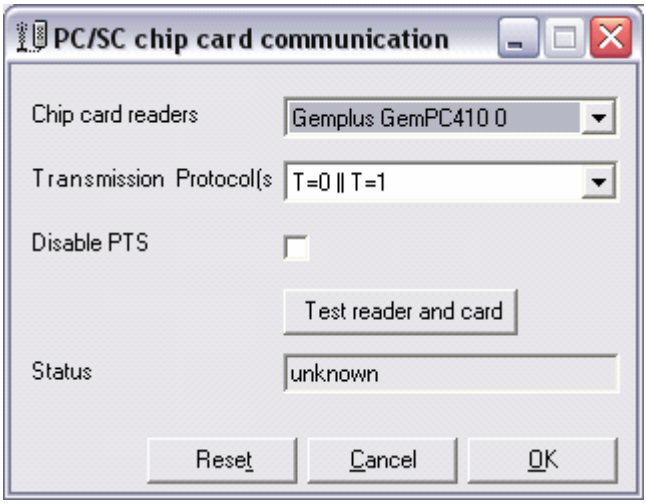
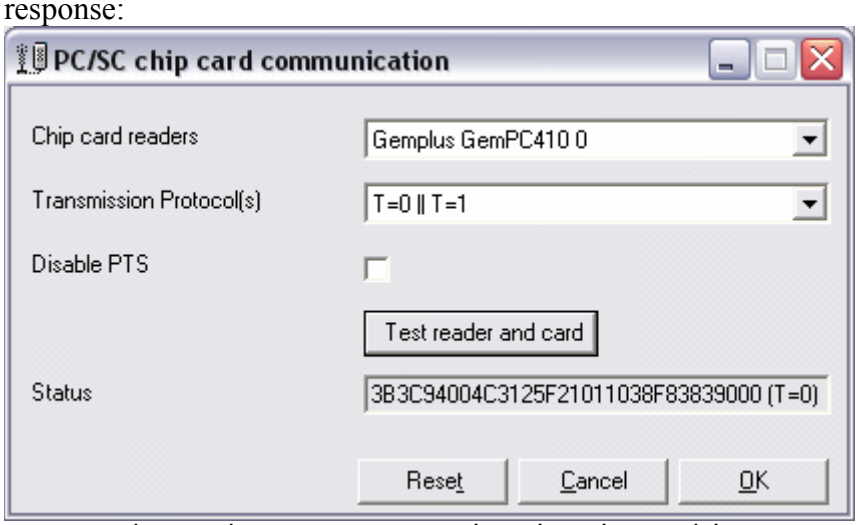
For extracting SIM-card data you need to have a working PC/SC compatible smart card reader. PC/SC is for chip card readers like Printer & Fax management for printers: it separates hardware from applications (please check http://www.pcscworkgroup.com/ for details).

We use the GemPC readers like (http://www.gemplus.com/products/gempctwin/) but any PC/SC compatible card reader will work. After installing a Gemplus reader you can use this program to test your reader and PC/SC subsystem: http://support.gemplus.com/gemdownload/common/filedownload.aspx?id=101 .

If the test is OK your Windows PC has a working PC/SC reader which can be used by TULP2G. After starting up TULP2G install the "PC/SC chip card communication plug-in" . If you now start an investigation and select the PC/SC plug-in and configure it you see a dialog like this:

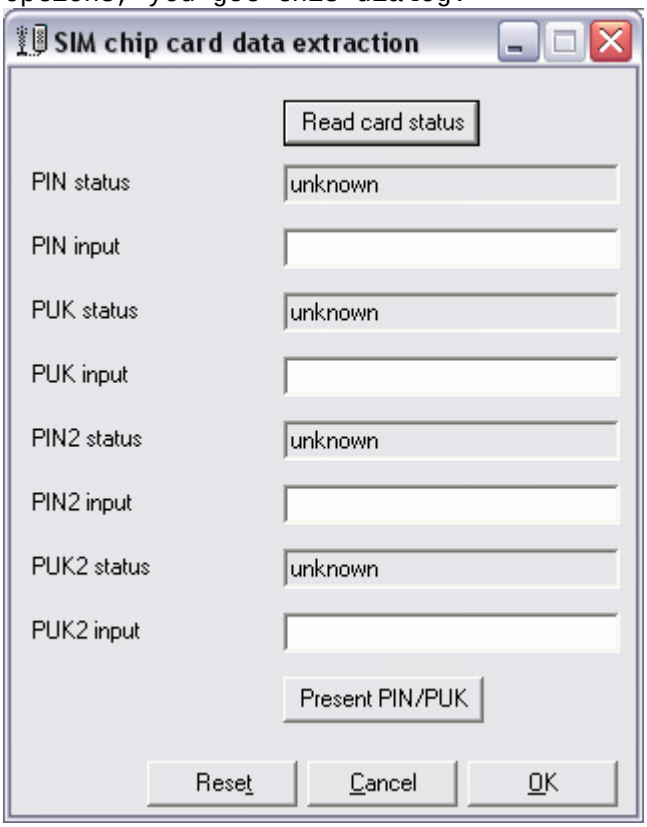


Insert a smart card and push the Test button, if the card is working you can see the reset response:

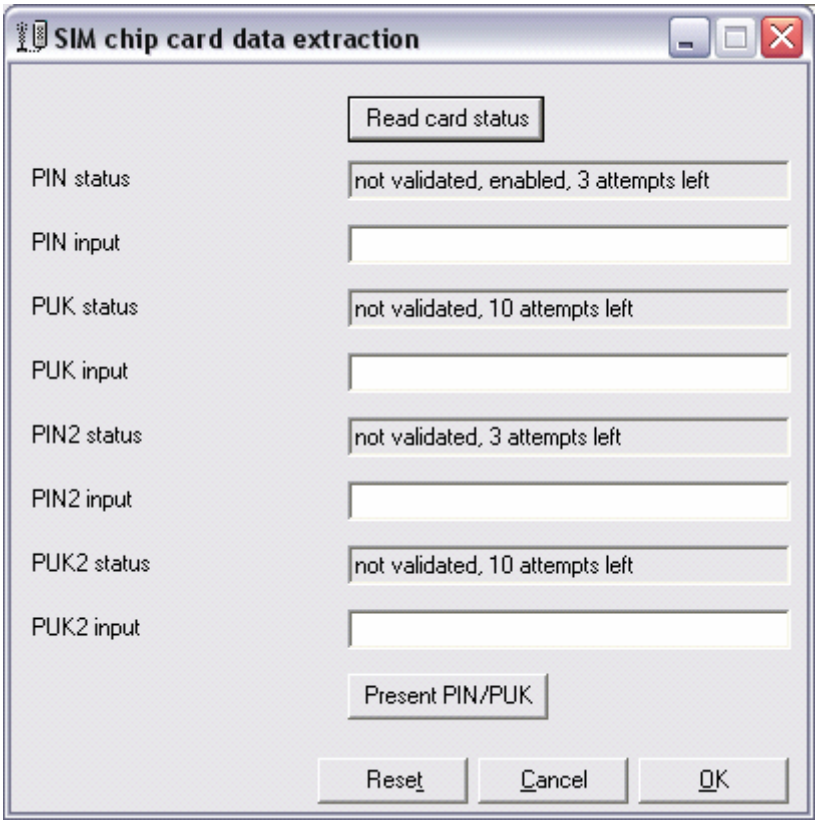


Now you know that your communication is working so continue with the protocol plug-in.

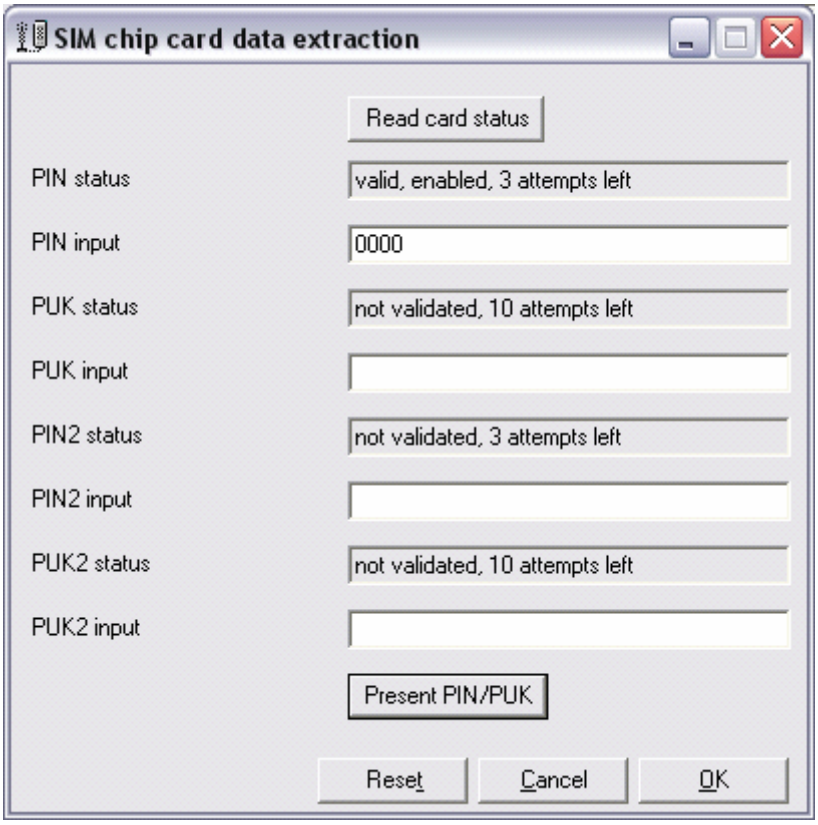
Select the “SIM card data extraction plug-in” and select the Configure options, you get this dialog:



Read the current card status to get the current PIN/PUK attempts:

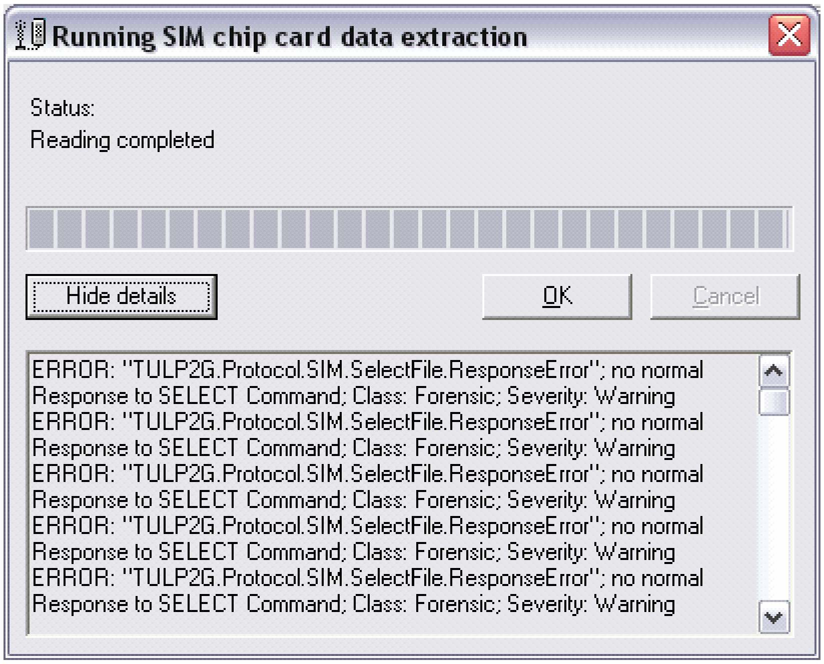


Now give the PIN code (if you know it) and push “Present PIN/PUK”. After a correct attempt the validation status changes:



Now you know that the PIN is correct and you can select OK and RUN the investigation Please note that the typed PIN will be used to do a card holder verification after pushing the RUN button. So if the PIN is incorrect after a “Present PIN/PUK” action and you select OK + RUN you loose one extra PIN attempt ! (this is logged in the Case file a can be seen in a Report).

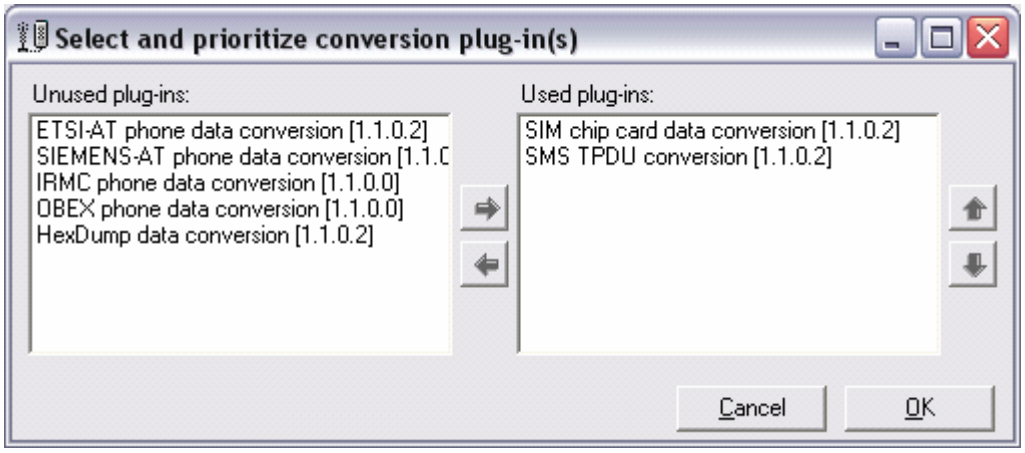
After pressing RUN all accessible file data is extracted. With “Show details” in the Progress dialog you get extraction diagnostics:



In this case all of level "Warning" . These warnings appear because the extraction plug-in tries to extract all possible SIM files as defined in the ETSI standards. A lot of defined files are not present in real-life SIMs so you will get a "SelectFile" error if you try to select these, non-existing, files.

After selecting OK you can save the case file so all low-level data is saved for future use. If you want to make a report go to the Report tab, select the "XML/HTML report" export plug-in, select the ReportSIM stylesheet like below:

Select the following Conversion plug-ins in this order:



Now RUN the Report and you will see a report in your Web-browser like this:
(I've used a brand new SIM so not much info in this card).

Show case data Show documentation Show "preformatted" SMS text

Netherlands Forensic Institute - TULP2G

Case name	TestCase
Case creator	Ronald
Creation date	23-1-2005 13:10:08
MD5 hash	95151E2A9C6CCF41F6A4FCE34D012103
SHA-1 hash	F5E5B42A2307FB52F5D1FBADF378F493D805CA96

Plug-in info

Plug-in type	Plug-in info
ExportPlugin	TULP2G.Export.XML, Version=1.1.0.2, Culture=neutral, PublicKeyToken=3480a3624ac48f93
ConversionPlugin	TULP2G.Conversion.SIM, Version=1.1.0.2, Culture=neutral, PublicKeyToken=3480a3624ac48f93
ConversionPlugin	TULP2G.Conversion.SMS, Version=1.1.0.2, Culture=neutral, PublicKeyToken=3480a3624ac48f93

Investigation *test*

Creation date	23-1-2005 13:10:11
MD5 hash	46B608047E5BF2701101D7C298684BB5
SHA-1 hash	A3F8891E36A83CA437C54FDB5074392C25E3125C

Plug-in info

Plug-in type	Plug-in info
CommunicationPlugin	TULP2G.Communication.PCSC@TULP2G.Communication.PCSC, Version=1.1.0.2, Culture=neutral, PublicKeyToken=3480a3624ac48f93
ProtocolPlugin	TULP2G.Protocol.ProtocolSIM@TULP2G.Protocol.SIM, Version=1.1.0.2, Culture=neutral, PublicKeyToken=3480a3624ac48f93

Card Holder Verification (CHV)

Data in an Subscriber Identity Module (SIM) can be protected with PINs (Personal Identity Numbers). A PIN consists of four to eight digits, is requested after a phone has been switched on, and can be entered using the phone's keyboard. The number of attempts to enter a PIN is limited to three. If none of the attempts is successful, access to the protected data will be blocked. This block can be cancelled with a PUK (PIN unblocking code). A PUK consists of eight digits and includes a new PIN. The number of attempts to enter a PUK is limited to ten. If none of the attempts is successful, the possibility to cancel the PIN block will be disabled permanently.The Card Holder Verification (CHV) table lists all CHV operations in chronological order done during the examination. There are two types of operations:

Verification

The verified PIN and or PUK code(s)

Status

The actual number of attempts left and the enabled/disabled state of the code (only for PIN).

	PIN	PUK	PIN2	PUK2
Status	3 (enabled)	10	3	10
Verification	0000			
Status	3 (enabled)	10	3	10
Verification	0000			
Status	3 (enabled)	10	3	10

Integrated Circuit Card(ICC) identification

A unique identification number for the SIM. Content is defined in CCITT Recomendation E.118 which defines a major industry identifier (89), a country code, an issuer identifier and a individual account identification number. CCITT stands for Comité Consultatif International Téléphonique et Télégraphique, an organization that sets international communications standards.

893120140406438439 (Netherlands, Orange)

International Mobile Subscriber Indentity (IMSI)

A unique identification number within the complete GSM network. This number consists of a country code, a network provider code and a subscriber number.

204204008796537 (Netherlands, Orange Nederland N.V.)

SIM service table

This table sums up all the services that can be supported by an SIM. Under allocated an indication is given of whether or not each service can be supported by the card; whether or not a service has been activated can be found under activated. All services in this list can be stored in an SIM

Nr.	Description	Allocated	Activated
0	CHV1 disable function	■	■
1	Fixed Dialling Numbers (FDN)	■	■
2	no description available	■	■
3	Short Message Storage (SMS)	■	■
4	Advice of Charge (AoC)	■	■
5	Capability Configuration Parameters (CCP)	■	■
6	PLMN selector	■	■
7	RFU	□	□
8	MSISDN	■	■
9	Extension1	■	■
10	Extension2	■	■
11	SMS Parameters	■	■
12	Last Number Dialled (LND)	■	■
13	Cell Broadcast Message Identifier	■	■
14	Group Identifier Level 1	■	■
15	Group Identifier Level 2	■	■
16	Service Provider Name	■	■
17	Service Dialling Numbers (SDN)	■	■
18	Extension3	□	□
19	RFU	□	□
20	VGCS Group Identifier List(EFvgcs and EFvgcss)	□	□
21	VBS Group Identifier List (EFvbs and EFvbss)	□	□
22	enhanced Mulli-Level Precedence and Pre-emption Service	□	□
23	Automatic Answer for eMLPP	□	□
24	Data download via SMS-CB	□	□
25	Data download via SMS-PP	■	■
26	Menu selection	■	■
27	Call control	□	□
28	Proactive SIM	■	■
29	Cell Broadcast Message Identifier Ranges	□	□
30	Barred Dialling Numbers (BDN)	□	□
31	Extension4	□	□
32	De-personalization Control Keys	□	□
33	Co-operative Network List	□	□
34	Show Message Status Reports	□	□
35	Network's indication of alerting in the MS	□	□

36	Mobile Originated Short Message control by SIM	□	□
37	GPRS	■	■
38	Image (IMG)	□	□
39	SoLSA (Support of Local Service Area)	□	□
40	USSD string data object supported in Call Controll	□	□
41	RUN AT COMMAND command	□	□
42	PLMN Selector List with Access Technology	□	□
43	OPLMN Seleclor List with Access Technology	□	□
44	HPLMN Access Technology	□	□
45	CPBCCH lnformation	□	□
46	Investigation Scan	□	□
47	Extended Capability Configuration Parameters	□	□
48	MExE	□	□
49	no description available	□	□
50	no description available	□	□
51	no description available	□	□

Service Provider Name (SPN)

Name of the service provider, with a field indicating whether the registered network should be shown on the display of the phone.

Orange (display of registered PLMN not required)

Subscriber dialling numbers

Names and phone numbers, to be entered by the user, intended for storing the subscriber's own numbers. The first number is often shown on the display of the GSM telephone when it is switched on. Other number that might be shown include fax and data numbers.

Abbreviated dialling numbers

Names and phone numbers, to be entered and changed by the subscriber, which can be chosen easily using the phone. Recovered number data is shown in italics. For long numbers a "...[4]" indicates that the rest of the number is stored in the "4'th" position of the "Extension1" file.

Pos.	Name	Number
1	Voicemail	+31628500550
2	Beltegoed	1244
3	Klantenservice	+31628500777
4	Vmail direkt	+31628500515
5	i binnenland	118

Fixed dialling numbers

Names and phone numbers, to be entered and changed by the subscriber, which can be chosen easily using the phone. A phone can be configured in such a way that only phone numbers from this list can be called. This list can only be adjusted by means of a second PIN code.Recovered number data is shown in italics. For long numbers a "...[4]" indicates that the rest of the number is stored in the "4'th" position of the "Extension2" file.

Last numbers dialled

This list contains the most recent dialed phone numbers of the phone in which the SIM was used most recently (not all phones store these dialed numbers in the SIM). The number chosen most recently is at the top of the list. When a phone number already occurs in the SIM or in the phone with a corresponding description, this description is also given in this list. The numbers of the connections which could not be established may also occur in this list.

Service dialling numbers

This list contains special service numbers.

Pos.	Name	Number
1	Voicemail	+31628500550
2	Beltegoed	1244
3	Klantenservice	+31628500777
4	Vmail direkt	+31628500515
5	i binnenland	118

Language preference

This list, entered by the card supplier and to be adjusted by the subscriber, indicates the subscriber's language preferences in descending priority. This preference can be used by the GSM telephone for selecting display texts in the correct language.

Priority	Coding group	Language	Coding	Message class	Compression
1	0 (Language using the default alphabet)	5 (Dutch)			
2	0 (Language using the default alphabet)	1 (English)			
3...4	15 (Data coding / message handling)		15 (8 bit data)	TE-specific	

Public Land Mobile Network (PLMN) selector

When a phone cannot find its own network, for instance because the phone is abroad, the phone will start searching for other GSM networks. This searching takes place in the order of the list shown. In this way network providers, and also subscribers, can specify their preference for networks to be used when the phone is outside the range of its own network.

Priority	Country	Network
1	208 (France)	01 (Orange France)
2	214 (Spain)	07 (Telefonica Moviles Espaa S.A.)
3	206 (Belgium)	10 (Mobistar S.A.)
4	222 (Italy)	88 (Wind Telecomunicazioni SpA)
5	234 (United Kingdom)	33 (Orange PCS Ltd)
6	232 (Austria)	05 (ONE GMBH)
7	228 (Switzerland)	03 (Orange Communications S.A)
8	268 (Portugal)	03 (Optimus Telecomunicacoes, S.A)
9	238 (Denmark)	30 (Orange A/S)
10	260 (Poland)	03 (PTK Centertel)
11	226 (Romania)	10 (Orange Romania SA)
12	231 (Slovak Republic)	01 (Orange Slovensko a.s)
13	602 (Egypt)	01 (The Egyptian Company for Mobile Services)
14	415 (Lebanon)	01 (FTML)
15	425 (Israel)	01 (Partner Communications Company Ltd)
16	259 (Moldova, Republic of)	01 (VoXtel S.A.)
17	608 (Senegal)	02 (Sentel GSM)
18	454 (Hong Kong)	04 (Hutchison Telecom (HK) Ltd)
19	404 (India)	20 (Hutchison Max Telecom Ltd)
20	612 (Cote d'Ivoire)	03 (Orange Cote D'Ivoire S.A.)

Home PLMN (HPLMN) search period

The interval in minutes during which a phone should search for its own network. This searching takes place when the phone is in the country of the subscriber, but is connected to a different (competing) network.

1 (6 minutes)

Forbidden PLMNs

This list consists of GSM networks that may not be selected automatically by the phone for establishing a connection. A network may be included in this list because this information has been added to the SIM by the subscriber's network provider or because the network with which the GSM telephone tried to establish a connection refuses this connection.When a new, refusing network should be added to a full list, the element which has been in the list longest (first position) will be erased. The new refusing network appears as the last item on the list. A subscriber may force an attempt to establish contact with a network from this list manually via the phone. If this attempt is successful, the network will be removed from the list.

Location information

A GSM network consists of cells which are responsible for radio communications between mobile phones and the network. A number of cells are grouped together in local areas. Each phone keeps the network informed about the local area where the phone is. In this way, the network can establish contact with a GSM subscriber by sending a search signal to all the cells in the local area where the GSM telephone is. The following information regarding the most recent local area is stored in the SIM:

TIMSI
: *A temporary IMSI which is adjusted each time the local area changes. This is done to make sure that subscribers cannot be traced on the basis of the IMSI.*

Update timer
: *This value indicates how often a phone should inform the network of the current local area. This data is used only in Phase 1 SIMs.*

Update status
: *The status of the transfer of location information.*

MCC
: *The country where the local area is situated.*

MNC
: *The network of which the local area forms part.*

LAC
: *A reference to the local area itself.*

TIMSI	Update timer	Update status
0xFFFFFFFF	255	not_updated
Local Area Information		
MCC	**MNC**	**LAC**
204 (Netherlands)	20 (Orange Nederland N.V.)	0x0000

Broadcast control channels

Broadcast control channels are communication channels to which all inactive phones respond in order to determine which cell from which network would be optimum for communication. The intention of this data is to simplify this selection process. Although not clearly specified, this list should contain the neigbouring cell frequencies broadcasted by the last cell of the home PLMN on which the phone camped

0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

Short Messages Service (SMS) parameters

Parameters that can be used by the GSM telephone for outgoing SMS messages. Each parameter consists of the following elements:

Position
: *Storage position of the parameter set*

Name
: *(Optional) text describing the set.*

TP-DestinationAddress
: *Number of a recipient (usually left blank, as this normally differs for each message).*

TP-ServiceCentreAddress
: *Number of a service centre where the messages are processed.*

TP-ValidityPeriod
: *The period of validity of a message. When a message has been sent but the recipient cannot be contacted, the service centre may decide, after the period of validity has lapsed, not to make any further attempts to deliver the message.*

Position	Name	Destination Address	Service Centre Address	Validity Period

1			+31628500561	162 Weeks

SMS status

An internal reference to the most recent outgoing SMS and an indication of the availability of SIM memory for storing messages, so that the GSM network can be informed as soon as memory is available.

Last transfer layer protocol message reference: 255, memory capacity exceeded: no.

SMS messages

Messages which can be received and sent with a mobile phone. The messages can also be sent in a different way: e.g. via the Internet or by telephoning a special number and recording a message, which is then converted into text and sent as an SMS message to a mobile phone. Below is an explanation of possible message elements.

Position
: *Storage position of the message.*

Ext. Type
: *Type of message according to the phone.*

Int. Type
: *Type of message according to the SMS decoder.*

Part
: *One storage position might be part of a larger message.*

Timestamp
: *Date and time when the message was received at the service centre. The date is shown as ﷿month-day-year﷿; the time is the local time at the service centre, followed by the number of hours of difference in comparison with Greenwich Mean Time. For messages of type REPORT the time stamp identifies the time when the service centre received the message related to the report*

Discharge timestamp
: *Parameter identifying the time associated with a particular status outcome*

Validity Period
: *When a message has been sent but the recipient cannot be contacted, the service centre may decide, after the period of validity has elapsed, not to make any further attempts to deliver the message.*

Service Centre Address
: *Number of the service centre where the messages is processed.*

Originating Address
: *Number of the sender.*

Destination Address
: *Number of the recipient.*