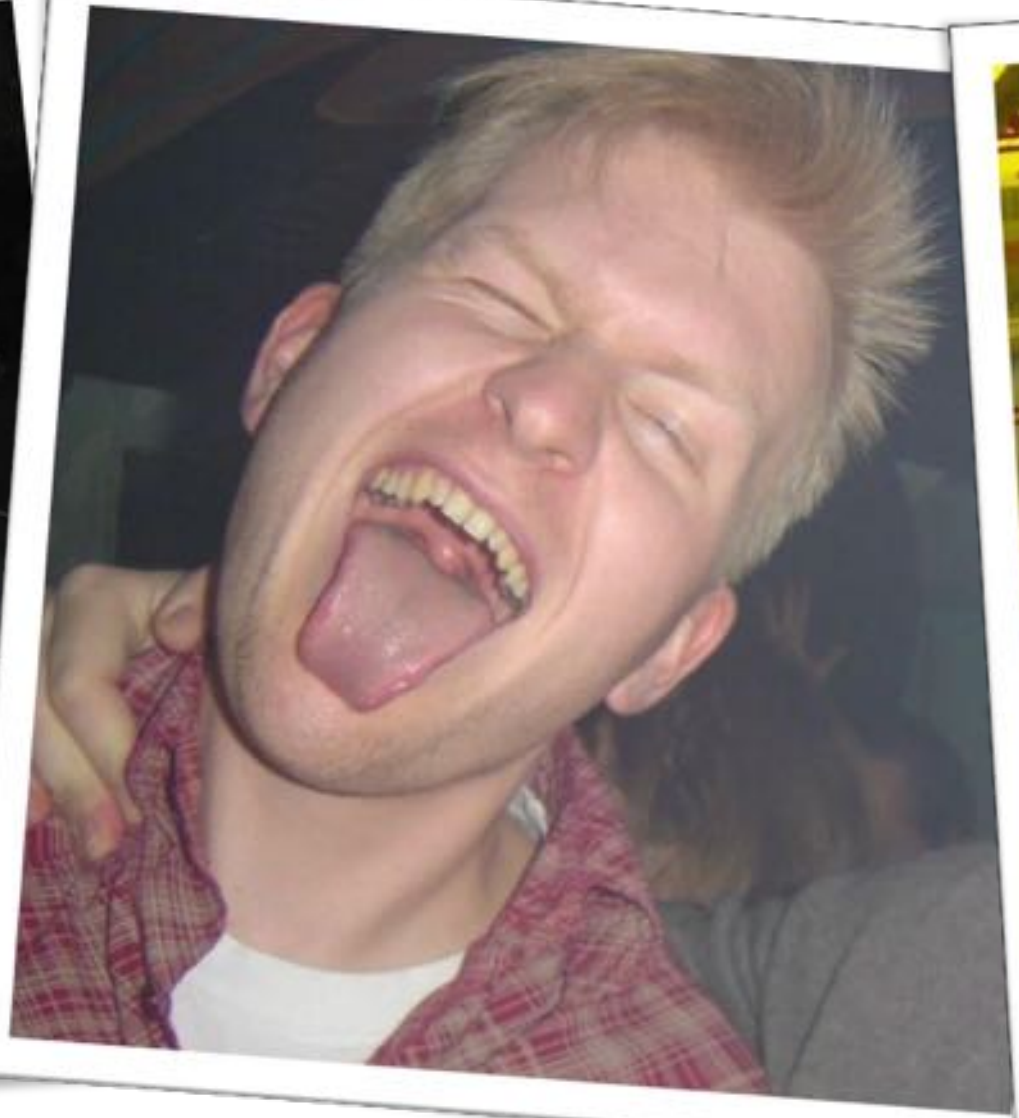
Tomi Tuominen

@tomituominen

Infosec Swiss Army Knife -- For every complex problem there is a solution that is clear, simple, and wrong.

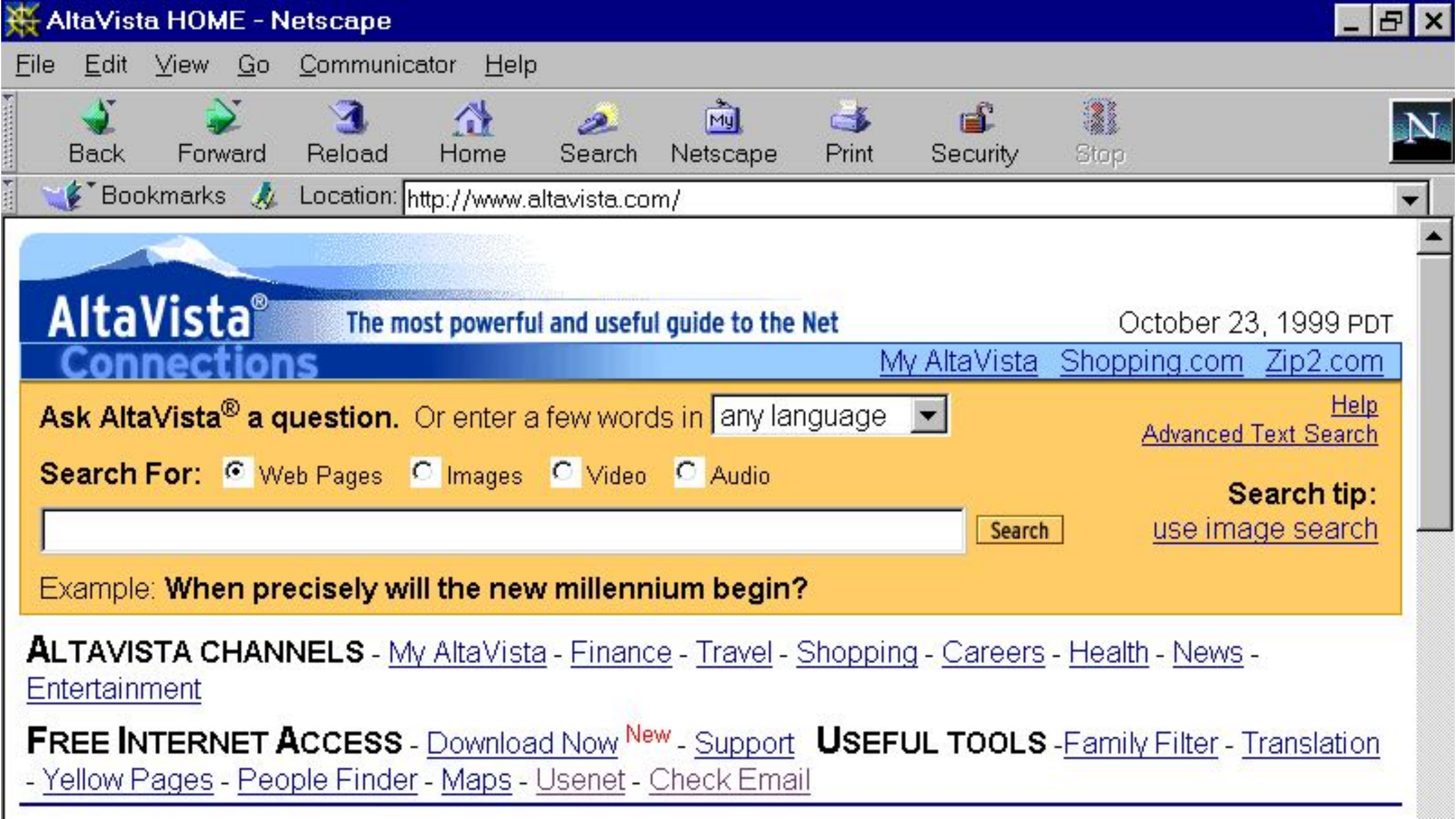
Helsinki, Finland

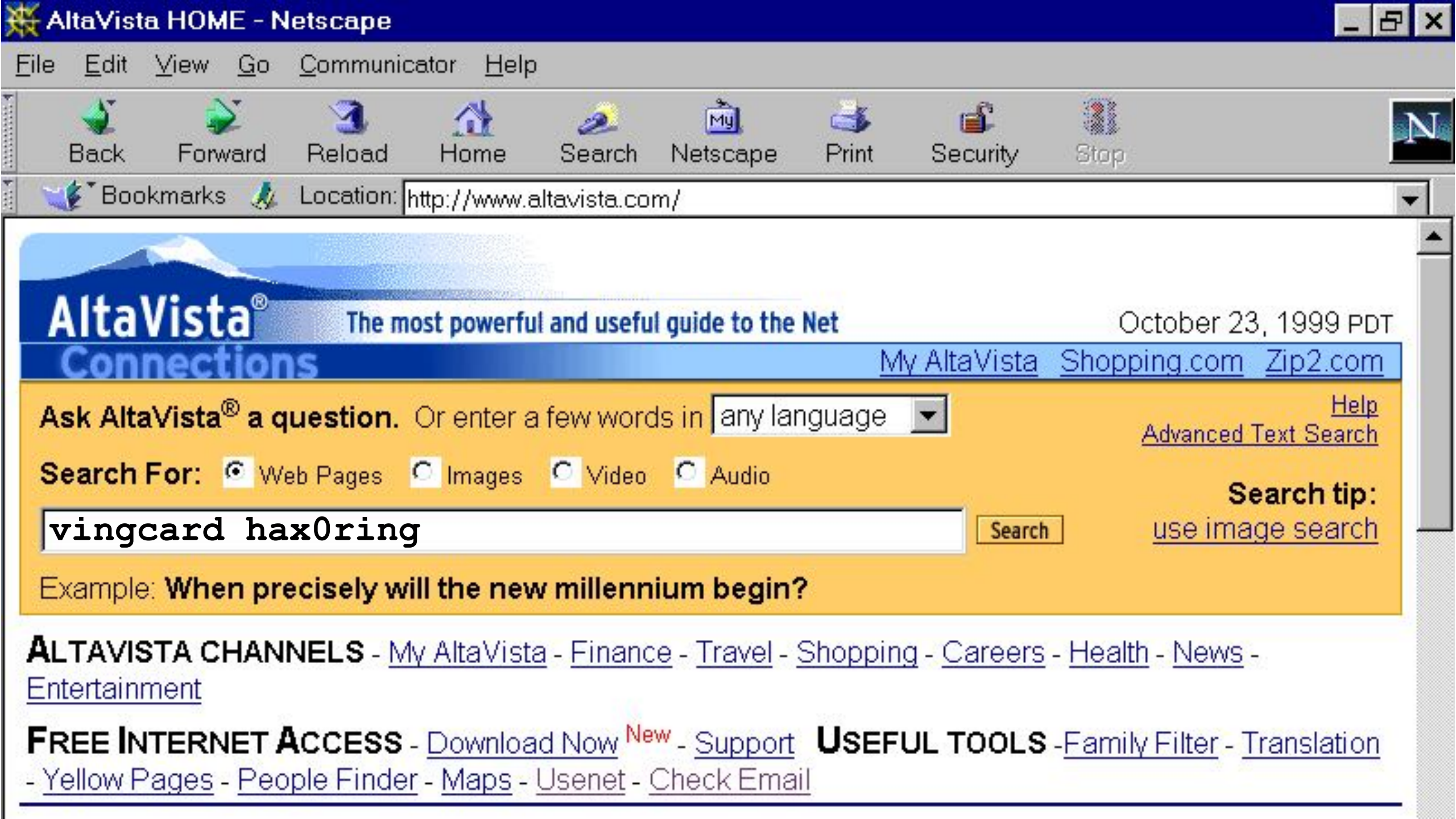
2003



GO WHERE NO [GENDER-NEUTRAL] HAS GONE BEFORE

F-Secure.


AltaVista HOME - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: http://www.altavista.com/
AltaVista®
Connections
The most powerful and useful guide to the Net
October 23, 1999 PDT
My AltaVista Shopping.com Zip2.com
Ask AltaVista® a question. Or enter a few words in any language
Help
Advanced Text Search
Search For: Web Pages Images Video Audio
Search tip:
use image search
Search
Example: When precisely will the new millennium begin?
ALTAVISTA CHANNELS - My AltaVista - Finance - Travel - Shopping - Careers - Health - News - Entertainment
FREE INTERNET ACCESS - Download Now New - Support
USEFUL TOOLS - Family Filter - Translation - Yellow Pages - People Finder - Maps - Usenet - Check Email


AltaVista HOME - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: http://www.altavista.com/
AltaVista®
The most powerful and useful guide to the Net
October 23, 1999 PDT
Connections
My AltaVista Shopping.com Zip2.com
Ask AltaVista® a question. Or enter a few words in any language
Help
Advanced Text Search
Search For: Web Pages Images Video Audio
Search tip:
use image search
vingcard hax0ring
Search
Example: When precisely will the new millennium begin?
ALTAVISTA CHANNELS - My AltaVista - Finance - Travel - Shopping - Careers - Health - News - Entertainment
FREE INTERNET ACCESS - Download Now New - Support
USEFUL TOOLS - Family Filter - Translation - Yellow Pages - People Finder - Maps - Usenet - Check Email

ZERO HITS

F-Secure.

CHALLENGE ACCEPTED

F-Secure.

ATTACK TREE

F-Secure.


vision
by VingCard

UNDERSTANDING THE TARGET

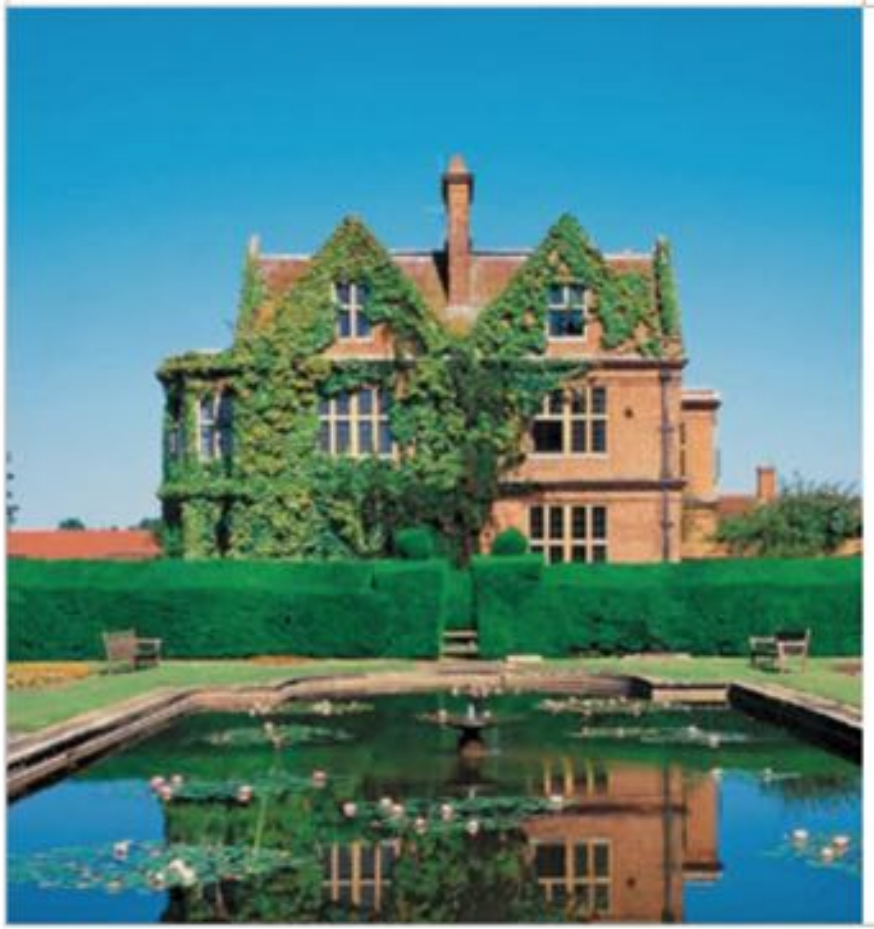
F-Secure.


VingCard®

VingCard Elsafe

SEARCH

About VingCard | News | Products | Pressroom | Contact Us | Support



Wherever you go, VingCard is there...

leading the world in hotel security solutions.

Latest News

M/S Nordnorge - Hurtigruten, Norway
July 2005

Hilton Beijing, China
July 2005

VISIT ELSAFE

Electronic Safes

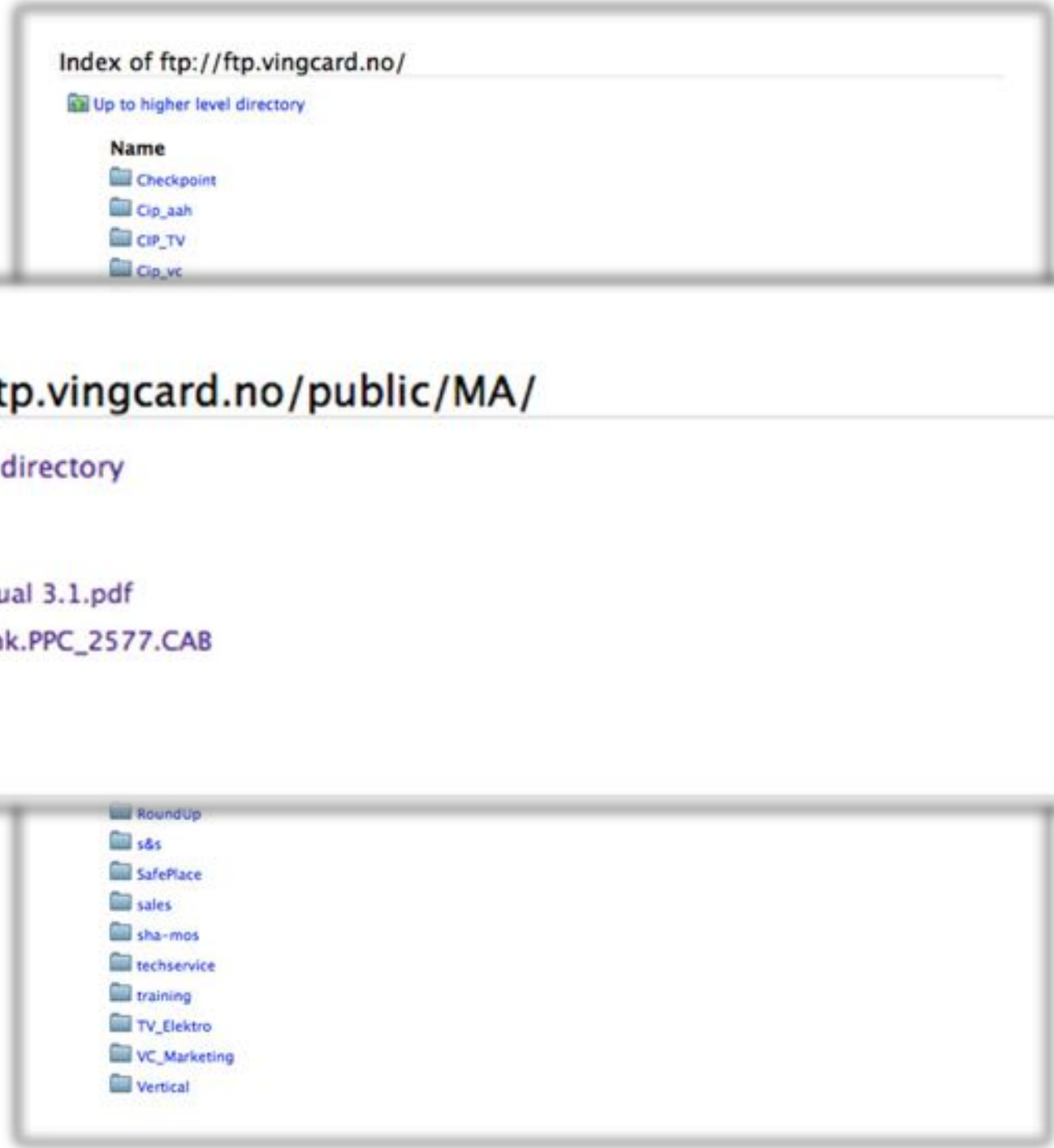
Visit Polarbar

Index of ftp://ftp.vingcard.no/

Up to higher level directory

Name

- Checkpoint
- Cip_aah
- CIP_TV
- Cip_vc
- Cyberguard
- egk
- Elsafe
- elsafe-proddata
- evw
- gude-log
- Guest
- Kingsgate
- Lasgruppen
- LicenseCodes
- Marine
- Marketing
- Mosoft
- persona
- Post
- public
- readme.txt
- RoundUp
- s&s
- SafePlace
- sales
- sha-mos
- techservice
- training
- TV_Elektro
- VC_Marketing
- Vertical



Index of ftp://ftp.vingcard.no/public/MA/

Up to higher level directory

Name

LockLink Manual 3.1.pdf

Vision LockLink.PPC_2577.CAB

VISION.zip

PATENTS

F-Secure.

US 2004078563A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2004/0078563 A1

Kimes et al. (43) Pub. Date: Apr. 22, 2004

(54) REMOTELY PROGRAMMABLE ELECTRONIC LOCK AND PROCESS ASP SOFTWARE TO GENERATE AND TRACK KEY ACTIVITY

(76) Inventors: **John Kimes**, Lake Arrowhead, CA (US); **Leo Felipe**, Costa Mesa, CA (US); **Kerry Hirschy**, Orlando, FL (US); **Nancy Miron**, Royal Oak, MI (US)

Correspondence Address:
Kwadjo Adusei-Poku
Masco Corporation
21001 Van Born Road
Taylor, MI 48180 (US)

(21) Appl. No.: **10/656,980**

(22) Filed: **Sep. 5, 2003**

Related U.S. Application Data

(60) Provisional application No. 60/409,257, filed on Sep. 9, 2002.

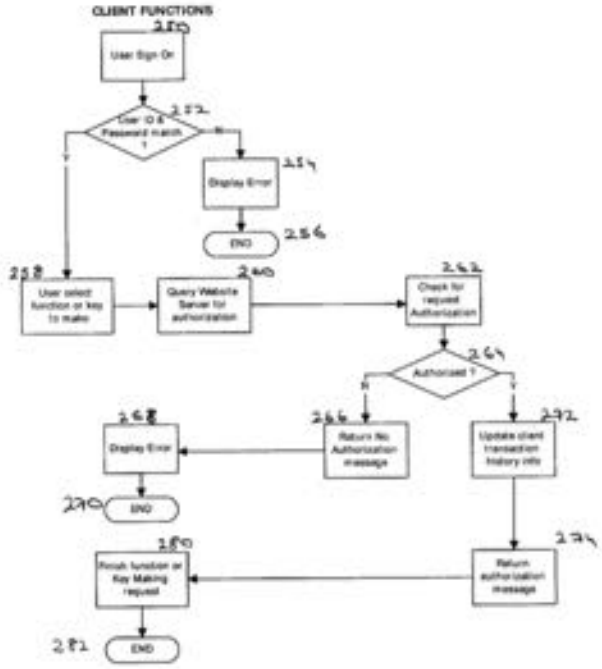
Publication Classification

(51) **Int. Cl.**[7] **H04L 9/00**

(52) **U.S. Cl.** **713/155**

(57) **ABSTRACT**

A remote security key encoding system comprising a client system containing a client identity, a client location and client account information, a service provider system connected to the client system via an Internet connection, and a financial institution system, connected to the client system and the service provider system via the Internet. When, over the Internet a client requests the encoding of a security key, the service provider system identifies the client, authenticates the client location, confirms that the client's account status is above some predetermined threshold, and encodes the security key per the client request. The client has the option of paying in advance for the key encoding services, and may replenish the client account at any time by logging onto the service provider's system.



US005939694A

United States Patent [19]

Holcomb et al.

[11] **Patent Number: 5,939,694**

[45] **Date of Patent: Aug. 17, 1999**

[54] **CHECK-IN STATION**

[75] Inventors: **Glen Holcomb**, Richland Hills, Tex.; **Halvor Aase**, Moss, Norway

[73] Assignee: **VingCard AS**, Norway

[21] Appl. No.: **08/966,004**

[22] Filed: **Nov. 7, 1997**

Related U.S. Application Data

[60] Provisional application No. 60/030,635, Nov. 8, 1996.

[51] **Int. Cl.**[6] **G06F 7/08**

[52] **U.S. Cl.** **235/381**; 235/382

[58] **Field of Search** 235/381, 382

[56] **References Cited**

U.S. PATENT DOCUMENTS

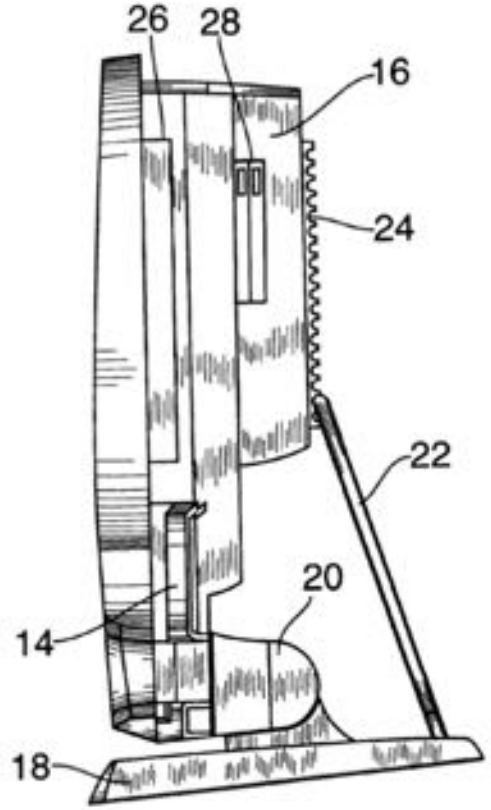
5,156,397 10/1992 Valenza, Jr. 235/381

Primary Examiner—Harold I. Pitts
Attorney, Agent, or Firm—Bierman Muserlian and Lucas

[57] **ABSTRACT**

The check-in station is a stand alone, vertically-oriented unit which generates key cards. The unit employs a touch screen connected to a processor and a card encoding unit. The touch screen, processor and card encoding unit are arranged in the unit so as to provide a compacted, user friendly machine.

6 Claims, 7 Drawing Sheets



US005933085A

United States Patent [19]

Holcomb et al.

[11] Patent Number: 5,933,085

[45] Date of Patent: Aug. 3, 1999

[54] **ENVIRONMENTAL CONTROL LOCK SYSTEM**

[75] Inventors: **Glen Holcomb**, N. Richland Hills; **William Reed**, Arlington, both of Tex.

[73] Assignee: **Vingcard a.s.**, Norway

[21] Appl. No.: **08/634,883**

[22] Filed: **Apr. 19, 1996**

[51] **Int. Cl.**[6] **G05D 23/00**; F28F 27/00

[52] **U.S. Cl.** ..... **340/825.31**; 340/825.34; 340/571; 235/382; 235/382.5; 70/278; 165/200; 165/201; 165/237; 307/116; 236/44 C; 236/44 R

[58] **Field of Search** ..... 340/825.31, 825.34, 340/539, 591; 235/382, 382.5; 70/278; 165/200, 201, 237; 307/116; 236/44 C, 44 R

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,101,886	7/1978	Grimes et al.	165/237
4,485,864	12/1984	Carroll et al.	165/11.1
4,534,194	8/1985	Aydin	70/278
4,717,816	1/1988	Raymond et al.	235/382.5
4,851,828	7/1989	Yamashita	340/825.31
5,591,950	1/1997	Imedio-Ocana	235/382.5

FOREIGN PATENT DOCUMENTS

696769	2/1996	European Pat. Off. .
2272481	5/1994	United Kingdom .
9520782	8/1995	WIPO .

OTHER PUBLICATIONS

North American Technologies, Inc. brochure—Sensorstat Occupancy Sensing HVAC Controller, No Month/Year.

North American Technologies, Inc. brochure—innPULSE Guest Room Management and Information System—Oct. 1993.

Teledex brochure—Comfort Central Guest Room Climate Control System, No Month/Year.

NRG Management Systems, Inc. brochure—In—Room Information System—NRG Management Systems No Month/Year.

Alerton Technologies, Inc. brochure—Energy Management & Controls for Hotels, May 1995.

Primary Examiner—William A. Cuchlinski, Jr.

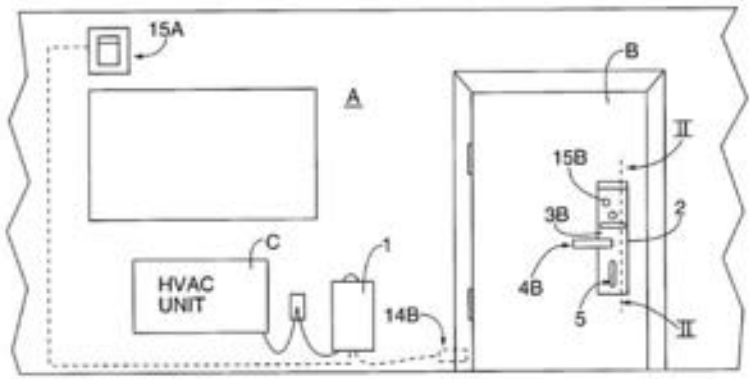
Assistant Examiner—Yonel Beaulieu

Attorney, Agent, or Firm—Bierman, Muserlian and Lucas

[57] **ABSTRACT**

The electric lock system combines an electric lock with an energy control unit such that when a guest key is used in the lock, the lock communicates with the energy control unit to move from an unsold state to a sold state. Optionally, the guest key has information which tells the lock when the guest will leave and the lock communicates to the energy control unit to move from the sold state to an unsold state. Another option, includes a motion detector and door switch which allows the lock to detect the presence of the guest in the room and allows the lock to further employ an occupied and unoccupied state. The combination of the electric lock system and the energy control unit provides energy savings in the heating and cooling of the room.

17 Claims, 9 Drawing Sheets



US005198643A

United States Patent [19]

Miron et al.

[11] Patent Number: 5,198,643

[45] Date of Patent: Mar. 30, 1993

[54] **ADAPTABLE ELECTRONIC KEY AND LOCK SYSTEM**

[75] Inventors: **Nancy C. Miron**, Royal Oak; **Vance E. Neff**, Birmingham, both of Mich.

[73] Assignee: **Computerized Security Systems, Inc.**, Troy, Mich.

[21] Appl. No.: **661,542**

[22] Filed: **Feb. 26, 1991**

[51] **Int. Cl.**[5] **E05B 47/00**

[52] **U.S. Cl.** **235/382**; 235/382.5

[58] **Field of Search** 235/382, 382.5, 380

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,209,782	6/1980	Donath et al.	235/382.5
4,283,710	8/1981	Genest et al.	235/382.5
4,315,247	2/1982	Germantown	235/382
4,415,893	11/1983	Roland et al.	235/382
4,677,284	6/1987	Genest	235/382
4,686,358	8/1987	Seckinger et al.	235/382
4,717,816	1/1988	Raymond et al.	235/493
4,752,876	1/1988	Couch et al.	235/381
4,789,859	12/1988	Clarkson et al.	235/382
4,811,012	3/1989	Rollins	235/382.5
4,870,400	9/1989	Downs et al.	235/382

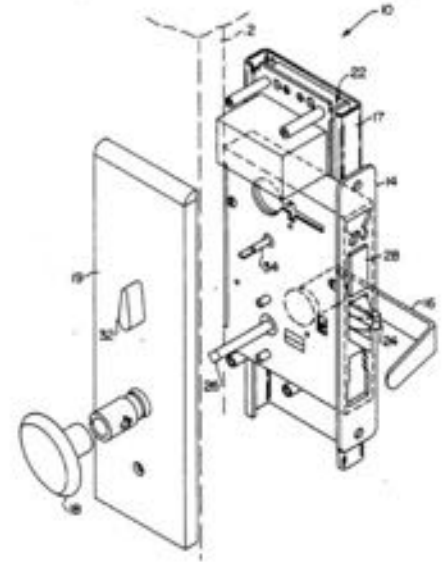
Primary Examiner—John W. Shepperd

Attorney, Agent, or Firm—Reising, Ethington, Barnard, Perry & Milton

[57] **ABSTRACT**

A locking system is utilized to control the locking and unlocking of a lock, such as on a door. The lock includes a magnetic card reader for reading a coded key card into a lock computer which in turn determines functions of and access to the lock. The key card includes a key code, key level code, and key record number stored thereon. The lock includes a memory accessed by the computer which is partitioned and includes a level storage area with level records identified by a lock level code and operational information for the level, and a key storage area for storing lock key records identified by a lock record number and associated with at least one lock level for storing key information associated with the record number. The computer validates a key card by reading and comparing the key level code to the lock level code to determine the level and the key record number to one of the lock record numbers identified with the level in the key storage area. The key code is representative of a real time based on time of issuance, and validation occurs by comparing a lock time to the key code. Additional functions include group pass codes, batch processing, and automatic unlatching times.

28 Claims, 33 Drawing Sheets



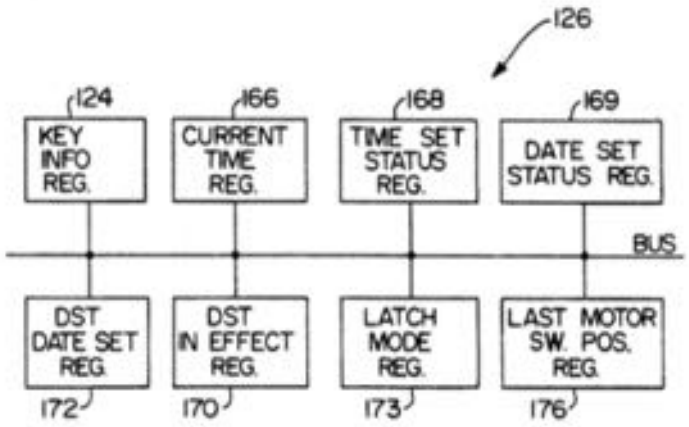


FIG. 5

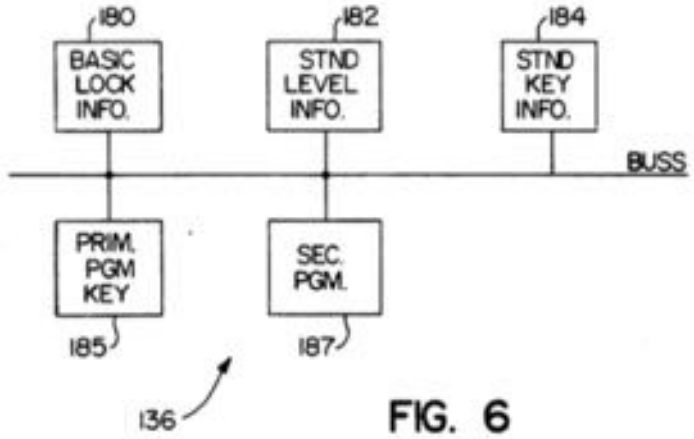


FIG. 6

FIG. 7

- LEVEL CODE
- KEY TYPE
- PROP. NUMBER
- KEY REC. #
- NEW KEY D/T
- EXP DATE OFFS.
- EXP TIME
- DUPL. KEY I.D.
- SEQ # /COMBIN.
- INVALID DAYS
- PASS AUTHOR. #
- OPEN/NON-OP
- OVERRIDE DEADBLT

34

US005198643A

United States Patent [19]

Miron et al.

[11] **Patent Number: 5,198,643**

[45] **Date of Patent: Mar. 30, 1993**

[54] **ADAPTABLE ELECTRONIC KEY AND LOCK SYSTEM**

[75] Inventors: **Nancy C. Miron**, Royal Oak; **Vance E. Neff**, Birmingham, both of Mich.

[73] Assignee: **Computerized Security Systems, Inc.**, Troy, Mich.

[21] Appl. No.: **661,542**

[22] Filed: **Feb. 26, 1991**

[51] **Int. Cl.**[5] **E05B 47/00**

[52] **U.S. Cl.** **235/382**; 235/382.5

[58] **Field of Search** 235/382, 382.5, 380

[56] **References Cited**

U.S. PATENT DOCUMENTS

0 Donath et al. 235/382.5
1 Genest et al. 235/382.5
2 Germantown 235/382
3 Roland et al. 235/382
7 Genest 235/382
7 Seckinger et al. 235/382
8 Raymond et al. 235/493
8 Couch et al. 235/381
8 Clarkson et al. 235/382
9 Rollins 235/382.5
9 Downs et al. 235/382

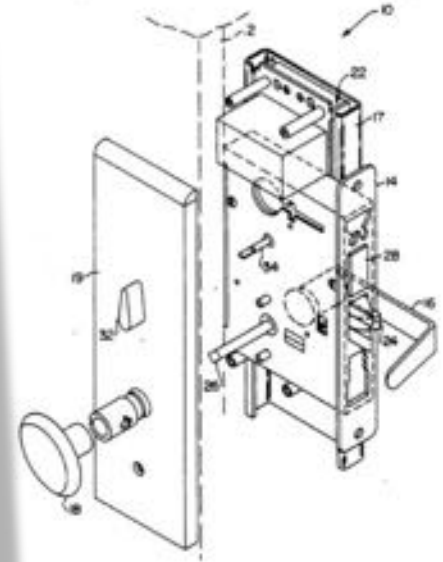
Attorney, Agent, or Firm—Reising, Ethington, Barnard, Perry & Milton

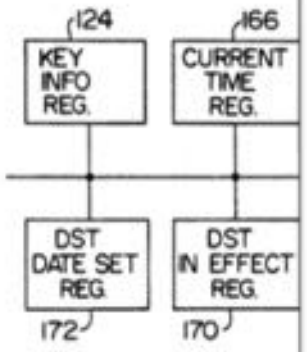
[57] **ABSTRACT**

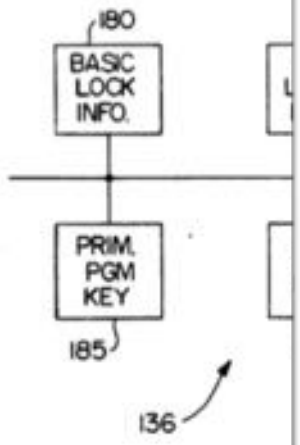
A locking system is utilized to control the locking and unlocking of a lock, such as on a door. The lock includes a magnetic card reader for reading a coded key card into a lock computer which in turn determines functions of and access to the lock. The key card includes a key code, key level code, and key record number stored thereon. The lock includes a memory accessed by the computer which is partitioned and includes a level storage area with level records identified by a lock level code and operational information for the level, and a key storage area for storing lock key records identified by a lock record number and associated with at least one lock level for storing key information associated with the record number. The computer validates a key card by reading and comparing the key level code to the lock level code to determine the level and the key record number to one of the lock record numbers identified with the level in the key storage area. The key code is representative of a real time based on time of issuance, and validation occurs by comparing a lock time to the key code. Additional functions include group pass codes, batch processing, and automatic unlatching times.

John W. Shepperd

28 Claims, 33 Drawing Sheets







the retracted and extended position. The outside door knob **16** includes a shank clutch **70** connected thereto. The clutch **58** matingly engages the shank clutch **70** in its extended position allowing unlocking of the door and disengages same to prevent opening of the door. A slide member **72** is fixedly attached to the shift fork **68** for pivoting same in the opposite directions. The slide member **72** is slideably retained on a support plate **73** by a bracket **74**. The bracket **74** includes a circular aperture **76** therethrough, and the slide member **72** includes a rectangular aperture **78**. An actuation gear **80** includes a tab **82** extending therefrom for engaging said apertures **76, 78**. The actuation gear **80** is rotatably controlled by and operatively connected to a worm gear **84**. A spring **86** is connected about the gears **80, 84** for biasing the actuation gear **80** to follow movement of the worm gear **84**. As the worm gear **84** rotates in a first direction, the actuation gear **80** follows moving the tab **82** in an upward direction therefore pulling the slide member **72** and extending the clutch **58**. As the worm gear **84** rotates in a second and opposite direction, the opposite operation occurs retracting the clutch **58**. The worm gear **84** includes coacting teeth **86** for engaging a worm shaft **88** having threads **90** thereon.

Motor/solenoid Actuation

A motor **92** rotates the worm shaft **88** in a first direction therefore causing rotation of the worm gear **84**, and rotates in a second direction to move the worm gear **84** in the opposite direction. A solenoid may be utilized wherein the solenoid is connected directly to the shift fork **68** for controlling the pivotal movement.

Motor Switches

In the motor embodiment, included are two motor turn switches **94, 96**. A first motor switch **94** is connected adjacent the worm gear **84** such that actuation and rotation to a first stroke actuates the motor switch **94** for turning the motor off. The worm gear **84** includes a tab **98** which engages the switch **94** upon rotation to a predetermined position. The second motor switch **96** is connected adjacent the actuation gear **80** for providing

LOCK CONTROL CIRCUITRY

Referring now to FIG. **4**, the microcomputer lock control circuit **42** will be described. The microcomputer **110** is a single chip, eight bit microcomputer; in the illustrative embodiment, it is a series N80C31BH made by AMD. The key reader **38** is controlled by and provides input to the microcomputer **110** as follows.

As described above, the recorded code on the key **34** is read from the key in a single stream of data. For this purpose, the magnetic key reader **38** is provided as shown in the schematic diagram of FIG. **4**. The magnetic key reader **38** comprises a magnetic tape read head **116** which coacts respectively with the recording track **114** on the magnetic stripe of the key. The read head **116** suitably takes the form of a conventional stereo pick up or read head. The magnetic read head **116** is connected with a differential amplifier circuit wherein the signal from the magnetic read head **116** is received through a pair of resistors **R1, R2** to the inverting and noninverting inputs of an operational amplifier **120** having feedback through the resistor **R3**, and the output connected to the inverting input of the second operational amplifier **122** having its noninverting input connected through a resistor **R4** to the output of the first operational amplifier **120**. Feedback is provided between the output and the noninverting input through a resistor **R5** and diode **D1** series wherein the output produces the digital signal which is transmitted to the microcomputer **110**. The key switch **56** is actuated to a closed condition upon full insertion of the key and it is actuated to an open condition upon withdrawal of the key. Thus, the data stream which is produced by the magnetic read head **116** from the recording track **114** on the key **34** is read into the microcomputer **110** upon withdrawal motion of the key. The motion of the key **34** causes a signal voltage to be induced in the read head **116** in accordance with the recorded magnetic signal on the respective track **114**.

The 147 bits received from the key **34** are stored in a key information register **124** in the random access memory (RAM) **126** of the microcomputer **110** (See FIG. **5**).

The key information is read into the microcomputer **110** from the key reader **38** and is temporarily stored in the key information register **124**. The key information

05198643A
umber: 5,198,643
Patent: Mar. 30, 1993

—Reising, Ethington, Barnard,

BSTRACT
lized to control the locking and
uch as on a door. The lock in-
reader for reading a coded key
puter which in turn determines
s to the lock. The key card in-
level code, and key record num-
he lock includes a memory ac-
r which is partitioned and in-
rea with level records identified
d operational information for the
ge area for storing lock key re-
k record number and associated
evel for storing key information
ord number. The computer vali-
ding and comparing the key level
code to determine the level and
to one of the lock record num-
e level in the key storage area.
entative of a real time based on
alidation occurs by comparing a
de. Additional functions include
h processing, and automatic un-

33 Drawing Sheets

- Bypass the physical lock without leaving visible marks

vision
by VingCard

THE PLAN

- **Get a physical lock**
- Analyze the lock and find a clever way to bypass the lock
- Profit

THE PLAN

- Get a physical lock
- **Analyze the lock and find a clever way to bypass the lock**
- Profit

THE PLAN

- Get a physical lock
- Analyze the lock and find a clever way to bypass the lock
- ~~Profit~~ **FAIL!**

We need a
better plan

- Bypass the electronic lock

***LockLink* Component**

1. Pocket PC with Windows software
2. Docking station
3. Serial connector to Vision PC
4. Power supply
5. Contact Card for programming doors

The parts 1 to 4 are delivered as a package.

The Vision LockLink software can be installed from a PC (using Microsoft ActiveSync) or by plugging a pre-programmed Compact Flash card into the Pocket PC.

Assassination of Mahmoud Al-Mabhouh

The **assassination of Mahmoud Al-Mabhouh** (Arabic: محمود المبحوح, Maḥmūd al-Mabḥūḥ; 14 February 1961 – 19 January 2010) took place on 19 January 2010, in a Dubai hotel room. Al-Mabhouh—a co-founder of the Izz ad-Din al-Qassam Brigades, the military wing of the Islamist Palestinian Hamas—was wanted by the Israeli government for the kidnapping and murder of two Israeli soldiers in 1989 as well as purchasing arms from Iran for use in Gaza; these have been cited as a possible motive for the assassination.[1] He also had other enemies, including Fatah. He had spent 2003 in prison in Egypt and was being sought by Jordanian intelligence.[2]

His assassination attracted international attention in part due to allegations that it was ordered by the Israeli government and carried out by Mossad agents holding fake or fraudulently obtained passports from several European countries and Australia.

The photographs of the 26 suspects and their aliases were subsequently placed on Interpol's most-wanted list. The Dubai police found that 12 of the suspects used British passports, along with six Irish, four French, one German, and three Australian passports.[3][4][5][6][7] Interpol and the Dubai police believed that the suspects stole the identities of real people, mostly Israeli dual citizens.[3][8] Two Palestinians, believed by Hamas to be former Fatah security officers and current employees of a senior Fatah official, were taken into custody in Dubai, on suspicions that one of them provided logistical assistance to the hit team. Despite Hamas's claim, Dubai would not comment on the incident or identify the two Palestinian suspects.

According to initial reports, Al-Mabhouh was drugged,[9] then electrocuted and suffocated.[5] Lt. Gen. Dhahi Khalfan Tamim of the Dubai Police Force said the suspects tracked Al-Mabhouh to Dubai from Damascus, Syria. They arrived from different European destinations and stayed at different hotels, presumably to avoid being detected

Assassination of Mahmoud Al-Mabhouh

Location	Dubai, United Arab Emirates
Date	19 January 2010
Target	Mahmoud al-Mabhouh
Attack type	Assassination
Weapons	Pillow, muscle relaxant

A readout of activity that took place on the hotel room's electronic door lock indicated that an attempt was made to reprogram al-Mabhouh's electronic door lock at this time. The investigators believe that the electronic lock on al-Mabhouh's door may have been reprogrammed and that the killers gained entry to his room this way.[39] The locks in question, VingCard Locklink brand (Dubai police video, 21:42), can be accessed and reprogrammed directly at the hotel room door.

Wikinews has related news: ***Hamas claims Israel assassinated commander in Dubai***

According to Dubai Police, he was dead by 9 p.m. that evening.[33] On 20 January 2010, the following day, a hotel cleaner attempted to gain entry, but found that the door was latched from the inside. A member of hotel security was then called in to open the door. After the door was opened, al-Mabhouh's body was discovered on the bed.[2][29][40] On the drawer next to the bed, the assassins had placed a small bottle of medicine to make it appear as if he had died of natural causes.

Investigation

Cause of death

Initially, Dubai authorities believed al-Mabhouh had died of natural causes.[41] Fawzi Benomran, the Dubai police coroner, said, "It was meant to look like death from natural causes during sleep." It took 10 days for the Dubai police to come to the conclusion that al-Mabhouh was assassinated. Benomran described the determination of the exact cause of death as "one of the most challenging cases" his department faced.[42]

The *Khaleej Times* quoted an unnamed senior police official as saying that four masked assailants had shocked al-Mabhouh's legs before using a pillow to suffocate him.[43] Another story reported by Uzi Mahnaimi stated that a hit team murdered al-Mabhouh with a heart-attack inducing drug, then proceeded to take photographs of his documents before leaving.[29]

Al-Mabhouh's family said that medical teams that examined his body determined that he died in his hotel room after being strangled and receiving a massive electric shock to the head, and that blood samples examined by a French laboratory confirms that electrocution was the cause of death.[40] According to Reuters news agency, traces of poison were found in al Mabhouh's autopsy.[44] Dubai authorities stated they were ruling the death a homicide and were working with the International Criminal Police Organization to investigate the incident.[45]

We need a
~~better~~ more elegant plan

- Clone an access token
- Produce an access token with more privileges
- Produce an access token with all privileges

THE PLAN

- **Understand magstripe**
- Get a magstripe encoder/decoder
- Get hotel cards
- Reverse engineer track data on the cards
- Profit

MAGNETIC STRIPE CARD

A **magnetic stripe card** is a type of card capable of storing data by modifying the magnetism of tiny iron-based magnetic particles on a band of magnetic material on the card.

STANDARD TRACK DATA

Track		Bits/inch	Bits/char	Content in chars
1	IATA	210	7	79 alphanumeric
2	ABA	75	5	40 numeric
3	THRIFT	210	5	107 numeric

EXAMPLE

Attribute	Char
Start sentinel	;
Data	1234567890
End sentinel	?
LRC	0

VINGCARD LOCK DATA

Track	Standard	Content in chars
1	ISO 3554	76 alphanumeric
2	ISO 3554	37 numeric
3	**Custom**	**Vingcard lockdata**

THE PLAN

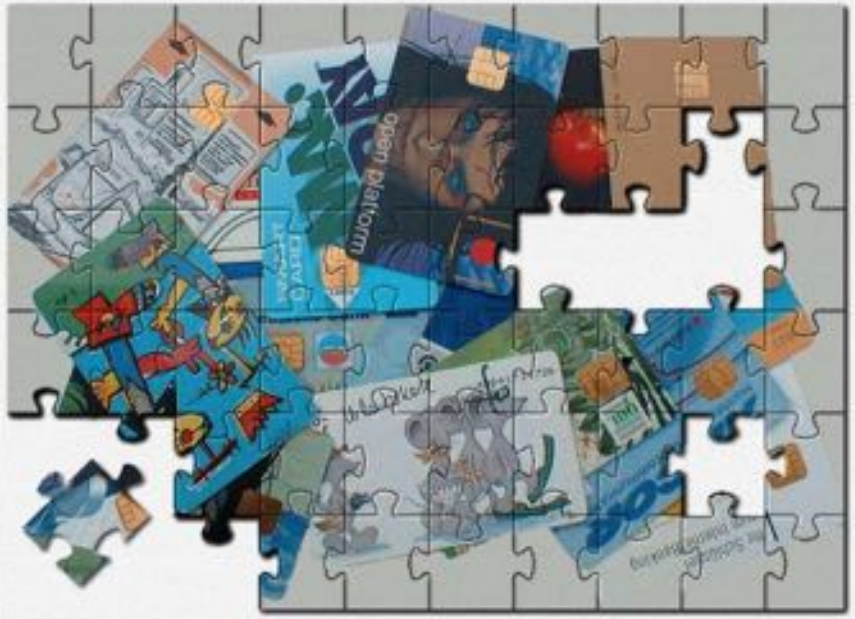
- Understand magstripe
- **Get a magstripe encoder/decoder**
- Get hotel cards
- Reverse engineer track data on the cards
- Profit

Deutsche Seiten

MIRROR

MAKInterface

What do you want to program today ?



English Pages

MIRROR

File Process Setup Help

Scan Port for Data

Stop Scanning

Swipe Time 575 ms

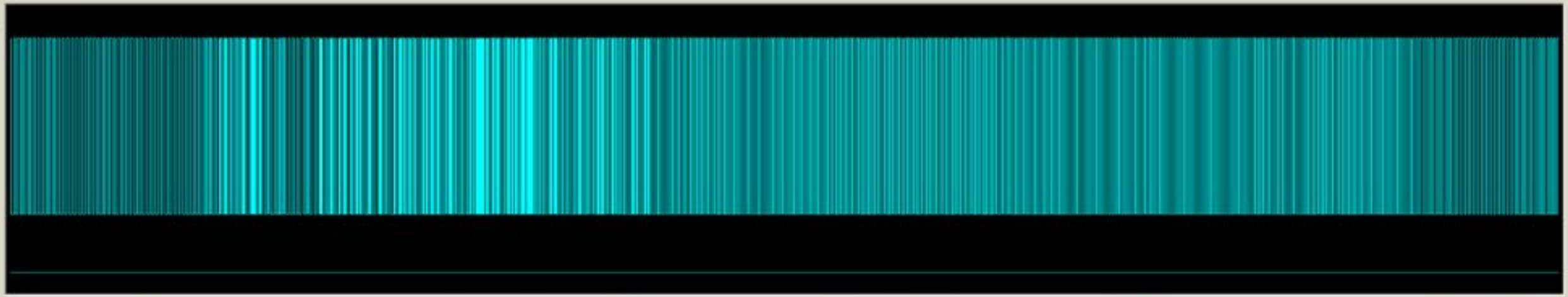
Av. Swipe Speed 22 cm/s

Min Swipe Speed 18 cm/s

Max Swipe Speed 27 cm/s

Status

Decode | Signal Analysis | Data Analysis | Write Tracks



Auto-Zoom

Tik	Chr	Nr	Flux	us	Bit
1		0	0	527	0.0
2		0	1	493	0.0
3		0	0	460	0.0
4		0	1	447	0.0
5		0	0	453	0.0
6		0	1	473	0.0
7		0	0	473	0.0
8		0	1	467	0.0
9		0	0	467	0.0
10		0	1	447	0.0
11		0	0	487	0.0
12		0	1	493	0.0
13		0	0	507	0.0
14		0	1	500	0.0
15		0	0	507	0.0
16		0	1	487	0.0
17		0	0	493	0.0
18		0	1	480	0.0
19		0	0	493	0.0
20		0	1	473	0.0
21		0	0	467	0.0
22		0	1	467	0.0
23		0	0	487	0.0
24		0	1	500	0.0

Delete Tick/Char

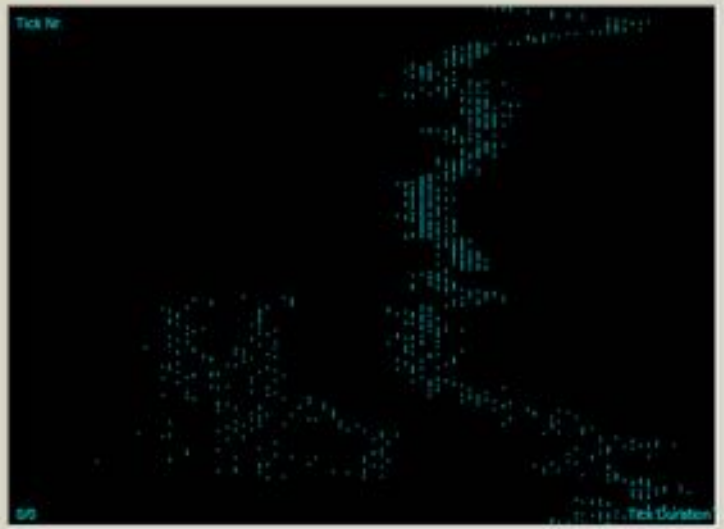
Modify

Insert

Ticks

Characters

AutoRecalc LRC



Track Density 278

Total Ticks 1023

First "1" Bit at 91

Character Set

THE PLAN

- Understand magstripe
- Get a magstripe encoder/decoder
- **Get hotel cards**
- Reverse engineer track data on the cards
- Profit


TELEPHONE


WESTIN

THE PLAN

- Understand magstripe
- Get a magstripe encoder/decoder
- Get hotel cards
- **Reverse engineer track data on the cards**
- Profit

```
42 d2 63 b2 9a 00 41 9c
59 69 c3 42 6a 41 44 c0
c0 82 bd 42 c0 96 53 42
42 42 42 42 42 42 42 42
42
```

UHHH ...

THE PLAN

- Understand magstripe
- Get a magstripe encoder/decoder
- Get hotel cards
- Reverse engineer track data on the cards
- ~~Profit~~ **FAIL!**

We need a
~~more elegant~~ plan

THE PLAN

- **Acquire a copy of Vision software**
- Reverse engineer the software and find a clever way to open the lock without access to the original key
- Pose like a boss

Index of /webdownloads/Vision_

Name	Last modified	Size	Description
Parent Directory		-	
Vision 6.3 Total CD .zip	27-May-2014 13:56	186M	
Vision Release Note V6.3.pdf	27-May-2014 13:57	483K	

THE PLAN

- Acquire a copy of Vision software
- **Reverse engineer the software and find a clever way to open the lock without access to the original key**
- Pose like a boss

UHHH ...

THE PLAN

- Acquire a copy of Vision software
- **Read and understand the product manuals**
- Reverse engineer the software and find a clever way to open the lock without access to the original key
- Pose like a boss

VingCard Technician
Terminal User Manua

Revisions

Name	Date	Reason
Ewan Dunlop	24 March 2010	Release V1.0, released with

VingCard VISION Software

Version 6.3

Software Release Notes

13 March 2014

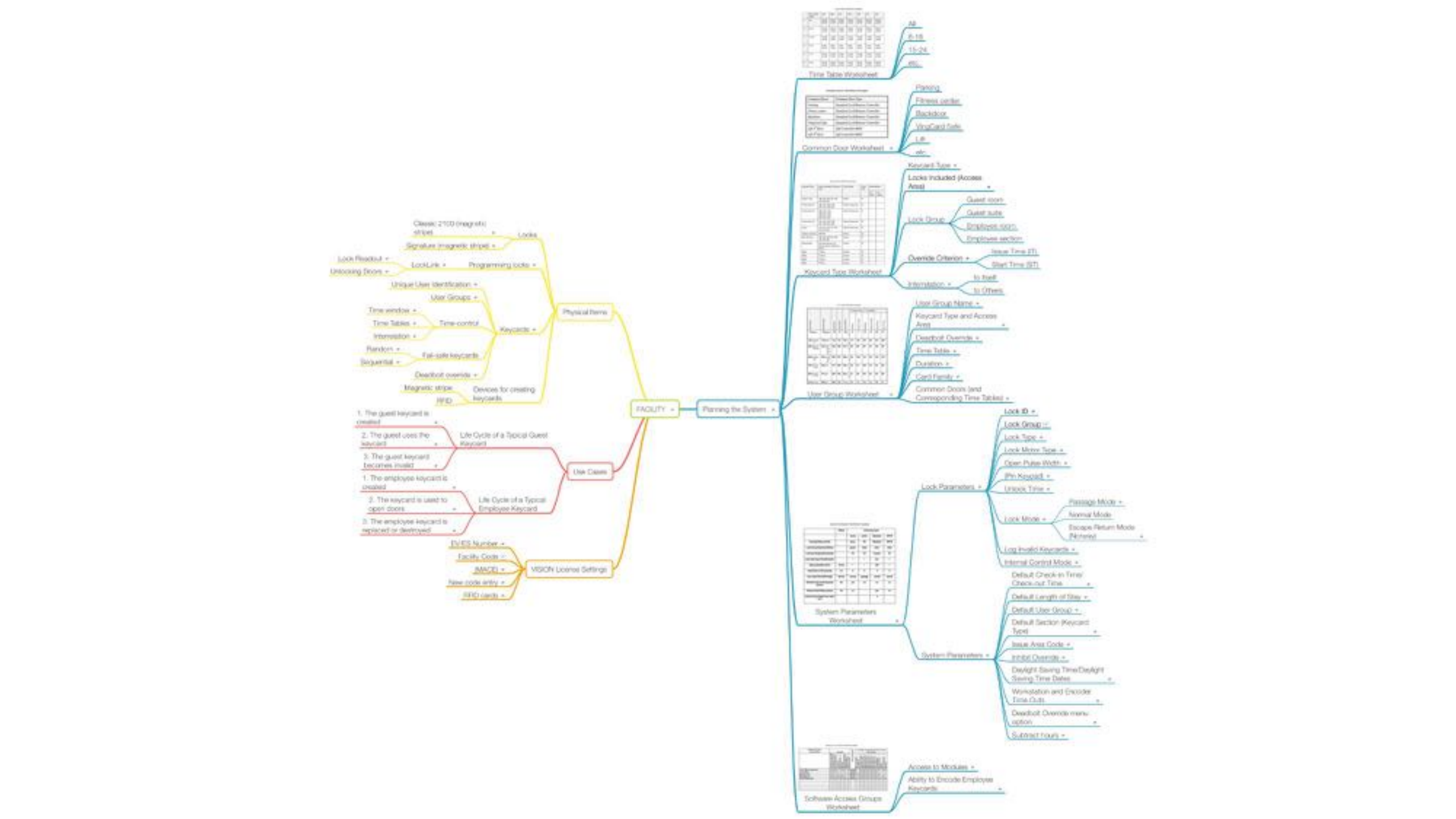
Written By

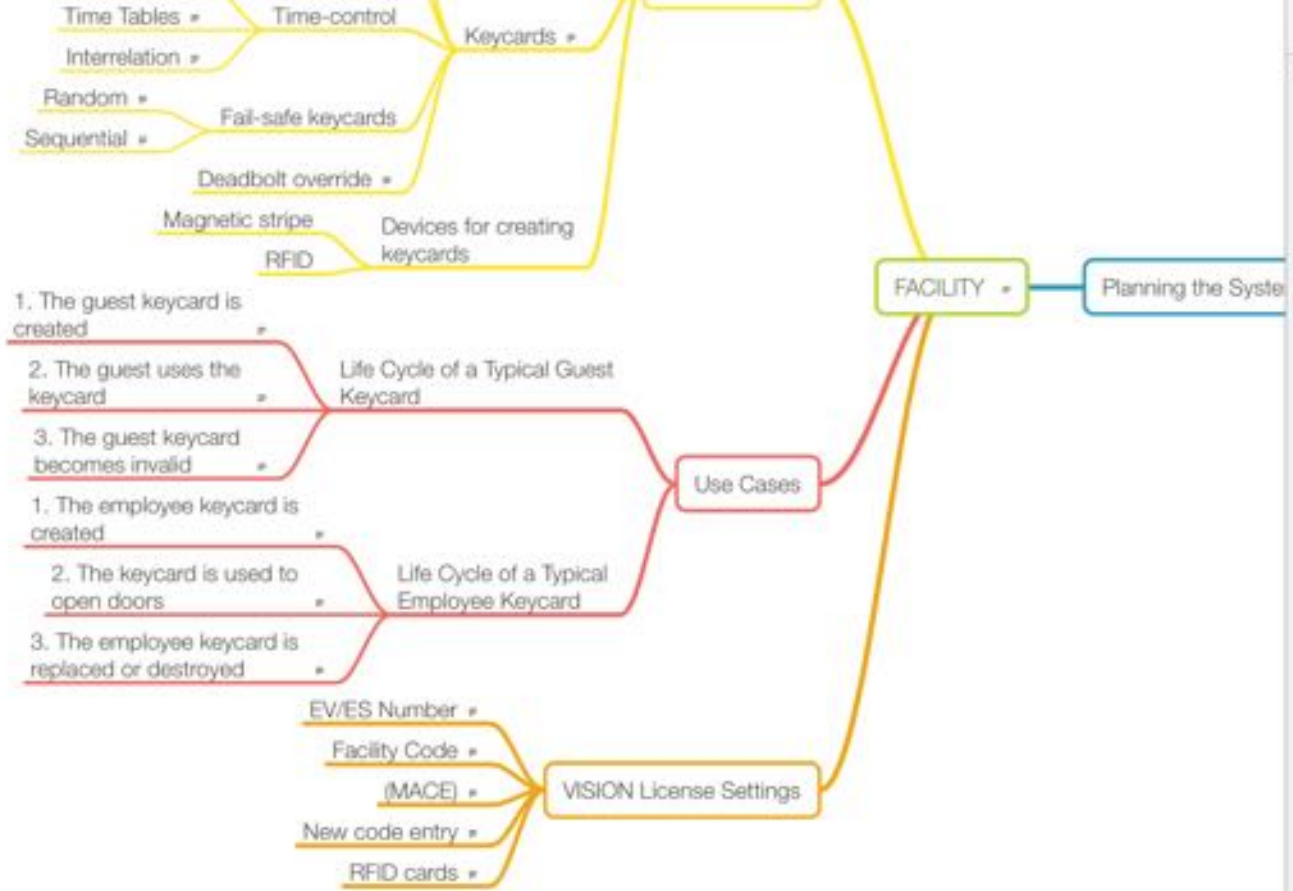
Leszek Bartczak

VISION Version 6.0

THE PLAN

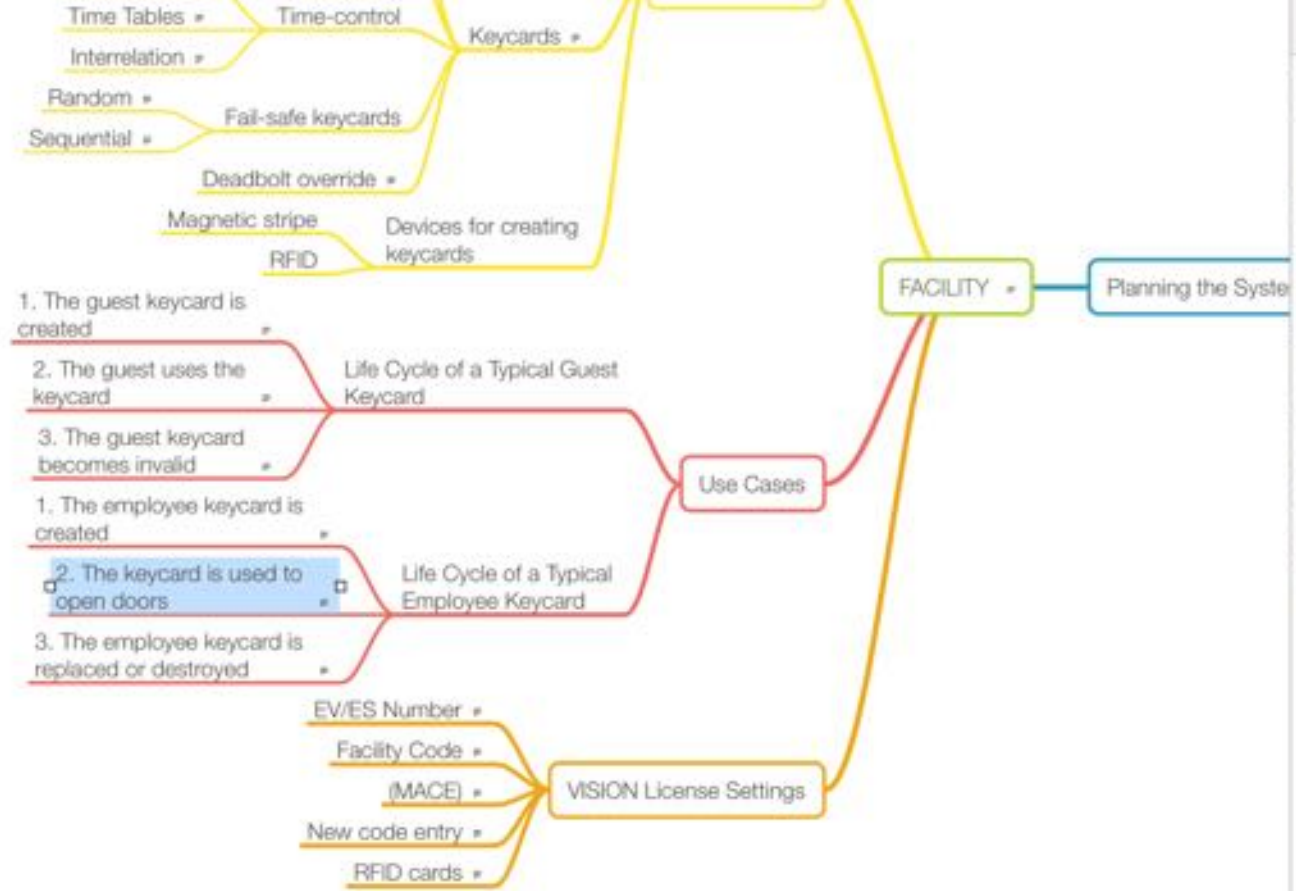
- Acquire a copy of Vision software
- ~~Read and understand the product manuals~~
- **Read, understand and document 500+ pages of manuals**
- Reverse engineer the software and find a clever way to open the lock without access to the original key
- Pose like a boss


FACILITY
Physical Items
Locks
Classic 2*103 (magnetic stripe)
Signature (magnetic stripe)
Programming cards
LockLink
Lock Readout
Unlocking Devices
Keycards
Unique User Identification
User Groups
Time-control
Time window
Time Tables
Interrelation
Fail-safe keycards
Random
Sequential
Deadbolt override
Devices for creating keycards
Magnetic stripe
RFID
Use Cases
Life Cycle of a Typical Guest Keycard
1. The guest keycard is created
2. The guest uses the keycard
3. The guest keycard becomes invalid
Life Cycle of a Typical Employee Keycard
1. The employee keycard is created
2. The keycard is used to open doors
3. The employee keycard is replaced or destroyed
VISION License Settings
EU-ES Number
Facility Code
IMAGE
New code entry
RFID cards
Planning the System
Time Table Worksheet
All
8-16
11-24
etc.
Common Door Worksheet
Planning
Fitness center
Backdoor
VingCard Sofo
Lift
etc.
Keycard Type Worksheet
Keycard Type
Locks included (Access Area)
Lock Group
Guest room
Guest suite
Employee room
Employee section
Override Criterion
Issue Time (IT)
Start Time (ST)
Interrelation
to itself
to Others
User Group Worksheet
User Group Name
Keycard Type and Access Area
Deadbolt Override
Time Table
Duration
Card Family
Common Doors (and Corresponding Time Tables)
System Parameters Worksheet
Lock Parameters
Lock ID
Lock Group
Lock Type
Lock Mirror Type
Open Pulse Width
Pin Keypad
Unlock Time
Lock Mode
Passage Mode
Normal Mode
Escape Return Mode (Normal)
Log Invalid Keycards
Internal Control Mode
System Parameters
Default Check-in Time/ Check-out Time
Default Length of Stay
Default User Group
Default Section (Keycard Type)
Issue Area Code
Inhibit Override
Daylight Saving Time/Daylight Saving Time Dates
Workstation and Encoder Time Outs
Deadbolt Override menu option
Subtract hours
Software Access Groups Worksheet
Access to Modules
Ability to Encode Employee Keycards



NOTES

Select a node to add notes



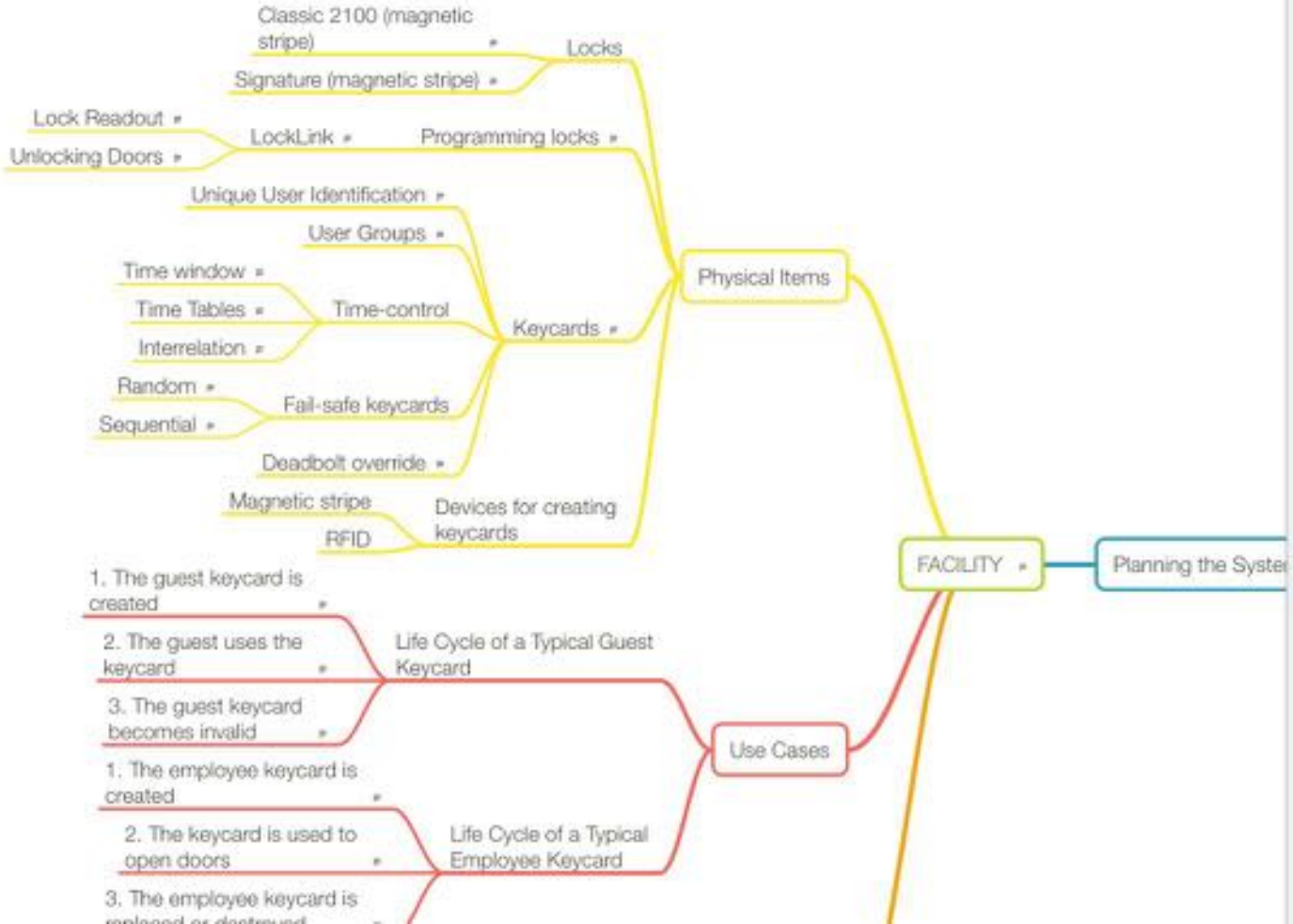
NOTES

When an employee keycard is inserted in a door, the door opens if the following conditions are met:

* The User Group on the keycard is valid for this lock. For example, a maid might have access only to guest rooms on a particular floor.

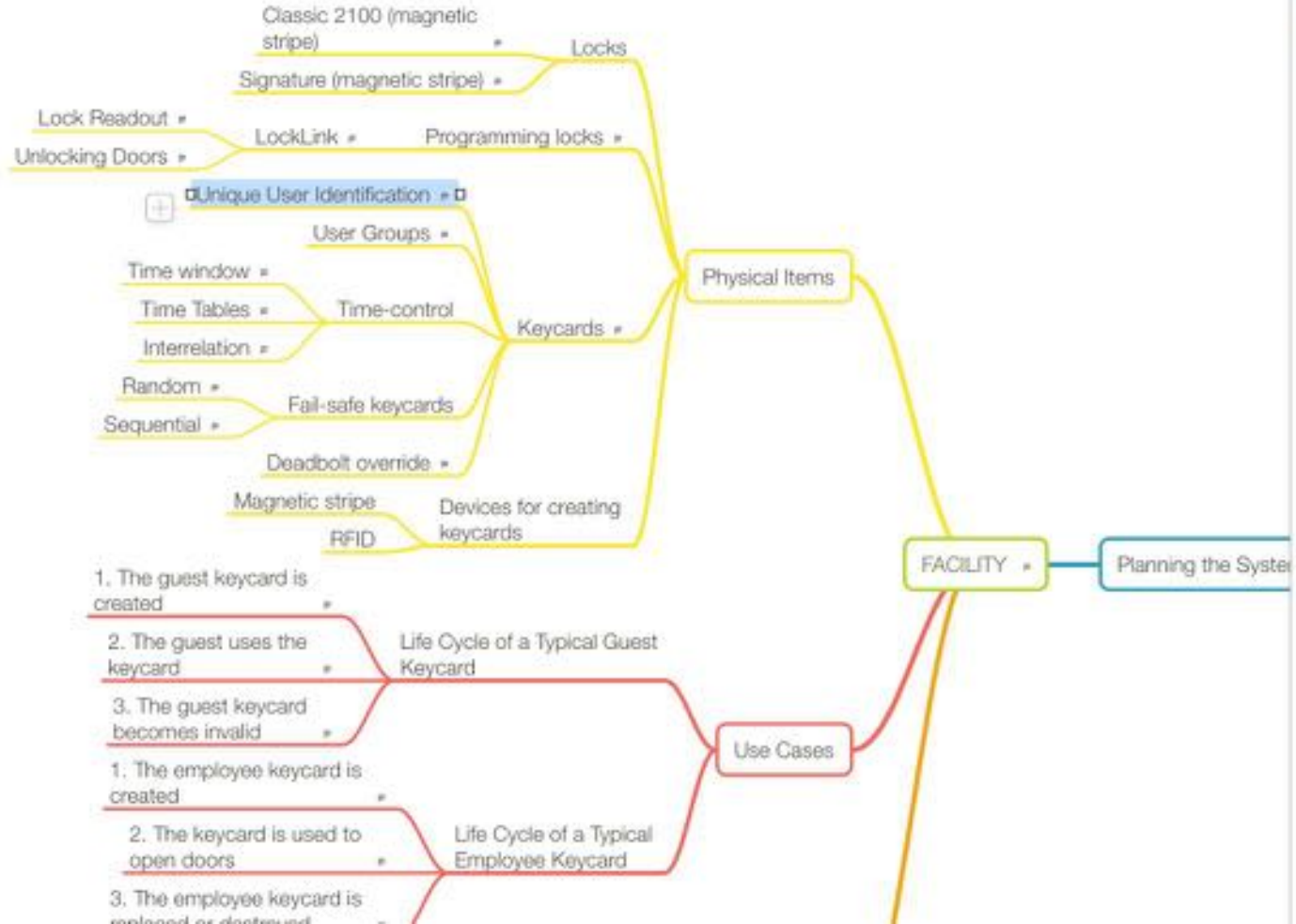
* The keycard has not expired based on the current date and time as set in the lock

* No special instructions have been given to the lock by a Void-list keycard, which prevents access by this keycard. This last situation is not very common and hotels normally only use this if an employee keycard is lost or if an employee is no longer employed by the hotel, but has not turned in his employee keycard.



NOTES

Select a node to add notes



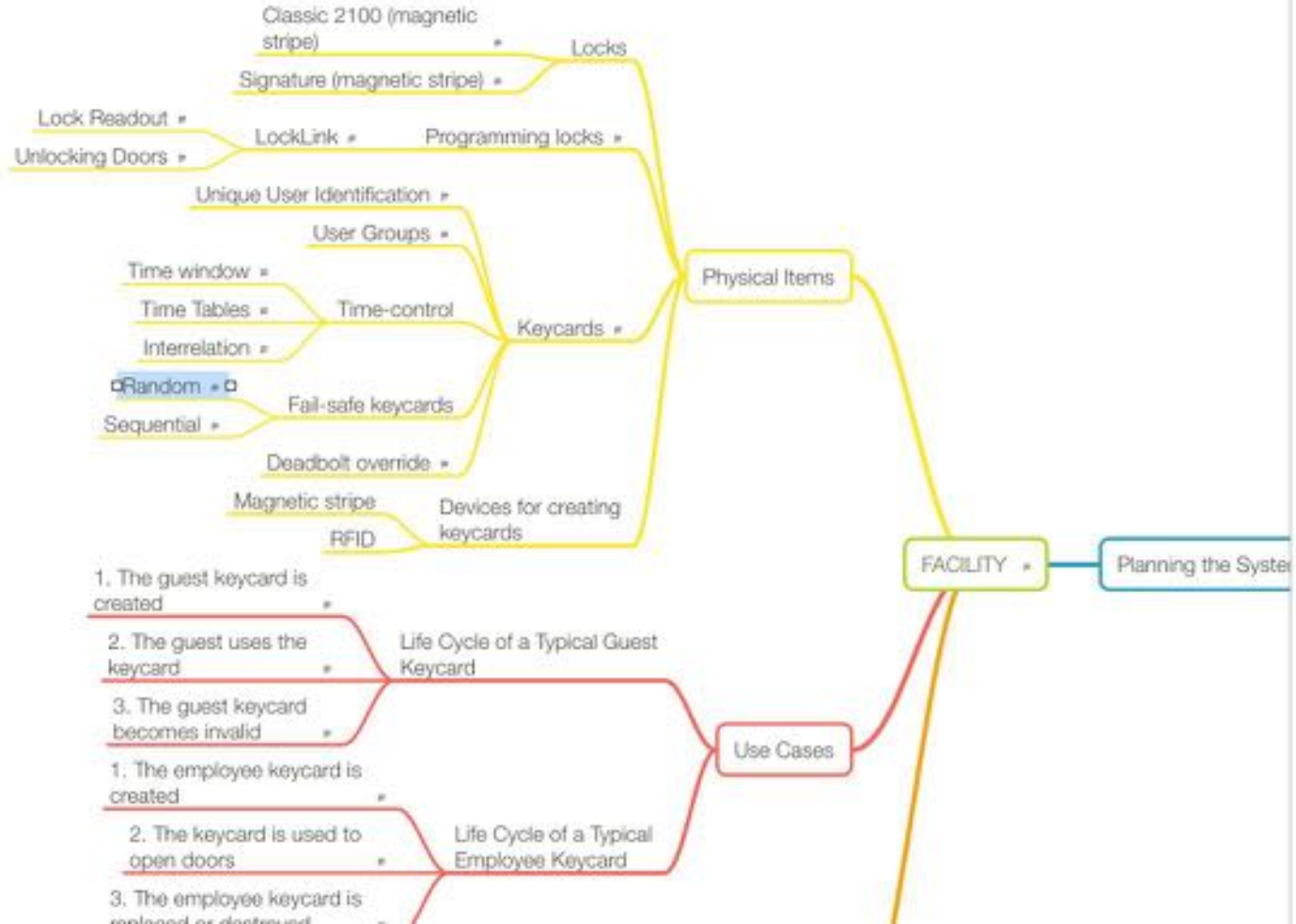
NOTES

Every issued keycard contains a Unique User ID code.

This user ID code can be used to identify hotel employees in their use of the locks.

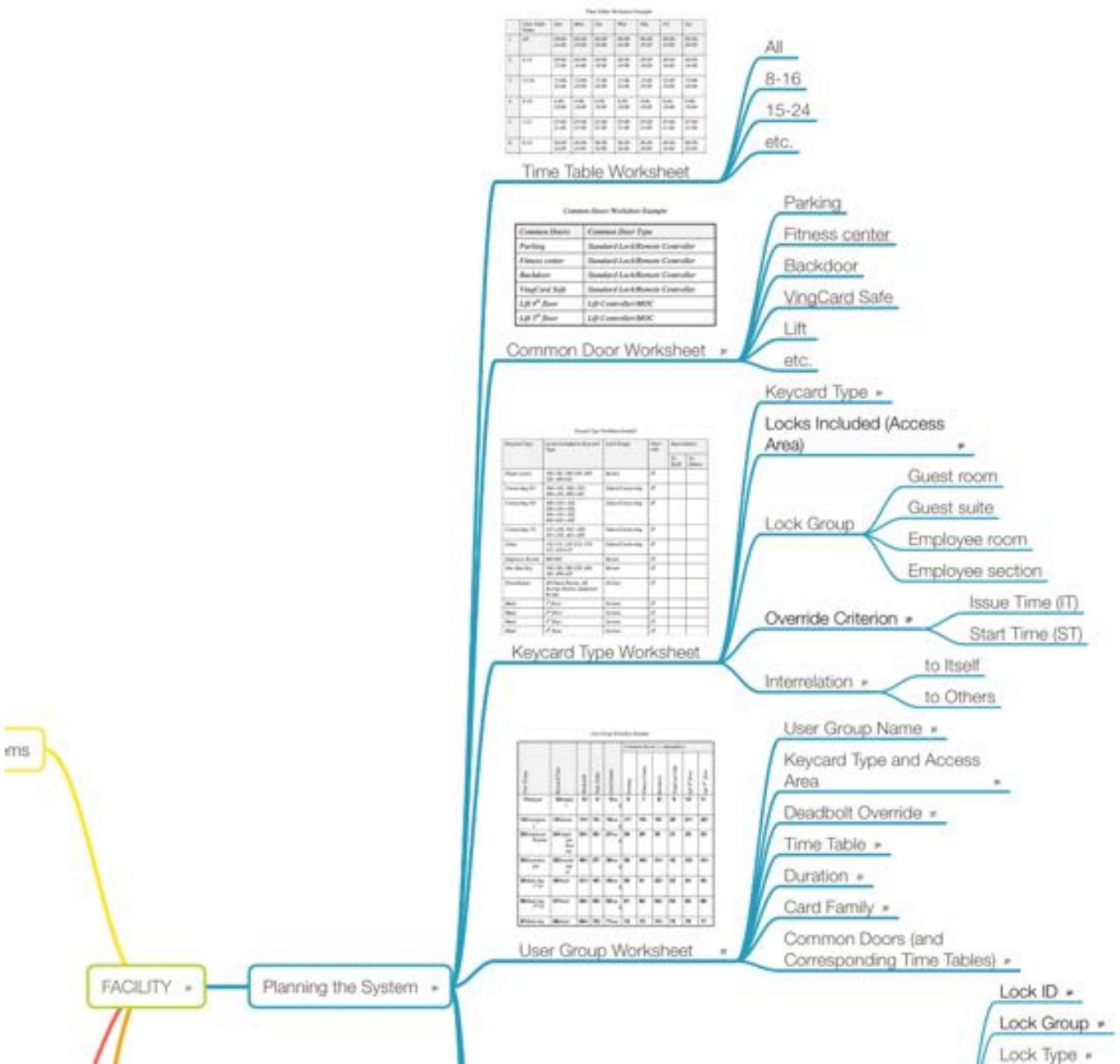
The code will also make it possible to distinguish between different current hotel guests – even those sharing a room. This means that keycards can be individually changed or replaced with no knock on effect on other keycard holders.

The VISION database contains names and cross-references to the user IDs. For employees, the name is used as identification both in keycard issuing and event reporting.



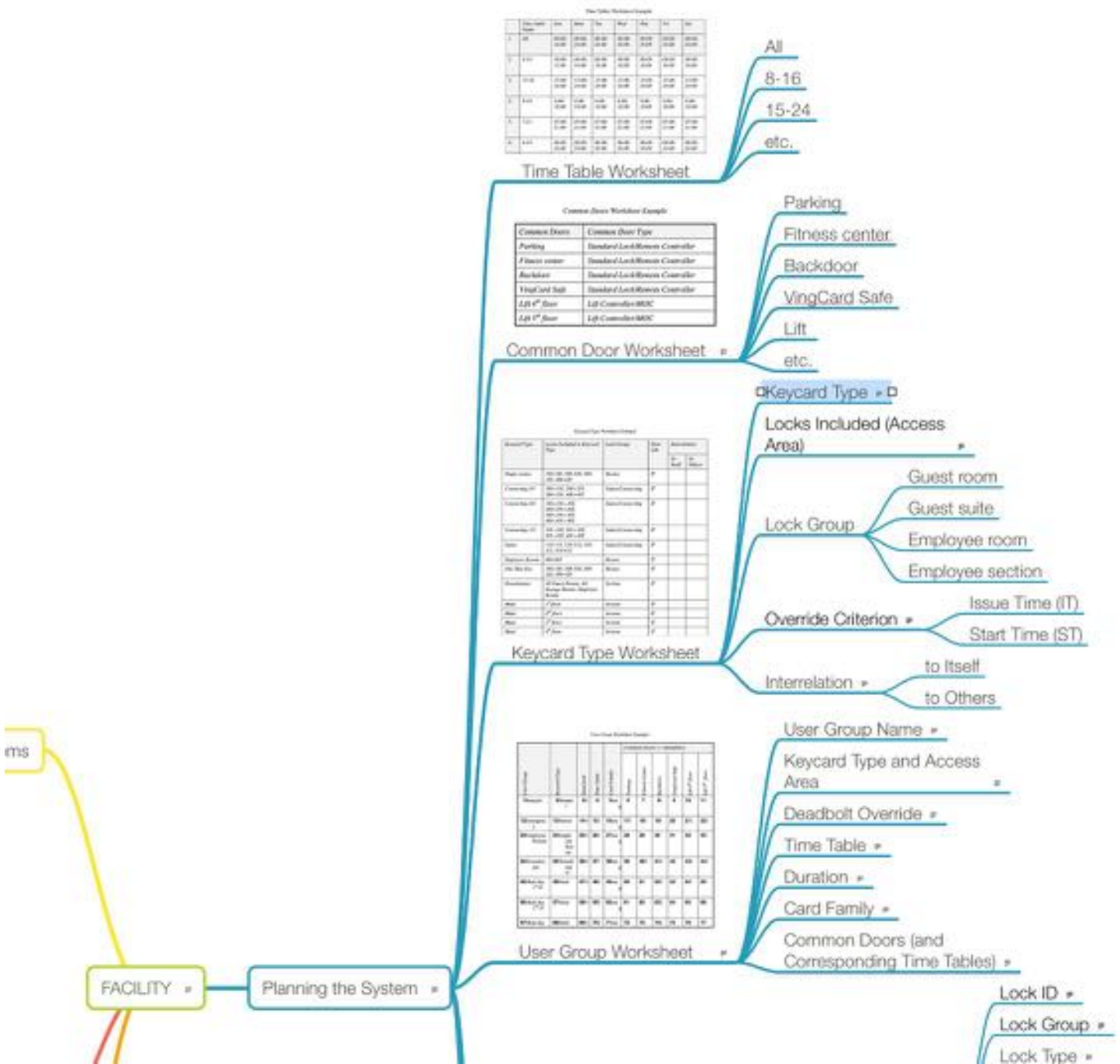
NOTES

This method creates Fail-safe keycards that can be used for ANY door. However, when the guest checks in, you will need to use a Fail-safe Programming Key and then a Fail-safe keycard on the door before giving the Fail-safe keycard to a guest.



NOTES

Select a node to add notes

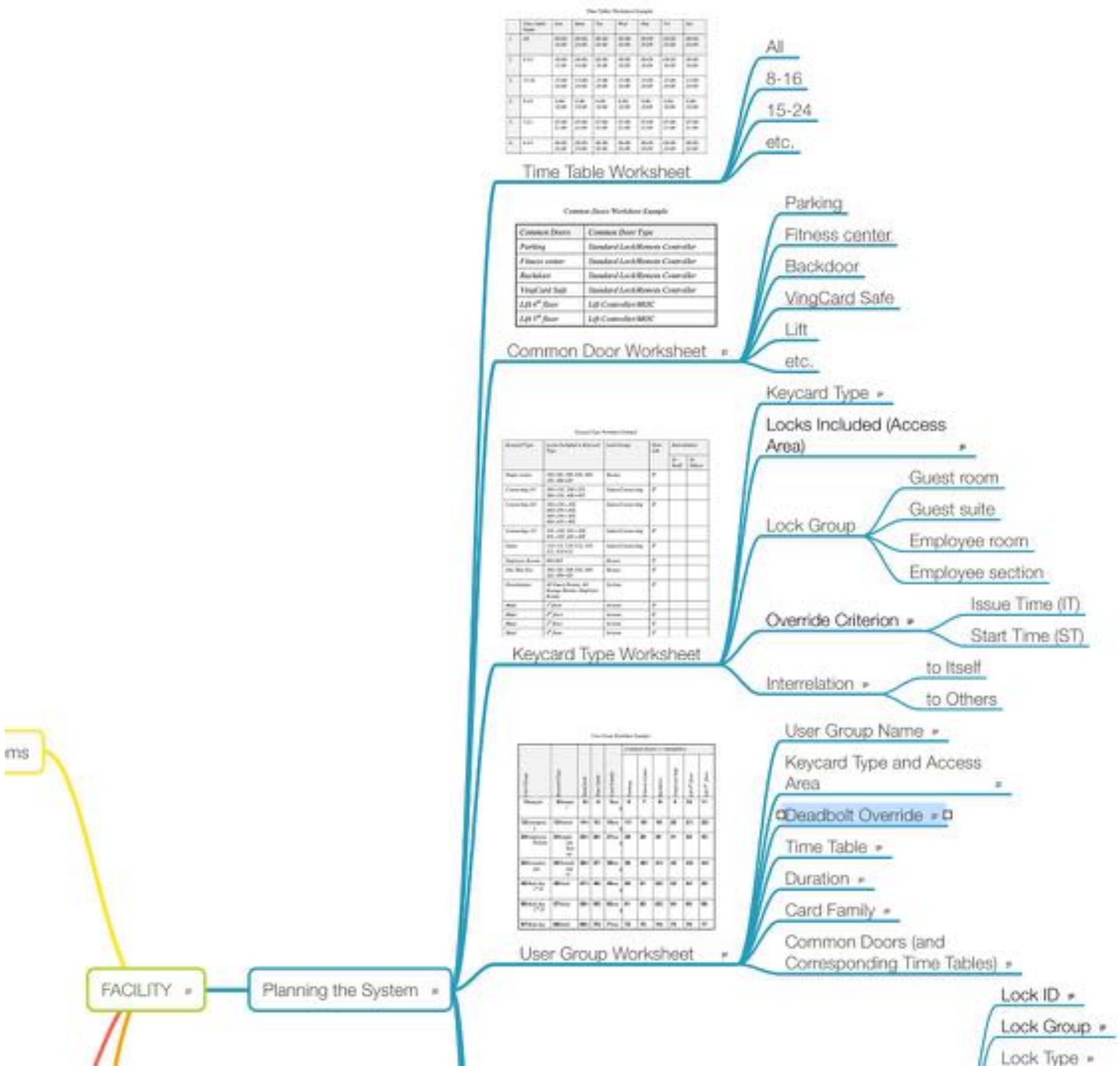


NOTES

You can have up to 30 different Keycard Types.

Typical employee Keycard Types:
* Maid
* Housekeeper
* Room Service etc.,

but guests may also be divided into Keycard Types such as Suite guest, Regular guest etc.

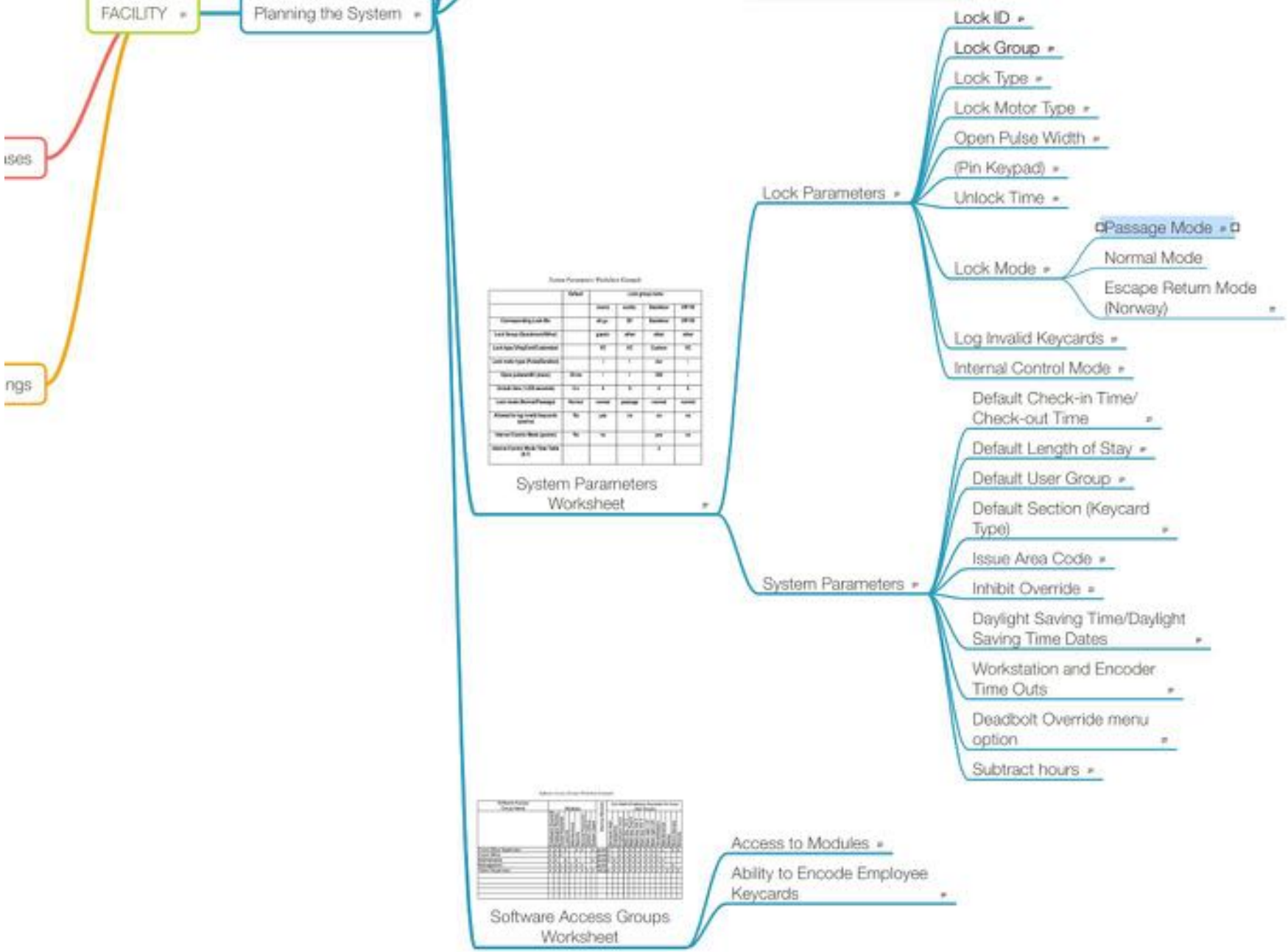


NOTES

Use this column to denote whether or not the User Group should have a default Deadbolt Override.

NOTE: Deadbolt Override allows a door to be opened even when the deadbolt is thrown, so you will normally not want most User Groups to have this type of access.

TIP: It is not necessary to specify Deadbolt Override capabilities for guest keycards or employee room keycards. The setting for whether Deadbolt Override will be an option when issuing keycards is specified in the System Parameters settings. It is set for all guest and all employee room keycards.



NOTES

Using a Passage-mode keycard on a door does not actually lock or unlock it, but causes the door to enter Passage Mode. In this mode, the next time the door is opened with a valid keycard it will remain unlocked until a valid keycard is used again to lock it.

The lock will remain in passage mode, switching between locked and unlocked with every valid keycard insertion, until the Passage-mode keycard is used again Then, the door reverts to normal behaviour - the next time the door is opened with a valid keycard it will NOT remain unlocked.

Passage-mode keycards are not made for a specific door, but can be used on ANY door.

Normally, Passage-Mode keycards are used for situations such as parties in banquet rooms or meetings in conference rooms when you want to allow the door to remain unlocked for a period.

FACILITY

Planning the System

ises

ngs

Lock Parameters

Lock ID

Lock Group

Lock Type

Lock Motor Type

Open Pulse Width

(Pin Keypad)

Unlock Time

Lock Mode

Passage Mode

Normal Mode

Escape Return Mode (Norway)

Log Invalid Keycards

Internal Control Mode

System Parameters Worksheet

System Parameters

Default Check-in Time/ Check-out Time

Default Length of Stay

Default User Group

Default Section (Keycard Type)

Issue Area Code

Inhibit Override

Daylight Saving Time/Daylight Saving Time Dates

Workstation and Encoder Time Outs

Deadbolt Override menu option

Subtract hours

Software Access Groups Worksheet

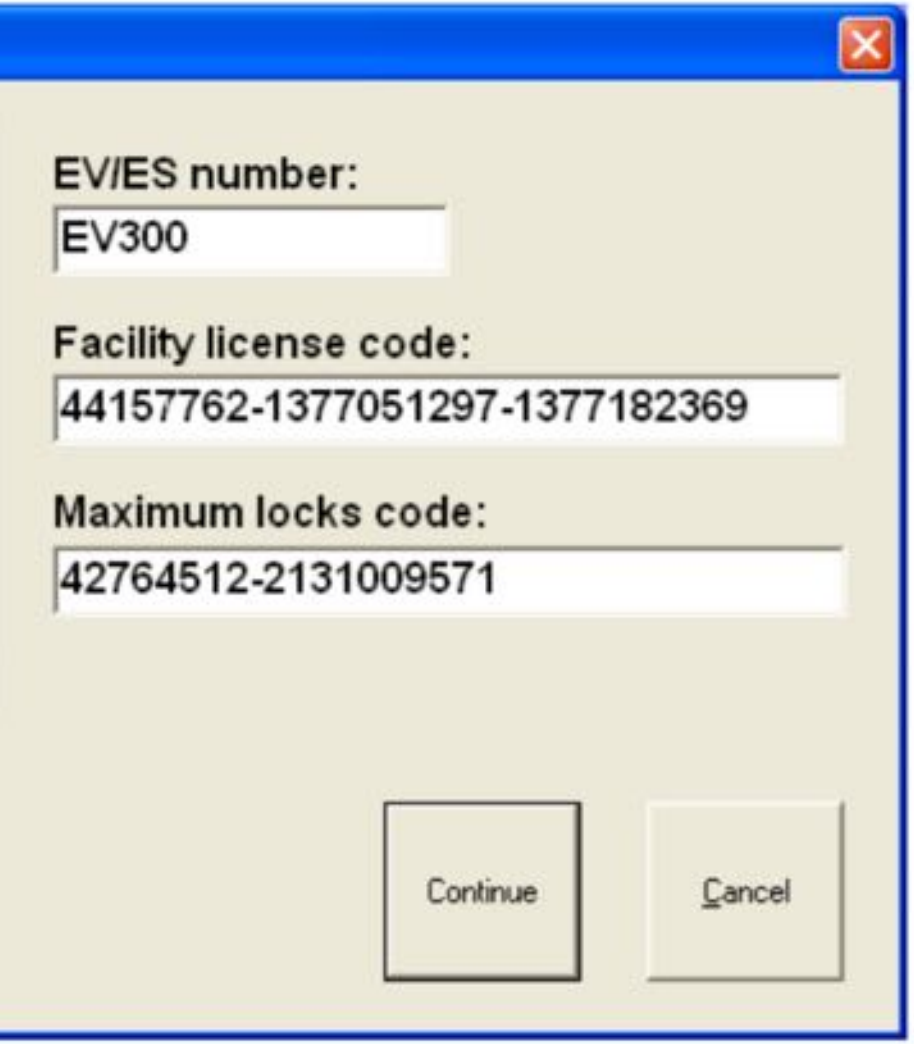
Access to Modules

Ability to Encode Employee Keycards

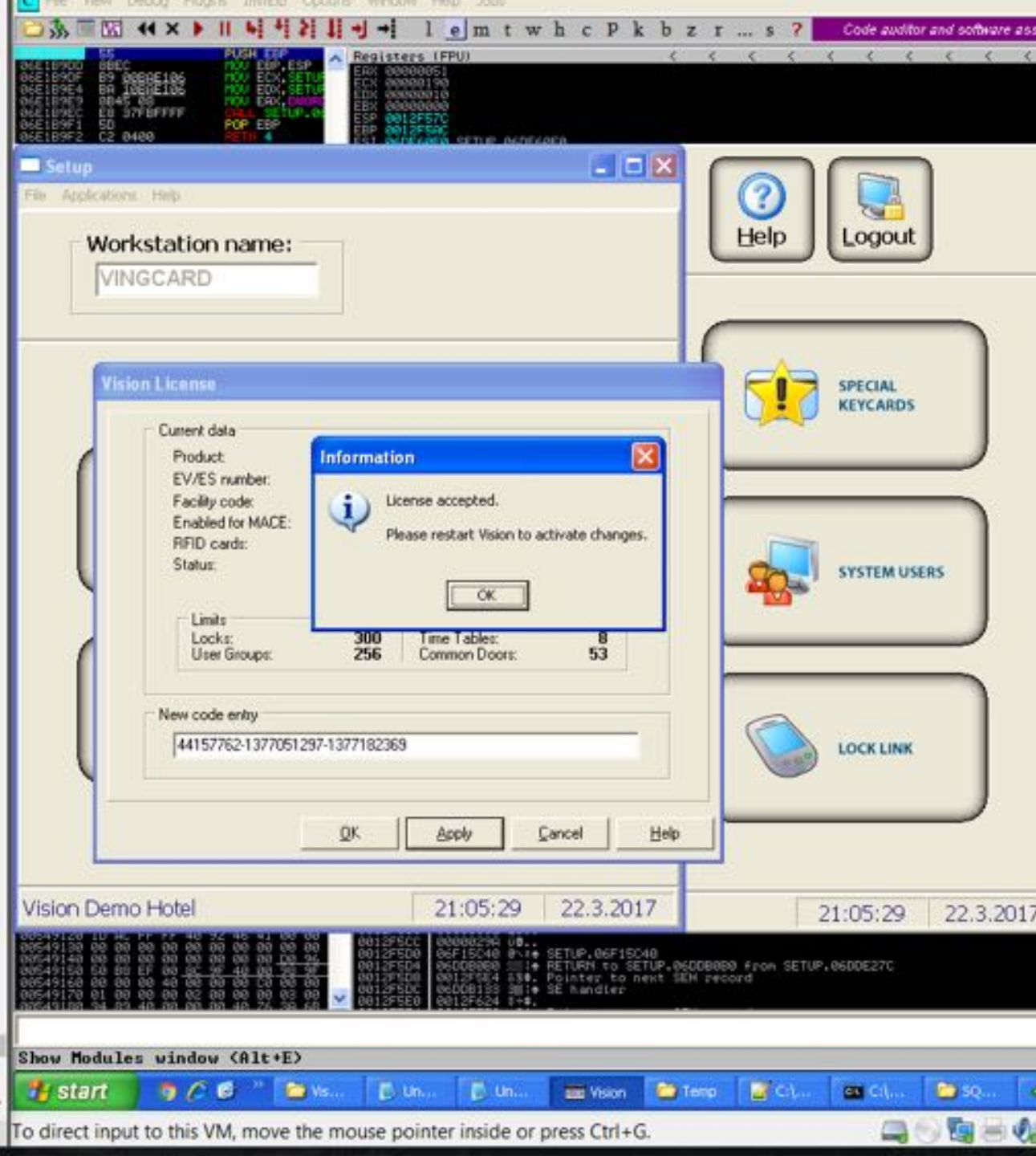
NOTES

In addition to specifying which modules a Software Access Group can access, you can also determine which User Groups the Software Access Group can encode keycards for.

When employees choose Add or Change in the Employee Keycards module, the only employee names that will be listed are those that match the User Groups for the operator's Software Access Group.



be prompted to add additional d
can install an empty, ready to us
existing database. You will alsc

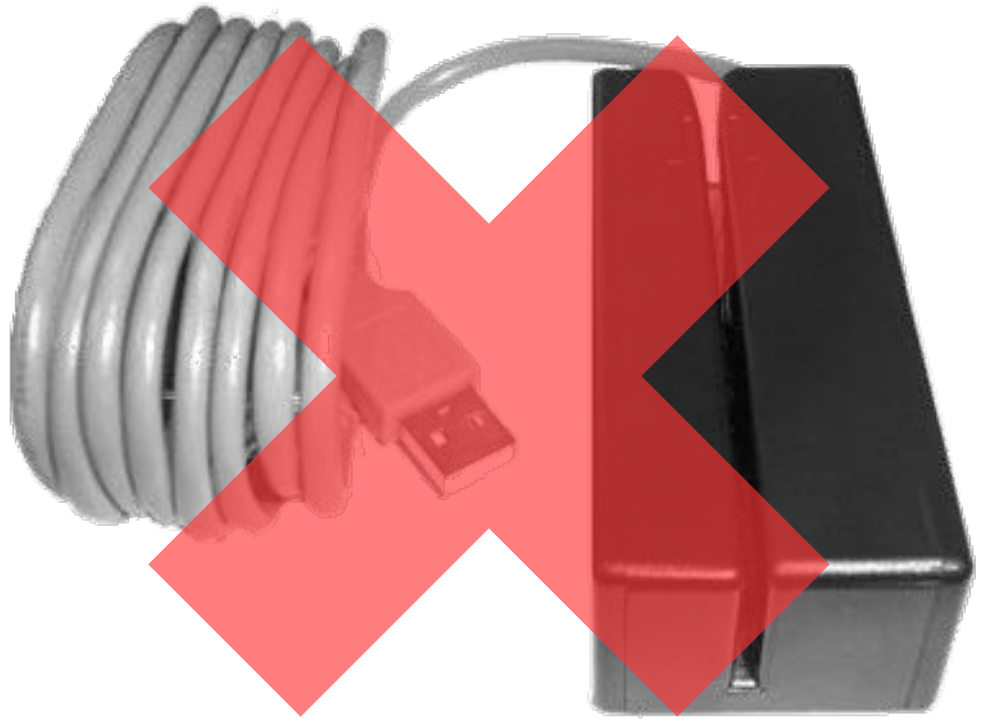


THE PLAN

- Acquire a copy of Vision software
- Read, understand and document 500+ pages of manuals
- **Build a hotel**
- Reverse engineer the software and find a clever way to open the lock without access to the original key
- Pose like a boss

THE PLAN

- Acquire a copy of Vision software
- Read, understand and document 500+ pages of manuals
- ~~Build a hotel~~ **Build a lab**
- Reverse engineer the software and find a clever way to open the lock without access to the original key
- Pose like a boss



Magnetic Stripe Card Encoder

EST-4938 Multitrack

An accurate and efficient keycard encoder for effective hotel front desk operations. This encoder is designed with curved lines to meet the latest design trends.

Magnetic Stripe Card Encoder

EST-4938 Multitrack

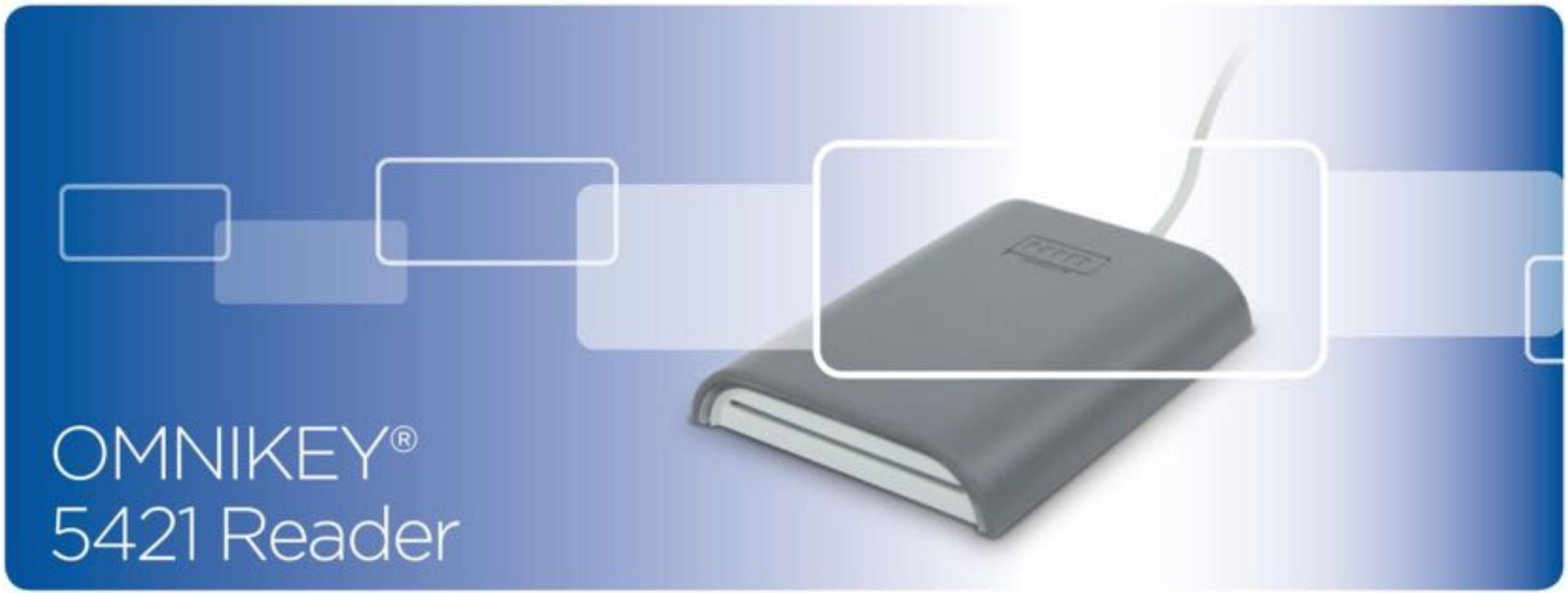
An accurate and efficient keycard encoder for effective hotel front desk operations. This encoder is designed with curved lines to meet the latest design trends.

THE PLAN

- Acquire a copy of Vision software
- Read, understand and document 500+ pages of manuals
- ~~Build a lab~~ **Build a lab with RFID reader**
- Reverse engineer the software and find a clever way to open the lock without access to the original key
- Pose like a boss

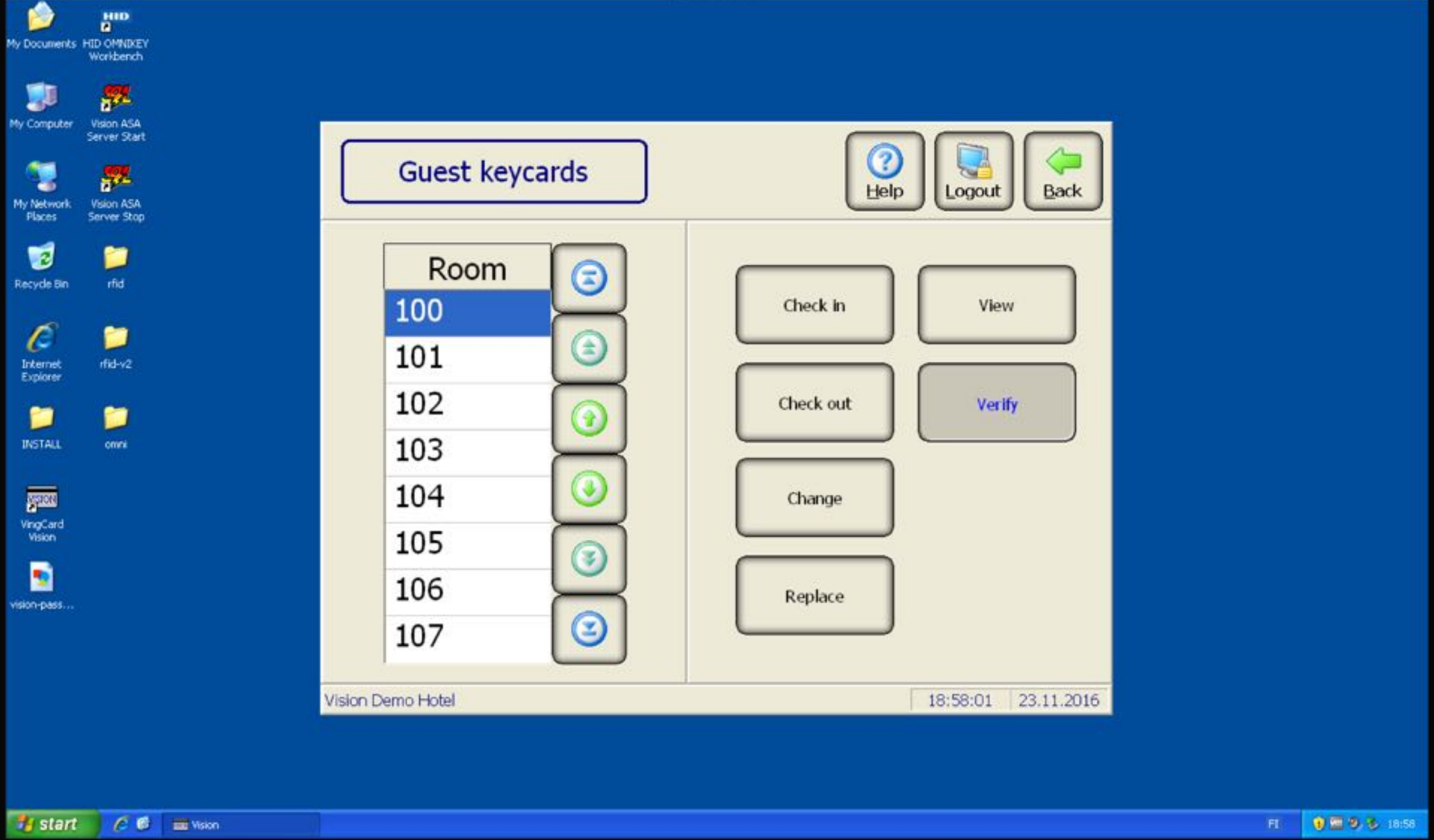
LOGICAL ACCESS SOLUTIONS

HID



F-Secure

20+ HOURS LATER …


My Documents
HID OMNIKEY Workbench
My Computer
Vision ASA Server Start
My Network Places
Vision ASA Server Stop
Recycle Bin
rfid
Internet Explorer
rfid-v2
INSTALL
omni
VingCard Vision
vision-pass...
Guest keycards
Help
Logout
Back
Room
100
101
102
103
104
105
106
107
Check in
View
Check out
Verify
Change
Replace
Vision Demo Hotel
18:58:01
23.11.2016
start
Vision
FI
18:58


My Documents
HID OMNIKEY Workbench
My Computer
Vision ASA Server Start
My Network Places
Vision ASA Server Stop
Recycle Bin
rfid
Internet Explorer
rfid-v2
INSTALL
omni
VingCard Vision
vision-pass...
Verify guest card
Verify
Help
Logout
Back
Main
Name
Result
Custom
More Data
Room
100
From date/time
23.11.2016
17:30
Until date/time
25.11.2016
14:00
User group
Regular Guest
Common doors
Yes
Info
Keycard for
Single Room
Issue area
1
User ID
1
Result
Valid keycard.
Not in database.
Vision Demo Hotel
18:58:12
23.11.2016
start
Vision
FI
18:58

THE PLAN

- Acquire a copy of Vision software
- Read, understand and document 500+ pages of manuals
- Build a lab with RFID reader
- **Acquire working knowledge of RFID**
- Reverse engineer the software and find a clever way to open the lock without access to the original key
- Pose like a boss

INTERNATIONAL STANDARD

ISO/IEC 14443-2

Identification integrated cir cards —

Part 2:
Radio freque

Cartes d'identification Cartes de proximité —

Partie 2: Puissance de

INTERNATIONAL STANDARD

ISO/IEC 14443-3

Identification integrated cir cards —

Part 3:
Initialization a

Cartes d'identification Cartes de proximité —

Partie 3: Initialisation et

MF0ULx1

MIFARE Ultralight EV1 - Contactless ticket IC

Rev. 3.1 — 30 June 2014
234531

Product data sheet
COMPANY PUBLIC

1. General description

NXP Semiconductors developed t
contactless smart ticket, smart car
Device (PCD). The MF0ULx1 is de
environment (see Ref. 1). The targ
in public transportation networks, l
serves as a replacement for conve
magnetic stripe tickets or coins. It
card families such as MIFARE DE

The MIFARE Ultralight EV1 is succ
functional backwards compatible.
efficient implementations and offer

The mechanical and electrical spe
meet the requirements of inlay and

1.1 Contactless energy and da

In a contactless system, the MF0U
MF0ULx1 fits the TFC.0 (Edmonds
Ref. 8.

The MF0ULx1 chip, which is availa
supports both TFC.1 and TFC.0 ti

1.2 Anticollision

An intelligent anticollision function
simultaneously. The anticollision a
the execution of a transaction with
interference from another card in t

MF0ICU1

MIFARE Ultralight contactless single-ticket IC

Rev. 3.9 — 23 July 2014
028639

Product data sheet
COMPANY PUBLIC

1. General description

The MIFARE MF0ICU1 has been developed by NXP Semiconductors to be used in a contactless smart ticket or smart card in combination with a Proximity Coupling Devices (PCD) in accordance with ISO/IEC 14443 A (see Ref. 1). It is intended for use as single trip or limited use tickets in public transportation networks, loyalty cards or day passes for events as a replacement for conventional ticketing solutions such as paper tickets, magnetic stripe tickets or coins.

As the usage of contactless proximity smart cards becomes more and more common, transport and event operators are switching to completely contactless solutions. The introduction of the MIFARE Ultralight for limited use tickets may lead to a reduction of system installation and maintenance costs. Terminals may be less vulnerable to damage and mechanical failures caused by ticket jams. MF0ICU1 can easily be integrated into existing schemes and even standard paper ticket vending equipment can be upgraded. This solution for low cost tickets can help operators to reduce the circulation of cash within the system.

The mechanical and electronical specifications of MIFARE Ultralight are tailored to meet the requirements of paper ticket manufacturers.

1.1 Contactless energy and data transfer

In the MIFARE system, the MF0ICU1 is connected to a coil with a few turns. The MF0ICU1 fits the TFC.0 (Edmondson) and TFC.1 (ISO) ticket formats as defined in BS EN753-2.


VingCard
Hold the card in close proximity to the door lock.
www.vingcard.com • www.elsafe.com

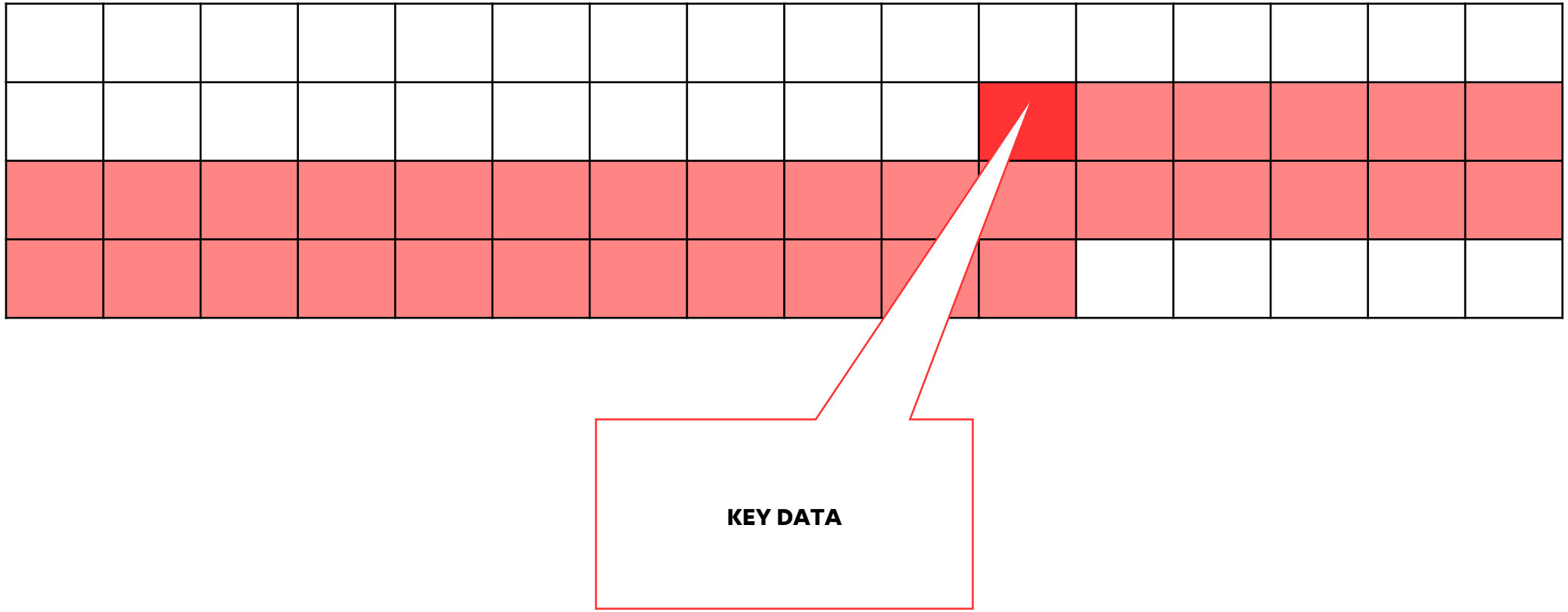
ULTRALIGHT

ULTRALIGHT EV1

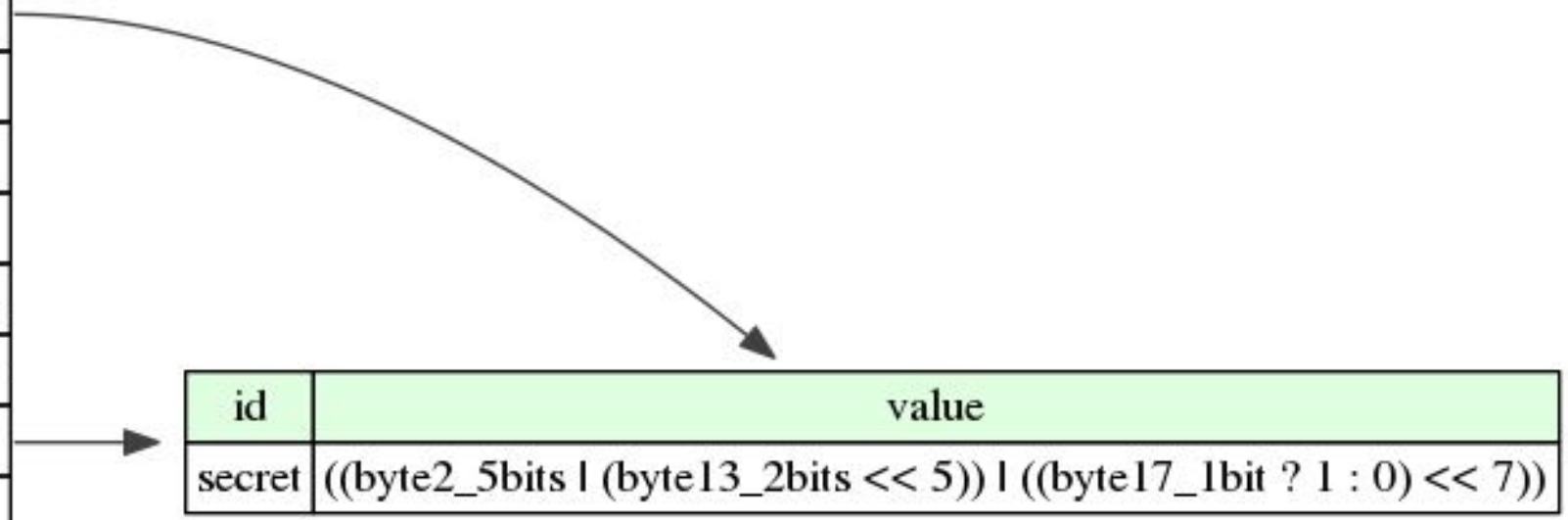
THE PLAN

- Acquire a copy of Vision software
- Read, understand and document 500+ pages of manuals
- Build a lab with RFID reader
- Acquire working knowledge of RFID
- **Reverse engineer the software and find a clever way to open the lock without access to the original key**
- Pose like a boss

KEY DATA ILLUSTRATED V1

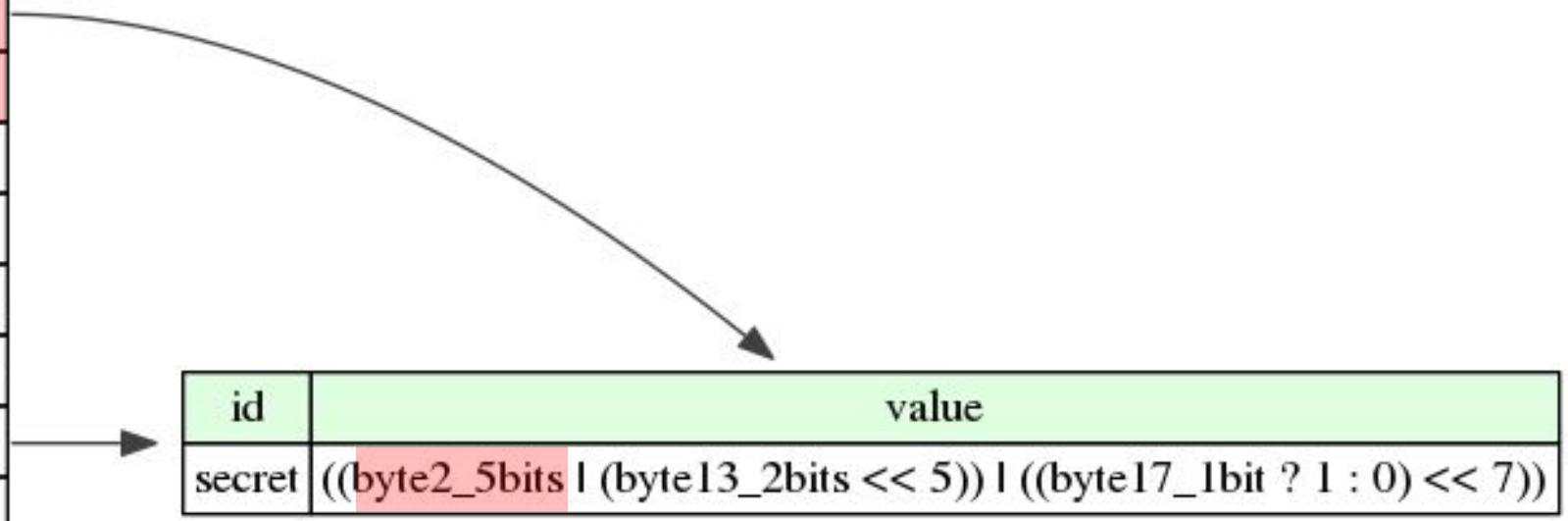


pos	size	type	id
0	1		byte1
1	2b	b2	byte2_field1
1:2	5b	b5	byte2_5bits
1:7	1b	BitsType1	byte2_field3
2	10		bytes3_12
12	2b	b2	byte13_field1
12:2	2b	b2	byte13_field2
12:4	2b	b2	byte13_field3
12:6	2b	b2	byte13_2bits
13	3		bytes14_16
16	6b	b6	byte17_field1
16:6	1b	BitsType1	byte17_1bit
16:7	1b	BitsType1	byte17_field2
17	16		bytes18_33



id	value
secret	((byte2_5bits | (byte13_2bits << 5)) | ((byte17_1bit ? 1 : 0) << 7))

pos	size	type	id
0	1		byte1
1	2b	b2	byte2_field1
1:2	5b	b5	byte2_5bits
1:7	1b	BitsType1	byte2_field3
2	10		bytes3_12
12	2b	b2	byte13_field1
12:2	2b	b2	byte13_field2
12:4	2b	b2	byte13_field3
12:6	2b	b2	byte13_2bits
13	3		bytes14_16
16	6b	b6	byte17_field1
16:6	1b	BitsType1	byte17_1bit
16:7	1b	BitsType1	byte17_field2
17	16		bytes18_33



id	value
secret	((byte2_5bits | (byte13_2bits << 5)) | ((byte17_1bit ? 1 : 0) << 7))

Kaitai Struct

A new way to develop parsers for binary structures.

Declarative: describe the very structure of the data, not how you read or write it

Language-neutral: write once, use in all supported languages:

- C++/STL
- C#
- Go (*)
- Java
- JavaScript
- Lua
- Perl
- PHP
- Python
- Ruby

0.8 released 2018-02-05

Download

Packed with tools and samples: includes a compiler, an IDE, a visualizer and library of format specs

Free & open source: feel free to use, modify and join the project

(*) entry-level support

Reading and writing binary formats is hard, especially if it's interchange format that should work across multitude of platforms and languages.

Have you ever found yourself writing repetitive, error-prone and hard-to-debug code that reads binary data structures from file / network stream and somehow represents them in memory for easier access?

Kaitai Struct tries to make this job easier — you only have to describe binary format once and then everybody can use it from their programming languages — cross-language, cross-platform.

```
meta:
  id: tcp_segment
  endian: be
seq:
  - id: src_port
    type: u2
  - id: dst_port
```

```
meta:
  id: vingcard

seq:
  - id: byte1
    size: 1

  - id: byte2_field1
    type: b2
  - id: byte2_5bits
    type: b5
  - id: byte2_field3
    type: b1

...

instances:
  secret:
    value: byte2_5bits | byte13_2bits << 5 | byte17_1bit.to_i << 7

```

Reading and writing binary formats is hard, especially if it's interchange format that should work across multitude of platforms and languages.

Have you ever found yourself writing repetitive, error-prone and hard-to-debug code that reads binary data structures from file / network stream and somehow represents them in memory for easier access?

Kaitai Struct tries to make this job easier — you only have to describe binary format once and then everybody can use it from their programming languages — cross-language, cross-platform.

What is Kaitai Struct?

Kaitai Struct is a declarative language used for describe various binary data structures, laid out in files or in memory: i.e. binary file formats, network stream packet formats, etc.

The main idea is that a particular format is described in Kaitai Struct language (`.ksy` file) and then can be compiled with `ksc` into source files in one of the supported programming languages. These modules will include a generated code for a parser that can read described data structure from a file / stream and give access to it in a nice, easy-to-comprehend API.

Using KS in your project

Typically, using formats described in KS in your project, involves the following steps:

- Describe the format — i.e. create a `.ksy` file
- Use visualizer to debug the format and ensure that it parses data properly
- Compile `.ksy` file into target language source file and include that file into your project
- Add KS runtime library for your particular language into your project (don't worry, it's small and it's there mostly to ensure readability of generated code)
- Use generated class(es) to parse your binary file / stream and access its components

Check out documentation for more information.

```
meta:
  id: tcp_segment
  endian: be
seq:
  - id: src_port
    type: u2
  - id: dst_port
    type: u2
  - id: seq_num
    type: u4
  - id: ack_num
    type: u4
```

```
public class TcpSegment extends KaitaiStruct {
    // ...
    private void _read() throws IOException {
        this.srcPort = _io.readU2be();
        this.dstPort = _io.readU2be();
        this.seqNum = _io.readU4be();
        this.ackNum = _io.readU4be();
    }
    // ...
```

THE QUEST FOR THE MASTER

F-Secure.

UPDATE THE FACILITY CODE ON A MASTER KEY

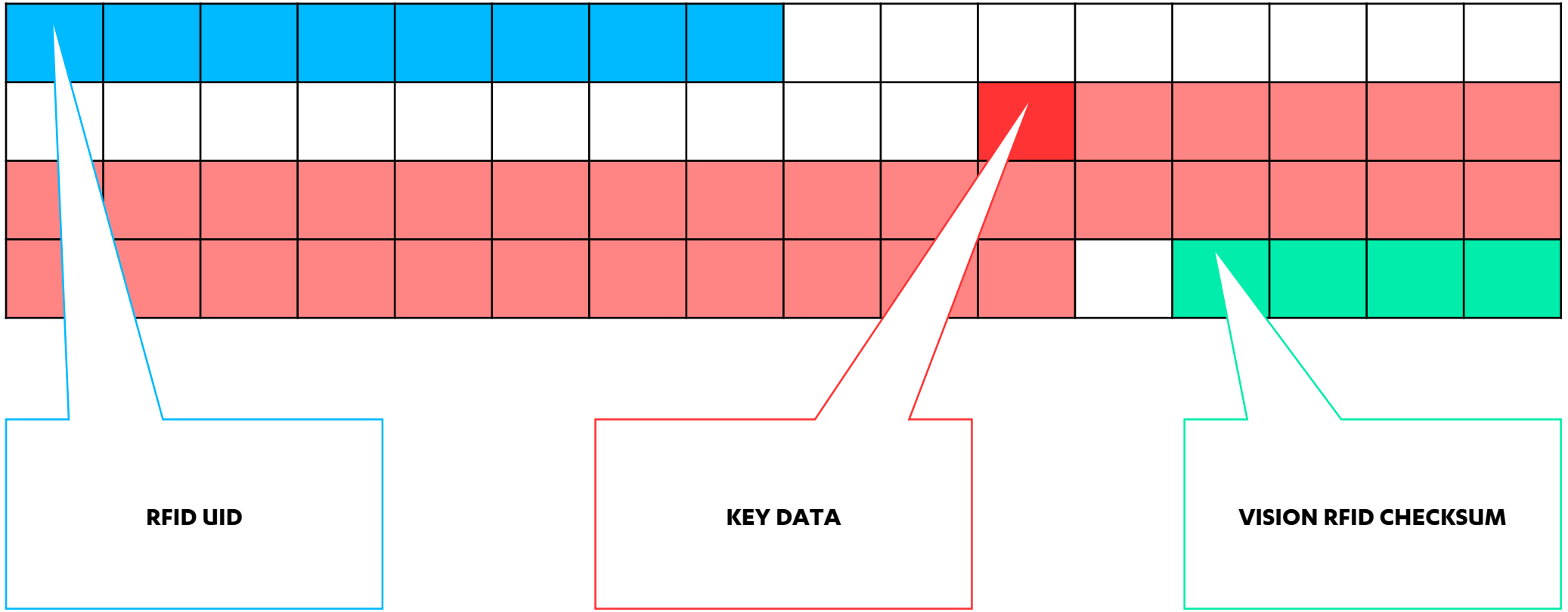
F-Secure.

FAIL

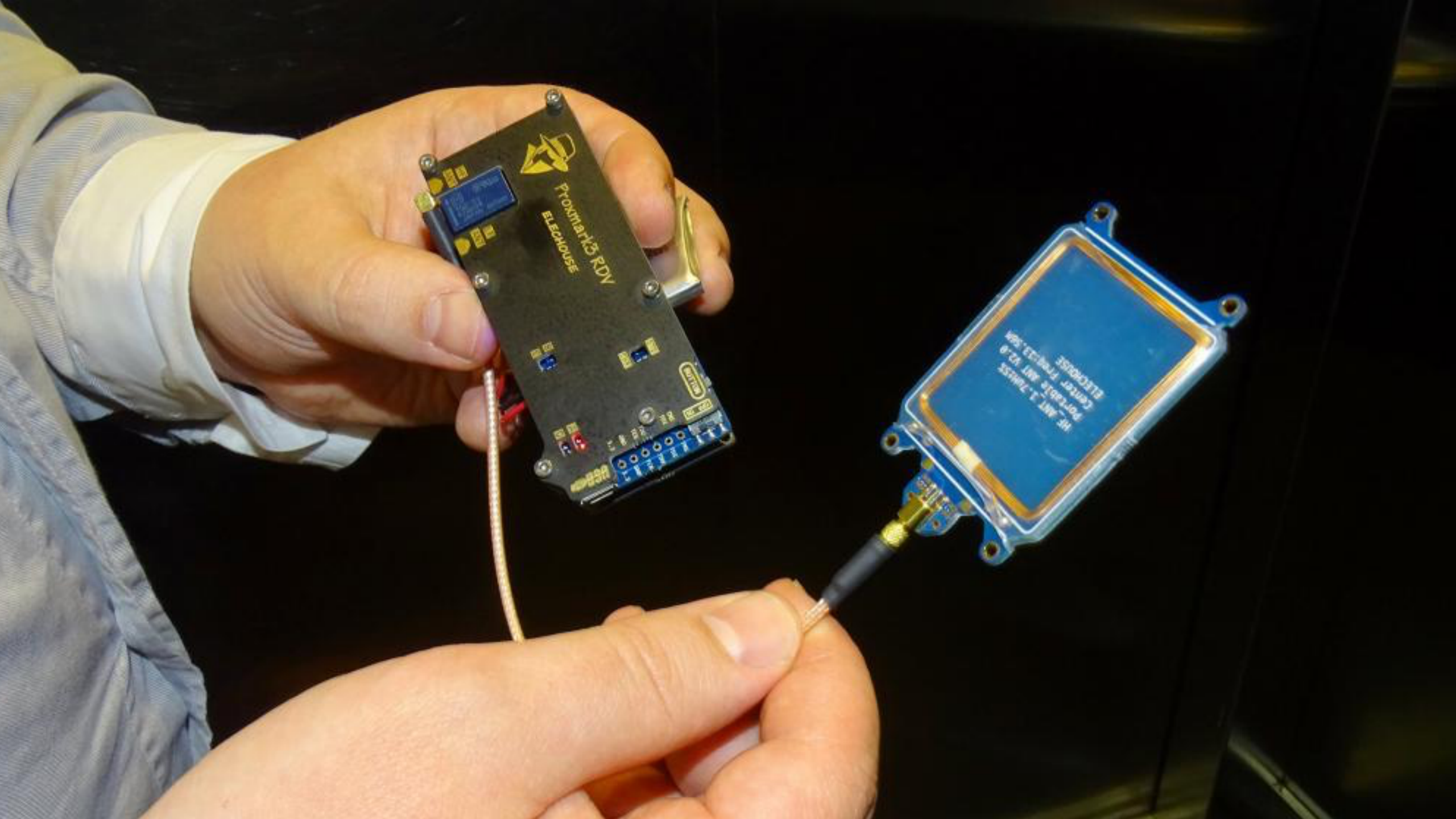
CLONE A KEY

FAIL

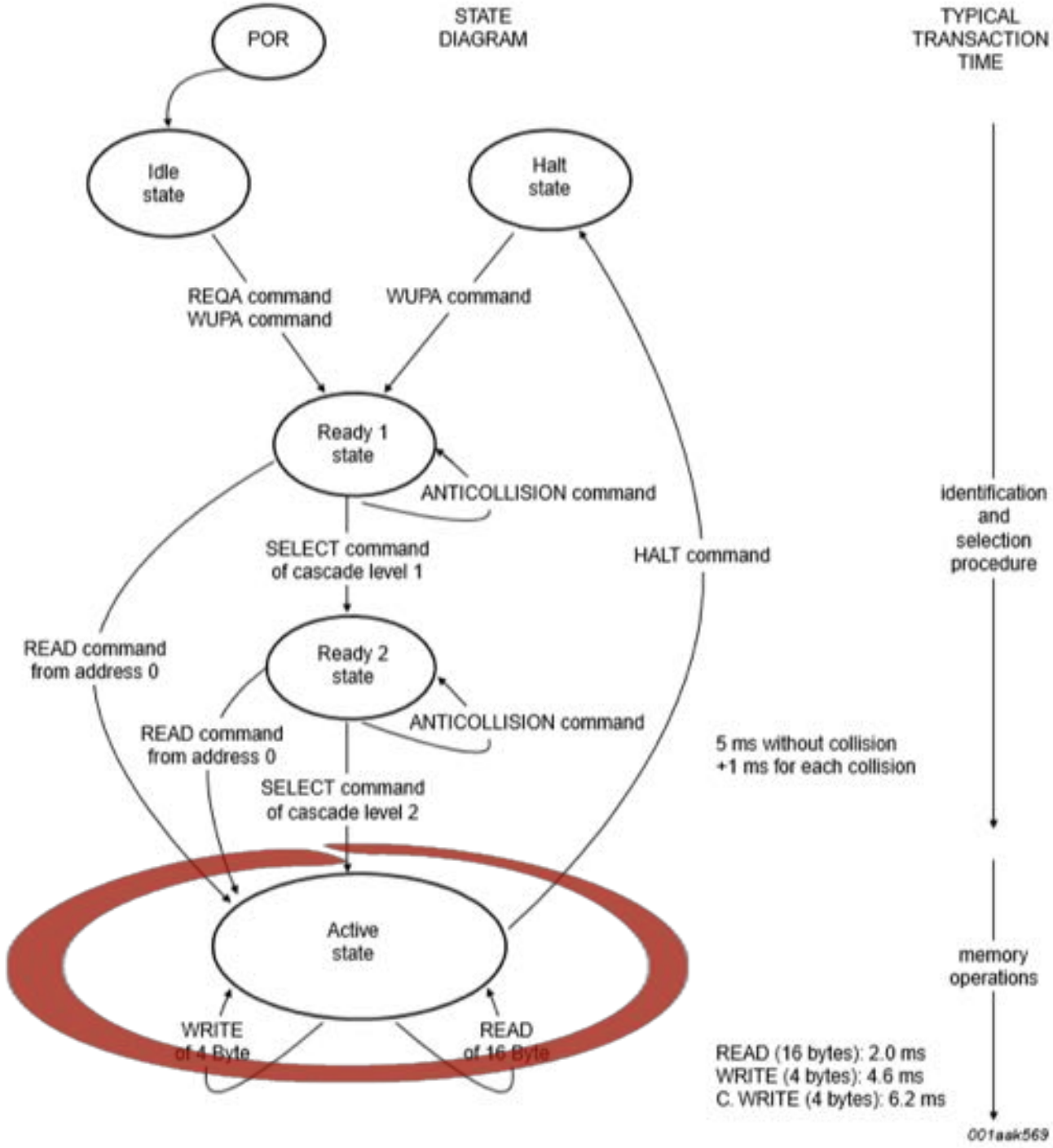
KEY DATA ILLUSTRATED V2



SIMULATE A KEY


Proxmark3 RDV
ELECHOUSE

FAIL


STATE DIAGRAM
TYPICAL TRANSACTION TIME
POR
Idle state
Halt state
REQA command
WUPA command
WUPA command
Ready 1 state
ANTICOLLISION command
SELECT command of cascade level 1
HALT command
READ command from address 0
Ready 2 state
ANTICOLLISION command
READ command from address 0
SELECT command of cascade level 2
Active state
WRITE of 4 Byte
READ of 16 Byte
identification and selection procedure
5 ms without collision
+1 ms for each collision
memory operations
READ (16 bytes): 2.0 ms
WRITE (4 bytes): 4.6 ms
C. WRITE (4 bytes): 6.2 ms
001aak569

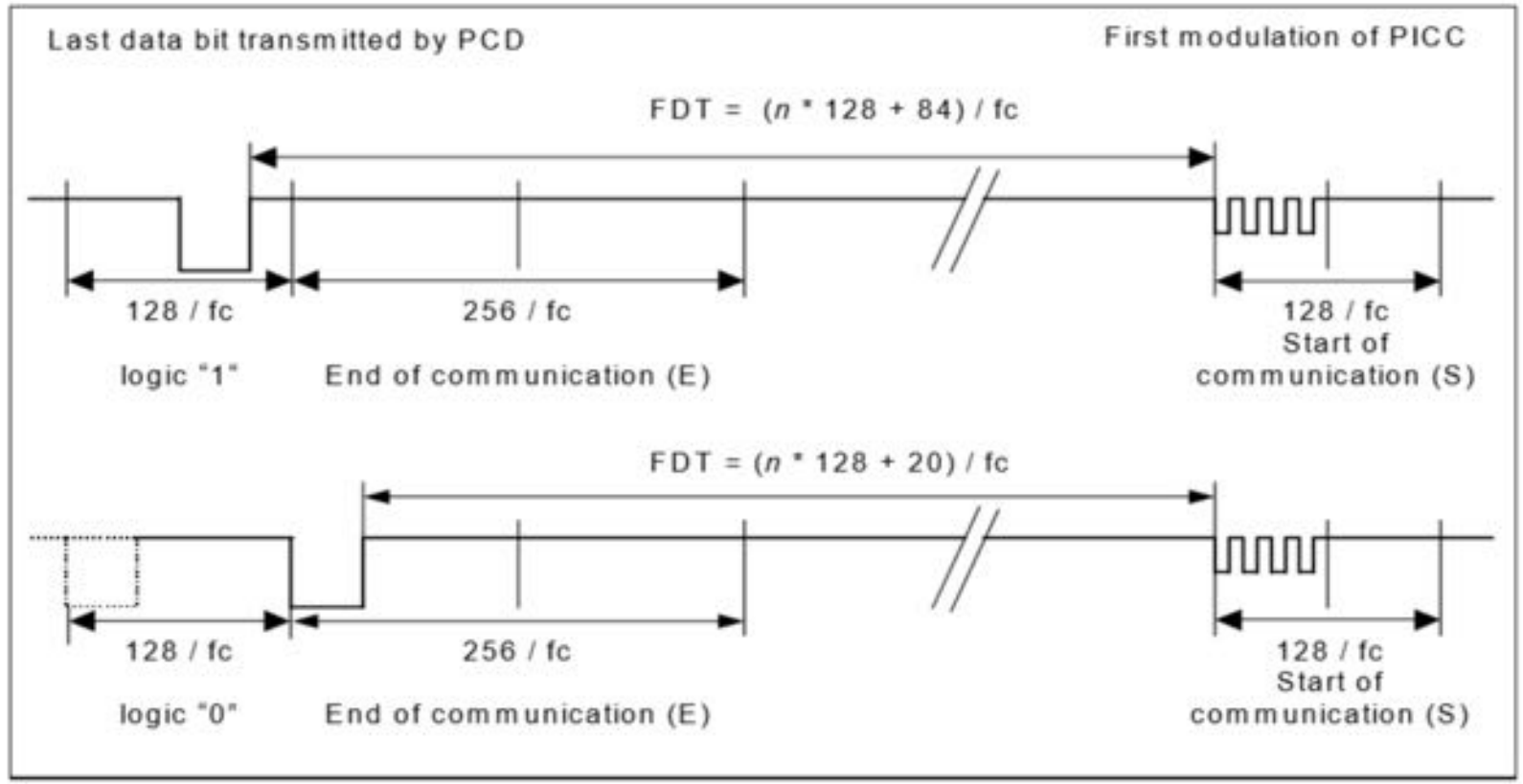


Figure 1 — Frame delay time PCD to PICC

Table 1 — Frame delay time PCD to PICC

Command type	*n* (integer value)	FDT	
		last bit = (1)b	last bit = (0)b
REQA Command WUPA Command ANTICOLLISION Command SELECT Command	9	1236 / *fc*	1172 / *fc*
All other commands	≥ 9	(*n* * 128 + 84) / *fc*	(*n* * 128 + 20) / *fc*

Improved logic for determining the correct Frame Delay Time (FDT) #87

New issue

Merged iceman1001 merged 1 commit into `iceman1001:master` from `timhir:master` on 6 Mar 2017

Conversation 6 Commits 1 Files changed 1 +10 −3

timhir commented on 6 Mar 2017

Improved logic for determining the correct Frame Delay Time (FDT) based value based on the last bit transmitted by the PCD.

The original logic did not always use the correct value. This caused the anticollision protocol to fail when simulating a tag with HID Omnikey 5421 reader.

This patch makes the third parameter (correctionNeeded) irrelevant. The function prototype and calls to EmSendCmd14443aRaw should probably be refactored, too.

`Improved logic for determining the correct Frame Delay Time (FDT) val…` ... ✕ 17ab9dc

Reviewers
No reviews

Assignees
No one assigned

Labels
None yet

Milestone
No milestone

QUEST FOR RELEVANT VALUES

F-Secure.

FAIL

QUEST FOR IRRELEVANT VALUES

F-Secure.

1 PROBLEM AND KEY SPACE IS ONE OF THEM

F-Secure.

CUSTOM PROXMARK FIRMWARE

F-Secure.

```
SimulateIso14443aTag(2, FLAG_7B_UID_IN_DATA, card_data);
```

```
SimulateIso14443aTag(2, FLAG_7B_UID_IN_DATA, card_data);

// This seems to be a working method to turn off the field...
iso14443a_setup(FPGA_HF_ISO14443A_READER_LISTEN);
```

PROXMARKING 1/SECOND

4 bits	8 bits	12 bits	16 bits
16 seconds	**4 minutes**	**1 hour**	**18 hours**

PROXMARKING 1/SECOND

20 bits	24 bits	28 bits	32 bits
12 days	**6 months**	**8 years**	**138 years**

ASSA ABLOY

Non Employees Log In Here

To log-in, please enter your username (usually your email address) and password.
ACP CI Companies - Use your User ID you were provided.
Need Help? Please email: University@assaabloy.com

You can browse the catalog anonymously HERE
Not Enrolled Yet? If you do not have a username or password, click HERE to enroll in the University.

Username:

Password:

Login

Forgot username or password?

Employees Log In Here

Employees, use the ASSA ABLOY Single Sign On page HERE

ABOUT BEING A GHOST

F-Secure.

F-Secure.

AUDIT TRAIL

F-Secure.

Signature RFID by VingCard

Where the design integrity is top priority of the property, there is a desire for the necessary hardware to blend into the environment becoming invisible for the end-user. Signature by VingCard is design conscious and appears to the most sophisticated styles in hotels worldwide.

Signature RFID uses 13,56 MHz technology and is compatible with the following standards:
- ISO 14.1443 A (MIFARE)
- ISO 14.1443 B
- ISO 15.693

Signature RFID is also compatible with NFC (Near Field Communication).

Features:
- Anti cloning technology
- Write-back, the RFID lock is able to write back to cards
- RFID cards can be integrated to multi applications
- Flash RAM memory
- 600 event audit trail
- Option dual reader
- Motorized lock case with locking mechanism located in the lock case
- High security heavy duty mortise lock case available in ANSI or EURO version with a 3-point anti friction steel latch and case hardened full 1-inch throw (ANSI) deadbolt
- The lock is designed to ANSI grade 1 standards
- Panic release

and examined by the LockLink, and transferred to the VISION system for a full print-out. For Locks capable of reading Smart Cards, lock events can also be transferred to VISION by a special **Readout** card.

The information about each entry is

- User ID code + Issue Area code
- Time of the event
- Value of override criterion (issue time, start time or end time)

The readout is a valuable tool both in prevention of crime as well as investigation of crime.

> **NOTE:** The Lock Event readouts are often used to prevent false accusations of hotel personnel.

Other Functions

Lock-out

Lock-out keycards are issued to specific employees (usually maids) and they are normally used to prevent guests from returning to a room between the time they check out and the time their keycard expires.

When the room is cleaned, the maid can use the Lock-out keycard on the door. Then, only new guests will be able to open the door. This will ensure that the room will remain clean until the new guest checks in.

AN ATTACKER CONTROLS ALL THE FIELDS EXCEPT TIMESTAMP

F-Secure.

AND TO MAKE IT WORSE …

***LockLink* Component**

1. Pocket PC with Windows software
2. Docking station
3. Serial connector to Vision PC
4. Power supply
5. Contact Card for programming doors

The parts 1 to 4 are delivered as a package.

The Vision LockLink software can be installed from a PC (using Microsoft ActiveSync) or by plugging a pre-programmed Compact Flash card into the Pocket PC.

F-Secure.

THE PLAN

- Acquire a copy of Vision software
- Read, understand and document 500+ pages of manuals
- Build a lab with RFID reader
- Acquire working knowledge of RFID
- Reverse engineer the software and find a clever way to open the lock without access to the original key
- **Pose like a boss**

Slightly edited version of the original photo:
https://media.scmagazine.com/images/2013/11/12/1213-luminaries-miller-valasek_492445.jpg


one more thing...

- Compromise the backend locally
- Compromise the backend remotely

THE PLAN

- **Analyze the software for possible weaknesses that could be exploited remotely**
- Pose even more

vision™
by VingCard

Help

Logout

GUEST KEYCARDS

EMPLOYEE KEYCARDS

SPECIAL KEYCARDS

REPORTS

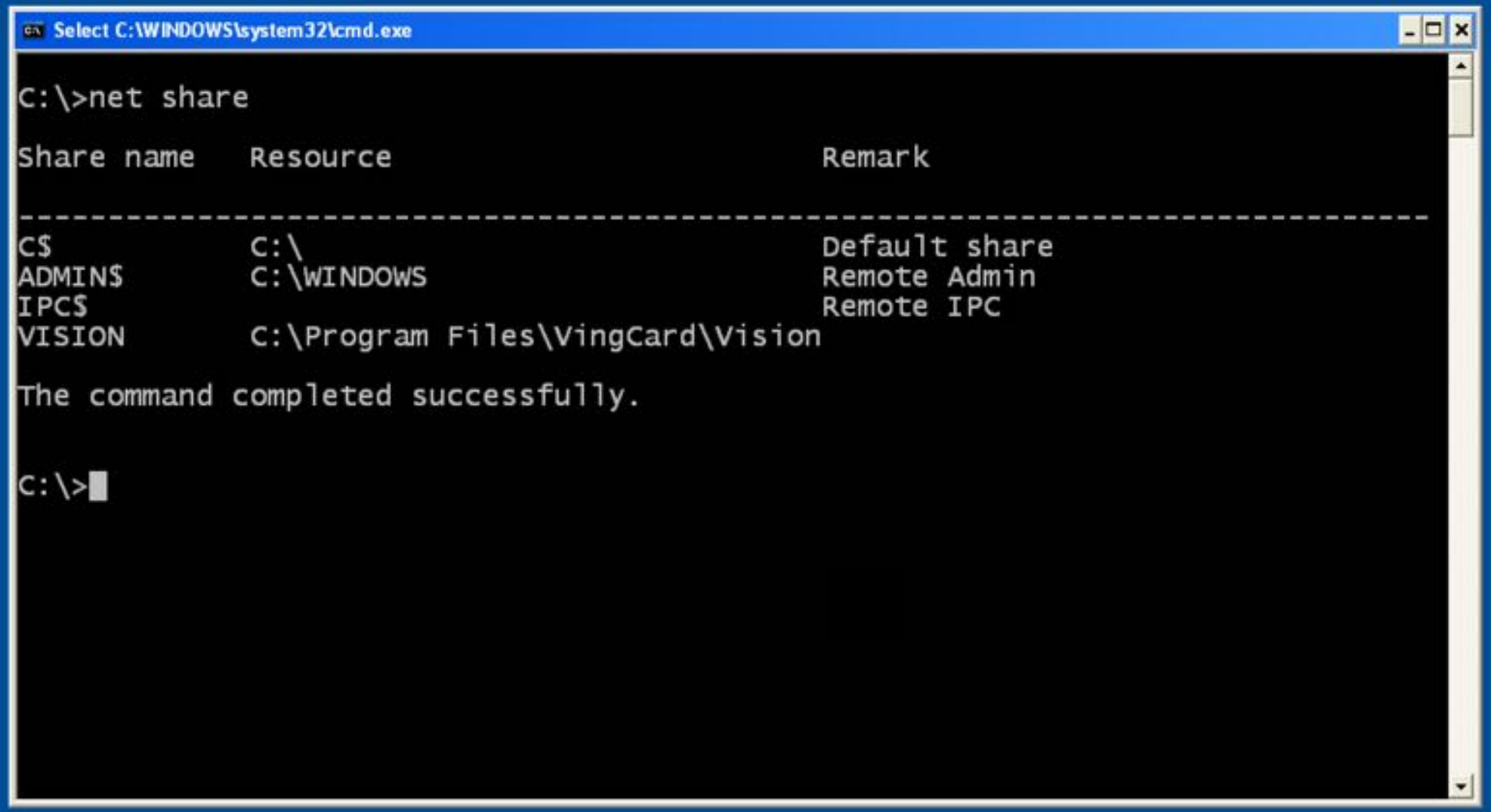
EMPLOYEE ROOMS

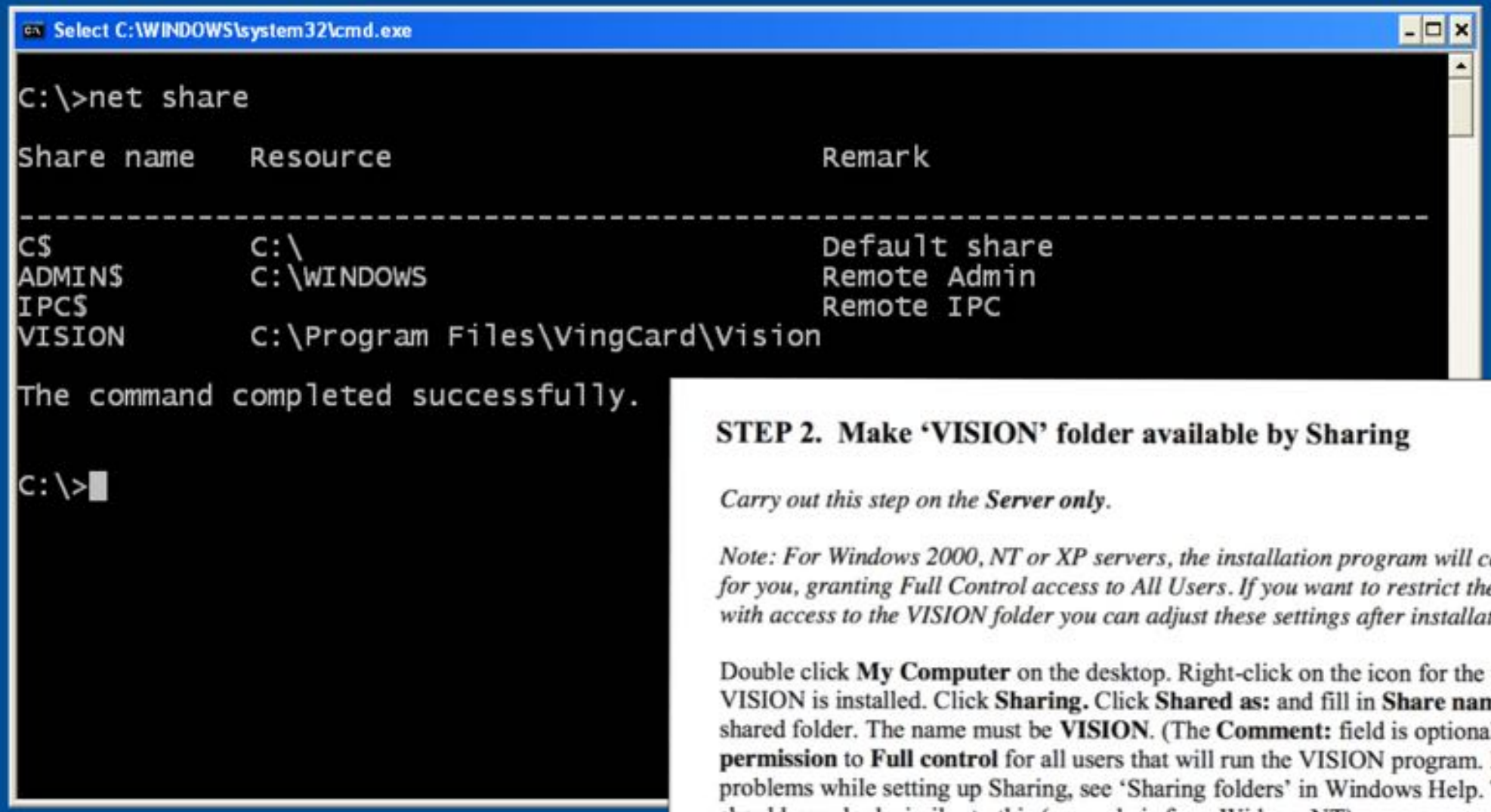
SYSTEM USERS

SYSTEM SETUP

BACKUP

LOCK LINK


Select C:\WINDOWS\system32\cmd.exe
C:\>net share
Share name Resource Remark
C$ C:\ Default share
ADMIN$ C:\WINDOWS Remote Admin
IPC$ Remote IPC
VISION C:\Program Files\VingCard\Vision
The command completed successfully.
C:\>

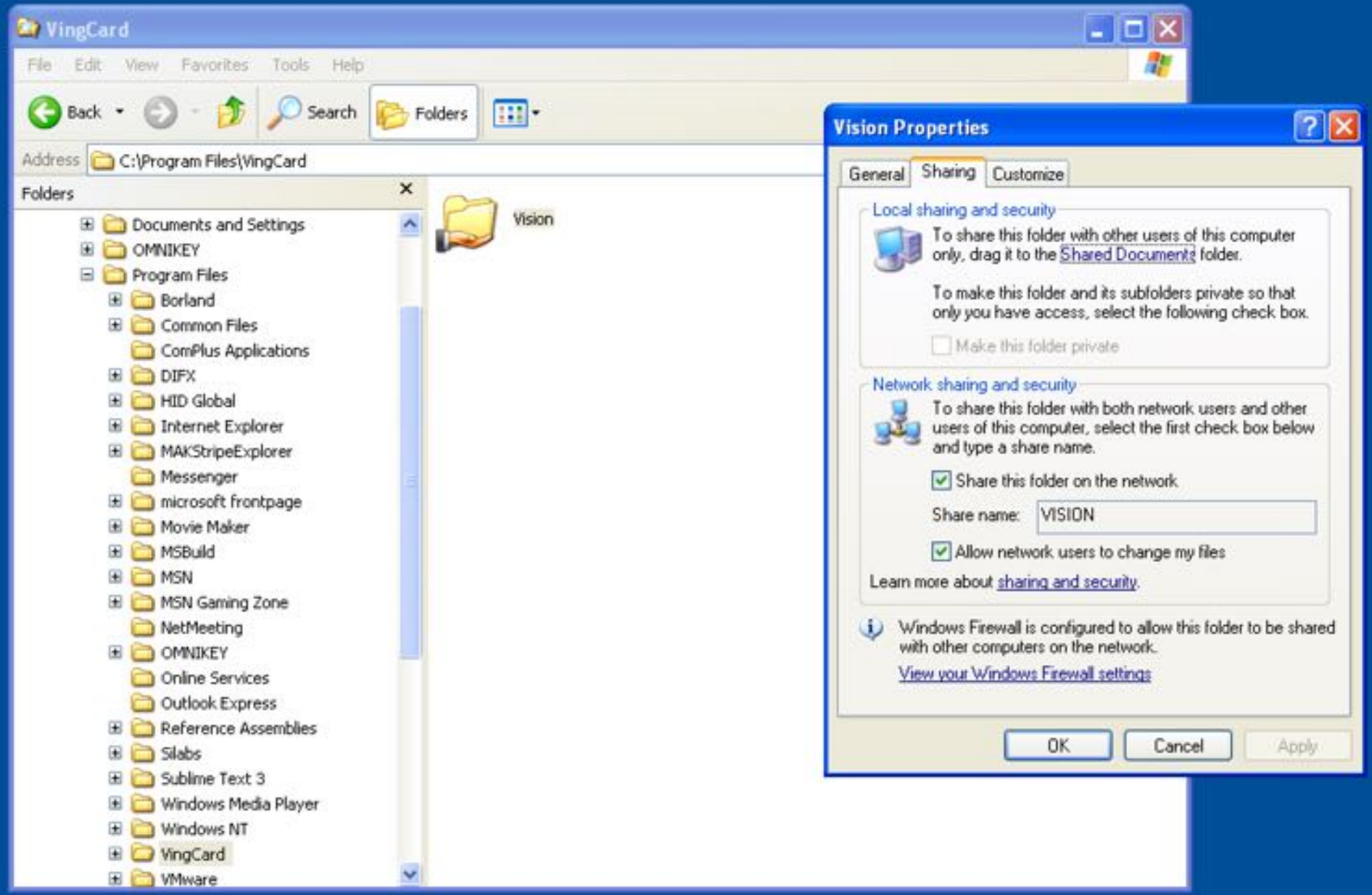


STEP 2. Make 'VISION' folder available by Sharing

*Carry out this step on the **Server only**.*

Note: For Windows 2000, NT or XP servers, the installation program will carry out this step for you, granting Full Control access to All Users. If you want to restrict the group of users with access to the VISION folder you can adjust these settings after installation.

Double click **My Computer** on the desktop. Right-click on the icon for the folder where VISION is installed. Click **Sharing.** Click **Shared as:** and fill in **Share name:** for your shared folder. The name must be **VISION**. (The **Comment:** field is optional.) Set **Sharing permission** to **Full control** for all users that will run the VISION program. If you encounter problems while setting up Sharing, see 'Sharing folders' in Windows Help. The window should now look similar to this (example is from Widows NT):

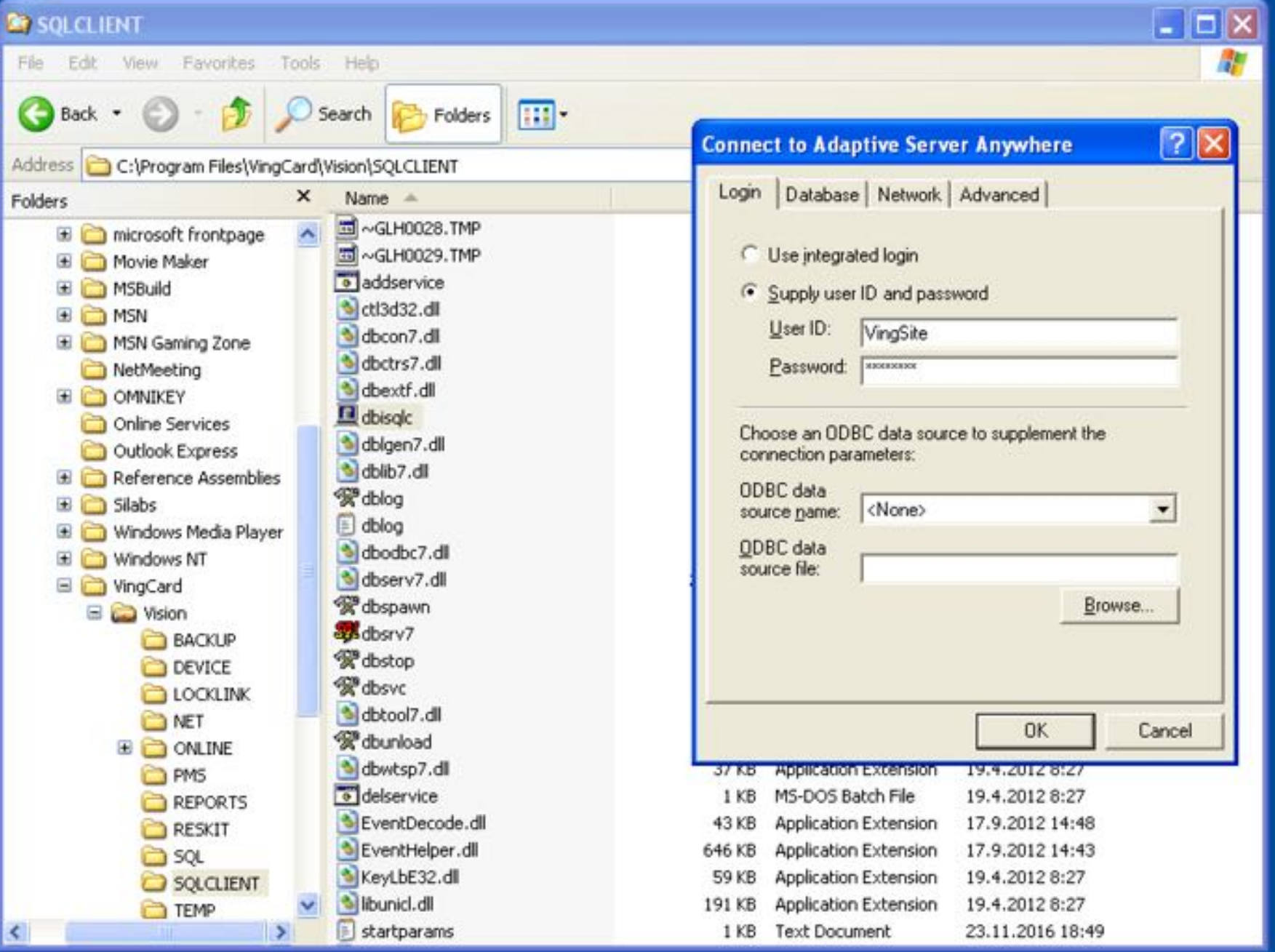

VingCard
File Edit View Favorites Tools Help
Back Search Folders
Address C:\Program Files\VingCard
Folders
Documents and Settings
OMNIKEY
Program Files
Borland
Common Files
ComPlus Applications
DIFX
HID Global
Internet Explorer
MAKStripeExplorer
Messenger
microsoft frontpage
Movie Maker
MSBuild
MSN
MSN Gaming Zone
NetMeeting
OMNIKEY
Online Services
Outlook Express
Reference Assemblies
Silabs
Sublime Text 3
Windows Media Player
Windows NT
VingCard
VMware
Vision
Vision Properties
General
Sharing
Customize
Local sharing and security
To share this folder with other users of this computer only, drag it to the Shared Documents folder.
To make this folder and its subfolders private so that only you have access, select the following check box.
Make this folder private
Network sharing and security
To share this folder with both network users and other users of this computer, select the first check box below and type a share name.
Share this folder on the network
Share name: VISION
Allow network users to change my files
Learn more about sharing and security.
Windows Firewall is configured to allow this folder to be shared with other computers on the network.
View your Windows Firewall settings
OK
Cancel
Apply

VISION DATABASE

- SYBASE Adaptive Server Anywhere
- Listening by default on port 2638
- Database passwords are derived from magic constants

VISION.DB DEMO DATABASE CREDENTIALS

Role	Username	Password
Application credentials	VingSite	huRt7GSW
Power user	VingSite1	hiZTPIVR
Admin user	DBA	hi44jJSW


SQLCLIENT
File Edit View Favorites Tools Help
Back Search Folders
Address C:\Program Files\VingCard\Vision\SQLCLIENT
Folders
Name
microsoft frontpage
Movie Maker
MSBuild
MSN
MSN Gaming Zone
NetMeeting
OMNIKEY
Online Services
Outlook Express
Reference Assemblies
Silabs
Windows Media Player
Windows NT
VingCard
Vision
BACKUP
DEVICE
LOCKLINK
NET
ONLINE
PMS
REPORTS
RESKIT
SQL
SQLCLIENT
TEMP
~GLH0028.TMP
~GLH0029.TMP
addservice
ctl3d32.dll
dbcon7.dll
dbctrs7.dll
dbextf.dll
dbisqlc
dblgen7.dll
dblib7.dll
dblog
dblog
dbodbc7.dll
dbserv7.dll
dbspawn
dbsrv7
dbstop
dbsvc
dbtool7.dll
dbunload
dbwtsp7.dll
delservice
EventDecode.dll
EventHelper.dll
KeyLbE32.dll
libunicl.dll
startparams
Connect to Adaptive Server Anywhere
Login
Database
Network
Advanced
Use integrated login
Supply user ID and password
User ID:
VingSite
Password:
Choose an ODBC data source to supplement the connection parameters:
ODBC data source name:
<None>
ODBC data source file:
Browse...
OK
Cancel
37 KB Application Extension 19.4.2012 8:27
1 KB MS-DOS Batch File 19.4.2012 8:27
43 KB Application Extension 17.9.2012 14:48
646 KB Application Extension 17.9.2012 14:43
59 KB Application Extension 19.4.2012 8:27
191 KB Application Extension 19.4.2012 8:27
1 KB Text Document 23.11.2016 18:49

Interactive SQL - vision (VingSite): vision

File Edit Command Window Help

Data

table_id	file_id	count	first_page	last_page	primary_root	creator	first_ext_page	last_ext_page	table_page_count	ext_page_count	table_name	table_type	view_def
1	0	221	1	2908	12	0	82	263	17	11	SYSTABLE	BASE	(NULL)
2	0	1779	2	2507	13	0	0	0	47	0	SYSCOLUMN	BASE	(NULL)
3	0	82	14	2946	15	0	0	0	3	0	SYSINDEX	BASE	(NULL)
4	0	110	16	1812	17	0	0	0	2	0	SYSIXCOL	BASE	(NULL)
5	0	124	18	943	19	0	0	0	3	0	SYSFOREIGNKEY	BASE	(NULL)
6	0	142	20	1513	21	0	0	0	2	0	SYSFKCOL	BASE	(NULL)
7	0	1	22	22	23	0	0	0	1	0	SYSFILE	BASE	(NULL)
8	0	24	24	24	25	0	0	0	1	0	SYSDOMAIN	BASE	(NULL)
9	0	11	27	27	28	0	0	0	1	0	SYSUSERPERM	BASE	(NULL)
10	0	234	29	2586	30	0	0	0	5	0	SYSTABLEPERM	BASE	(NULL)
11	0	0	31	31	32	0	0	0	1	0	SYSCOLPERM	BASE	(NULL)
12	0	118	33	361	42	0	0	0	2	0	SYSOPTION	BASE	(NULL)
13	0	14	34	34	35	0	0	0	1	0	SYSGROUP	BASE	(NULL)
14	0	1	36	36	38	0	41	41	1	1	SYSCOLLATION	BASE	(NULL)
15	0	270	44	3252	45	0	245	3223	32	58	SYSPROCEDURE	BASE	(NULL)
16	0	1090	47	1550	48	0	0	0	22	0	SYSPROCPARM	BASE	(NULL)
17	0	90	49	3228	50	0	765	2930	12	6	SYSTRIGGER	BASE	(NULL)
18	0	212	51	722	52	0	0	0	2	0	SYSPROCPERM	BASE	(NULL)
19	0	0	53	53	54	0	0	0	1	0	SYSPUBLICATION	BASE	(NULL)
20	0	0	55	55	56	0	0	0	1	0	SYSARTICLE	BASE	(NULL)
21	0	0	58	58	59	0	0	0	1	0	SYSARTICLECOL	BASE	(NULL)
22	0	0	60	60	61	0	0	0	1	0	SYSREMOTEUSER	BASE	(NULL)
23	0	0	63	63	64	0	0	0	1	0	SYSSUBSCRIPTION	BASE	(NULL)
24	0	0	65	65	0	0	0	0	1	0	SYSUSERMESSAGES	BASE	(NULL)
25	0	1283	67	634	68	0	0	0	34	0	SYSUSERTYPE	BASE	(NULL)
26	0	0	73	73	75	0	0	0	1	0	SYSEXTENT	BASE	(NULL)
27	0	5	76	76	77	0	0	0	1	0	SYSREMOTETYPE	BASE	(NULL)

Statistics

221 rows in query (I/O estimate 18)
PLAN> SYSTABLE (seq)

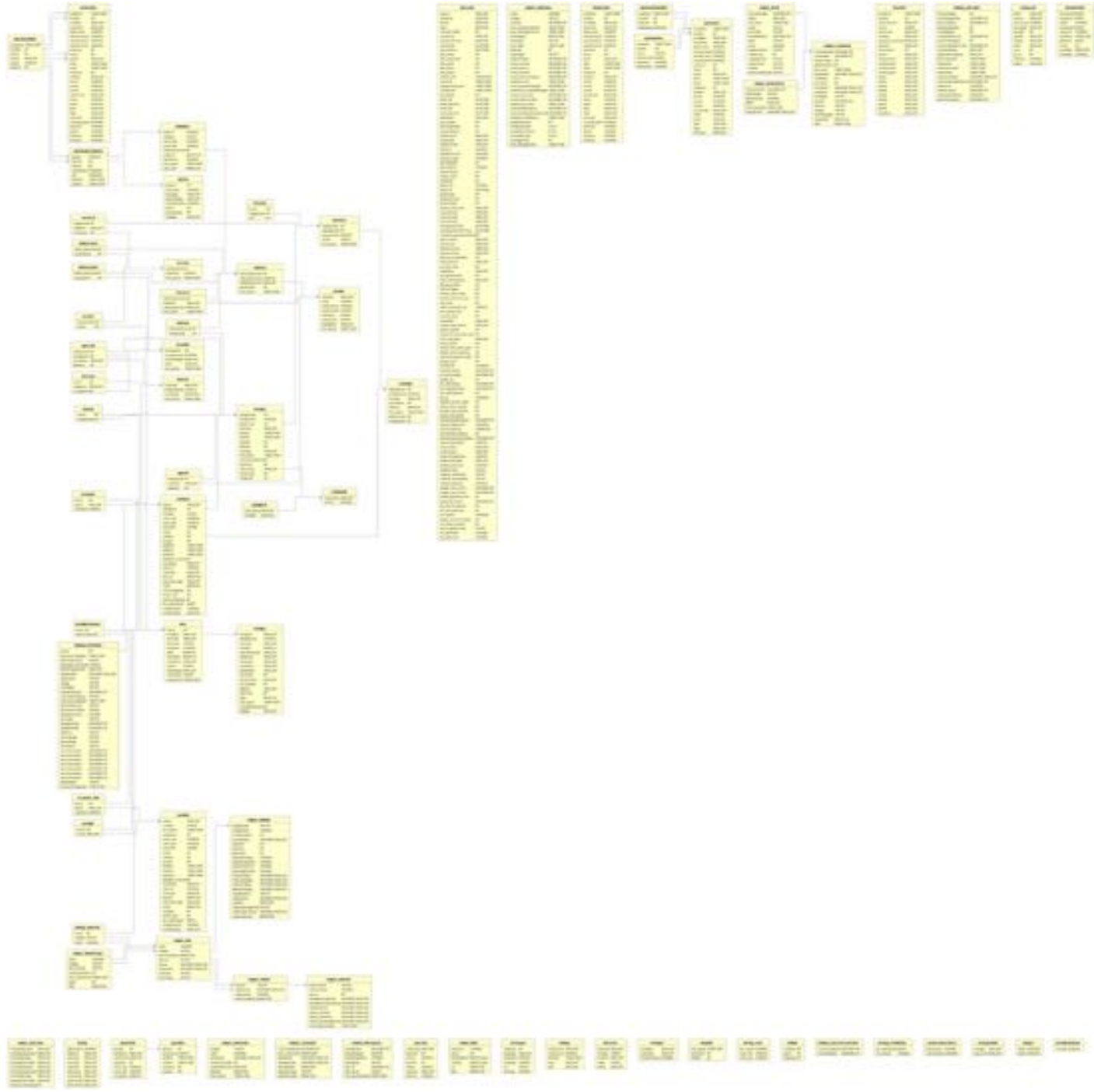
Command

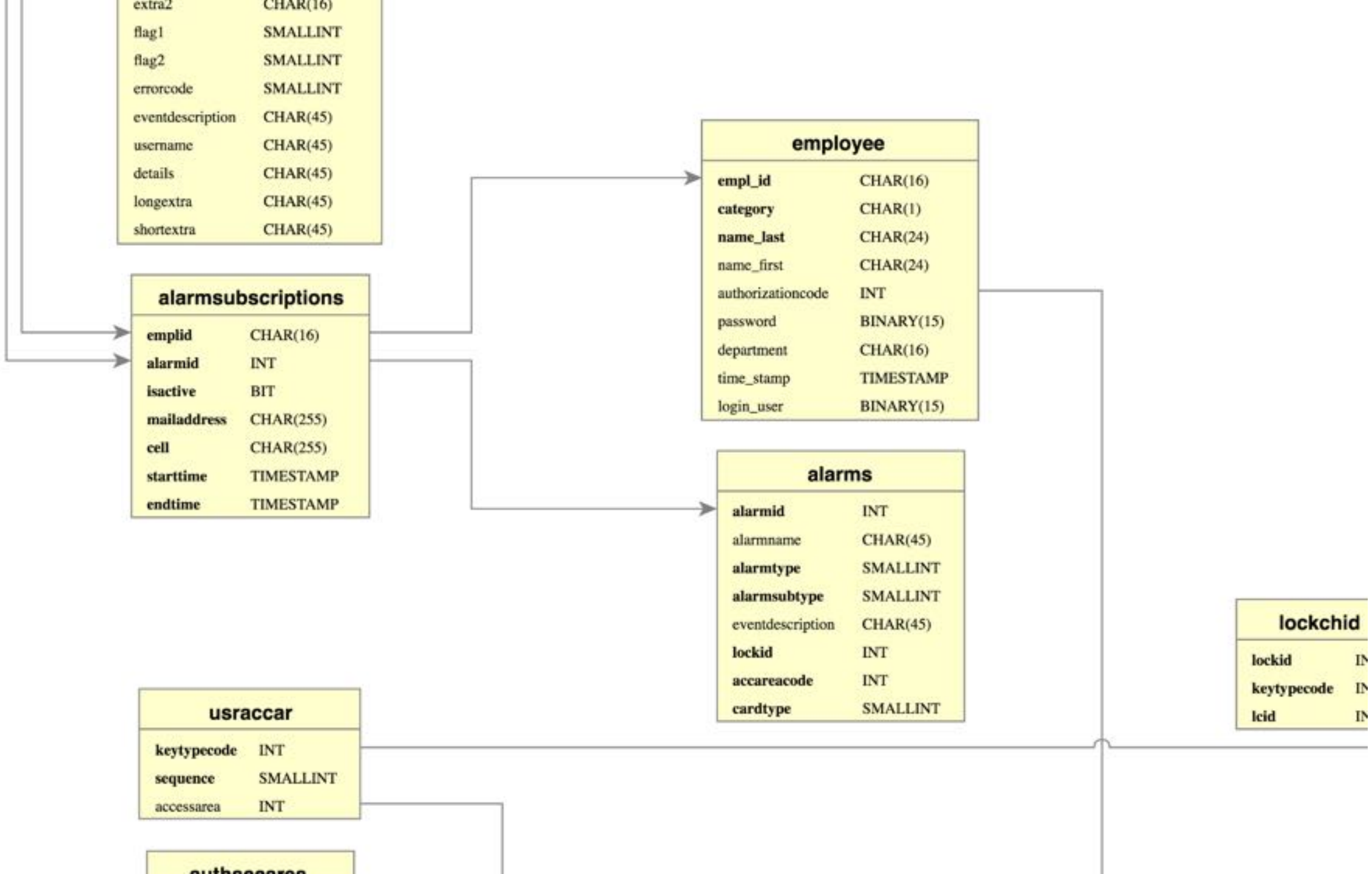
Execute

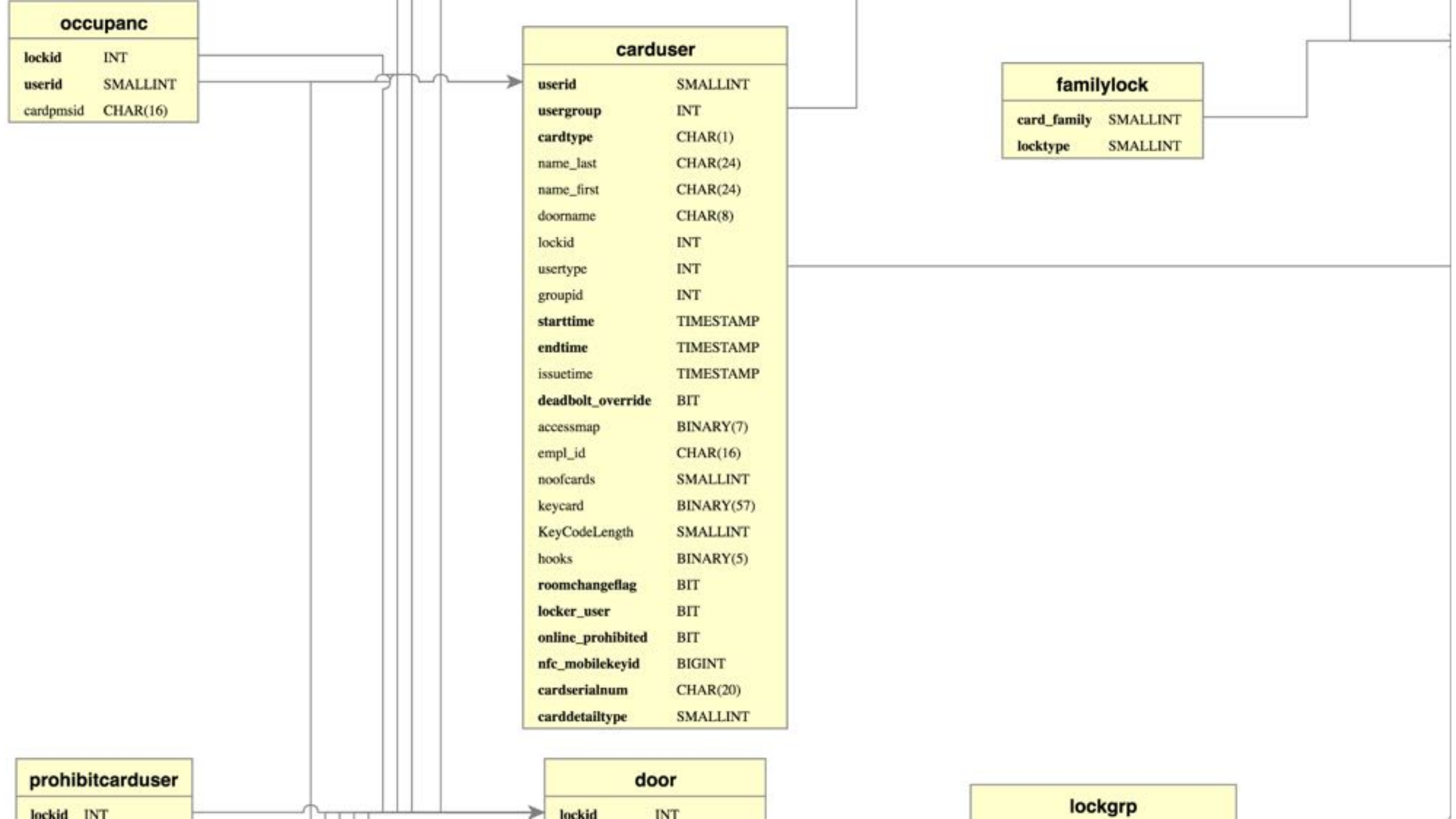
Stop

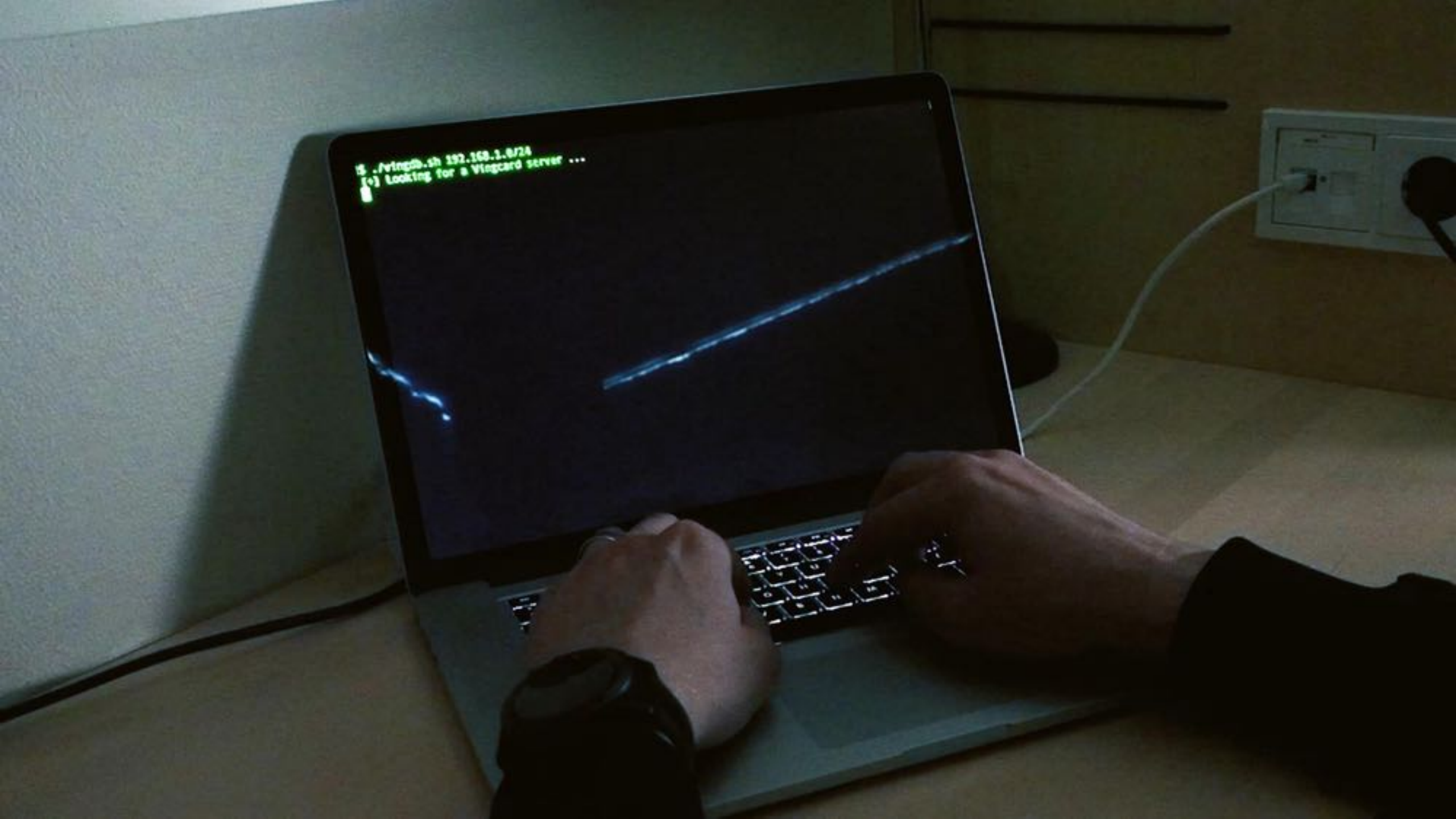
SELECT * FROM SYSTABLE

SELECT * FROM SYSTABLE




extra2 CHAR(16)
flag1 SMALLINT
flag2 SMALLINT
errorcode SMALLINT
eventdescription CHAR(45)
username CHAR(45)
details CHAR(45)
longextra CHAR(45)
shortextra CHAR(45)
employee
empl_id CHAR(16)
category CHAR(1)
name_last CHAR(24)
name_first CHAR(24)
authorizationcode INT
password BINARY(15)
department CHAR(16)
time_stamp TIMESTAMP
login_user BINARY(15)
alarmsubscriptions
emplid CHAR(16)
alarmid INT
isactive BIT
mailaddress CHAR(255)
cell CHAR(255)
starttime TIMESTAMP
endtime TIMESTAMP
alarms
alarmid INT
alarmname CHAR(45)
alarmtype SMALLINT
alarmsubtype SMALLINT
eventdescription CHAR(45)
lockid INT
accareacode INT
cardtype SMALLINT
lockchid
lockid IN
keytypecode IN
lcid IN
usraccar
keytypecode INT
sequence SMALLINT
accessarea INT


occupanc
lockid INT
userid SMALLINT
cardpmsid CHAR(16)
carduser
userid SMALLINT
usergroup INT
cardtype CHAR(1)
name_last CHAR(24)
name_first CHAR(24)
doorname CHAR(8)
lockid INT
usertype INT
groupid INT
starttime TIMESTAMP
endtime TIMESTAMP
issuetime TIMESTAMP
deadbolt_override BIT
accessmap BINARY(7)
empl_id CHAR(16)
noofcards SMALLINT
keycard BINARY(57)
KeyCodeLength SMALLINT
hooks BINARY(5)
roomchangeflag BIT
locker_user BIT
online_prohibited BIT
nfc_mobilekeyid BIGINT
cardserialnum CHAR(20)
carddetailtype SMALLINT
familylock
card_family SMALLINT
locktype SMALLINT
prohibitcarduser
lockid INT
door
lockid INT
lockgrp


$ ./vtnpdb.sh 192.168.1.0/24
[+] Looking for a Vtngcard server ...

THE PLAN

- Analyze the software for possible weaknesses that could be exploited remotely
- **Pose even more**

Slightly edited version of the original photo:
https://media.scmagazine.com/images/2013/11/12/1213-luminaries-miller-valasek_492445.jpg

Jump to Conclusions

???

JUMP AGAIN

STRIKE OUT

COULD BE

LOOSE ONE TURN

YES!

NO!

ACCEPT

GO

Jerry Gamblin
@JGamblin

Seuraa

Sometimes, hacking is just someone spending more time on something than anyone else might reasonably expect.

16.04 - 25. maalisk. 2017

773 uudelleentwiittausta **1 556** tykkäystä

25 773 1,6 t.

THANK YOU

- **ASSA Abloy**; we will never forget that you guys treated us with respect and took this very seriously from the very beginning.
- For more information please visit:

  https://www.assaabloyhospitality.com/en/aah/com/about-us/product-support/product-security-policy/

F-Secure.

GREETINGS

H for being our hotel key courier, **O** for some hardware analysis, **Man of Steel** for some early reverse engineering, **Dist** for 3D printing sorcery, **ph-neutral** crew for rocking the house, Team **Vulndev** for being awesome, **Halvar** for being a gentle giant and **t2** crew for everything else.

All the others we forgot!

Q&A

F-Secure.