ETSI TS 101 888 V4.2.1 (2003-12)

Technical Specification

Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Test Scenarios; Security testing - H.323 environment

Reference

RTS/TIPHON-06014R4[2]

Keywords

H.323, IP, protocol, telephony, testing, security,
VoIP

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Project Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON).

1 Scope

The scope of the present document is to define the security test specifications for TIPHON Release 4 for the H.323 [5] environment.

The security methods considered in the present document are related only to IP based networks. The signalling path and the media path in the SCN is considered to be secure ("Trust by wire").

This security test specification does not explain recommendation H.235 [2] and the annexes, nor does it explain how to implement the security procedures. For further information on H.235, please refer to [2] or [4].

Rather, the present document provides a step-wise implementation approach showing example security message processing along with the generated output.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

[1] ITU-T Recommendation H.225.0: "Call signalling protocols and media stream packetization for packet based multimedia communication systems".

[2] ITU-T Recommendation H.235: "Security and Encryption for H.series (H.323 and other H.245 based) multimedia terminals ".

[3] ITU-T Recommendation H.235 Annex F: "Hybrid Security Profile".

[4] ITU-T Recommendation H.245: "Control protocol for multimedia communication".

[5] ITU-T Recommendation H.323: "Packet based multimedia communications systems".

[6] ETSI TS 101 883: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Interface Protocol Requirements Definition; Implementation of TIPHON architecture using H.323".

3 Definitions and abbreviations

3.1 Definitions

For the purpose of the present document, the definitions given in the IUT-T Recommendations H.225.0 [1], H.235 [2], H.245 [4] and H.323 [5].

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

A	Audio
ARQ	Admissions ReQuest
ACF	Admissions ConFirm
ARJ	Admissions Reject
A/V	Audio/Video
D	Data
DRQ	Disengage Request
DCF	Disengage Confirm
IP	Internet Protocol
LRQ	Location Request
LCF	Location Confirm
QoS	Quality of Service
SCN	Switched Circuit Networks

4 Security test strategy

Security testing should be performed after a vendor has completed product and system testing with the ETSI testing standards.

The basic idea for security testing is to show the generation and insertion of the security bits into the specific parameters of the H.323 [5] messages. Because this mechanism is exactly the same on the senders and the receiver's side, no distinction is necessary.

To test entities for their implementation of security two entities (that are already interworking) need to be connected. In the case of an incorrect security information it is necessary to go into the detail of the generation of the security bits. In order to be able to determine the reason for this failure the security tests strategy is just to look at the different steps of the generation and insertion of the security bits into the protocol elements. This is the only way to determine the failure.

The Security testing shall be performed for the following configurations:

- Signalling path:
  - Gatekeeper and Terminal;
  - Gatekeeper and Gateway;
  - Gatekeeper and Gatekeeper.
- Media path:
  - Terminal and Terminal;
  - Terminal and Gateway;
  - Gateway and Gateway.

- Global Service Providers:
  - BES and TRC;
  - BES and CH;
  - BES and CA.

The security testing shall be performed in three different parts where the first part deals with the security testing for the signalling path (Terminal, Gatekeeper, Gateway) using annex D of H.235 [2]. The second part deals with the security aspects for the signalling path equivalent to the first but using annex F of H.235 [2] and the media path using H.235. The third part handles the security testing from the BES to the global service providers.

5 H.235 Annex D

5.1 Overview

Figure 1 shows the basic steps to be taken at the originating entity and illustrates the procedures specified by Annex D of H.235 [2], in particular clauses D.6.3.2 and D.6.3.3.

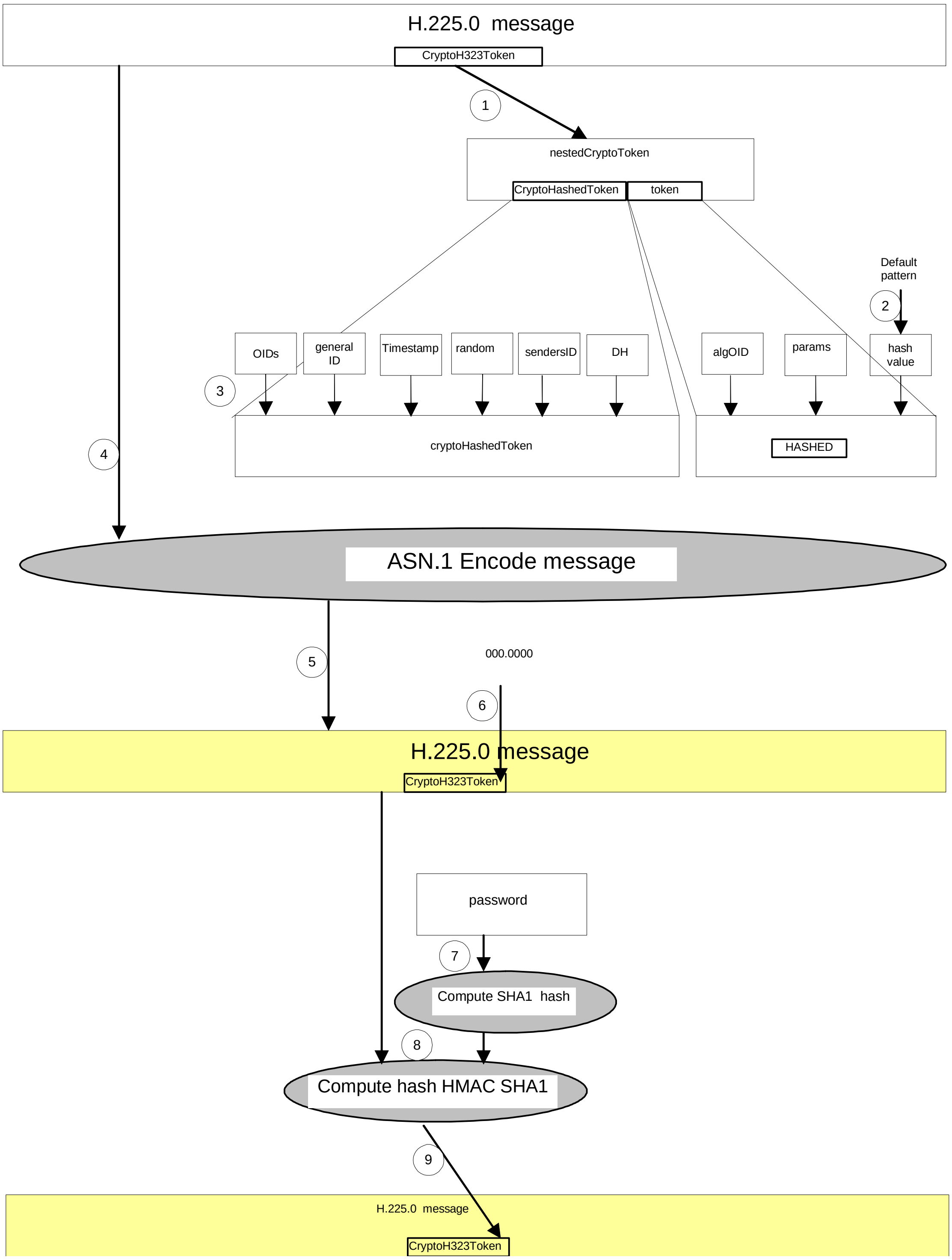

Figure 1: Stepwise approach for sender

Figure 2 shows the basic steps to be taken at the receiving side starting with the entire message, decoding, breaking it into pieces and extracting the necessary parts and the final computation/verification step.

NOTE 1: The figures just visualize the essential steps as an example and correlate with the print out in clause 5.3; in any case, the procedures and description of annex D of H.235 [2] take precedence.

NOTE 2: The print out in clause 5.4 reflect H.235 V2 with the sendersID used.

NOTE 3: The figures and print out reflect a scenario endpoint to gatekeeper; other scenarios and examples are not shown.

NOTE 4: The default pattern is a local value that is being used temporarily when computing the hash value, see clause D.6.3.3.2 of H.235 [2].

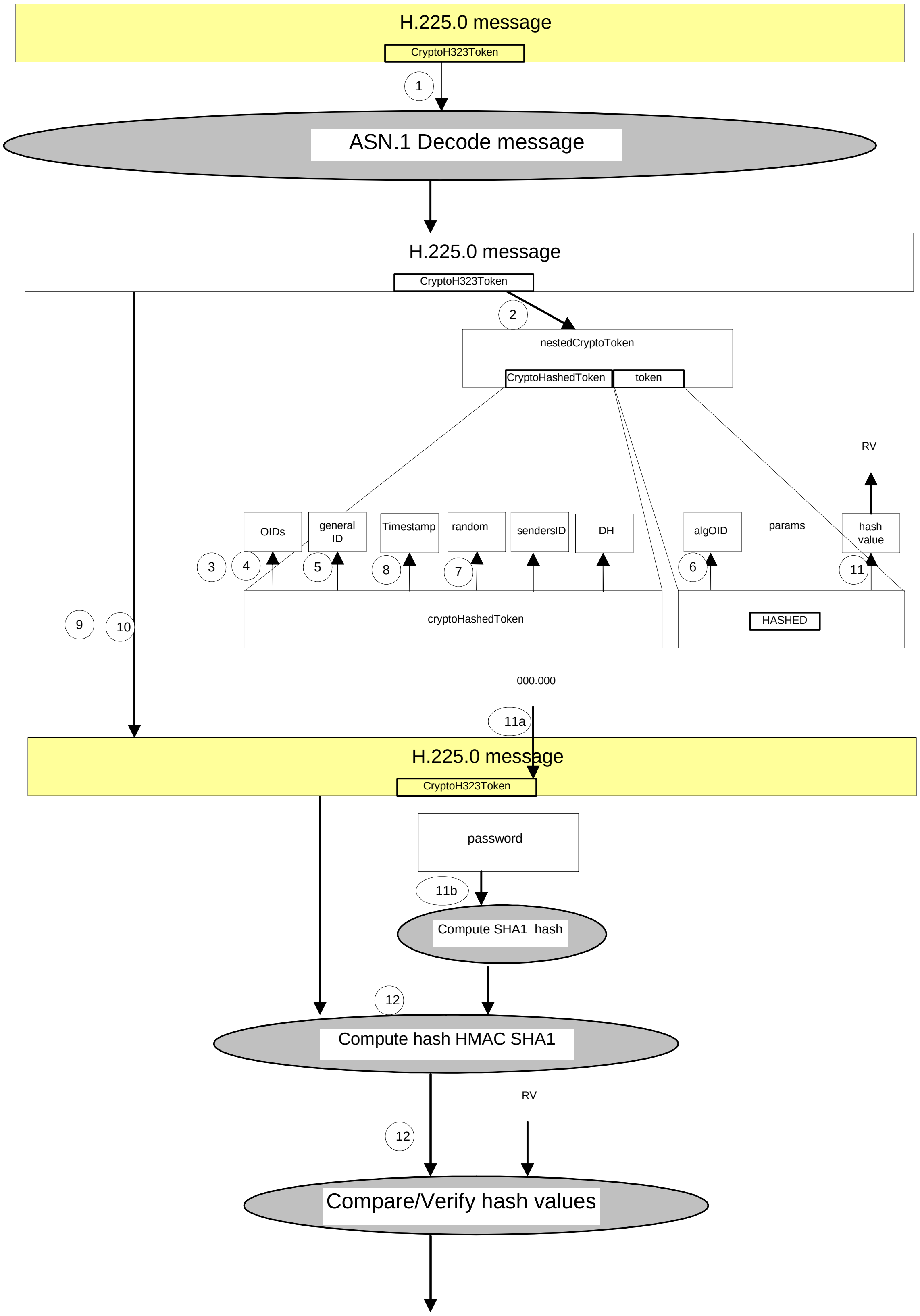

Figure 2: Stepwise approach for receiver

5.2 Received message

The examples shown in clauses 5.2 and 5.3 use the RRQ sent by a Terminal and received at the Gatekeeper. The print out in clauses 5.2 and 5.3 reflects H.235V1, i.e. sendersID is not used.

- The received RRQ message is given in binary and with all fields shown.
- The received binary message part is given and the separate steps shown for the verification.

Password = fries

SHA1 = 91 27 1C 95 F0 A3 A0 6F 0D 79 75 B1 19 5F A1 28 8A 86 B6 D4

A received RRQ message with embedded Cryptotoken:

```
*********************************
*  RECEIVE RRQ FROM EP AT GK  *
*********************************


14:34:12 TPKTCHAN: Address:
14:34:12 TPKTCHAN:  0> <14> TransportAddress = (0) .  <1084> CHOICE ...
14:34:12 TPKTCHAN:  1> . <289> ipAddress = (0) .  <1081> SEQUENCE
14:34:12 TPKTCHAN:  2> . . <290> ip = (4) '...j' =0x8b17ca6a <139.23.202.106> .  <1066> OCTET STRING
(4..4)
14:34:12 TPKTCHAN:  2> . . <292> port = (1720) .  <115> INTEGER (0..65535)
14:34:21 UDPCHAN: New message (channel 0) recv <-- registrationRequest:
14:34:21 UDPCHAN: Address:
14:34:21 UDPCHAN:  0> <669> TransportAddress = (0) .  <1084> CHOICE ...
14:34:21 UDPCHAN:  1> . <670> ipAddress = (0) .  <1081> SEQUENCE
14:34:21 UDPCHAN:  2> . . <671> ip = (4) '...j' =0x8b17ca6a <139.23.202.106> .  <1066> OCTET STRING
(4..4)
14:34:21 UDPCHAN:  2> . . <673> port = (1151) .  <115> INTEGER (0..65535)
14:34:21 UDPCHAN: Binary:
14:34:21 UDPCHAN: 00000   0f 80 3a 27 06 00 08 91 4a 00 02 00 08 2b 0c 02    |.€:'..."J....+..|
14:34:21 UDPCHAN: 00016   88 53 02 06 01 80 84 01 40 00 08 00 00 00 00 00    |ˆS...€„.@.......|
14:34:21 UDPCHAN: 00032   00 21 72 00 5b 6f 20 00 52 00 07 00 00 fb 38 00    |.!r.[o .R....û8.|
14:34:21 UDPCHAN: 00048   12 fa 68 00 12 c5 19 00 50 6f 20 00 52 00 07 00    |.úh..Å..Po .R...|
14:34:21 UDPCHAN: 00064   00 fb 38 00 12 fa 68 00 12 00 00 00 00 00 00 00    |.û8..úh.........|
14:34:21 UDPCHAN: 00080   00 6c c0 00 50 fb 38 00 12 fa 94 00 12 fa 9c 00    |.lÀ.Pû8..ú"..úœ.|
14:34:21 UDPCHAN: 00096   12 01 ec 00 00 02 36 00 00 00 0e 00 00 02 36 00    |..ì...6.......6.|
14:34:21 UDPCHAN: 00112   00 60 76 3d 18 20 ec f3 2e 00 00 00 00 9d b5 72    |.`v=. ìó.....•µr|
14:34:21 UDPCHAN: 00128   5a 00 50 00 c2 01 ee 00 00 00 00 00 00 ff ff ff    |Z.P.Â.î......ÿÿÿ|
14:34:21 UDPCHAN: 00144   ff 20 31 20 33 32 31 32 20 1e 00 00 01 00 8b 17    |ÿ 1 3212 .....‹.|
14:34:21 UDPCHAN: 00160   ca 6a 04 80 01 00 8b 17 ca 6a 04 7f 22 c0 0b 0b    |Êj.€..‹.Êj.•"À..|
14:34:21 UDPCHAN: 00176   00 0b 0f 54 65 73 74 20 61 70 70 6c 69 63 61 74    |...Test applicat|
14:34:21 UDPCHAN: 00192   69 6f 6e 08 52 41 44 56 69 73 69 6f 6e 00 02 08    |ion.RADVision...|
14:34:21 UDPCHAN: 00208   00 46 c3 56 53 54 39 34 48 54 04 00 35 00 33 00    |.FÃVST94HT..5.3.|
14:34:21 UDPCHAN: 00224   34 00 30 00 33 60 0b 0b 00 0b 0f 54 65 73 74 20    |4.0.3`.....Test |
14:34:21 UDPCHAN: 00240   61 70 70 6c 69 63 61 74 69 6f 6e 08 52 41 44 56    |application.RADV|
14:34:21 UDPCHAN: 00256   69 73 69 6f 6e 12 2b 80 56 01 74 07 00 08 81 6b    |ision.+€V.t...•k|
14:34:21 UDPCHAN: 00272   00 01 01 45 00 07 00 08 81 6b 00 01 05 c0 3a 22    |...E....•k...À:"|
14:34:21 UDPCHAN: 00288   62 db 01 29 22 00 53 00 69 00 65 00 6d 00 65 00    |bÛ.)".S.i.e.m.e.|
14:34:21 UDPCHAN: 00304   6e 00 73 00 20 00 47 00 61 00 74 00 65 00 6b 00    |n.s. .G.a.t.e.k.|
14:34:21 UDPCHAN: 00320   65 00 65 00 70 00 65 00 72 07 00 08 81 6b 00 01    |e.e.p.e.r...•k..|
14:34:21 UDPCHAN: 00336   06 00 60 07 89 a6 ee 75 bb 59 c1 a6 ca a4 72 01    |..`.‰¦îu»YÁ¦Ê¤r.|
14:34:21 UDPCHAN: 00352   00 01 00 01 00 01 00                               |.......|


14:34:21 UDPCHAN: Message:
14:34:21 UDPCHAN:  0> <584> RasMessage = (6502) .  <771> CHOICE ...
14:34:21 UDPCHAN:  1> . <586> registrationRequest = (4294967185) .  <702> SEQUENCE ...
14:34:21 UDPCHAN:  2> . . <587> requestSeqNum = (14888) .  <883> INTEGER (1..65535)
14:34:21 UDPCHAN:  2> . . <588> protocolIdentifier = (6)  { itu-t recommendation h 2250 0 2 }.
<878> OBJECT IDENTIFIER
14:34:21 UDPCHAN:  2> . . <590> nonStandardData = (4294967185) .  <972> SEQUENCE
14:34:21 UDPCHAN:  3> . . . <591> nonStandardIdentifier = (10964) .  <969> CHOICE ...
14:34:21 UDPCHAN:  4> . . . . <592> object = (8)  { iso identified-organization 12 2 1107 2 6 1 }.
<121> OBJECT IDENTIFIER
14:34:21 UDPCHAN:  3> . . . <594> data = (132) '.@........!r.[o .R.....8...h.....Po
.R.....8...h..........l..P.8...............6.......6..`v=. .........rZ.P.............. 1 321'
=0x014000080000000000002172005b6f2000.  <125> OCTET STRING
14:34:21 UDPCHAN:  2> . . <601> discoveryComplete = (0) .  <83> BOOLEAN
14:34:21 UDPCHAN:  2> . . <602> callSignalAddress = (1) .  <381> SEQUENCE OF
14:34:21 UDPCHAN:  3> . . . <603> * = (6669) .  <1084> CHOICE ...
14:34:21 UDPCHAN:  4> . . . . <604> ipAddress = (4294967185) .  <1081> SEQUENCE
14:34:21 UDPCHAN:  5> . . . . . <605> ip = (4) '...j' =0x8b17ca6a <139.23.202.106> .  <1066> OCTET
STRING (4..4)
14:34:21 UDPCHAN:  5> . . . . . <607> port = (1152) .  <115> INTEGER (0..65535)
14:34:21 UDPCHAN:  2> . . <608> rasAddress = (1) .  <381> SEQUENCE OF
14:34:21 UDPCHAN:  3> . . . <609> * = (6669) .  <1084> CHOICE ...
14:34:21 UDPCHAN:  4> . . . . <610> ipAddress = (4294967185) .  <1081> SEQUENCE
14:34:21 UDPCHAN:  5> . . . . . <611> ip = (4) '...j' =0x8b17ca6a <139.23.202.106> .  <1066> OCTET
```

```
STRING (4..4)
14:34:21 UDPCHAN:  5> . . . . . <613> port = (1151) .  <115> INTEGER (0..65535)
14:34:21 UDPCHAN:  2> . . <614> terminalType = (4294967185) .  <1050> SEQUENCE ...
14:34:21 UDPCHAN:  3> . . . <615> vendor = (4294967185) .  <980> SEQUENCE ...
14:34:21 UDPCHAN:  4> . . . . <616> vendor = (4294967185) .  <975> SEQUENCE ...
14:34:21 UDPCHAN:  5> . . . . . <617> t35CountryCode = (11) .  <116> INTEGER (0..255)
14:34:21 UDPCHAN:  5> . . . . . <618> t35Extension = (11) .  <116> INTEGER (0..255)
14:34:21 UDPCHAN:  5> . . . . . <619> manufacturerCode = (11) .  <115> INTEGER (0..65535)
14:34:21 UDPCHAN:  4> . . . . <620> productId = (16) 'Test application'
=0x546573742061707706c69636174696f6e.  <979> OCTET STRING (1..256)
14:34:21 UDPCHAN:  4> . . . . <622> versionId = (9) 'RADVision' =0x524144566973696f6e.  <979> OCTET
STRING (1..256)
14:34:21 UDPCHAN:  3> . . . <624> terminal = (4294967185) .  <986> SEQUENCE ...
14:34:21 UDPCHAN:  3> . . . <625> mc = (0) .  <83> BOOLEAN
14:34:21 UDPCHAN:  3> . . . <626> undefinedNode = (0) .  <83> BOOLEAN
14:34:21 UDPCHAN:  2> . . <627> terminalAlias = (2) .  <380> SEQUENCE OF
14:34:21 UDPCHAN:  3> . . . <628> * = (3942) .  <962> CHOICE ...
14:34:21 UDPCHAN:  4> . . . . <629> e164 = (17) '13902320210601152'
=0x3133393032333230323130363031313532.  <961> IA5String (1..128) FROM '#*,0123456789'
14:34:21 UDPCHAN:  3> . . . <631> * = (4187) .  <962> CHOICE ...
14:34:21 UDPCHAN:  4> . . . . <632> h323-ID = (10) '.5.3.4.0.3' =0x00350033003400300033.  <960>
BMPString (1..256)
14:34:21 UDPCHAN:  2> . . <634> endpointVendor = (4294967185) .  <980> SEQUENCE ...
14:34:21 UDPCHAN:  3> . . . <635> vendor = (4294967185) .  <975> SEQUENCE ...
14:34:21 UDPCHAN:  4> . . . . <636> t35CountryCode = (11) .  <116> INTEGER (0..255)
14:34:21 UDPCHAN:  4> . . . . <637> t35Extension = (11) .  <116> INTEGER (0..255)
14:34:21 UDPCHAN:  4> . . . . <638> manufacturerCode = (11) .  <115> INTEGER (0..65535)
14:34:21 UDPCHAN:  3> . . . <639> productId = (16) 'Test application'
=0x546573742061707706c69636174696f6e.  <979> OCTET STRING (1..256)
14:34:21 UDPCHAN:  3> . . . <641> versionId = (9) 'RADVision' =0x524144566973696f6e.  <979> OCTET
STRING (1..256)
14:34:21 UDPCHAN:  2> . . <643> cryptoTokens = (1) .  <283> SEQUENCE OF
14:34:21 UDPCHAN:  3> . . . <644> * = (4466) .  <832> CHOICE ...
14:34:21 UDPCHAN:  4> . . . . <645> nestedcryptoToken = (9106) .  <192> CHOICE ...
14:34:21 UDPCHAN:  5> . . . . . <646> cryptoHashedToken = (4294967185) .  <177> SEQUENCE
14:34:21 UDPCHAN:  6> . . . . . . <647> tokenOID = (7)  { itu-t recommendation h 235 0 1 1 }.  <121>
OBJECT IDENTIFIER
14:34:21 UDPCHAN:  6> . . . . . . <649> hashedVals = (4294967185) .  <239> SEQUENCE ...
14:34:21 UDPCHAN:  7> . . . . . . . <650> tokenOID = (7)  { itu-t recommendation h 235 0 1 5 }.
<121> OBJECT IDENTIFIER
14:34:21 UDPCHAN:  7> . . . . . . . <652> timeStamp = (975332060) .  <281> INTEGER (1..-1)
14:34:21 UDPCHAN:  7> . . . . . . . <653> random = (41) .  <280> INTEGER
14:34:21 UDPCHAN:  7> . . . . . . . <654> generalID = (36) '.S.i.e.m.e.n.s. .G.a.t.e.k.e.e.p.e.r'
=0x005300690065006d0065006e0073002000.  <278> BMPString (1..128)
14:34:21 UDPCHAN:  6> . . . . . . <657> token = (4294967185) .  <231> SEQUENCE
14:34:21 UDPCHAN:  7> . . . . . . . <658> algorithmOID = (7)  { itu-t recommendation h 235 0 1 6 }.
<121> OBJECT IDENTIFIER
14:34:21 UDPCHAN:  7> . . . . . . . <660> paramS = (4294967185) .  <226> SEQUENCE ...
14:34:21 UDPCHAN:  8> . . . . . . . . <661> null = (4294967173) .  <95> NULL
14:34:21 UDPCHAN:  7> . . . . . . . <662> hash = (96) '....u.Y....r' =0x0789a6ee75bb59c1a6caa47200.
<139> BIT STRING
14:34:21 UDPCHAN:  2> . . <664> keepAlive = (0) .  <83> BOOLEAN
14:34:21 UDPCHAN:  2> . . <665> willSupplyUUIEs = (0) .  <83> BOOLEAN
14:34:21 UDPCHAN:  2> . . <666> maintainConnection = (0) .  <83> BOOLEAN
14:34:21 UDPCHAN:  2> . . <667> supportsAnnexECallSignalling = (0) .  <83> BOOLEAN
```

5.3 Separate steps

Verification steps for the obtained CryptoToken:

```
*********************************
*  RECEIVE RRQ FROM EP AT GK  *
*********************************

00:08:31 | _UDP_IN_registrationRequest_for_nodeId_492_(packet length 215 Bytes)_____________
0000:08:31 | 0000: 0e 80 3a 27  06 00 08 91  4a 00 02 00  01 00 8b 17  '..:'....J.......'
0000:08:31 | 0010: ca 6a 04 80  01 00 8b 17  ca 6a 04 7f  22 c0 0b 0b  '.j.......j.."...'
0000:08:31 | 0020: 00 0b 0f 54  65 73 74 20  61 70 70 6c  69 63 61 74  '...Test applicat'
0000:08:31 | 0030: 69 6f 6e 08  52 41 44 56  69 73 69 6f  6e 00 02 08  'ion.RADVision...'
0000:08:31 | 0040: 00 46 c3 56  53 54 39 34  48 54 04 00  35 00 33 00  '.F.VST94HT..5.3.'
0000:08:31 | 0050: 34 00 30 00  33 60 0b 0b  00 0b 0f 54  65 73 74 20  '4.0.3`.....Test '
0000:08:32 | 0060: 61 70 70 6c  69 63 61 74  69 6f 6e 08  52 41 44 56  'application.RADV'
0000:08:32 | 0070: 69 73 69 6f  6e 12 2b 80  56 01 74 07  00 08 81 6b  'ision.+.V.t....k'
0000:08:32 | 0080: 00 01 01 45  00 07 00 08  81 6b 00 01  05 c0 3a 22  '...E.....k....:"'
0000:08:32 | 0090: 62 db 01 29  22 00 53 00  69 00 65 00  6d 00 65 00  'b..)".S.i.e.m.e.'
0000:08:32 | 00a0: 6e 00 73 00  20 00 47 00  61 00 74 00  65 00 6b 00  'n.s. .G.a.t.e.k.'
0000:08:32 | 00b0: 65 00 65 00  70 00 65 00  72 07 00 08  81 6b 00 01  'e.e.p.e.r....k..'
0000:08:33 | 00c0: 06 00 60 07  89 a6 ee 75  bb 59 c1 a6  ca a4 72 01  '..`....u.Y....r.'
0000:08:33 | 00d0: 00 01 00 01  00 01 00                               '.......'
0000:08:33 | _______________________________________________________
0000:08:33 | -------------------------------------------------------
```

1. Determine IP-Address:

```
0000:08:33 | New message recv <- registrationRequest on RAS from 492
0000:08:33 | Read IP Address for EP 139.23.202.106:1151
```

2. Read alias:

```
0000:08:66 | EP Alias 53403-> Get User Info (from external database):
0000:08:66 | -> User=Fries, UID=53403, PWLen=20, LC=Wed Aug 25 13:52:19 1999
0000:08:66 | -> Hashed Passphrase (fries sha1-hashed):
0000:08:67 | 0000: 91 27 1c 95  f0 a3 a0 6f  0d 79 75 b1  19 5f a1 28  '.'.....o.yu.._.('
0000:08:67 | 0010: 8a 86 b6 d4                                         '....'
```

3. Read CryptoTokenOID:

```
0000:08:67 | Recv/RecvFrom: Found Crypto Token: token len = 15 Bytes, tokenOID =
0000:08:67 | 0000: 30 20 30 20  38 20 32 33  35 20 30 20  31 20 31     '0 0 8 235 0 1 1'
```

4. Read ClearTokenOID:

```
0000:08:67 | Recv/RecvFrom: Found Crypto Token: token len = 15 Bytes, tokenOID (2) =
0000:08:67 | 0000: 30 20 30 20  38 20 32 33  35 20 30 20  31 20 35     '0 0 8 235 0 1 5'
```

5. Read generalID:

```
0000:08:68 | RecvFrom: Found Crypto Token: token len = 36 Bytes, generalID =
0000:08:68 | 0000: 00 53 00 69  00 65 00 6d  00 65 00 6e  00 73 00 20  '.S.i.e.m.e.n.s. '
0000:08:68 | 0010: 00 47 00 61  00 74 00 65  00 6b 00 65  00 65 00 70  '.G.a.t.e.k.e.e.p'
0000:08:68 | 0020: 00 65 00 72                                         '.e.r'
```

6. Read algorithmOID:

```
0000:08:68 | Recv/RecvFrom: Found Crypto Token: token len = 15 Bytes, algorithmOID =
0000:08:68 | 0000: 30 20 30 20  38 20 32 33  35 20 30 20  31 20 36     '0 0 8 235 0 1 6'
```

7. Read Sequence Number:

```
0000:08:68 | Recv/RecvFrom: Found Crypto Token: sequence_number = 41
```

8. Read timestamp:

```
0000:08:68 | Recv/RecvFrom: Found Crypto Token: timestamp = 975332060
```

9. Read token value:

```
0000:08:68 | Recv/RecvFrom: Found Crypto Token: token len = 96 Bits, token value =
0000:08:68 | 0000: 07 89 a6 ee  75 bb 59 c1  a6 ca a4 72               '....u.Y....r'
```

10. Perform verification checks:

```
0000:08:68 | Recv/RecvFrom: (h235_checkToken) clear token OID check passed
0000:08:68 | Recv/RecvFrom: (h235_checkToken) crypto token OID check passed
0000:08:68 | Recv/RecvFrom: (h235_checkToken) crypto algorithm OID check passed
0000:08:68 | Recv/RecvFrom: (h235_checkToken) time value in range
0000:08:68 | Recv/RecvFrom: (h235_checkToken) generalID check passed
```

11. Locate and read hash value:

```
0000:08:69 | Recv/RecvFrom: (h235_checkToken) found ICV in raw message on position 195
0000:08:69 | 0000: 07 89 a6 ee  75 bb 59 c1  a6 ca a4 72               '....u.Y....r'
```

12. Re-compute hash value:

```
0000:08:69 | Crypto-Module: Start Message Hash Session
0000:08:69 | Crypto-Module: End Message Hash Session
```

13. Verify hash value:

```
0000:08:69 | ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
0000:08:69 | +                                                                        +
0000:08:69 | +                      SUCCESSFUL INTEGRITY CHECK                        +
0000:08:69 | + Recv/RecvFrom: registrationRequest on RAS:
0000:08:69 | + VALID TOKEN received from User Fries (ID: 53403)
0000:08:69 | +                                                                        +
0000:08:69 | ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

5.4 RRQ message with H.235 V2

This example shows an initial RRQ message (without any senders ID) that is being encoded with H.235 [2] Version 2.

Password = fries

SHA1 = 91 27 1C 95 F0 A3 A0 6F 0D 79 75 B1 19 5F A1 28 8A 86 B6 D4

```
13:45:14 UDPCHAN: INFO  - New message (channel 0)  recv <-- registrationRequest:
13:45:14 UDPCHAN: Address:
13:45:14 UDPCHAN:  0> <557> TransportAddress = (0) .  <4579> CHOICE ...
13:45:14 UDPCHAN:  1> . <558> ipAddress = (0) .  <4570> SEQUENCE
13:45:14 UDPCHAN:  2> . . <559> ip = (4) '‹.Ì.' =0x8b17cc2e <139.23.204.46> .  <4520> OCTET STRING
(4..4)
13:45:14 UDPCHAN:  2> . . <561> port = (1575) .  <155> INTEGER (0..65535)
13:45:14 UDPCHAN: Binary:
13:45:14 UDPCHAN: 00000   0e c0 7a fe 06 00 08 91 4a 00 04 00 01 00 8b 17    |.Àzþ..."J.....‹.|
13:45:14 UDPCHAN: 00016   cc 2e 06 26 01 00 8b 17 cc 2e 06 27 22 c0 0b 0b    |Ì..&..‹.Ì..'"À..|
13:45:14 UDPCHAN: 00032   00 0b 0f 54 65 73 74 20 61 70 70 6c 69 63 61 74    |...Test applicat|
13:45:14 UDPCHAN: 00048   69 6f 6e 08 52 41 44 56 49 53 49 4f 4e 00 02 02    |ion.RADVISION...|
13:45:14 UDPCHAN: 00064   00 86 73 64 04 00 35 00 33 00 34 00 30 00 33 22    |.†sd..5.3.4.0.3"|
13:45:14 UDPCHAN: 00080   00 53 00 69 00 65 00 6d 00 65 00 6e 00 73 00 20    |.S.i.e.m.e.n.s. |
13:45:14 UDPCHAN: 00096   00 47 00 61 00 74 00 65 00 6b 00 65 00 65 00 70    |.G.a.t.e.k.e.e.p|
13:45:14 UDPCHAN: 00112   00 65 00 72 60 0b 0b 00 0b 0f 54 65 73 74 20 61    |.e.r`.....Test a|
13:45:14 UDPCHAN: 00128   70 70 6c 69 63 61 74 69 6f 6e 08 52 41 44 56 49    |pplication.RADVI|
13:45:14 UDPCHAN: 00144   53 49 4f 4e 28 2b 00 00 57 01 74 07 00 08 81 6b    |SION(+..W.t...•k|
13:45:14 UDPCHAN: 00160   00 02 01 45 00 07 00 08 81 6b 00 02 05 c0 3c e3    |...E....•k...À<ã|
13:45:14 UDPCHAN: 00176   9b c9 02 21 7c 22 00 53 00 69 00 65 00 6d 00 65    |›É.!|".S.i.e.m.e|
13:45:14 UDPCHAN: 00192   00 6e 00 73 00 20 00 47 00 61 00 74 00 65 00 6b    |.n.s. .G.a.t.e.k|
13:45:14 UDPCHAN: 00208   00 65 00 65 00 70 00 65 00 72 07 00 08 81 6b 00    |.e.e.p.e.r...•k.|
13:45:14 UDPCHAN: 00224   02 06 00 60 6d 3b ad 49 bf c9 73 87 0a 82 ac 06    |...`m;-I¿És‡.,¬.|
13:45:14 UDPCHAN: 00240   01 00 01 00 01 00                                  |......|
13:45:14 UDPCHAN: Message:
13:45:14 UDPCHAN:  0> <483> RasMessage = (0) .  <2731> CHOICE ...
13:45:14 UDPCHAN:  1> . <484> registrationRequest = (4294967185) .  <2461> SEQUENCE ...
13:45:14 UDPCHAN:  2> . . <485> requestSeqNum = (31487) .  <3615> INTEGER (1..65535)
13:45:14 UDPCHAN:  2> . . <486> protocolIdentifier = (6) { itu-t recommendation h 2250 0 4 }.
<3594> OBJECT IDENTIFIER
13:45:14 UDPCHAN:  2> . . <488> discoveryComplete = (0) .  <0> BOOLEAN
13:45:14 UDPCHAN:  2> . . <489> callSignalAddress = (1) .  <1151> SET OF CHOICE ...
13:45:14 UDPCHAN:  3> . . . <490> * = (10714) .  <4579> CHOICE ...
13:45:14 UDPCHAN:  4> . . . . <491> ipAddress = (4294967185) .  <4570> SEQUENCE
13:45:14 UDPCHAN:  5> . . . . . <492> ip = (4) '‹.Ì.' =0x8b17cc2e <139.23.204.46> .  <4520> OCTET
STRING (4..4)
13:45:14 UDPCHAN:  5> . . . . . <494> port = (1574) .  <155> INTEGER (0..65535)
13:45:14 UDPCHAN:  2> . . <495> rasAddress = (1) .  <1151> SET OF CHOICE ...
13:45:14 UDPCHAN:  3> . . . <496> * = (10714) .  <4579> CHOICE ...
13:45:14 UDPCHAN:  4> . . . . <497> ipAddress = (4294967185) .  <4570> SEQUENCE
13:45:14 UDPCHAN:  5> . . . . . <498> ip = (4) '‹.Ì.' =0x8b17cc2e <139.23.204.46> .  <4520> OCTET
STRING (4..4)
13:45:14 UDPCHAN:  5> . . . . . <500> port = (1575) .  <155> INTEGER (0..65535)
13:45:14 UDPCHAN:  2> . . <501> terminalType = (4294967185) .  <4403> SEQUENCE ...
13:45:14 UDPCHAN:  3> . . . <502> vendor = (4294967185) .  <4186> SEQUENCE ...
13:45:14 UDPCHAN:  4> . . . . <503> vendor = (4294967185) .  <4169> SEQUENCE ...
13:45:14 UDPCHAN:  5> . . . . . <504> t35CountryCode = (11) .  <45> INTEGER (0..255)
13:45:14 UDPCHAN:  5> . . . . . <505> t35Extension = (11) .  <45> INTEGER (0..255)
13:45:14 UDPCHAN:  5> . . . . . <506> manufacturerCode = (11) .  <155> INTEGER (0..65535)
13:45:14 UDPCHAN:  4> . . . . <507> productId = (16) 'Test application'
=0x54657374206170706c69636174696f6e .  <4181> OCTET STRING (1..256)
13:45:14 UDPCHAN:  4> . . . . <509> versionId = (9) 'RADVISION' =0x524144564953494f4e .  <4181>
OCTET STRING (1..256)
13:45:14 UDPCHAN:  3> . . . <511> terminal = (4294967185) .  <4204> SEQUENCE ...
13:45:14 UDPCHAN:  3> . . . <512> mc = (0) .  <0> BOOLEAN
13:45:14 UDPCHAN:  3> . . . <513> undefinedNode = (0) .  <0> BOOLEAN
13:45:14 UDPCHAN:  2> . . <514> terminalAlias = (2) .  <1147> SET OF CHOICE ...
13:45:14 UDPCHAN:  3> . . . <515> * = (8122) .  <4095> CHOICE ...
13:45:14 UDPCHAN:  4> . . . . <516> e164 = (5) '53403' =0x3533343033 .  <4089> IA5String (1..128)
FROM '#*,0123456789'
13:45:14 UDPCHAN:  3> . . . <518> * = (9613) .  <4095> CHOICE ...
13:45:14 UDPCHAN:  4> . . . . <519> h323-ID = (10) '.5.3.4.0.3' =0x00350033003400300033 .  <4084>
BMPString (1..256)
13:45:14 UDPCHAN:  2> . . <521> gatekeeperIdentifier = (36) '.S.i.e.m.e.n.s. .G.a.t.e.k.e.e.p.e.r'
=0x005300690065006d0065006e007300200047006100740065006b00650065007000650072 .  <3610> BMPString
(1..128)
13:45:14 UDPCHAN:  2> . . <524> endpointVendor = (4294967185) .  <4186> SEQUENCE ...
13:45:14 UDPCHAN:  3> . . . <525> vendor = (4294967185) .  <4169> SEQUENCE ...
13:45:14 UDPCHAN:  4> . . . . <526> t35CountryCode = (11) .  <45> INTEGER (0..255)
13:45:14 UDPCHAN:  4> . . . . <527> t35Extension = (11) .  <45> INTEGER (0..255)
13:45:14 UDPCHAN:  4> . . . . <528> manufacturerCode = (11) .  <155> INTEGER (0..65535)
13:45:14 UDPCHAN:  3> . . . <529> productId = (16) 'Test application'
=0x54657374206170706c69636174696f6e .  <4181> OCTET STRING (1..256)
13:45:14 UDPCHAN:  3> . . . <531> versionId = (9) 'RADVISION' =0x524144564953494f4e .  <4181> OCTET
STRING (1..256)
13:45:14 UDPCHAN:  2> . . <533> cryptoTokens = (1) .  <752> SET OF CHOICE ...
13:45:14 UDPCHAN:  3> . . . <534> * = (12045) .  <3421> CHOICE ...
13:45:14 UDPCHAN:  4> . . . . <535> nestedcryptoToken = (7314) .  <384> CHOICE ...
```

```
13:45:14 UDPCHAN:  5> . . . . . <536> cryptoHashedToken = (4294967185) .  <339> SEQUENCE
13:45:14 UDPCHAN:  6> . . . . . . <537> tokenOID = (7) { itu-t recommendation h 235 0 2 1 }.  <171>
OBJECT IDENTIFIER
13:45:14 UDPCHAN:  6> . . . . . . <539> hashedVals = (4294967185) .  <556> SEQUENCE ...
13:45:14 UDPCHAN:  7> . . . . . . . <540> tokenOID = (7) { itu-t recommendation h 235 0 2 5 }.
<171> OBJECT IDENTIFIER
13:45:14 UDPCHAN:  7> . . . . . . . <542> timeStamp = (1021549514) .  <738> INTEGER (1..-1)
13:45:14 UDPCHAN:  7> . . . . . . . <543> random = (8572) .  <735> INTEGER
13:45:14 UDPCHAN:  7> . . . . . . . <544> generalID = (36) '.S.i.e.m.e.n.s. .G.a.t.e.k.e.e.p.e.r'
=0x005300690065006d0065006e00730020004700610074006500b0065006500700065072 .  <725> BMPString
(1..128)
13:45:14 UDPCHAN:  6> . . . . . . <547> token = (4294967185) .  <532> SEQUENCE
13:45:14 UDPCHAN:  7> . . . . . . . <548> algorithmOID = (7) { itu-t recommendation h 235 0 2 6 }.
<171> OBJECT IDENTIFIER
13:45:14 UDPCHAN:  7> . . . . . . . <550> paramS = (4294967185) .  <507> SEQUENCE ...
13:45:14 UDPCHAN:  8> . . . . . . . . <551> null = (4294967173) .  <9> NULL
13:45:14 UDPCHAN:  7> . . . . . . . <552> hash = (96) 'm;-I¿És‡.,¬.' =0x6d3bad49bfc973870a82ac06 .
<243> BIT STRING
13:45:14 UDPCHAN:  2> . . <554> keepAlive = (0) .  <0> BOOLEAN
13:45:14 UDPCHAN:  2> . . <555> willSupplyUUIEs = (0) .  <0> BOOLEAN
13:45:14 UDPCHAN:  2> . . <556> maintainConnection = (0) .  <0> BOOLEAN
```

5.5 Following RFC with sendersID

The following message shows the corresponding RCF (including the senders ID).

```
13:45:14 UDPCHAN: INFO  - New message (channel 0)  sent --> registrationConfirm:
13:45:14 UDPCHAN: Address:
13:45:14 UDPCHAN:  0> <599> TransportAddress = (0) .  <4579> CHOICE ...
13:45:14 UDPCHAN:  1> . <600> ipAddress = (0) .  <4570> SEQUENCE
13:45:14 UDPCHAN:  2> . . <601> ip = (4) '‹.Ì.' =0x8b17cc2e <139.23.204.46> .  <4520> OCTET STRING
(4..4)
13:45:14 UDPCHAN:  2> . . <603> port = (1575) .  <155> INTEGER (0..65535)
13:45:14 UDPCHAN: Message:
13:45:14 UDPCHAN:  0> <565> RasMessage = (0) .  <2731> CHOICE ...
13:45:14 UDPCHAN:  1> . <566> registrationConfirm = (0) .  <2382> SEQUENCE ...
13:45:14 UDPCHAN:  2> . . <598> requestSeqNum = (31487) .  <3615> INTEGER (1..65535)
13:45:14 UDPCHAN:  2> . . <567> protocolIdentifier = (6) { itu-t recommendation h 2250 0 4 }.
<3594> OBJECT IDENTIFIER
13:45:14 UDPCHAN:  2> . . <569> callSignalAddress = (4294966741) .  <1151> SET OF CHOICE ...
13:45:14 UDPCHAN:  3> . . . <570> * = (0) .  <4579> CHOICE ...
13:45:14 UDPCHAN:  4> . . . . <571> ipAddress = (0) .  <4570> SEQUENCE
13:45:14 UDPCHAN:  5> . . . . . <572> ip = (4) '‹.Ì.' =0x8b17cc2e <139.23.204.46> .  <4520> OCTET
STRING (4..4)
13:45:14 UDPCHAN:  5> . . . . . <574> port = (1720) .  <155> INTEGER (0..65535)
13:45:14 UDPCHAN:  2> . . <579> terminalAlias = (0) .  <1147> SET OF CHOICE ...
13:45:14 UDPCHAN:  3> . . . <580> * = (0) .  <4095> CHOICE ...
13:45:14 UDPCHAN:  4> . . . . <581> e164 = (5) '53403' =0x3533343033 .  <4089> IA5String (1..128)
FROM '#*,0123456789'
13:45:14 UDPCHAN:  3> . . . <583> * = (0) .  <4095> CHOICE ...
13:45:14 UDPCHAN:  4> . . . . <584> h323-ID = (10) '.5.3.4.0.3' =0x00350033003400300033 .  <4084>
BMPString (1..256)
13:45:14 UDPCHAN:  2> . . <590> gatekeeperIdentifier = (36) '.S.i.e.m.e.n.s. .G.a.t.e.k.e.e.p.e.r'
=0x005300690065006d0065006e00730020004700610074006500b0065006500700065072 .  <3610> BMPString
(1..128)
13:45:14 UDPCHAN:  2> . . <575> endpointIdentifier = (80)
'.0.0.0.0.0.0.1.1.0.6.4.8.0.0.7.8.5.1.2.7.3.0.7.1.7.2.0.7.8.5.1.2.7.3.0.7.1.5.7.5'
=0x0030003000300030003000300031003100300036003400380030003000370038003500310032003700330030003700310
037003200300037003800350031003200370033003000370031003500370035 .  <3597> BMPString (1..128)
13:45:14 UDPCHAN:  2> . . <604> cryptoTokens = (4294966741) .  <752> SET OF CHOICE ...
13:45:14 UDPCHAN:  3> . . . <605> * = (4294966741) .  <3421> CHOICE ...
13:45:14 UDPCHAN:  4> . . . . <606> nestedcryptoToken = (4294966741) .  <384> CHOICE ...
13:45:14 UDPCHAN:  5> . . . . . <607> cryptoHashedToken = (4294966741) .  <339> SEQUENCE
13:45:14 UDPCHAN:  6> . . . . . . <608> tokenOID = (7) { itu-t recommendation h 235 0 2 1 }.  <171>
OBJECT IDENTIFIER
13:45:14 UDPCHAN:  6> . . . . . . <610> hashedVals = (4294966741) .  <556> SEQUENCE ...
13:45:14 UDPCHAN:  7> . . . . . . . <611> tokenOID = (7) { itu-t recommendation h 235 0 2 5 }.
<171> OBJECT IDENTIFIER
13:45:14 UDPCHAN:  7> . . . . . . . <622> timeStamp = (1021549514) .  <738> INTEGER (1..-1)
13:45:14 UDPCHAN:  7> . . . . . . . <621> random = (8290) .  <735> INTEGER
13:45:14 UDPCHAN:  7> . . . . . . . <613> generalID = (80)
'.0.0.0.0.0.0.1.1.0.6.4.8.0.0.7.8.5.1.2.7.3.0.7.1.7.2.0.7.8.5.1.2.7.3.0.7.1.5.7.5'
=0x0030003000300030003000300031003100300036003400380030003000370038003500310032003700330030003700310
037003200300037003800350031003200370033003000370031003500370035 .  <725> BMPString (1..128)
13:45:14 UDPCHAN:  7> . . . . . . . <618> sendersID = (36) '.S.i.e.m.e.n.s. .G.a.t.e.k.e.e.p.e.r'
=0x005300690065006d0065006e00730020004700610074006500b0065006500700065072 .  <725> BMPString
(1..128)
13:45:14 UDPCHAN:  6> . . . . . . <623> token = (4294966741) .  <532> SEQUENCE
13:45:14 UDPCHAN:  7> . . . . . . . <624> algorithmOID = (7) { itu-t recommendation h 235 0 2 6 }.
<171> OBJECT IDENTIFIER
13:45:14 UDPCHAN:  7> . . . . . . . <626> paramS = (4294966741) .  <507> SEQUENCE ...
13:45:14 UDPCHAN:  8> . . . . . . . . <627> null = (0) .  <9> NULL
13:45:14 UDPCHAN:  7> . . . . . . . <628> hash = (96) '‹.Ì.'....ÿ.ÿ' =0x8b17cc2e2706000000ff00ff .
<243> BIT STRING
13:45:14 UDPCHAN:  2> . . <577> willRespondToIRR = (0) .  <0> BOOLEAN
13:45:14 UDPCHAN:  2> . . <593> preGrantedARQ = (0) .  <2355> SEQUENCE ...
```

```
13:45:14 UDPCHAN:  3> . . . <594> makeCall = (0) .  <0> BOOLEAN
13:45:14 UDPCHAN:  3> . . . <595> useGKCallSignalAddressToMakeCall = (0) .  <0> BOOLEAN
13:45:14 UDPCHAN:  3> . . . <596> answerCall = (0) .  <0> BOOLEAN
13:45:14 UDPCHAN:  3> . . . <597> useGKCallSignalAddressToAnswer = (0) .  <0> BOOLEAN
13:45:14 UDPCHAN:  2> . . <578> maintainConnection = (0) .  <0> BOOLEAN
13:45:14 UDPCHAN: Binary:
13:45:14 UDPCHAN: 00000   12 c0 7a fe 06 00 08 91 4a 00 04 01 00 8b 17 cc    |.Àzþ..."J....‹.Ì|
13:45:14 UDPCHAN: 00016   2e 06 b8 02 02 00 86 73 64 04 00 35 00 33 00 34    |..¸...†sd..5.3.4|
13:45:14 UDPCHAN: 00032   00 30 00 33 22 00 53 00 69 00 65 00 6d 00 65 00    |.0.3".S.i.e.m.e.|
13:45:14 UDPCHAN: 00048   6e 00 73 00 20 00 47 00 61 00 74 00 65 00 6b 00    |n.s. .G.a.t.e.k.|
13:45:14 UDPCHAN: 00064   65 00 65 00 70 00 65 00 72 4e 00 30 00 30 00 30    |e.e.p.e.rN.0.0.0|
13:45:14 UDPCHAN: 00080   00 30 00 30 00 30 00 31 00 31 00 30 00 36 00 34    |.0.0.0.1.1.0.6.4|
13:45:14 UDPCHAN: 00096   00 38 00 30 00 30 00 37 00 38 00 35 00 31 00 32    |.8.0.0.7.8.5.1.2|
13:45:14 UDPCHAN: 00112   00 37 00 33 00 30 00 37 00 31 00 37 00 32 00 30    |.7.3.0.7.1.7.2.0|
13:45:14 UDPCHAN: 00128   00 37 00 38 00 35 00 31 00 32 00 37 00 33 00 30    |.7.8.5.1.2.7.3.0|
13:45:14 UDPCHAN: 00144   00 37 00 31 00 35 00 37 00 35 20 2e 00 80 ab 01    |.7.1.5.7.5 ..€«.|
13:45:14 UDPCHAN: 00160   74 07 00 08 81 6b 00 02 01 c5 00 07 00 08 81 6b    |t...•k...Å....•k|
13:45:14 UDPCHAN: 00176   00 02 05 c0 3c e3 9b c9 02 20 62 4e 00 30 00 30    |...À<ã›É. bN.0.0|
13:45:14 UDPCHAN: 00192   00 30 00 30 00 30 00 30 00 31 00 31 00 30 00 36    |.0.0.0.0.1.1.0.6|
13:45:14 UDPCHAN: 00208   00 34 00 38 00 30 00 30 00 37 00 38 00 35 00 31    |.4.8.0.0.7.8.5.1|
13:45:14 UDPCHAN: 00224   00 32 00 37 00 33 00 30 00 37 00 31 00 37 00 32    |.2.7.3.0.7.1.7.2|
13:45:14 UDPCHAN: 00240   00 30 00 37 00 38 00 35 00 31 00 32 00 37 00 33    |.0.7.8.5.1.2.7.3|
13:45:14 UDPCHAN: 00256   00 30 00 37 00 31 00 35 00 37 00 35 02 80 25 22    |.0.7.1.5.7.5.€%"|
13:45:14 UDPCHAN: 00272   00 53 00 69 00 65 00 6d 00 65 00 6e 00 73 00 20    |.S.i.e.m.e.n.s. |
13:45:14 UDPCHAN: 00288   00 47 00 61 00 74 00 65 00 6b 00 65 00 65 00 70    |.G.a.t.e.k.e.e.p|
13:45:14 UDPCHAN: 00304   00 65 00 72 07 00 08 81 6b 00 02 06 00 60 81 af    |.e.r...•k....`•¯|
13:45:14 UDPCHAN: 00320   09 03 4a 3a c3 5f 52 ae 51 46 01 00 01 00 01 00    |..J:Ã_R®QF......|
```

5.6 Test configurations

5.6.1 Gatekeeper and terminal

Clauses 5.1, 5.2, 5.3, 5.4 and 5.5 correlate to a test configuration of a Terminal and a Gatekeeper.

5.6.2 Gatekeeper and gateway

The Gatekeeper-to-Gateway communications according to H.235 [2] annex D is very similar to the terminal Gatekeeper communication. The generalID and the sendersID are the only fields that have different values.

5.6.3 Gatekeeper and Gatekeeper

The Gatekeeper-to-Gatekeeper communications according to annex D of H.235 [2] is very similar to the terminal Gatekeeper communication. The generalID and the sendersID are the only fields that have different values.

6 H.235, annex F

6.1 Overview

Figure 3 shows the basic steps to be taken for the signature computation at the originating entity. This figure illustrates the procedures specified by annex F of H.235 [2], in particular referring to the annex E clauses E.5, E.9, E.10 and E.11.

NOTE: Annex F procedures referring to annex D are not shown in the processing figures, this is analogous to clause 5.

Steps 4 and 5 in figure 3 relate to the computation of the RSA digital signature. This might be accomplished by compound crypto function. Similarly, steps 5, 6 and 7 in Figure 4 relate to the verification of the RSA digital signature and might be covered by a compound crypto function as well.

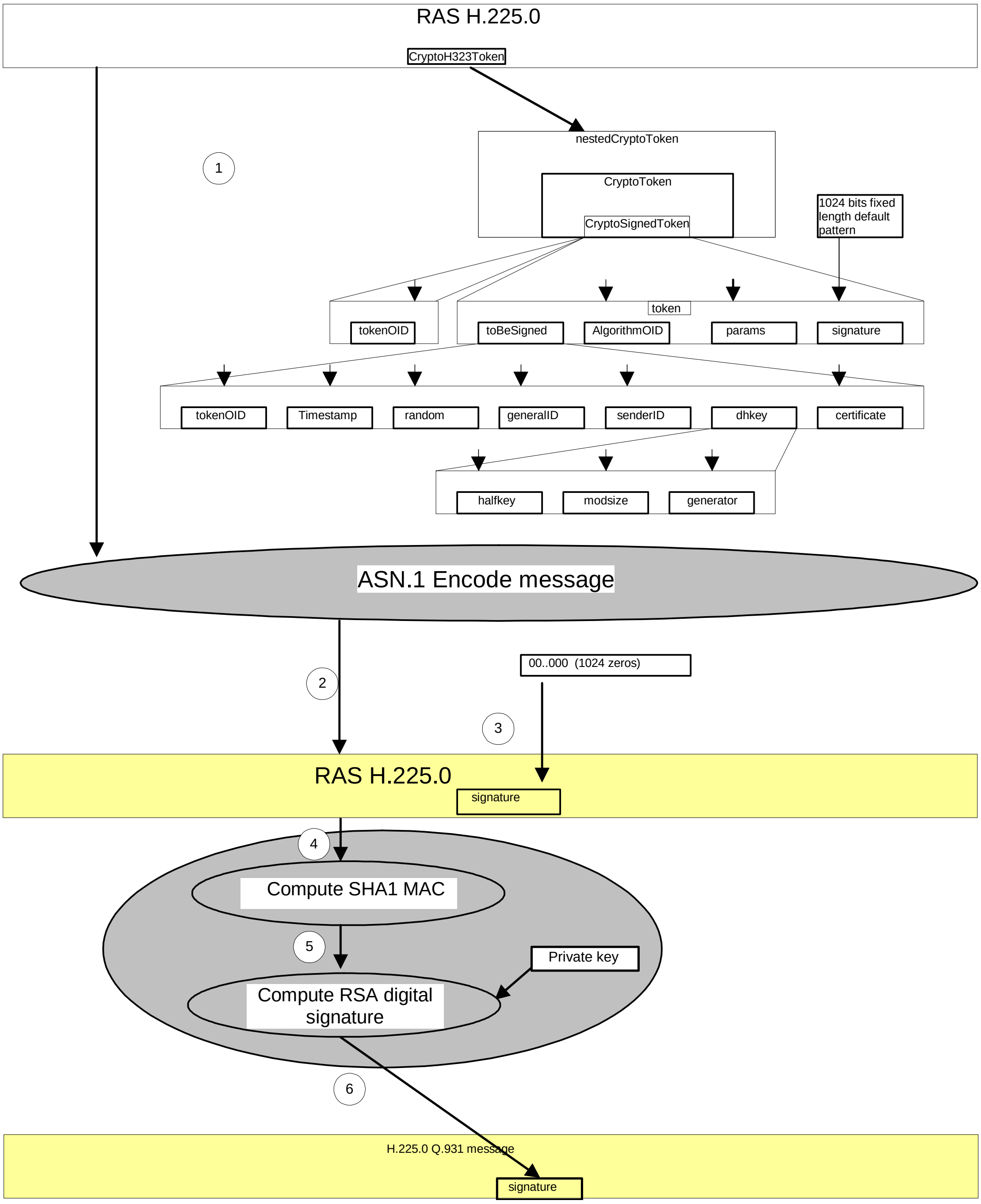

Figure 3: Signature computation at sender

The recipient receives the message and then proceeds as follows.

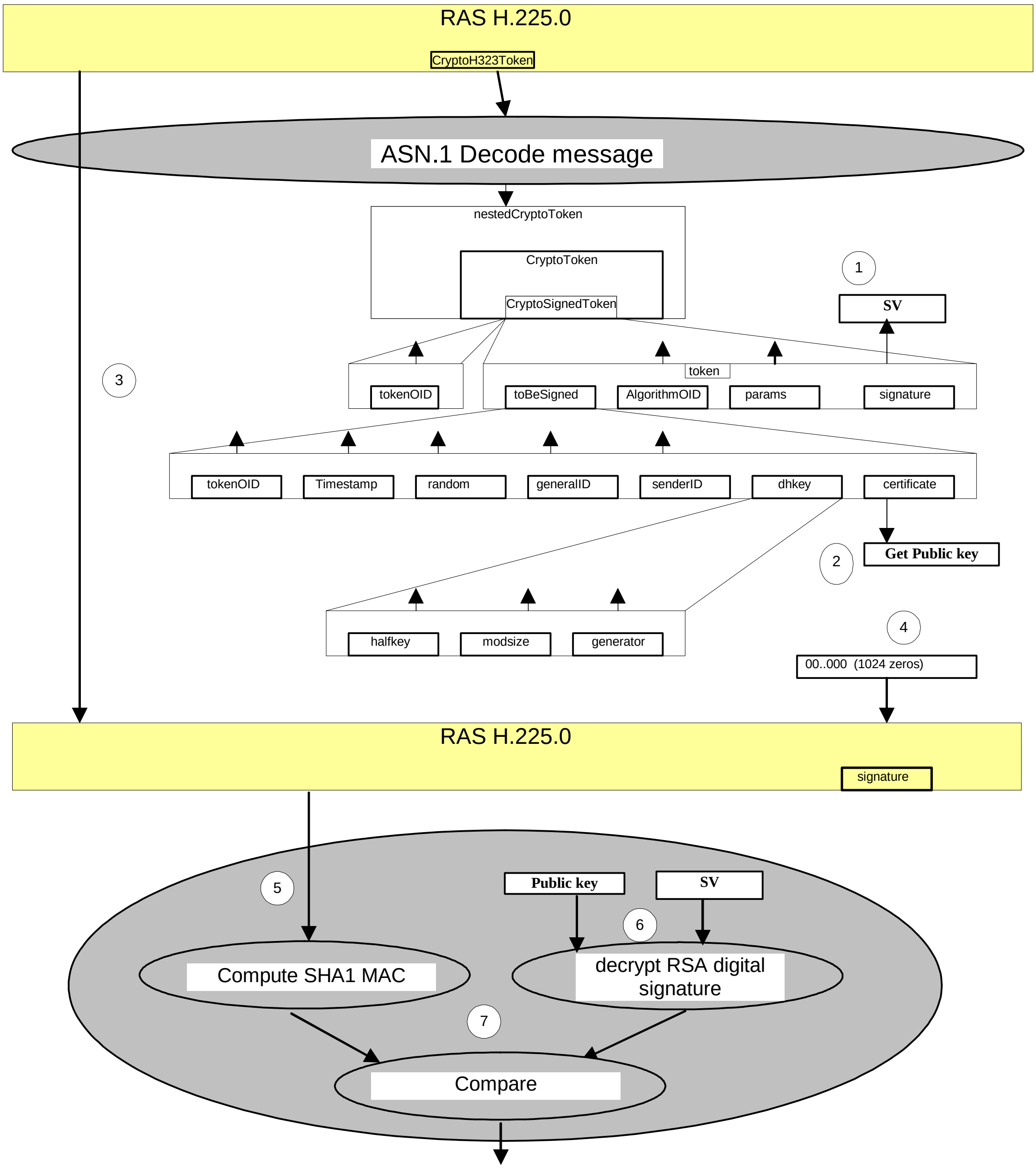

Figure 4: Signature verification at receiver

6.2 RRQ with DH Set received by the Gatekeeper with signed token

Client DH-random: (1 024 bits)

```
   1615753650388531786931829110933311099877226272014490278684636500483042912640710206528703444870653
   2820537869722304948514422899783943294063028114544576337078350248783000412379683978269286650820987
   1536243493251174703907122669526301704176837523226057098069728854797292942895710342191803251906952
   005656993434621826
```

```
14:48:37 TPKTCHAN: Registered TPKTCHAN    TPKT Messages
14:48:37 PERERR: Registered PERERR      PER Error Messages
14:48:37 UDPCHAN: Registered UDPCHAN  RAS Message Channels
14:48:46 UDPCHAN: INFO  - New message (channel 0)  recv <-- registrationRequest:
14:48:46 UDPCHAN: Address:
14:48:46 UDPCHAN:  0> <615> TransportAddress = (0) .  <4579> CHOICE ...
```

```
14:48:46 UDPCHAN:  1> . <616> ipAddress = (0) .  <4570> SEQUENCE
14:48:46 UDPCHAN:  2> . . <617> ip = (4) '‹.Ëµ' =0x8b17cbb5 <139.23.203.181> .  <4520> OCTET STRING
(4..4)
14:48:46 UDPCHAN:  2> . . <619> port = (1658) .  <155> INTEGER (0..65535)
14:48:46 UDPCHAN: Binary:
14:48:46 UDPCHAN: 00000   0e c0 2b a9 06 00 08 91 4a 00 04 00 01 00 8b 17    |.À+©..."J.....‹.|
14:48:46 UDPCHAN: 00016   cb b5 06 79 01 00 8b 17 cb b5 06 7a 22 c0 0b 0b    |Ëµ.y..‹.Ëµ.z"À..|
14:48:46 UDPCHAN: 00032   00 0b 0f 54 65 73 74 20 61 70 70 6c 69 63 61 74    |...Test applicat|
14:48:46 UDPCHAN: 00048   69 6f 6e 08 52 41 44 56 69 73 69 6f 6e 00 02 02    |ion.RADVision...|
14:48:46 UDPCHAN: 00064   00 76 36 b4 04 00 34 00 33 00 30 00 33 00 38 22    |.v6´..4.3.0.3.8"|
14:48:46 UDPCHAN: 00080   00 53 00 69 00 65 00 6d 00 65 00 6e 00 73 00 20    |.S.i.e.m.e.n.s. |
14:48:46 UDPCHAN: 00096   00 47 00 61 00 74 00 65 00 6b 00 65 00 65 00 70    |.G.a.t.e.k.e.e.p|
14:48:46 UDPCHAN: 00112   00 65 00 72 60 0b 0b 00 0b 0f 54 65 73 74 20 61    |.e.r`.....Test a|
14:48:46 UDPCHAN: 00128   70 70 6c 69 63 61 74 69 6f 6e 08 52 41 44 56 69    |pplication.RADVi|
14:48:46 UDPCHAN: 00144   73 69 6f 6e 28 2b 00 00 84 87 01 72 07 00 08 81    |sion(+..„‡.r...•|
14:48:46 UDPCHAN: 00160   6b 00 02 14 57 00 07 00 08 81 6b 00 02 15 c0 3c    |k...W....•k...À<|
14:48:46 UDPCHAN: 00176   fc b7 2c 00 04 00 f6 aa 3c 28 03 9a 01 d5 b8 38    |ü·,...öª<(.š.Õ¸8|
14:48:46 UDPCHAN: 00192   cf ab 92 5c 50 e0 d5 6f 93 0c ae 63 d1 ed e1 e9    |Ï«"\PàÕo".®cÑíáé|
14:48:46 UDPCHAN: 00208   24 1b b9 d6 43 80 b9 1e 0d 01 88 29 c2 9a 58 7a    |$.¹ÖC€¹...ˆ)ÂšXz|
14:48:46 UDPCHAN: 00224   39 05 9d 49 72 8d 34 12 61 74 90 e9 0b 70 e7 cd    |9.•Ir•4.at•é.pçÍ|
14:48:46 UDPCHAN: 00240   16 51 e2 e3 73 3a 8e bd 0e d2 86 24 b1 0f ae 73    |.Qâãs:Ž½.Ò†$±.®s|
14:48:46 UDPCHAN: 00256   69 44 64 5b b3 4a e8 82 3e 14 ac 65 cb 98 14 f4    |iDd[³Jè,>.¬eË˜.ô|
14:48:46 UDPCHAN: 00272   5d 55 3f 76 91 e6 ef c5 2f cf aa e9 71 29 4d e5    |]U?v"æïÅ/Ïªéq)Må|
14:48:46 UDPCHAN: 00288   c5 20 70 26 54 30 76 33 b2 26 55 e3 d2 c8 5c b3    |Å p&T0v3²&UãÒÈ\³|
14:48:46 UDPCHAN: 00304   9b 49 59 52 fb 70 04 00 ff ff ff ff ff ff ff ff    |›IYRûp..ÿÿÿÿÿÿÿÿ|
14:48:46 UDPCHAN: 00320   c9 0f da a2 21 68 c2 34 c4 c6 62 8b 80 dc 1c d1    |É.Ú¢!hÂ4ÄÆb‹€Ü.Ñ|
14:48:46 UDPCHAN: 00336   29 02 4e 08 8a 67 cc 74 02 0b be a6 3b 13 9b 22    |).N.ŠgÌt..¾¦;.›"|
14:48:46 UDPCHAN: 00352   51 4a 08 79 8e 34 04 dd ef 95 19 b3 cd 3a 43 1b    |QJ.yŽ4.Ýï•.³Í:C.|
14:48:46 UDPCHAN: 00368   30 2b 0a 6d f2 5f 14 37 4f e1 35 6d 6d 51 c2 45    |0+.mò_.7Oá5mmQÂE|
14:48:46 UDPCHAN: 00384   e4 85 b5 76 62 5e 7e c6 f4 4c 42 e9 a6 37 ed 6b    |ä…µvb^~ÆôLBé¦7ík|
14:48:46 UDPCHAN: 00400   0b ff 5c b6 f4 06 b7 ed ee 38 6b fb 5a 89 9f a5    |.ÿ\¶ô.·íî8kûZ‰Ÿ¥|
14:48:46 UDPCHAN: 00416   ae 9f 24 11 7c 4b 1f e6 49 28 66 51 ec e6 53 81    |®Ÿ$.|K.æI(fQìæS•|
14:48:46 UDPCHAN: 00432   ff ff ff ff ff ff ff ff 00 08 02 01 29 00 07 00    |ÿÿÿÿÿÿÿÿ....)...|
14:48:46 UDPCHAN: 00448   08 81 6b 00 02 17 82 a7 30 82 02 a3 30 82 02 0c    |.•k...,§0,.£0,..|
14:48:46 UDPCHAN: 00464   a0 03 02 01 02 02 01 32 30 0d 06 09 2a 86 48 86    | ......20...*†H†|
14:48:46 UDPCHAN: 00480   f7 0d 01 01 05 05 00 30 81 81 31 28 30 26 06 03    |÷......0••1(0&..|
14:48:46 UDPCHAN: 00496   55 04 03 13 1f 49 50 4c 20 43 65 72 74 69 66 69    |U....IPL Certifi|
14:48:46 UDPCHAN: 00512   63 61 74 69 6f 6e 20 41 75 74 68 6f 72 69 74 79    |cation Authority|
14:48:46 UDPCHAN: 00528   20 52 53 41 31 0b 30 09 06 03 55 04 06 13 02 64    | RSA1.0...U....d|
14:48:46 UDPCHAN: 00544   65 31 13 30 11 06 03 55 04 0a 13 0a 53 69 65 6d    |e1.0...U....Siem|
14:48:46 UDPCHAN: 00560   65 6e 73 20 41 47 31 10 30 0e 06 03 55 04 0b 13    |ens AG1.0...U...|
14:48:46 UDPCHAN: 00576   07 5a 54 20 49 4b 20 33 31 0f 30 0d 06 03 55 04    |.ZT IK 31.0...U.|
14:48:46 UDPCHAN: 00592   07 13 06 4d 75 6e 69 63 68 31 10 30 0e 06 03 55    |...Munich1.0...U|
14:48:46 UDPCHAN: 00608   04 08 13 07 42 61 76 61 72 69 61 30 1e 17 0d 30    |....Bavaria0...0|
14:48:46 UDPCHAN: 00624   32 30 33 32 31 30 39 30 30 31 37 5a 17 0d 30 34    |20321090017Z..04|
14:48:46 UDPCHAN: 00640   30 33 31 30 30 39 30 30 31 36 5a 30 58 31 15 30    |0310090016Z0X1.0|
14:48:46 UDPCHAN: 00656   13 06 03 55 04 03 13 0c 43 6c 69 65 6e 74 31 20    |...U....Client1 |
14:48:46 UDPCHAN: 00672   48 33 32 33 31 0c 30 0a 06 03 55 04 0b 13 03 49    |H3231.0...U....I|
14:48:46 UDPCHAN: 00688   43 33 31 13 30 11 06 03 55 04 0a 13 0a 53 69 65    |C31.0...U....Sie|
14:48:46 UDPCHAN: 00704   6d 65 6e 73 20 41 47 31 0f 30 0d 06 03 55 04 07    |mens AG1.0...U..|
14:48:46 UDPCHAN: 00720   13 06 4d 75 6e 69 63 68 31 0b 30 09 06 03 55 04    |..Munich1.0...U.|
14:48:46 UDPCHAN: 00736   06 13 02 44 45 30 81 9d 30 0d 06 09 2a 86 48 86    |...DE0••0...*†H†|
14:48:46 UDPCHAN: 00752   f7 0d 01 01 01 05 00 03 81 8b 00 30 81 87 02 81    |÷.......•‹.0•‡.•|
14:48:46 UDPCHAN: 00768   81 00 d7 94 6e b4 93 0a 56 3f dd 11 67 ed 32 1e    |•.×"n´".V?Ý.gí2.|
14:48:46 UDPCHAN: 00784   9b 4a a8 b1 45 15 0d c9 9c b7 f9 53 d2 2e 18 21    |›J¨±E..Éœ·ùSÒ..!|
14:48:46 UDPCHAN: 00800   95 4e 18 c5 d8 f8 c6 15 37 20 6d 34 fb 65 cc 34    |•N.ÅØøÆ.7 m4ûeÌ4|
14:48:46 UDPCHAN: 00816   50 fe 2d 39 38 fd 4a d0 84 db b2 31 4e 9b ec 8c    |Pþ-98ýJÐ„Û²1N›ìŒ|
14:48:46 UDPCHAN: 00832   90 6d f5 89 f5 d4 04 d4 0e ea 31 1f 39 a1 d6 44    |•mõ‰õÔ.Ô.ê1.9¡ÖD|
14:48:46 UDPCHAN: 00848   7d 9a 88 7d 42 3e d1 c9 24 28 99 e3 d7 1f 19 f4    |}šˆ}B>ÑÉ$(™ã×..ô|
14:48:46 UDPCHAN: 00864   be 19 58 34 21 41 06 36 f1 8d 1b 3c 9b 37 44 6a    |¾.X4!A.6ñ•.<›7Dj|
14:48:46 UDPCHAN: 00880   1e 41 50 69 3d 40 ae 09 cd 87 ce ea b5 c1 8e a7    |.APi=@®.Í‡ÎêµÁŽ§|
14:48:46 UDPCHAN: 00896   f7 93 02 01 03 a3 55 30 53 30 11 06 09 60 86 48    |÷"...£U0S0...`†H|
14:48:46 UDPCHAN: 00912   01 86 f8 42 01 01 04 04 03 02 00 80 30 1d 06 03    |.†øB.......€0...|
14:48:46 UDPCHAN: 00928   55 1d 0e 04 16 04 14 57 0a 9d 02 0b 22 b1 ac f3    |U......W.•.."±¬ó|
14:48:46 UDPCHAN: 00944   24 46 dc 30 66 9b 80 fe 21 1d 76 30 1f 06 03 55    |$FÜ0f›€þ!.v0...U|
14:48:46 UDPCHAN: 00960   1d 23 04 18 30 16 80 14 06 78 87 5c 34 0e 65 82    |.#..0.€..x‡\4.e,|
14:48:46 UDPCHAN: 00976   67 67 4f 24 f4 93 31 a9 13 4f 58 b4 30 0d 06 09    |ggO$ô"1©.OX´0...|
14:48:46 UDPCHAN: 00992   2a 86 48 86 f7 0d 01 01 05 05 00 03 81 81 00 1f    |*†H†÷.......••..|
14:48:46 UDPCHAN: 01008   53 87 a3 bd 36 a2 f5 98 0c 6c 84 55 0c 40 66 6c    |S‡£½6¢õ˜.l„U.@fl|
14:48:46 UDPCHAN: 01024   61 fd 4d a0 d9 54 50 24 78 b2 a7 1a 60 16 92 9e    |aýM ÙTP$x²§.`."ž|
14:48:46 UDPCHAN: 01040   8b 51 f6 69 fe 75 67 bd d3 fd 0f 21 93 80 fa d7    |‹Qöiþug½Óý.!"€ú×|
14:48:46 UDPCHAN: 01056   f2 e6 07 6c 89 b2 37 59 67 16 25 a5 2b a1 1d 28    |òæ.l‰²7Yg.%¥+¡.(|
14:48:46 UDPCHAN: 01072   84 62 a3 df 58 27 2f 0a 94 ff c5 77 1a 23 8d ec    |„b£ßX'/."ÿÅw.#•ì|
14:48:46 UDPCHAN: 01088   6e 77 b8 1f 09 28 59 7b f5 5d 13 ac a1 f3 97 f4    |nw¸..(Y{õ].¬¡ó—ô|
14:48:46 UDPCHAN: 01104   b4 f1 51 3b 5d 2c b5 d0 b4 83 06 99 4e b5 a3 6c    |´ñQ;],µÐ´ƒ.™Nµ£l|
14:48:46 UDPCHAN: 01120   77 c9 51 fb 2b 4f 22 aa 24 f8 06 c3 c1 9c 6e 22    |wÉQû+O"ª$ø.ÃÁœn"|
14:48:46 UDPCHAN: 01136   00 53 00 69 00 65 00 6d 00 65 00 6e 00 73 00 20    |.S.i.e.m.e.n.s. |
14:48:46 UDPCHAN: 01152   00 47 00 61 00 74 00 65 00 6b 00 65 00 65 00 70    |.G.a.t.e.k.e.e.p|
14:48:46 UDPCHAN: 01168   00 65 00 72 09 2a 86 48 86 f7 0d 01 01 05 00 84    |.e.r.*†H†÷.....„|
14:48:46 UDPCHAN: 01184   00 41 81 30 45 f8 b2 30 61 7d 0f 66 4b a5 28 5f    |.A•0Eø²0a}.fK¥(_|
14:48:46 UDPCHAN: 01200   25 4e 98 51 e4 9d e7 85 f5 84 91 01 a8 65 bd a5    |%N˜Qä•ç…õ„".¨e½¥|
14:48:46 UDPCHAN: 01216   06 ea f0 ab ef 35 1b 8c 7a fa ed e8 cc a1 4d 45    |.êð«ï5.ŒzúíèÌ¡ME|
14:48:46 UDPCHAN: 01232   5e 72 b9 cd f6 d5 d0 be 38 a1 04 08 68 9b aa 1a    |^r¹ÍöÕÐ¾8¡..h›ª.|
14:48:46 UDPCHAN: 01248   3a e5 99 98 eb 5a c7 10 80 ed a1 0f 3c 5a 8c a4    |:å™˜ëZÇ.€í¡.<ZŒ¤|
14:48:46 UDPCHAN: 01264   ef 98 56 1e 91 6b 6f 7c 1b 75 91 23 04 4b 6a d4    |ï˜V."ko|.u"#.KjÔ|
14:48:46 UDPCHAN: 01280   73 aa ea f8 74 84 12 ac b7 8b 92 3f 4c cf ec f5    |sªêøt„.¬·‹"?LÏìõ|
14:48:46 UDPCHAN: 01296   81 97 cc 03 7e ef 81 84 98 3b 7b e0 1c 9d c6 4f    |•—Ì.~ï•„˜;{à.•ÆO|
14:48:46 UDPCHAN: 01312   d1 01 00 01 00 01 00                               |Ñ......|
14:48:46 UDPCHAN: Message:
```

```
14:48:46 UDPCHAN:  0> <486> RasMessage = (0) .  <2731> CHOICE ...
14:48:46 UDPCHAN:  1> . <487> registrationRequest = (4294967185) .  <2461> SEQUENCE ...
14:48:46 UDPCHAN:  2> . . <488> requestSeqNum = (11178) .  <3615> INTEGER (1..65535)
14:48:46 UDPCHAN:  2> . . <489> protocolIdentifier = (6) { itu-t recommendation h 2250 0 4 }.
<3594> OBJECT IDENTIFIER
14:48:46 UDPCHAN:  2> . . <491> discoveryComplete = (0) .  <0> BOOLEAN
14:48:46 UDPCHAN:  2> . . <492> callSignalAddress = (1) .  <1151> SET OF CHOICE ...
14:48:46 UDPCHAN:  3> . . . <493> * = (10714) .  <4579> CHOICE ...
14:48:46 UDPCHAN:  4> . . . . <494> ipAddress = (4294967185) .  <4570> SEQUENCE
14:48:46 UDPCHAN:  5> . . . . . <495> ip = (4) '‹.Ëµ' =0x8b17cbb5 <139.23.203.181> .  <4520> OCTET
STRING (4..4)
14:48:46 UDPCHAN:  5> . . . . . <497> port = (1657) .  <155> INTEGER (0..65535)
14:48:46 UDPCHAN:  2> . . <498> rasAddress = (1) .  <1151> SET OF CHOICE ...
14:48:46 UDPCHAN:  3> . . . <499> * = (10714) .  <4579> CHOICE ...
14:48:46 UDPCHAN:  4> . . . . <500> ipAddress = (4294967185) .  <4570> SEQUENCE
14:48:46 UDPCHAN:  5> . . . . . <501> ip = (4) '‹.Ëµ' =0x8b17cbb5 <139.23.203.181> .  <4520> OCTET
STRING (4..4)
14:48:46 UDPCHAN:  5> . . . . . <503> port = (1658) .  <155> INTEGER (0..65535)
14:48:46 UDPCHAN:  2> . . <504> terminalType = (4294967185) .  <4403> SEQUENCE ...
14:48:46 UDPCHAN:  3> . . . <505> vendor = (4294967185) .  <4186> SEQUENCE ...
14:48:46 UDPCHAN:  4> . . . . <506> vendor = (4294967185) .  <4169> SEQUENCE ...
14:48:46 UDPCHAN:  5> . . . . . <507> t35CountryCode = (11) .  <45> INTEGER (0..255)
14:48:46 UDPCHAN:  5> . . . . . <508> t35Extension = (11) .  <45> INTEGER (0..255)
14:48:46 UDPCHAN:  5> . . . . . <509> manufacturerCode = (11) .  <155> INTEGER (0..65535)
14:48:46 UDPCHAN:  4> . . . . <510> productId = (16) 'Test application'
=0x546573742061706c69636174696f6e .  <4181> OCTET STRING (1..256)
14:48:46 UDPCHAN:  4> . . . . <512> versionId = (9) 'RADVision' =0x524144566973696f6e .  <4181>
OCTET STRING (1..256)
14:48:46 UDPCHAN:  3> . . . <514> terminal = (4294967185) .  <4204> SEQUENCE ...
14:48:46 UDPCHAN:  3> . . . <515> mc = (0) .  <0> BOOLEAN
14:48:46 UDPCHAN:  3> . . . <516> undefinedNode = (0) .  <0> BOOLEAN
14:48:46 UDPCHAN:  2> . . <517> terminalAlias = (2) .  <1147> SET OF CHOICE ...
14:48:46 UDPCHAN:  3> . . . <518> * = (8122) .  <4095> CHOICE ...
14:48:46 UDPCHAN:  4> . . . . <519> e164 = (5) '43038' =0x3433303338 .  <4089> IA5String (1..128)
FROM '#*,0123456789'
14:48:46 UDPCHAN:  3> . . . <521> * = (9613) .  <4095> CHOICE ...
14:48:46 UDPCHAN:  4> . . . . <522> h323-ID = (10) '.4.3.0.3.8' =0x00340033003000330038 .  <4084>
BMPString (1..256)
14:48:46 UDPCHAN:  2> . . <524> gatekeeperIdentifier = (36) '.S.i.e.m.e.n.s. .G.a.t.e.k.e.e.p.e.r'
=0x005300690065006d0065006e00730020004700610074006500650065007000650072 .  <3610> BMPString
(1..128)
14:48:46 UDPCHAN:  2> . . <527> endpointVendor = (4294967185) .  <4186> SEQUENCE ...
14:48:46 UDPCHAN:  3> . . . <528> vendor = (4294967185) .  <4169> SEQUENCE ...
14:48:46 UDPCHAN:  4> . . . . <529> t35CountryCode = (11) .  <45> INTEGER (0..255)
14:48:46 UDPCHAN:  4> . . . . <530> t35Extension = (11) .  <45> INTEGER (0..255)
14:48:46 UDPCHAN:  4> . . . . <531> manufacturerCode = (11) .  <155> INTEGER (0..65535)
14:48:46 UDPCHAN:  3> . . . <532> productId = (16) 'Test application'
=0x546573742061706c69636174696f6e .  <4181> OCTET STRING (1..256)
14:48:46 UDPCHAN:  3> . . . <534> versionId = (9) 'RADVision' =0x524144566973696f6e .  <4181> OCTET
STRING (1..256)
14:48:46 UDPCHAN:  2> . . <536> cryptoTokens = (1) .  <752> SET OF CHOICE ...
14:48:46 UDPCHAN:  3> . . . <537> * = (12045) .  <3421> CHOICE ...
14:48:46 UDPCHAN:  4> . . . . <538> nestedcryptoToken = (7371) .  <384> CHOICE ...
14:48:46 UDPCHAN:  5> . . . . . <539> cryptoSignedToken = (4294967185) .  <366> SEQUENCE
14:48:46 UDPCHAN:  6> . . . . . . <540> tokenOID = (7) { itu-t recommendation h 235 0 2 20 }.  <171>
OBJECT IDENTIFIER
14:48:46 UDPCHAN:  6> . . . . . . <542> token = (4294967185) .  <351> SEQUENCE
14:48:46 UDPCHAN:  7> . . . . . . . <543> toBeSigned = (4294967185) .  <471> SEQUENCE ...
14:48:46 UDPCHAN:  8> . . . . . . . . <544> tokenOID = (7) { itu-t recommendation h 235 0 2 21 }.
<171> OBJECT IDENTIFIER
14:48:46 UDPCHAN:  8> . . . . . . . . <546> timeStamp = (1023194925) .  <738> INTEGER (1..-1)
14:48:46 UDPCHAN:  8> . . . . . . . . <547> dhkey = (4294967185) .  <699> SEQUENCE ...
14:48:46 UDPCHAN:  9> . . . . . . . . . <548> halfkey = (1024)
'öª<(.š.Õ¸8Ï«"\PàÕo".®cÑíáé$.¹ÖC€¹...^)ÂšXz9.•Ir•4.at•é.pçÍ.Qâãs:Ž½.Ò†$±.®siDd[³Jè,>.¬eË˜.ô]U?v"æïÅ/
Ïªéq)MåÅ p&T0v3²&UãÒÈ\³›IYRûp'
=0xf6aa3c28039a01d5b838cfab925c50e0d56f930cae63d1ede1e9241bb9d64380b91e0d018829c29a587a39059d49728d3
412617490e90b70e7cd1651e2e3733a8ebd0ed28624b10fae736944645bb34ae8823e14ac65cb9814f45d553f7691e6efc52
fcfaae971294de5c520702654307633b22655e3d2c85cb39b495952fb70 .  <695> BIT STRING (0..2048)
14:48:46 UDPCHAN:  9> . . . . . . . . . <555> modSize = (1024)
'ÿÿÿÿÿÿÿÿÉ.Ú¢!hÂ4ÄÆb‹€Ü.Ñ).N.ŠgÌt..¾¦;.›"QJ.yŽ4.Ýï•.³Í:C.0+.mò_.7Oá5mmQÂEä…µvb^~ÆôLBé¦7ík.ÿ\¶ô.·íî8k
ûZ‰Ÿ¥®Ÿ$.|K.æI(fQìæS•ÿÿÿÿÿÿÿÿ'
=0xffffffffffffffffc90fdaa22168c234c4c6628b80dc1cd129024e088a67cc74020bbea63b139b22514a08798e3404dde
f9519b3cd3a431b302b0a6df25f14374fe1356d6d51c245e485b576625e7ec6f44c42e9a637ed6b0bff5cb6f406b7edee386
bfb5a899fa5ae9f24117c4b1fe649286651ece65381ffffffffffffffff .  <695> BIT STRING (0..2048)
14:48:46 UDPCHAN:  9> . . . . . . . . . <562> generator = (8) '.' =0x02 .  <695> BIT STRING
(0..2048)
14:48:46 UDPCHAN:  8> . . . . . . . . <564> random = (41) .  <735> INTEGER
14:48:46 UDPCHAN:  8> . . . . . . . . <565> certificate = (4294967185) .  <628> SEQUENCE ...
14:48:46 UDPCHAN:  9> . . . . . . . . . <566> type = (7) { itu-t recommendation h 235 0 2 23 }.
<171> OBJECT IDENTIFIER
14:48:46 UDPCHAN:  9> . . . . . . . . . <568> certificate = (679)
'0,.£0,.. ......20...*†H†÷......0••1(0&..U....IPL Certification Authority
RSA1.0...U....de1.0...U....Siemens AG1.0...U....ZT IK 3'
=0x308202a33082020ca003020102020132300d06092a864886f70d01010505003081813128302606035504031 31f49504c2
04365727469666963617469 6f6e20417574686f7269747920525341310b3009060355040613026465311330110603550 40a1
30a5369656d656e732041473110300e060355040b13075a5420494b2033 .  <183> OCTET STRING
14:48:46 UDPCHAN:  8> . . . . . . . . <598> generalID = (36) '.S.i.e.m.e.n.s. .G.a.t.e.k.e.e.p.e.r'
=0x005300690065006d0065006e00730020004700610074006500650065007000650072 .  <725> BMPString
(1..128)
```

```
14:48:46 UDPCHAN:  7> . . . . . . . . <601> algorithmOID = (9) { iso member-body 840 113549 1 1 5 }.
<171> OBJECT IDENTIFIER
14:48:46 UDPCHAN:  7> . . . . . . . . <603> paramS = (4294967185) .  <507> SEQUENCE ...
14:48:46 UDPCHAN:  8> . . . . . . . . . <604> null = (4294967173) .  <9> NULL
14:48:46 UDPCHAN:  7> . . . . . . . . <605> signature = (1024)
'A•0Eø²0a}.fK¥(_%N˜Qä•ç…õ„".¨e½¥.êð«ï5.ŒzúíèÏ¡ME^r¹ÍöÕÐ¾8¡..h›ª.:å™˜ëZÇ.€í¡.<ZŒ¤ï˜V."ko|.u"#.KjÔsªêø
t„.¬·‹"?LÏìõ•—Ï.~ï•„˜;{à.•ÆOÑ'
=0x41813045f8b230617d0f664ba5285f254e9851e49de785f5849101a865bda506eaf0abef351b8c7afaede8cca14d455e7
2b9cdf6d5d0be38a10408689baa1a3ae59998eb5ac71080eda10f3c5a8ca4ef98561e916b6f7c1b759123044b6ad473aaeaf
8748412acb78b923f4ccfecf58197cc037eef8184983b7be01c9dc64fd1 .  <243> BIT STRING
14:48:46 UDPCHAN:  2> . . <612> keepAlive = (0) .  <0> BOOLEAN
14:48:46 UDPCHAN:  2> . . <613> willSupplyUUIEs = (0) .  <0> BOOLEAN
14:48:46 UDPCHAN:  2> . . <614> maintainConnection = (0) .  <0> BOOLEAN
```

6.3 RCF with DH Set of GK received by the client with signed token

GK DH-random: (1 024 bits)

```
   9390268247154670201806609118680498038790601506578338730504420508313000325899248276853509228147732
   8828319730420973655997292393412337374634110544626634732015153773012864764269211617363255175192022
   1668985166616300045437680107010993667772447261688573562223788685881307798416443383537252191409119
   89964818051098489
```

```
14:48:46 UDPCHAN: INFO  - New message (channel 0)  recv <-- registrationConfirm:
14:48:46 UDPCHAN: Address:
14:48:46 UDPCHAN:  0> <1159> TransportAddress = (0) .  <4579> CHOICE ...
14:48:46 UDPCHAN:  1> . <1160> ipAddress = (0) .  <4570> SEQUENCE
14:48:46 UDPCHAN:  2> . . <1161> ip = (4) '‹.Ëµ' =0x8b17cbb5 <139.23.203.181> .  <4520> OCTET STRING
(4..4)
14:48:46 UDPCHAN:  2> . . <1163> port = (1719) .  <155> INTEGER (0..65535)
14:48:46 UDPCHAN: Binary:
14:48:46 UDPCHAN: 00000   12 c0 2b a9 06 00 08 91 4a 00 04 01 00 8b 17 cb    |.À+©..."J....‹.Ë|
14:48:46 UDPCHAN: 00016   b5 06 b8 02 02 00 76 36 b4 04 00 34 00 33 00 30    |µ.¸...v6´..4.3.0|
14:48:46 UDPCHAN: 00032   00 33 00 38 22 00 53 00 69 00 65 00 6d 00 65 00    |.3.8".S.i.e.m.e.|
14:48:46 UDPCHAN: 00048   6e 00 73 00 20 00 47 00 61 00 74 00 65 00 6b 00    |n.s. .G.a.t.e.k.|
14:48:46 UDPCHAN: 00064   65 00 65 00 70 00 65 00 72 52 00 30 00 30 00 30    |e.e.p.e.rR.0.0.0|
14:48:46 UDPCHAN: 00080   00 30 00 30 00 30 00 32 00 30 00 30 00 36 00 36    |.0.0.0.2.0.0.6.6|
14:48:46 UDPCHAN: 00096   00 30 00 37 00 33 00 33 00 30 00 34 00 39 00 39    |.0.7.3.3.0.4.9.9|
14:48:46 UDPCHAN: 00112   00 38 00 35 00 39 00 33 00 31 00 31 00 37 00 32    |.8.5.9.3.1.1.7.2|
14:48:46 UDPCHAN: 00128   00 30 00 33 00 30 00 34 00 39 00 39 00 38 00 35    |.0.3.0.4.9.9.8.5|
14:48:46 UDPCHAN: 00144   00 39 00 33 00 31 00 31 00 36 00 35 00 38 20 2e    |.9.3.1.1.6.5.8 .|
14:48:46 UDPCHAN: 00160   00 84 e8 01 72 07 00 08 81 6b 00 02 14 d7 00 07    |.„è.r...•k...×..|
14:48:46 UDPCHAN: 00176   00 08 81 6b 00 02 15 c0 3c fc b7 2d 00 04 00 d0    |..•k...À<ü·-...Ð|
14:48:46 UDPCHAN: 00192   86 28 11 d6 e0 dd 8d f0 f2 f0 06 cf 72 3a 52 f5    |†(.ÖàÝ•ðòð.Ïr:Rõ|
14:48:46 UDPCHAN: 00208   8d 25 f1 9a 8b c9 de eb 40 ff 8f 1a b9 81 e7 3d    |•%ñš‹ÉÞë@ÿ•.¹•ç=|
14:48:46 UDPCHAN: 00224   83 2e 56 2f 21 61 45 f9 a6 b6 e7 94 65 32 e5 21    |ƒ.V/!aEù¦¶ç"e2å!|
14:48:46 UDPCHAN: 00240   48 e9 e4 0e 92 72 0d db 5d ec bb d6 e9 d9 85 af    |Héä."r.Û]ì»ÖéÙ…¯|
14:48:46 UDPCHAN: 00256   32 fa 9d fd 24 89 82 d3 2f cf 0b 72 40 5d 72 32    |2ú•ý$‰‚Ó/Ï.r@]r2|
14:48:46 UDPCHAN: 00272   31 a2 b0 b7 53 96 af d6 1b e8 80 b9 92 ce 15 59    |1¢°·S–¯Ö.è€¹"Î.Y|
14:48:46 UDPCHAN: 00288   64 0e 04 cf 7f a2 c7 5c 33 eb 58 1c 9a 2e 35 46    |d..Ï•¢Ç\3ëX.š.5F|
14:48:46 UDPCHAN: 00304   22 56 71 29 08 67 b3 0b 54 d2 38 ed 0f 1b 9c 04    |"Vq).g³.TÒ8í..œ.|
14:48:46 UDPCHAN: 00320   00 ff ff ff ff ff ff ff ff c9 0f da a2 21 68 c2    |.ÿÿÿÿÿÿÿÿÉ.Ú¢!hÂ|
14:48:46 UDPCHAN: 00336   34 c4 c6 62 8b 80 dc 1c d1 29 02 4e 08 8a 67 cc    |4ÄÆb‹€Ü.Ñ).N.ŠgÌ|
14:48:46 UDPCHAN: 00352   74 02 0b be a6 3b 13 9b 22 51 4a 08 79 8e 34 04    |t..¾¦;.›"QJ.yŽ4.|
14:48:46 UDPCHAN: 00368   dd ef 95 19 b3 cd 3a 43 1b 30 2b 0a 6d f2 5f 14    |Ýï•.³Í:C.0+.mò_.|
14:48:46 UDPCHAN: 00384   37 4f e1 35 6d 6d 51 c2 45 e4 85 b5 76 62 5e 7e    |7Oá5mmQÂEä…µvb^~|
14:48:46 UDPCHAN: 00400   c6 f4 4c 42 e9 a6 37 ed 6b 0b ff 5c b6 f4 06 b7    |ÆôLBé¦7ík.ÿ\¶ô.·|
14:48:46 UDPCHAN: 00416   ed ee 38 6b fb 5a 89 9f a5 ae 9f 24 11 7c 4b 1f    |íî8kûZ‰Ÿ¥®Ÿ$.|K.|
14:48:46 UDPCHAN: 00432   e6 49 28 66 51 ec e6 53 81 ff ff ff ff ff ff ff    |æI(fQìæS•ÿÿÿÿÿÿÿ|
14:48:46 UDPCHAN: 00448   ff 00 08 02 01 29 00 07 00 08 81 6b 00 02 17 82    |ÿ....)....•k...,|
14:48:46 UDPCHAN: 00464   b0 30 82 02 ac 30 82 02 15 a0 03 02 01 02 02 01    |°0,.¬0,.. ......|
14:48:46 UDPCHAN: 00480   34 30 0d 06 09 2a 86 48 86 f7 0d 01 01 05 05 00    |40...*†H†÷......|
14:48:46 UDPCHAN: 00496   30 81 81 31 28 30 26 06 03 55 04 03 13 1f 49 50    |0••1(0&..U....IP|
14:48:46 UDPCHAN: 00512   4c 20 43 65 72 74 69 66 69 63 61 74 69 6f 6e 20    |L Certification |
14:48:46 UDPCHAN: 00528   41 75 74 68 6f 72 69 74 79 20 52 53 41 31 0b 30    |Authority RSA1.0|
14:48:46 UDPCHAN: 00544   09 06 03 55 04 06 13 02 64 65 31 13 30 11 06 03    |...U....de1.0...|
14:48:46 UDPCHAN: 00560   55 04 0a 13 0a 53 69 65 6d 65 6e 73 20 41 47 31    |U....Siemens AG1|
14:48:46 UDPCHAN: 00576   10 30 0e 06 03 55 04 0b 13 07 5a 54 20 49 4b 20    |.0...U....ZT IK |
14:48:46 UDPCHAN: 00592   33 31 0f 30 0d 06 03 55 04 07 13 06 4d 75 6e 69    |31.0...U....Muni|
14:48:46 UDPCHAN: 00608   63 68 31 10 30 0e 06 03 55 04 08 13 07 42 61 76    |ch1.0...U....Bav|
14:48:46 UDPCHAN: 00624   61 72 69 61 30 1e 17 0d 30 32 30 33 32 31 30 39    |aria0...02032109|
14:48:46 UDPCHAN: 00640   32 33 30 30 5a 17 0d 30 34 30 33 31 30 30 39 32    |2300Z..040310092|
14:48:46 UDPCHAN: 00656   32 35 39 5a 30 5f 31 1b 30 19 06 03 55 04 03 13    |259Z0_1.0...U...|
14:48:46 UDPCHAN: 00672   12 67 61 74 65 6b 65 65 70 65 72 20 48 33 32 33    |.gatekeeper H323|
14:48:46 UDPCHAN: 00688   32 47 4b 31 0d 30 0b 06 03 55 04 0b 13 04 49 43    |2GK1.0...U....IC|
14:48:46 UDPCHAN: 00704   20 33 31 13 30 11 06 03 55 04 0a 13 0a 53 69 65    | 31.0...U....Sie|
14:48:46 UDPCHAN: 00720   6d 65 6e 73 20 41 47 31 0f 30 0d 06 03 55 04 07    |mens AG1.0...U..|
14:48:46 UDPCHAN: 00736   13 06 4d 75 6e 69 63 68 31 0b 30 09 06 03 55 04    |..Munich1.0...U.|
14:48:46 UDPCHAN: 00752   06 13 02 44 45 30 81 9f 30 0d 06 09 2a 86 48 86    |...DE0•Ÿ0...*†H†|
14:48:46 UDPCHAN: 00768   f7 0d 01 01 01 05 00 03 81 8d 00 30 81 89 02 81    |÷.......••.0•‰.•|
14:48:46 UDPCHAN: 00784   81 00 c6 c2 3d 31 fb 87 b7 f3 40 32 5c a2 a4 d1     |•.ÆÂ=1û‡·ó@2\¢¤Ñ|
14:48:46 UDPCHAN: 00800   f1 fc a4 3c 13 64 ac f8 70 cf d3 af 11 e3 71 a9     |ñü¤<.d¬øpÏÓ¯.ãq©|
14:48:46 UDPCHAN: 00816   b5 50 0d 79 ae 3c 09 66 63 ca 11 bc 12 75 0b d8     |µP.y®<.fcÊ.¼.u.Ø|
14:48:46 UDPCHAN: 00832   ab 2d 69 4b 73 d1 d7 f1 ea f3 38 de 4d bc 4e b0     |«-iKsÑ×ñêó8ÞM¼N°|
14:48:46 UDPCHAN: 00848   a1 12 bd 4e 9b bc fc 84 13 85 a3 a2 38 a4 f8 09     |¡.½N›¼ü„.…£¢8¤ø.|
14:48:46 UDPCHAN: 00864   0c 8c 1b a3 df ec 56 92 75 3c dc f0 c3 ac a9 97     |.Œ.£ßìV"u<ÜðÃ¬©—|
14:48:46 UDPCHAN: 00880   c7 ba 84 2e 21 bb f3 5b 5d 06 88 be 46 e6 a9 aa     |Çº„.!»ó[].ˆ¾Fæ©ª|
14:48:46 UDPCHAN: 00896   d4 7d 2a de 7f cf db 2a a5 5d b2 91 79 87 04 6b     |Ô}*Þ•ÏÛ*¥]²"y‡.k|
14:48:46 UDPCHAN: 00912   d0 1b 02 03 01 00 01 a3 55 30 53 30 11 06 09 60     |Ð......£U0S0...`|
14:48:46 UDPCHAN: 00928   86 48 01 86 f8 42 01 01 04 04 03 02 00 40 30 1d     |†H.†øB.......@0.|
14:48:46 UDPCHAN: 00944   06 03 55 1d 0e 04 16 04 14 3b 1a 3d cc fb 26 fc     |..U.....;.=Ìû&ü|
14:48:46 UDPCHAN: 00960   c2 5e fc 12 39 79 b6 ab db a6 48 10 f7 30 1f 06     |Â^ü.9y¶«Û¦H.÷0..|
14:48:46 UDPCHAN: 00976   03 55 1d 23 04 18 30 16 80 14 06 78 87 5c 34 0e     |.U.#..0.€..x‡\4.|
14:48:46 UDPCHAN: 00992   65 82 67 67 4f 24 f4 93 31 a9 13 4f 58 b4 30 0d     |e,ggO$ô"1©.OX´0.|
14:48:46 UDPCHAN: 01008   06 09 2a 86 48 86 f7 0d 01 01 05 05 00 03 81 81     |..*†H†÷.......••|
14:48:46 UDPCHAN: 01024   00 96 af dc 1f 28 8b 0d 75 f8 d9 e5 93 36 a7 32     |.–¯Ü.(‹.uøÙå"6§2|
14:48:46 UDPCHAN: 01040   42 81 8e b2 74 16 51 54 7d 2b b7 b8 a0 c2 79 1b     |B•Ž²t.QT}+·¸ Ây.|
14:48:46 UDPCHAN: 01056   86 91 3c 92 3f a2 ef 02 d2 ee fa f5 66 6d a6 8e     |†"<"?¢ï.Òîúõfm¦Ž|
14:48:46 UDPCHAN: 01072   3d 90 40 e6 76 ff 25 d8 9b 1c 67 18 16 3d 39 49     |=•@ævÿ%Ø›.g..=9I|
14:48:46 UDPCHAN: 01088   4f d8 45 99 7f 7c ee 63 18 13 04 8b f8 28 4e 51     |OØE™•|îc...‹ø(NQ|
14:48:46 UDPCHAN: 01104   66 13 df 06 bb b1 48 7f 21 6b 16 fa ff 4d 33 b2     |f.ß.»±H•!k.úÿM3²|
14:48:46 UDPCHAN: 01120   f3 4d f8 27 78 df 57 0b c1 ae 92 9a f7 2c 4c 3c     |óMø'xßW.Á®"š÷,L<|
14:48:46 UDPCHAN: 01136   09 75 82 a1 05 dd 0a 46 1f f3 b2 6f 31 e2 f4 1b     |.u,¡.Ý.F.ó²o1âô.|
14:48:46 UDPCHAN: 01152   27 52 00 30 00 30 00 30 00 30 00 30 00 30 00 32     |'R.0.0.0.0.0.0.2|
14:48:46 UDPCHAN: 01168   00 30 00 30 00 36 00 36 00 30 00 37 00 33 00 33     |.0.0.6.6.0.7.3.3|
14:48:46 UDPCHAN: 01184   00 30 00 34 00 39 00 39 00 38 00 35 00 39 00 33     |.0.4.9.9.8.5.9.3|
14:48:46 UDPCHAN: 01200   00 31 00 31 00 37 00 32 00 30 00 33 00 30 00 34     |.1.1.7.2.0.3.0.4|
14:48:46 UDPCHAN: 01216   00 39 00 39 00 38 00 35 00 39 00 33 00 31 00 31     |.9.9.8.5.9.3.1.1|
14:48:46 UDPCHAN: 01232   00 36 00 35 00 38 02 80 25 22 00 53 00 69 00 65     |.6.5.8.€%".S.i.e|
14:48:46 UDPCHAN: 01248   00 6d 00 65 00 6e 00 73 00 20 00 47 00 61 00 74     |.m.e.n.s. .G.a.t|
14:48:46 UDPCHAN: 01264   00 65 00 6b 00 65 00 65 00 70 00 65 00 72 09 2a     |.e.k.e.e.p.e.r.*|
14:48:46 UDPCHAN: 01280   86 48 86 f7 0d 01 01 05 00 84 00 8f fa 5f 06 b7     |†H†÷.....„.•ú_.·|
14:48:46 UDPCHAN: 01296   8c cb a9 18 e8 0d e3 12 2b e2 f3 7e 14 8e f1 27     |ŒË©.è.ã.+âó~.Žñ'|
14:48:46 UDPCHAN: 01312   d5 20 03 6c 33 c7 6e f1 7a 41 eb 2e ac f6 5a 9e     |Õ .l3ÇnñzAë.¬öZž|
14:48:46 UDPCHAN: 01328   11 9b f1 de 19 4c 82 5c 03 68 c4 4d 98 2b 1f 3e     |.›ñÞ.L,\.hÄM˜+.>|
14:48:46 UDPCHAN: 01344   2b e6 2a 60 d4 87 c9 b9 3a b8 9d 20 3c 7d ff 4b     |+æ*`Ô‡É¹:¸• <}ÿK|
14:48:46 UDPCHAN: 01360   df e1 f7 ec 69 b0 28 01 41 7c fa f8 d4 81 9d ed     |ßá÷ìi°(.A|úøÔ••í|
14:48:46 UDPCHAN: 01376   2c 0b 0b ce 23 7b df 24 0e 60 22 4b 0f 4c c3 e7     |,..Î#{ß$.`"K.LÃç|
14:48:46 UDPCHAN: 01392   de 58 a2 a7 0c 1a 12 0e bf 3c 87 e6 86 12 3e 59     |ÞX¢§....¿<‡æ†.>Y|
14:48:46 UDPCHAN: 01408   48 48 e5 3a 92 12 76 df b9 4a ae 01 00 01 00 01     |HHå:".vß¹J®.....|
14:48:46 UDPCHAN: 01424   00                                                  |.|
14:48:46 UDPCHAN: Message:
14:48:46 UDPCHAN:  0> <1045> RasMessage = (0) .  <2731> CHOICE ...
14:48:46 UDPCHAN:  1> . <1046> registrationConfirm = (4294967185) .  <2382> SEQUENCE ...
14:48:46 UDPCHAN:  2> . . <1047> requestSeqNum = (11178) .  <3615> INTEGER (1..65535)
14:48:46 UDPCHAN:  2> . . <1048> protocolIdentifier = (6) { itu-t recommendation h 2250 0 4 }.
<3594> OBJECT IDENTIFIER
14:48:46 UDPCHAN:  2> . . <1050> callSignalAddress = (1) .  <1151> SET OF CHOICE ...
14:48:46 UDPCHAN:  3> . . . <1051> * = (10714) .  <4579> CHOICE ...
14:48:46 UDPCHAN:  4> . . . . <1052> ipAddress = (4294967185) .  <4570> SEQUENCE
14:48:46 UDPCHAN:  5> . . . . . <1053> ip = (4) '‹.Ëµ' =0x8b17cbb5 <139.23.203.181> .  <4520> OCTET
STRING (4..4)
14:48:46 UDPCHAN:  5> . . . . . <1055> port = (1720) .  <155> INTEGER (0..65535)
14:48:46 UDPCHAN:  2> . . <1056> terminalAlias = (2) .  <1147> SET OF CHOICE ...
14:48:46 UDPCHAN:  3> . . . <1057> * = (8122) .  <4095> CHOICE ...
14:48:46 UDPCHAN:  4> . . . . <1058> e164 = (5) '43038' =0x3433303338 .  <4089> IA5String (1..128)
FROM '#*,0123456789'
14:48:46 UDPCHAN:  3> . . . <1060> * = (9613) .  <4095> CHOICE ...
14:48:46 UDPCHAN:  4> . . . . <1061> h323-ID = (10) '.4.3.0.3.8' =0x00340033003000330038 .  <4084>
BMPString (1..256)
14:48:46 UDPCHAN:  2> . . <1063> gatekeeperIdentifier = (36) '.S.i.e.m.e.n.s. .G.a.t.e.k.e.e.p.e.r'
=0x005300690065006d0065006e00730020004700610074006500b0065006500700650072 .  <3610> BMPString
(1..128)
14:48:46 UDPCHAN:  2> . . <1066> endpointIdentifier = (84)
'.0.0.0.0.0.0.2.0.0.6.6.0.7.3.3.0.4.9.9.8.5.9.3.1.1.7.2.0.3.0.4.9.9.8.5.9.3.1.1.6.5.8'
=0x0030003000300030003000300032003000300036003600300037003300330030003400390039003800350039003300310
03100370032003000330030003400390039003800350039003300310031003600350038 .  <3597> BMPString (1..128)
14:48:46 UDPCHAN:  2> . . <1071> cryptoTokens = (1) .  <752> SET OF CHOICE ...
14:48:46 UDPCHAN:  3> . . . <1072> * = (12045) .  <3421> CHOICE ...
14:48:46 UDPCHAN:  4> . . . . <1073> nestedcryptoToken = (7371) .  <384> CHOICE ...
14:48:46 UDPCHAN:  5> . . . . . <1074> cryptoSignedToken = (4294967185) .  <366> SEQUENCE
14:48:46 UDPCHAN:  6> . . . . . . <1075> tokenOID = (7) { itu-t recommendation h 235 0 2 20 }.
<171> OBJECT IDENTIFIER
14:48:46 UDPCHAN:  6> . . . . . . <1077> token = (4294967185) .  <351> SEQUENCE
14:48:46 UDPCHAN:  7> . . . . . . . <1078> toBeSigned = (4294967185) .  <471> SEQUENCE ...
14:48:46 UDPCHAN:  8> . . . . . . . . <1079> tokenOID = (7) { itu-t recommendation h 235 0 2 21 }.
<171> OBJECT IDENTIFIER
14:48:46 UDPCHAN:  8> . . . . . . . . <1081> timeStamp = (1023194926) .  <738> INTEGER (1..-1)
14:48:46 UDPCHAN:  8> . . . . . . . . <1082> dhkey = (4294967185) .  <699> SEQUENCE ...
14:48:46 UDPCHAN:  9> . . . . . . . . . <1083> halfkey = (1024)
'Ð†(.ÖàÝ•ðòð.Ïr:Rõ•%ñš‹ÉÞë@ÿ•.¹•ç=ƒ.V/!aEù¦¶ç"e2å!Héä."r.Û]ì»ÖéÙ…¯2ú•ý$‰,Ó/Ï.r@]r21¢°·S–
¯Ö.è€¹"Î.Yd..Ï•¢Ç\3ëX.š.5F"Vq).g³.TÒ8í..œ'
=0xd0862811d6e0dd8df0f2f006cf723a52f58d25f19a8bc9deeb40ff8f1ab981e73d832e562f216145f9a6b6e7946532e52
148e9e40e92720ddb5decbbd6e9d985af32fa9dfd248982d32fcf0b72405d723231a2b0b75396afd61be880b992ce1559640
e04cf7fa2c75c33eb581c9a2e3546225671290867b30b54d238ed0f1b9c .  <695> BIT STRING (0..2048)
14:48:46 UDPCHAN:  9> . . . . . . . . . <1090> modSize = (1024)
'ÿÿÿÿÿÿÿÿÉ.Ú¢!hÂ4ÄÆb‹€Ü.Ñ).N.ŠgÌt..¾¦;.›"QJ.yŽ4.Ýï•.³Í:C.0+.mò_.7Oá5mmQÂEä…µvb^~ÆôLBé¦7ík.ÿ\¶ô.·íî8k
ûZ‰Ÿ¥®Ÿ$.|K.æI(fQìæS•ÿÿÿÿÿÿÿÿ'
=0xffffffffffffffffc90fdaa22168c234c4c6628b80dc1cd129024e088a67cc74020bbea63b139b22514a08798e3404dde
```

```
f9519b3cd3a431b302b0a6df25f14374fe1356d6d51c245e485b576625e7ec6f44c42e9a637ed6b0bff5cb6f406b7edee386
bfb5a899fa5ae9f24117c4b1fe649286651ece65381fffffffffffffff .  <695> BIT STRING (0..2048)
14:48:46 UDPCHAN:  9> . . . . . . . . . <1097> generator = (8) '.' =0x02 .  <695> BIT STRING
(0..2048)
14:48:46 UDPCHAN:  8> . . . . . . . . <1099> random = (41) .  <735> INTEGER
14:48:46 UDPCHAN:  8> . . . . . . . . <1100> certificate = (4294967185) .  <628> SEQUENCE ...
14:48:46 UDPCHAN:  9> . . . . . . . . . <1101> type = (7) { itu-t recommendation h 235 0 2 23 }.
<171> OBJECT IDENTIFIER
14:48:46 UDPCHAN:  9> . . . . . . . . . <1103> certificate = (688)
'0,.¬0,.. ......40...*†H†÷......0••1(0&..U....IPL Certification Authority
RSA1.0...U....de1.0...U....Siemens AG1.0...U....ZT IK 3'
=0x308202ac30820215a003020102020134300d06092a864886f70d01010505003081813128302606035504031 31f49504c2
04365727469666963617469 6f6e20417574686f726974792052534131 0b300906035504061302646531133011060355040a1
30a5369656d656e7320414731103 00e060355040b13075a5420494b2033 .  <183> OCTET STRING
14:48:46 UDPCHAN:  8> . . . . . . . . <1133> generalID = (84)
'.0.0.0.0.0.0.2.0.0.6.6.0.7.3.3.0.4.9.9.8.5.9.3.1.1.7.2.0.3.0.4.9.9.8.5.9.3.1.1.6.5.8'
=0x0030003000300030003000300032003000300036003600300037003300330030003400390039003800350039003300310
031003700320030003300300034003900390038003500390033003100310036003500 38 .  <725> BMPString (1..128)
14:48:46 UDPCHAN:  8> . . . . . . . . <1138> sendersID = (36) '.S.i.e.m.e.n.s. .G.a.t.e.k.e.e.p.e.r'
=0x0053006900650 06d0065006e00730020004700610074006500 6b00650065007000650072 .  <725> BMPString
(1..128)
14:48:46 UDPCHAN:  7> . . . . . . . <1141> algorithmOID = (9) { iso member-body 840 113549 1 1 5 }.
<171> OBJECT IDENTIFIER
14:48:46 UDPCHAN:  7> . . . . . . . <1143> paramS = (4294967185) .  <507> SEQUENCE ...
14:48:46 UDPCHAN:  8> . . . . . . . . <1144> null = (4294967173) .  <9> NULL
14:48:46 UDPCHAN:  7> . . . . . . . <1145> signature = (1024) '•ú_.·ŒË©.è.ã.+âó~.Žñ'Õ
.l3ÇnñzAë.¬öZž.›ñÞ.L,\.hÄM˜+.>+æ*`Ô‡É¹:¸•
<}ÿKßá÷ìi°(.A|úøÔ••í,..Î#{ß$.`"K.LÃçÞX¢§....¿<‡æ†.>YHHå:".vß¹J®'
=0x8ffa5f06b78ccba918e80de3122be2f37e148ef127d520036c33c76ef17a41eb2eacf65a9e119bf1de194c825c0368c44
d982b1f3e2be62a60d487c9b93ab89d203c7dff4bdfe1f7ec69b02801417cfaf8d4819ded2c0b0bce237bdf240e60224b0f4
cc3e7de58a2a70c1a120ebf3c87e686123e594848e53a921276dfb94aae .  <243> BIT STRING
14:48:46 UDPCHAN:  2> . . <1152> willRespondToIRR = (0) .  <0> BOOLEAN
14:48:46 UDPCHAN:  2> . . <1153> preGrantedARQ = (4294967185) .  <2355> SEQUENCE ...
14:48:46 UDPCHAN:  3> . . . <1154> makeCall = (0) .  <0> BOOLEAN
14:48:46 UDPCHAN:  3> . . . <1155> useGKCallSignalAddressToMakeCall = (0) .  <0> BOOLEAN
14:48:46 UDPCHAN:  3> . . . <1156> answerCall = (0) .  <0> BOOLEAN
14:48:46 UDPCHAN:  3> . . . <1157> useGKCallSignalAddressToAnswer = (0) .  <0> BOOLEAN
14:48:46 UDPCHAN:  2> . . <1158> maintainConnection = (0) .  <0> BOOLEAN
```

6.4 ARQ now with baseline security received by the Gatekeeper with CryptoHashedToken

```
14:49:00 UDPCHAN: INFO  - New message (channel 0)  recv <-- admissionRequest:
14:49:00 UDPCHAN: Address:
14:49:00 UDPCHAN:  0> <1068> TransportAddress = (0) .  <4579> CHOICE ...
14:49:00 UDPCHAN:  1> . <1069> ipAddress = (0) .  <4570> SEQUENCE
14:49:00 UDPCHAN:  2> . . <1070> ip = (4) '‹.Ëµ' =0x8b17cbb5 <139.23.203.181> .  <4520> OCTET STRING
(4..4)
14:49:00 UDPCHAN:  2> . . <1072> port = (1660) .  <155> INTEGER (0..65535)
14:49:00 UDPCHAN: Binary:
14:49:00 UDPCHAN: 00000   27 90 3f b4 0a 90 00 30 00 30 00 30 00 30 00 31    |'•?´.•.0.0.0.0.1|
14:49:00 UDPCHAN: 00016   00 31 00 32 00 30 00 30 00 37 00 31 00 34 00 37    |.1.2.0.0.7.1.4.7|
14:49:00 UDPCHAN: 00032   00 31 00 33 00 30 00 34 00 39 00 39 00 38 00 35    |.1.3.0.4.9.9.8.5|
14:49:00 UDPCHAN: 00048   00 39 00 33 00 31 00 31 00 37 00 32 00 30 00 33    |.9.3.1.1.7.2.0.3|
14:49:00 UDPCHAN: 00064   00 30 00 34 00 39 00 39 00 38 00 35 00 39 00 33    |.0.4.9.9.8.5.9.3|
14:49:00 UDPCHAN: 00080   00 31 00 31 00 36 00 36 00 30 01 02 00 76 36 b0    |.1.1.6.6.0...v6°|
14:49:00 UDPCHAN: 00096   02 02 00 86 73 64 04 00 35 00 33 00 34 00 30 00    |...†sd..5.3.4.0.|
14:49:00 UDPCHAN: 00112   33 00 8b 17 cb b5 06 7d 40 05 00 29 40 02 17 c3    |3.‹.Ëµ.}@..)@..Ã|
14:49:00 UDPCHAN: 00128   03 77 00 00 10 32 0e 56 34 34 34 34 ef 08 e5 20    |.w...2.V4444ï.å |
14:49:00 UDPCHAN: 00144   00 01 00 11 00 02 17 c3 03 77 00 00 10 32 0d 56    |.......Ã.w...2.V|
14:49:00 UDPCHAN: 00160   34 34 34 34 ef 25 22 00 53 00 69 00 65 00 6d 00    |4444ï%".S.i.e.m.|
14:49:00 UDPCHAN: 00176   65 00 6e 00 73 00 20 00 47 00 61 00 74 00 65 00    |e.n.s. .G.a.t.e.|
14:49:00 UDPCHAN: 00192   6b 00 65 00 65 00 70 00 65 00 72 80 ae 01 74 07    |k.e.e.p.e.r€®.t.|
14:49:00 UDPCHAN: 00208   00 08 81 6b 00 02 01 c5 00 07 00 08 81 6b 00 02    |..•k...Å....•k..|
14:49:00 UDPCHAN: 00224   05 c0 3c fc b7 3b 01 2a 22 00 53 00 69 00 65 00    |.À<ü·;.*".S.i.e.|
14:49:00 UDPCHAN: 00240   6d 00 65 00 6e 00 73 00 20 00 47 00 61 00 74 00    |m.e.n.s. .G.a.t.|
14:49:00 UDPCHAN: 00256   65 00 6b 00 65 00 65 00 70 00 65 00 72 02 80 55    |e.k.e.e.p.e.r.€U|
14:49:00 UDPCHAN: 00272   52 00 30 00 30 00 30 00 30 00 31 00 31 00 32 00    |R.0.0.0.0.1.1.2.|
14:49:00 UDPCHAN: 00288   30 00 30 00 37 00 31 00 34 00 37 00 31 00 33 00    |0.0.7.1.4.7.1.3.|
14:49:00 UDPCHAN: 00304   30 00 34 00 39 00 39 00 38 00 35 00 39 00 33 00    |0.4.9.9.8.5.9.3.|
14:49:00 UDPCHAN: 00320   31 00 31 00 37 00 32 00 30 00 33 00 30 00 34 00    |1.1.7.2.0.3.0.4.|
14:49:00 UDPCHAN: 00336   39 00 39 00 38 00 35 00 39 00 33 00 31 00 31 00    |9.9.8.5.9.3.1.1.|
14:49:00 UDPCHAN: 00352   36 00 36 00 30 07 00 08 81 6b 00 02 06 00 60 bf    |6.6.0...•k....`¿|
14:49:00 UDPCHAN: 00368   d5 f6 a8 21 75 bf 18 79 4f 4f e9 01 00             |Õö¨!u¿.yOOé..|
14:49:00 UDPCHAN: Message:
14:49:00 UDPCHAN:  0> <1000> RasMessage = (0) .  <2731> CHOICE ...
14:49:00 UDPCHAN:  1> . <1001> admissionRequest = (4294967185) .  <2004> SEQUENCE ...
14:49:00 UDPCHAN:  2> . . <1002> requestSeqNum = (16309) .  <3615> INTEGER (1..65535)
14:49:00 UDPCHAN:  2> . . <1003> callType = (13487) .  <1989> CHOICE ...
14:49:00 UDPCHAN:  3> . . . <1004> pointToPoint = (4294967173) .  <9> NULL
14:49:00 UDPCHAN:  2> . . <1005> callModel = (9058) .  <1980> CHOICE ...
14:49:00 UDPCHAN:  3> . . . <1006> gatekeeperRouted = (4294967173) .  <9> NULL
14:49:00 UDPCHAN:  2> . . <1007> endpointIdentifier = (84)
'.0.0.0.0.1.1.2.0.0.7.1.4.7.1.3.0.4.9.9.8.5.9.3.1.1.7.2.0.3.0.4.9.9.8.5.9.3.1.1.6.6.0'
=0x0030003000300030003100310032003000300037003100340037003100330030003400390039003800350039003300310
```

```
0310037003200300033003000340039003900380035003900330031003100360036003O .  <3597> BMPString (1..128)
14:49:00 UDPCHAN:  2> . . <1012> destinationInfo = (1) .  <1147> SET OF CHOICE ...
14:49:00 UDPCHAN:  3> . . . <1013> * = (8122) .  <4095> CHOICE ...
14:49:00 UDPCHAN:  4> . . . . <1014> e164 = (5) '43038' =0x3433303338 .  <4089> IA5String (1..128)
FROM '#*,0123456789'
14:49:00 UDPCHAN:  2> . . <1016> srcInfo = (2) .  <1147> SET OF CHOICE ...
14:49:00 UDPCHAN:  3> . . . <1017> * = (8122) .  <4095> CHOICE ...
14:49:00 UDPCHAN:  4> . . . . <1018> e164 = (5) '53403' =0x3533343033 .  <4089> IA5String (1..128)
FROM '#*,0123456789'
14:49:00 UDPCHAN:  3> . . . <1020> * = (9613) .  <4095> CHOICE ...
14:49:00 UDPCHAN:  4> . . . . <1021> h323-ID = (10) '.5.3.4.0.3' =0x00350033003400300033 .  <4084>
BMPString (1..256)
14:49:00 UDPCHAN:  2> . . <1023> srcCallSignalAddress = (10714) .  <4579> CHOICE ...
14:49:00 UDPCHAN:  3> . . . <1024> ipAddress = (4294967185) .  <4570> SEQUENCE
14:49:00 UDPCHAN:  4> . . . . <1025> ip = (4) '‹.Ëµ' =0x8b17cbb5 <139.23.203.181> .  <4520> OCTET
STRING (4..4)
14:49:00 UDPCHAN:  4> . . . . <1027> port = (1661) .  <155> INTEGER (0..65535)
14:49:00 UDPCHAN:  2> . . <1028> bandWidth = (1280) .  <3606> INTEGER (0..-1)
14:49:00 UDPCHAN:  2> . . <1029> callReferenceValue = (10560) .  <3602> INTEGER (0..65535)
14:49:00 UDPCHAN:  2> . . <1030> conferenceID = (16) '..Ã.w...2.V4444ï'
=0x0217c30377000010320e5634343434ef .  <3620> OCTET STRING (16..16)
14:49:00 UDPCHAN:  2> . . <1032> activeMC = (0) .  <0> BOOLEAN
14:49:00 UDPCHAN:  2> . . <1033> answerCall = (0) .  <0> BOOLEAN
14:49:00 UDPCHAN:  2> . . <1034> canMapAlias = (0) .  <0> BOOLEAN
14:49:00 UDPCHAN:  2> . . <1035> callIdentifier = (4294967185) .  <3568> SEQUENCE ...
14:49:00 UDPCHAN:  3> . . . <1036> guid = (16) '..Ã.w...2.V4444ï'
=0x0217c30377000010320d5634343434ef .  <3625> OCTET STRING (16..16)
14:49:00 UDPCHAN:  2> . . <1038> gatekeeperIdentifier = (36) '.S.i.e.m.e.n.s. .G.a.t.e.k.e.e.p.e.r'
=0x005300690065006d0065006e00730020004700610074006500650070006500720
(1..128)
14:49:00 UDPCHAN:  2> . . <1041> cryptoTokens = (1) .  <752> SET OF CHOICE ...
14:49:00 UDPCHAN:  3> . . . <1042> * = (12045) .  <3421> CHOICE ...
14:49:00 UDPCHAN:  4> . . . . <1043> nestedcryptoToken = (7314) .  <384> CHOICE ...
14:49:00 UDPCHAN:  5> . . . . . <1044> cryptoHashedToken = (4294967185) .  <339> SEQUENCE
14:49:00 UDPCHAN:  6> . . . . . . <1045> tokenOID = (7) { itu-t recommendation h 235 0 2 1 }.  <171>
OBJECT IDENTIFIER
14:49:00 UDPCHAN:  6> . . . . . . <1047> hashedVals = (4294967185) .  <556> SEQUENCE ...
14:49:00 UDPCHAN:  7> . . . . . . . <1048> tokenOID = (7) { itu-t recommendation h 235 0 2 5 }.
<171> OBJECT IDENTIFIER
14:49:00 UDPCHAN:  7> . . . . . . . <1050> timeStamp = (1023194940) .  <738> INTEGER (1..-1)
14:49:00 UDPCHAN:  7> . . . . . . . <1051> random = (42) .  <735> INTEGER
14:49:00 UDPCHAN:  7> . . . . . . . <1052> generalID = (36) '.S.i.e.m.e.n.s. .G.a.t.e.k.e.e.p.e.r'
=0x005300690065006d0065006e0073002000470061007400650065006b00650065007000650072 .  <725> BMPString
(1..128)
14:49:00 UDPCHAN:  7> . . . . . . . <1055> sendersID = (84)
'.0.0.0.0.1.1.2.0.0.7.1.4.7.1.3.0.4.9.9.8.5.9.3.1.1.7.2.0.3.0.4.9.9.8.5.9.3.1.1.6.6.0'
=0x0030003000300030003100310032003000300037003100340037003100330030003400390039003800350039003300310
031003700320030003300300034003900390038003500390033003100310036003600300 .  <725> BMPString (1..128)
14:49:00 UDPCHAN:  6> . . . . . . <1060> token = (4294967185) .  <532> SEQUENCE
14:49:00 UDPCHAN:  7> . . . . . . . <1061> algorithmOID = (7) { itu-t recommendation h 235 0 2 6 }.
<171> OBJECT IDENTIFIER
14:49:00 UDPCHAN:  7> . . . . . . . <1063> paramS = (4294967185) .  <507> SEQUENCE ...
14:49:00 UDPCHAN:  8> . . . . . . . . <1064> null = (4294967173) .  <9> NULL
14:49:00 UDPCHAN:  7> . . . . . . . <1065> hash = (96) '¿Õö¨!u¿.yOOé' =0xbfd5f6a82175bf18794f4fe9 .
<243> BIT STRING
14:49:00 UDPCHAN:  2> . . <1067> willSupplyUUIEs = (0) .  <0> BOOLEAN
14:49:00 UDPCHAN: INFO  - New message (channel 0)  sent --> admissionConfirm:
14:49:00 UDPCHAN: Address:
14:49:00 UDPCHAN:  0> <1111> TransportAddress = (0) .  <4579> CHOICE ...
14:49:00 UDPCHAN:  1> . <1112> ipAddress = (0) .  <4570> SEQUENCE
14:49:00 UDPCHAN:  2> . . <1113> ip = (4) '‹.Ëµ' =0x8b17cbb5 <139.23.203.181> .  <4520> OCTET STRING
(4..4)
14:49:00 UDPCHAN:  2> . . <1115> port = (1660) .  <155> INTEGER (0..65535)
14:49:00 UDPCHAN: Message:
14:49:00 UDPCHAN:  0> <1076> RasMessage = (0) .  <2731> CHOICE ...
14:49:00 UDPCHAN:  1> . <1077> admissionConfirm = (0) .  <1884> SEQUENCE ...
14:49:00 UDPCHAN:  2> . . <1110> requestSeqNum = (16309) .  <3615> INTEGER (1..65535)
14:49:00 UDPCHAN:  2> . . <1078> bandWidth = (1280) .  <3606> INTEGER (0..-1)
14:49:00 UDPCHAN:  2> . . <1079> callModel = (0) .  <1980> CHOICE ...
14:49:00 UDPCHAN:  3> . . . <1096> gatekeeperRouted = (0) .  <9> NULL
14:49:00 UDPCHAN:  2> . . <1105> destCallSignalAddress = (0) .  <4579> CHOICE ...
14:49:00 UDPCHAN:  3> . . . <1106> ipAddress = (0) .  <4570> SEQUENCE
14:49:00 UDPCHAN:  4> . . . . <1107> ip = (4) '‹.Ëµ' =0x8b17cbb5 <139.23.203.181> .  <4520> OCTET
STRING (4..4)
14:49:00 UDPCHAN:  4> . . . . <1109> port = (1720) .  <155> INTEGER (0..65535)
14:49:00 UDPCHAN:  2> . . <1097> destinationInfo = (0) .  <1147> SET OF CHOICE ...
14:49:00 UDPCHAN:  3> . . . <1098> * = (0) .  <4095> CHOICE ...
14:49:00 UDPCHAN:  4> . . . . <1099> e164 = (5) '43038' =0x3433303338 .  <4089> IA5String (1..128)
FROM '#*,0123456789'
14:49:00 UDPCHAN:  2> . . <1101> destinationType = (0) .  <4403> SEQUENCE ...
14:49:00 UDPCHAN:  3> . . . <1102> terminal = (0) .  <4204> SEQUENCE ...
14:49:00 UDPCHAN:  3> . . . <1103> mc = (0) .  <0> BOOLEAN
14:49:00 UDPCHAN:  3> . . . <1104> undefinedNode = (0) .  <0> BOOLEAN
14:49:00 UDPCHAN:  2> . . <1116> cryptoTokens = (4294966741) .  <752> SET OF CHOICE ...
14:49:00 UDPCHAN:  3> . . . <1117> * = (4294966741) .  <3421> CHOICE ...
14:49:00 UDPCHAN:  4> . . . . <1118> nestedcryptoToken = (4294966741) .  <384> CHOICE ...
14:49:00 UDPCHAN:  5> . . . . . <1119> cryptoHashedToken = (4294966741) .  <339> SEQUENCE
14:49:00 UDPCHAN:  6> . . . . . . <1120> tokenOID = (7) { itu-t recommendation h 235 0 2 1 }.  <171>
OBJECT IDENTIFIER
```

```
14:49:00 UDPCHAN:  6> . . . . . . <1122> hashedVals = (4294966741) .  <556> SEQUENCE ...
14:49:00 UDPCHAN:  7> . . . . . . . <1123> tokenOID = (7) { itu-t recommendation h 235 0 2 5 }.
<171> OBJECT IDENTIFIER
14:49:00 UDPCHAN:  7> . . . . . . . <1134> timeStamp = (1023194940) .  <738> INTEGER (1..-1)
14:49:00 UDPCHAN:  7> . . . . . . . <1133> random = (18468) .  <735> INTEGER
14:49:00 UDPCHAN:  7> . . . . . . . <1125> generalID = (84)
'.0.0.0.0.1.1.2.0.0.7.1.4.7.1.3.0.4.9.9.8.5.9.3.1.1.7.2.0.3.0.4.9.9.8.5.9.3.1.1.6.6.0'
=0x0030003000300030003100310032003000300037003100340037003100330030003400390039003800350039003300310
03100370032003000330030003400390039003800350039003300310031003600360030 .  <725> BMPString (1..128)
14:49:00 UDPCHAN:  7> . . . . . . . <1130> sendersID = (36) '.S.i.e.m.e.n.s. .G.a.t.e.k.e.e.p.e.r'
=0x005300690065006d0065006e007300200047006100740065006b00650065007000650072 .  <725> BMPString
(1..128)
14:49:00 UDPCHAN:  6> . . . . . . <1135> token = (4294966741) .  <532> SEQUENCE
14:49:00 UDPCHAN:  7> . . . . . . . <1136> algorithmOID = (7) { itu-t recommendation h 235 0 2 6 }.
<171> OBJECT IDENTIFIER
14:49:00 UDPCHAN:  7> . . . . . . . <1138> paramS = (4294966741) .  <507> SEQUENCE ...
14:49:00 UDPCHAN:  8> . . . . . . . . <1139> null = (0) .  <9> NULL
14:49:00 UDPCHAN:  7> . . . . . . . <1140> hash = (96) '‹.Ëµ|....ÿ.ÿ' =0x8b17cbb57c06000000ff00ff .
<243> BIT STRING
14:49:00 UDPCHAN:  2> . . <1081> willRespondToIRR = (0) .  <0> BOOLEAN
14:49:00 UDPCHAN:  2> . . <1082> uuiesRequested = (0) .  <1829> SEQUENCE ...
14:49:00 UDPCHAN:  3> . . . <1083> setup = (0) .  <0> BOOLEAN
14:49:00 UDPCHAN:  3> . . . <1084> callProceeding = (0) .  <0> BOOLEAN
14:49:00 UDPCHAN:  3> . . . <1085> connect = (0) .  <0> BOOLEAN
14:49:00 UDPCHAN:  3> . . . <1086> alerting = (0) .  <0> BOOLEAN
14:49:00 UDPCHAN:  3> . . . <1087> information = (0) .  <0> BOOLEAN
14:49:00 UDPCHAN:  3> . . . <1088> releaseComplete = (0) .  <0> BOOLEAN
14:49:00 UDPCHAN:  3> . . . <1089> facility = (0) .  <0> BOOLEAN
14:49:00 UDPCHAN:  3> . . . <1090> progress = (0) .  <0> BOOLEAN
14:49:00 UDPCHAN:  3> . . . <1091> empty = (0) .  <0> BOOLEAN
14:49:00 UDPCHAN:  3> . . . <1092> status = (0) .  <0> BOOLEAN
14:49:00 UDPCHAN:  3> . . . <1093> statusInquiry = (0) .  <0> BOOLEAN
14:49:00 UDPCHAN:  3> . . . <1094> setupAcknowledge = (0) .  <0> BOOLEAN
14:49:00 UDPCHAN:  3> . . . <1095> notify = (0) .  <0> BOOLEAN
14:49:00 UDPCHAN: Binary:
14:49:00 UDPCHAN: 00000   2a 00 3f b4 40 05 00 40 8b 17 cb b5 06 b8 29 44    |*.?´@..@‹.Ëµ.¸)D|
14:49:00 UDPCHAN: 00016   c0 00 06 01 02 00 76 36 b0 02 02 00 80 af 01 74    |À.....v6°...€¯.t|
14:49:00 UDPCHAN: 00032   07 00 08 81 6b 00 02 01 c5 00 07 00 08 81 6b 00    |...•k...Å....•k.|
14:49:00 UDPCHAN: 00048   02 05 c0 3c fc b7 3b 02 48 24 52 00 30 00 30 00    |..À<ü·;.H$R.0.0.|
14:49:00 UDPCHAN: 00064   30 00 30 00 31 00 31 00 32 00 30 00 30 00 37 00    |0.0.1.1.2.0.0.7.|
14:49:00 UDPCHAN: 00080   31 00 34 00 37 00 31 00 33 00 30 00 34 00 39 00    |1.4.7.1.3.0.4.9.|
14:49:00 UDPCHAN: 00096   39 00 38 00 35 00 39 00 33 00 31 00 31 00 37 00    |9.8.5.9.3.1.1.7.|
14:49:00 UDPCHAN: 00112   32 00 30 00 33 00 30 00 34 00 39 00 39 00 38 00    |2.0.3.0.4.9.9.8.|
14:49:00 UDPCHAN: 00128   35 00 39 00 33 00 31 00 31 00 36 00 36 00 30 02    |5.9.3.1.1.6.6.0.|
14:49:00 UDPCHAN: 00144   80 25 22 00 53 00 69 00 65 00 6d 00 65 00 6e 00    |€%".S.i.e.m.e.n.|
14:49:00 UDPCHAN: 00160   73 00 20 00 47 00 61 00 74 00 65 00 6b 00 65 00    |s. .G.a.t.e.k.e.|
14:49:00 UDPCHAN: 00176   65 00 70 00 65 00 72 07 00 08 81 6b 00 02 06 00    |e.p.e.r...•k....|
14:49:00 UDPCHAN: 00192   60 f5 7e 16 8b 8f 75 4f 52 81 cf ef 82 01 00 0b    |`õ~.‹•uOR•Ïï,...|
14:49:00 UDPCHAN: 00208   80 01 f8 01 00 01 00 01 00 01 00                   |€.ø........|
```

6.5 ACF received by the Client with cryptohashed token

```
14:49:00 UDPCHAN: INFO  - New message (channel 0)  recv <-- admissionConfirm:
14:49:00 UDPCHAN: Address:
14:49:00 UDPCHAN:  0> <1870> TransportAddress = (0) .  <4579> CHOICE ...
14:49:00 UDPCHAN:  1> . <1871> ipAddress = (0) .  <4570> SEQUENCE
14:49:00 UDPCHAN:  2> . . <1872> ip = (4) '‹.Ëµ' =0x8b17cbb5 <139.23.203.181> .  <4520> OCTET STRING
(4..4)
14:49:00 UDPCHAN:  2> . . <1874> port = (1719) .  <155> INTEGER (0..65535)
14:49:00 UDPCHAN: Binary:
14:49:00 UDPCHAN: 00000   2a 00 2b aa 40 05 00 40 8b 17 cb b5 06 79 28 44    |*.+ª@..@‹.Ëµ.y(D|
14:49:00 UDPCHAN: 00016   c0 00 02 02 00 80 ae 01 74 07 00 08 81 6b 00 02    |À....€®.t...•k..|
14:49:00 UDPCHAN: 00032   01 c5 00 07 00 08 81 6b 00 02 05 c0 3c fc b7 3b    |.Å....•k...À<ü·;|
14:49:00 UDPCHAN: 00048   01 2b 52 00 30 00 30 00 30 00 30 00 30 00 30 00    |.+R.0.0.0.0.0.0.|
14:49:00 UDPCHAN: 00064   32 00 30 00 30 00 36 00 36 00 30 00 37 00 33 00    |2.0.0.6.6.0.7.3.|
14:49:00 UDPCHAN: 00080   33 00 30 00 34 00 39 00 39 00 38 00 35 00 39 00    |3.0.4.9.9.8.5.9.|
14:49:00 UDPCHAN: 00096   33 00 31 00 31 00 37 00 32 00 30 00 33 00 30 00    |3.1.1.7.2.0.3.0.|
14:49:00 UDPCHAN: 00112   34 00 39 00 39 00 38 00 35 00 39 00 33 00 31 00    |4.9.9.8.5.9.3.1.|
14:49:00 UDPCHAN: 00128   31 00 36 00 35 00 38 02 80 25 22 00 53 00 69 00    |1.6.5.8.€%".S.i.|
14:49:00 UDPCHAN: 00144   65 00 6d 00 65 00 6e 00 73 00 20 00 47 00 61 00    |e.m.e.n.s. .G.a.|
14:49:00 UDPCHAN: 00160   74 00 65 00 6b 00 65 00 65 00 70 00 65 00 72 07    |t.e.k.e.e.p.e.r.|
14:49:00 UDPCHAN: 00176   00 08 81 6b 00 02 06 00 60 03 19 a2 69 db 1c 38    |..•k....`..¢iÛ.8|
14:49:00 UDPCHAN: 00192   0b c0 8d 38 e9 01 00 0b 80 01 f8 01 00 01 00 01    |.À•8é...€.ø.....|
14:49:00 UDPCHAN: 00208   00 01 00                                           |...|
14:49:00 UDPCHAN: Message:
14:49:00 UDPCHAN:  0> <1814> RasMessage = (0) .  <2731> CHOICE ...
14:49:00 UDPCHAN:  1> . <1815> admissionConfirm = (4294967185) .  <1884> SEQUENCE ...
14:49:00 UDPCHAN:  2> . . <1816> requestSeqNum = (11179) .  <3615> INTEGER (1..65535)
14:49:00 UDPCHAN:  2> . . <1817> bandWidth = (1280) .  <3606> INTEGER (0..-1)
14:49:00 UDPCHAN:  2> . . <1818> callModel = (9058) .  <1980> CHOICE ...
14:49:00 UDPCHAN:  3> . . . <1819> gatekeeperRouted = (4294967173) .  <9> NULL
14:49:00 UDPCHAN:  2> . . <1820> destCallSignalAddress = (10714) .  <4579> CHOICE ...
14:49:00 UDPCHAN:  3> . . . <1821> ipAddress = (4294967185) .  <4570> SEQUENCE
14:49:00 UDPCHAN:  4> . . . . <1822> ip = (4) '‹.Ëµ' =0x8b17cbb5 <139.23.203.181> .  <4520> OCTET
STRING (4..4)
14:49:00 UDPCHAN:  4> . . . . <1824> port = (1657) .  <155> INTEGER (0..65535)
```

```
14:49:00 UDPCHAN:  2> . . <1825> destinationType = (4294967185) .  <4403> SEQUENCE ...
14:49:00 UDPCHAN:  3> . . . <1826> terminal = (4294967185) .  <4204> SEQUENCE ...
14:49:00 UDPCHAN:  3> . . . <1827> mc = (0) .  <0> BOOLEAN
14:49:00 UDPCHAN:  3> . . . <1828> undefinedNode = (0) .  <0> BOOLEAN
14:49:00 UDPCHAN:  2> . . <1829> cryptoTokens = (1) .  <752> SET OF CHOICE ...
14:49:00 UDPCHAN:  3> . . . <1830> * = (12045) .  <3421> CHOICE ...
14:49:00 UDPCHAN:  4> . . . . <1831> nestedcryptoToken = (7314) .  <384> CHOICE ...
14:49:00 UDPCHAN:  5> . . . . . <1832> cryptoHashedToken = (4294967185) .  <339> SEQUENCE
14:49:00 UDPCHAN:  6> . . . . . . <1833> tokenOID = (7) { itu-t recommendation h 235 0 2 1 }.  <171>
OBJECT IDENTIFIER
14:49:00 UDPCHAN:  6> . . . . . . <1835> hashedVals = (4294967185) .  <556> SEQUENCE ...
14:49:00 UDPCHAN:  7> . . . . . . . <1836> tokenOID = (7) { itu-t recommendation h 235 0 2 5 }.
<171> OBJECT IDENTIFIER
14:49:00 UDPCHAN:  7> . . . . . . . <1838> timeStamp = (1023194940) .  <738> INTEGER (1..-1)
14:49:00 UDPCHAN:  7> . . . . . . . <1839> random = (43) .  <735> INTEGER
14:49:00 UDPCHAN:  7> . . . . . . . <1840> generalID = (84)
'.0.0.0.0.0.0.2.0.0.6.6.0.7.3.3.0.4.9.9.8.5.9.3.1.1.7.2.0.3.0.4.9.9.8.5.9.3.1.1.6.5.8'
=0x00300030003000300030003000320030003000360036003000370033003300300034003900390038003500390033003100310
0310037003200300033003000340039003900380035003900330031003100360035003 8 .  <725> BMPString (1..128)
14:49:00 UDPCHAN:  7> . . . . . . . <1845> sendersID = (36) '.S.i.e.m.e.n.s. .G.a.t.e.k.e.e.p.e.r'
=0x005300690065006d0065006e00730020004700610074006500 6b00650065007000650072 .  <725> BMPString
(1..128)
14:49:00 UDPCHAN:  6> . . . . . . <1848> token = (4294967185) .  <532> SEQUENCE
14:49:00 UDPCHAN:  7> . . . . . . . <1849> algorithmOID = (7) { itu-t recommendation h 235 0 2 6 }.
<171> OBJECT IDENTIFIER
14:49:00 UDPCHAN:  7> . . . . . . . <1851> paramS = (4294967185) .  <507> SEQUENCE ...
14:49:00 UDPCHAN:  8> . . . . . . . . <1852> null = (4294967173) .  <9> NULL
14:49:00 UDPCHAN:  7> . . . . . . . <1853> hash = (96) '..¢iÛ.8.À•8é' =0x0319a269db1c380bc08d38e9 .
<243> BIT STRING
14:49:00 UDPCHAN:  2> . . <1855> willRespondToIRR = (0) .  <0> BOOLEAN
14:49:00 UDPCHAN:  2> . . <1856> uuiesRequested = (4294967185) .  <1829> SEQUENCE ...
14:49:00 UDPCHAN:  3> . . . <1857> setup = (0) .  <0> BOOLEAN
14:49:00 UDPCHAN:  3> . . . <1858> callProceeding = (0) .  <0> BOOLEAN
14:49:00 UDPCHAN:  3> . . . <1859> connect = (0) .  <0> BOOLEAN
14:49:00 UDPCHAN:  3> . . . <1860> alerting = (0) .  <0> BOOLEAN
14:49:00 UDPCHAN:  3> . . . <1861> information = (0) .  <0> BOOLEAN
14:49:00 UDPCHAN:  3> . . . <1862> releaseComplete = (0) .  <0> BOOLEAN
14:49:00 UDPCHAN:  3> . . . <1863> facility = (0) .  <0> BOOLEAN
14:49:00 UDPCHAN:  3> . . . <1864> progress = (0) .  <0> BOOLEAN
14:49:00 UDPCHAN:  3> . . . <1865> empty = (0) .  <0> BOOLEAN
14:49:00 UDPCHAN:  3> . . . <1866> status = (0) .  <0> BOOLEAN
14:49:00 UDPCHAN:  3> . . . <1867> statusInquiry = (0) .  <0> BOOLEAN
14:49:00 UDPCHAN:  3> . . . <1868> setupAcknowledge = (0) .  <0> BOOLEAN
14:49:00 UDPCHAN:  3> . . . <1869> notify = (0) .  <0> BOOLEAN
14:49:00 TPKTCHAN  : INFO  - New message (channel 1) sent --> alerting:
14:49:00 TPKTCHAN  : INFO  - Message:
14:49:00 TPKTCHAN  :  0> <1436> Q931Message = (0) .  <6213> SEQUENCE [PRIVATE 1]
14:49:00 TPKTCHAN  :  1> . <1437> protocolDiscriminator = (8) .  <45> INTEGER (0..255)
14:49:00 TPKTCHAN  :  1> . <1877> callReferenceValue = (4294966741) .  <6201> CHOICE
14:49:00 TPKTCHAN  :  2> . . <1878> twoBytes = (35082) .  <6187> INTEGER [EMPTY 2] (0..65535)
14:49:00 TPKTCHAN  :  1> . <1438> message = (4294966741) .  <6148> CHOICE ...
14:49:00 TPKTCHAN  :  2> . . <1439> alerting = (0) .  <6120> SET [EMPTY 1] ...
14:49:00 TPKTCHAN  :  3> . . . <1440> userUser = (0) .  <5461> SEQUENCE [APPLICATION 126]
14:49:00 TPKTCHAN  :  4> . . . . <1441> protocolDiscriminator = (5) .  <45> INTEGER (0..255)
14:49:00 TPKTCHAN  :  4> . . . . <1442> h323-UserInformation = (4294966741) .  <5451> SEQUENCE
[PRIVATE 0] ...
14:49:00 TPKTCHAN  :  5> . . . . . <1443> h323-uu-pdu = (4294966741) .  <5401> SEQUENCE ...
14:49:00 TPKTCHAN  :  6> . . . . . . <1444> h323-message-body = (4294966741) .  <5359> CHOICE ...
14:49:00 TPKTCHAN  :  7> . . . . . . . <1445> alerting = (0) .  <5266> SEQUENCE ...
14:49:00 TPKTCHAN  :  8> . . . . . . . . <1446> protocolIdentifier = (6) { itu-t recommendation h
2250 0 4 }.  <3594> OBJECT IDENTIFIER
14:49:00 TPKTCHAN  :  8> . . . . . . . . <1882> destinationInfo = (0) .  <4403> SEQUENCE ...
14:49:00 TPKTCHAN  :  9> . . . . . . . . . <1883> vendor = (0) .  <4186> SEQUENCE ...
14:49:00 TPKTCHAN  : 10> . . . . . . . . . . <1884> vendor = (0) .  <4169> SEQUENCE ...
14:49:00 TPKTCHAN  : 11> . . . . . . . . . . . <1885> t35CountryCode = (11) .  <45> INTEGER (0..255)
14:49:00 TPKTCHAN  : 11> . . . . . . . . . . . <1886> t35Extension = (11) .  <45> INTEGER (0..255)
14:49:00 TPKTCHAN  : 11> . . . . . . . . . . . <1887> manufacturerCode = (11) .  <155> INTEGER
(0..65535)
14:49:00 TPKTCHAN  : 10> . . . . . . . . . . <1888> productId = (16) 'Test application'
=0x54657374206170706c69636174696f6e .  <4181> OCTET STRING (1..256)
14:49:00 TPKTCHAN  : 10> . . . . . . . . . . <1890> versionId = (9) 'RADVision'
=0x524144566973696f6e .  <4181> OCTET STRING (1..256)
14:49:00 TPKTCHAN  :  9> . . . . . . . . . <1892> terminal = (0) .  <4204> SEQUENCE ...
14:49:00 TPKTCHAN  :  9> . . . . . . . . . <1893> mc = (0) .  <0> BOOLEAN
14:49:00 TPKTCHAN  :  9> . . . . . . . . . <1894> undefinedNode = (0) .  <0> BOOLEAN
14:49:00 TPKTCHAN  :  8> . . . . . . . . <1879> callIdentifier = (4294966741) .  <3568> SEQUENCE ...
14:49:00 TPKTCHAN  :  9> . . . . . . . . . <1880> guid = (16) '..Â.w...2.V4444ï'
=0x0217c30377000010320d5634343434ef .  <3625> OCTET STRING (16..16)
14:49:00 TPKTCHAN  :  8> . . . . . . . . <1896> cryptoTokens = (4294966741) .  <752> SET OF CHOICE
...
14:49:00 TPKTCHAN  :  9> . . . . . . . . . <1897> * = (4294966741) .  <3421> CHOICE ...
14:49:00 TPKTCHAN  : 10> . . . . . . . . . . <1898> nestedcryptoToken = (4294966741) .  <384> CHOICE
...
14:49:00 TPKTCHAN  : 11> . . . . . . . . . . . <1899> cryptoHashedToken = (4294966741) .  <339>
SEQUENCE
14:49:00 TPKTCHAN  : 12> . . . . . . . . . . . . <1900> tokenOID = (7) { itu-t recommendation h 235
0 2 1 }.  <171> OBJECT IDENTIFIER
14:49:00 TPKTCHAN  : 12> . . . . . . . . . . . . <1902> hashedVals = (4294966741) .  <556> SEQUENCE
...
```

```
14:49:00 TPKTCHAN  : 13> . . . . . . . . . . . . . . <1903> tokenOID = (7) { itu-t recommendation h
235 0 2 5 }.  <171> OBJECT IDENTIFIER
14:49:00 TPKTCHAN  : 13> . . . . . . . . . . . . . . <1914> timeStamp = (1023194940) .  <738> INTEGER
(1..-1)
14:49:00 TPKTCHAN  : 13> . . . . . . . . . . . . . . <1913> random = (43) .  <735> INTEGER
14:49:00 TPKTCHAN  : 13> . . . . . . . . . . . . . . <1905> generalID = (36) '.S.i.e.m.e.n.s.
.G.a.t.e.k.e.e.p.e.r' =0x005300690065006d0065006e0073002000470061007400650006b0065006500700065007 2 .
<725> BMPString (1..128)
14:49:00 TPKTCHAN  : 13> . . . . . . . . . . . . . . <1908> sendersID = (84)
'.0.0.0.0.0.0.2.0.0.6.6.0.7.3.3.0.4.9.9.8.5.9.3.1.1.7.2.0.3.0.4.9.9.8.5.9.3.1.1.6.5.8'
=0x0030003000300030003000300032003000300036003600300037003300330030003400390039003800350039003300310
031003700320030003300300034003900390038003500390033003100310036003500 38 .  <725> BMPString (1..128)
14:49:00 TPKTCHAN  : 12> . . . . . . . . . . . . . <1915> token = (4294966741) .  <532> SEQUENCE
14:49:00 TPKTCHAN  : 13> . . . . . . . . . . . . . . <1916> algorithmOID = (7) { itu-t recommendation
h 235 0 2 6 }.  <171> OBJECT IDENTIFIER
14:49:00 TPKTCHAN  : 13> . . . . . . . . . . . . . . <1918> paramS = (4294966741) .  <507> SEQUENCE
...
14:49:00 TPKTCHAN  : 14> . . . . . . . . . . . . . . . <1919> null = (0) .  <9> NULL
14:49:00 TPKTCHAN  : 13> . . . . . . . . . . . . . . <1920> hash = (96) '‹.Ëµy....ÿ.ÿ'
=0x8b17cbb57906000000ff00ff .  <243> BIT STRING
14:49:00 TPKTCHAN  :  8> . . . . . . . . . <1448> multipleCalls = (0) .  <0> BOOLEAN
14:49:00 TPKTCHAN  :  8> . . . . . . . . . <1449> maintainConnection = (0) .  <0> BOOLEAN
14:49:00 TPKTCHAN  :  8> . . . . . . . . . <1450> presentationIndicator = (4294966741) .  <4784>
CHOICE ...
14:49:00 TPKTCHAN  :  9> . . . . . . . . . . <1451> presentationAllowed = (0) .  <9> NULL
14:49:00 TPKTCHAN  :  8> . . . . . . . . . <1452> screeningIndicator = (4294966741) .  <4765>
ENUMERATED ...
14:49:00 TPKTCHAN  :  9> . . . . . . . . . . <1453> userProvidedVerifiedAndFailed = (0) .  <9> NULL
14:49:00 TPKTCHAN  :  6> . . . . . . . <1895> h245Tunneling = (0) .  <0> BOOLEAN
14:49:00 TPKTCHAN  : INFO  - Binary:
14:49:00 TPKTCHAN  : 00000   08 02 89 0a 01 7e 00 fd 05 23 80 06 00 08 91 4a    |..‰..~.ý.#€..."J|
14:49:00 TPKTCHAN  : 00016   00 04 22 c0 0b 0b 00 0b 0f 54 65 73 74 20 61 70    |.."À.....Test ap|
14:49:00 TPKTCHAN  : 00032   70 6c 69 63 61 74 69 6f 6e 08 52 41 44 56 69 73    |plication.RADVis|
14:49:00 TPKTCHAN  : 00048   69 6f 6e 01 b2 d8 00 11 00 02 17 c3 03 77 00 00    |ion.²Ø.....Ã.w..|
14:49:00 TPKTCHAN  : 00064   10 32 0d 56 34 34 34 34 ef 80 ae 01 74 07 00 08    |.2.V4444ï€®.t...|
14:49:00 TPKTCHAN  : 00080   81 6b 00 02 01 c5 00 07 00 08 81 6b 00 02 05 c0    |•k...Å....•k...À|
14:49:00 TPKTCHAN  : 00096   3c fc b7 3b 01 2b 22 00 53 00 69 00 65 00 6d 00    |<ü·;.+".S.i.e.m.|
14:49:00 TPKTCHAN  : 00112   65 00 6e 00 73 00 20 00 47 00 61 00 74 00 65 00    |e.n.s. .G.a.t.e.|
14:49:00 TPKTCHAN  : 00128   6b 00 65 00 65 00 70 00 65 00 72 02 80 55 52 00    |k.e.e.p.e.r.€UR.|
14:49:00 TPKTCHAN  : 00144   30 00 30 00 30 00 30 00 30 00 30 00 32 00 30 00    |0.0.0.0.0.0.2.0.|
14:49:00 TPKTCHAN  : 00160   30 00 36 00 36 00 30 00 37 00 33 00 33 00 30 00    |0.6.6.0.7.3.3.0.|
14:49:00 TPKTCHAN  : 00176   34 00 39 00 39 00 38 00 35 00 39 00 33 00 31 00    |4.9.9.8.5.9.3.1.|
14:49:00 TPKTCHAN  : 00192   31 00 37 00 32 00 30 00 33 00 30 00 34 00 39 00    |1.7.2.0.3.0.4.9.|
14:49:00 TPKTCHAN  : 00208   39 00 38 00 35 00 39 00 33 00 31 00 31 00 36 00    |9.8.5.9.3.1.1.6.|
14:49:00 TPKTCHAN  : 00224   35 00 38 07 00 08 81 6b 00 02 06 00 60 52 dc a2    |5.8...•k....`RÜ¢|
14:49:00 TPKTCHAN  : 00240   a7 80 3d 92 1d 43 ca 8b a0 01 00 01 00 01 00 01    |§€=".CÊ‹ .......|
14:49:00 TPKTCHAN  : 00256   40 10 80 01 00                                     |@.€..|
```

6.6 Private key of Gatekeeper

```
imported private key info:
. privatekeyinfo->version: 00
. privatekeyinfo->privateKeyAlgorithm: 1 2 840 113549 1 1 1
. . algid->parameters: 0500 ( NULL )

. privatekeyinfo->privateKey:
. . 3082025c02010002818100c6c23d31fb87b7f340325ca2a4d1f1fca43c1364ac
. . f870cfd3af11e371a9b5500d79ae3c096663ca11bc12750bd8ab2d694b73d1d7
. . f1eaf338de4dbc4eb0a112bd4e9bbcfc841385a3a238a4f8090c8c1ba3dfec56
. . 92753cdcf0c3aca997c7ba842e21bbf35b5d0688be46e6a9aad47d2ade7fcfdb
. . 2aa55db2917987046bd01b0203010001028180 10c7c35cddec86663e0c426fe4
. . d468c6b8a2edcc39223c7bff562f7f71502fa3938fab5b1c3c0dbeb8a2953856
. . 88b3630119c2ac7bbbcbe73eecddc941277e61ad8841e990371cdc1d03964126
. . afb3623ec66d9d00b9c21a706ad2818a2e6031c2a37dd830e5e1154614540f5e
. . 95d04a78303940c624039b241f1ebb749e0101024100e8e0e6148c1b61f824f6
. . 385ffe9597d8771b2273eccfb75ce134d22483cff2c974d9277ec543fb32c292
. . d30e50223a8b1cdc1ca3dda72a027d0218a55cdd169b024100da7e1d36b4f256
. . 417b8a1edd565142bc260d8ea09aad4805875bc194e2be0d4a221ae39519d2a1
. . 05a4b0b28d51d83bea89832d39403ddc47be392456240b04810241008164a4b2
. . 79fea4fab99ecd48192e89464f3796770ef7830c6a5d6cfdb8f78c10ff89c0f6
. . 21295aa3a394ed0c20de43e513ce0163d33e948af96676c73ac7e54d02403be6
. . 5d3df54786cc37013bcaf4721cb8963a1b42fe84c8fcf309fdbd429855ee6001
. . 3d295046056d15a4779ef4b43260ef482e2ac6e8eeae20816bebcdbfd3810240
. . 384347dec74fc01d43ef31030ce851b2ae4e256f02f5bf68f0e6b6d5024bc2b7
. . b9d1aa281d0b3a411a8eac0659425b1c3a377c1101ac2f5619facf0a861edd4b


. privatekeyinfo->attributes:
. . attributes->attributes[0]: attribute not null
```

6.7 Certificate of Gatekeeper

```
. cert->tbs:
. . cert_tbs->version: 02
. . cert_tbs->issuer: /cn=IPL Certification Authority RSA/c=de/o=Siemens AG/ou=ZT IK
3/l=Munich/sp=Bavaria
. . cert_tbs->issuerUI: pointer was NULL
. . cert_tbs->serialNumber: 52
. . cert_tbs->signature:
. . . algid->algorithm: 1 2 840 113549 1 1 5
. . . algid->parameters: 0500 ( NULL )
. . cert_tbs->subject: /cn=gatekeeper H3232GK/ou=IC 3/o=Siemens AG/l=Munich/c=DE
. . cert_tbs->subjectPKI:
. . . spki->subjectAI:
. . . . algid->algorithm: 1 2 840 113549 1 1 1
. . . . algid->parameters: 0500 ( NULL )

. . . spki->subjectPK:
. . . . 30818902818100c6c23d31fb87b7f340325ca2a4d1f1fca43c1364acf870cfd3
. . . . af11e371a9b5500d79ae3c096663ca11bc12750bd8ab2d694b73d1d7f1eaf338
. . . . de4dbc4eb0a112bd4e9bbcfc841385a3a238a4f8090c8c1ba3dfec5692753cdc
. . . . f0c3aca997c7ba842e21bbf35b5d0688be46e6a9aad47d2ade7fcfdb2aa55db2
. . . . 917987046bd01b0203010001

. . cert_tbs->subjectUI: pointer was NULL

. . cert_tbs->validity:
. . . notBefore: 21.03.2002 10:23:00
. . . notAfter: 10.03.2004 10:22:59
. . cert_tbs->extensions:
. . . extensions->extensions[ 0 ]:
. . . . extension describer: no extension describer available
. . . . extension->extnID: 2 16 840 1 113730 1 1
. . . . extension->critical: 0
. . . . extension->extnValue: 03020040
. . . extensions->extensions[ 1 ]:
. . . . extension describer:
. . . . . subjectKeyIdentifier
. . . . extension->extnID: 2 5 29 14
. . . . extension->critical: 0
. . . . extension->extnValue: 04143b1a3dccfb26fcc25efc123979b6abdba64810f7
. . . extensions->extensions[ 2 ]:
. . . . extension describer:
. . . . . authorityKeyIdentifier
. . . . extension->extnID: 2 5 29 35
. . . . extension->critical: 0
. . . . extension->extnValue: 301680140678875c340e658267674f24f49331a9134f58b4
. cert->signature:
. . signature->signAI:
. . . algid->algorithm: 1 2 840 113549 1 1 5
. . . algid->parameters: 0500 ( NULL )

. . signature->signBS
. . . 96afdc1f288b0d75f8d9e59336a73242818eb2741651547d2bb7b8a0c2791b86
. . . 913c923fa2ef02d2eefaf5666da68e3d9040e676ff25d89b1c6718163d39494f
. . . d845997f7cee631813048bf8284e516613df06bbb1487f216b16faff4d33b2f3
. . . 4df82778df570bc1ae929af72c4c3c097582a105dd0a461ff3b26f31e2f41b27
```

6.8 Private key of endpoint

```
. privatekeyinfo->version: 0
. privatekeyinfo->privateKeyAlgorithm:
. . algid->algorithm: 1 2 840 113549 1 1 1
. . algid->parameters: 0500 ( NULL )

. privatekeyinfo->privateKey:
. . 3082025d02010002818100d7946eb4930a563fdd1167ed321e9b4aa8b145150d
. . c99cb7f953d22e1821954e18c5d8f8c61537206d34fb65cc3450fe2d3938fd4a
. . d084dbb2314e9bec8c906df589f5d404d40eea311f39a1d6447d9a887d423ed1
. . c9242899e3d71f19f4be19583421410636f18d1b3c9b37446a1e4150693d40ae
. . 09cd87ceeab5c18ea7f79302010302818100 8fb849cdb75c397fe8b64548cc14
. . 67871b20d8b8b3dbbdcffb8d36c9656bb8debb2e90a5d9637a159e235243dd78
. . 35fec8d0d0a8dc8b033d21763467f308604814e6b002d0364f12ca88f3b86cf0
. . 378bb7e22a5cef9eb315457da16d470653c5a57904db2861574468fbb52cc285
. . bb9b610b4de42569f1724c8a19a7a2042afb024100f411e4623a0c5fe513308f
. . bbf8ac9010371dd4ef8ee7ef6c2088d05235869ff34d0a73d6d52cd424d1c227
. . 2f9fa74d0c7b7a3b3953c0c4719cfea93b424b4a15024100e21e096d92763868
. . ee213c513a2f9a38bd8c2dc3db73281c911e94a8f9e4a07d92f4262174781a81
. . ac00e44480fa37cbc35e0d31222a1eeabf1ce60ad9566d07024100a2b698417c
. . 083fee0ccb0a7d50730ab57a13e34a5f454a4815b08ae179046aa2335c4d39e3
. . 7338188bd6c4ca6a6f88b2fcfc277b8d2b2da1135470d22c32316302410096be
. . b0f3b6f97af09ec0d2e0d175117b29081e82924cc56860bf0dc5fbedc053b74d
. . 6ec0f85011abc800982dab517a87d79408cb6c1c149c7f68995c90e448af0241
. . 00b6f200831f79417d1a91c7252a5f587dc9cf157ae80b521f7db7f34af9ce17
. . 3369d6c0aadfcee8c446fface88937442dec35fa89182cc2927ea0a519cd87a2
. . 86

. privatekeyinfo->attributes:
. . attributes->attributes[0]: attribute not null
```

6.9 Certificate of endpoint

```
. cert->tbs:
. . cert_tbs->version: 02
. . cert_tbs->issuer: /cn=IPL Certification Authority RSA/c=de/o=Siemens AG/ou=ZT IK
3/l=Munich/sp=Bavaria
. . cert_tbs->issuerUI: pointer was NULL
. . cert_tbs->serialNumber: 50

. . cert_tbs->signature:
. . . algid->algorithm: 1 2 840 113549 1 1 5
. . . algid->parameters: 0500 ( NULL )
. . cert_tbs->subject: /cn=Client1 H323/ou=IC3/o=Siemens AG/l=Munich/c=DE

. . cert_tbs->subjectPKI:
. . . spki->subjectAI:
. . . . algid->algorithm: 1 2 840 113549 1 1 1
. . . . algid->parameters: 0500 ( NULL )

. . . spki->subjectPK:
. . . . 30818702818100d7946eb4930a563fdd1167ed321e9b4aa8b145150dc99cb7f9
. . . . 53d22e1821954e18c5d8f8c61537206d34fb65cc3450fe2d3938fd4ad084dbb2
. . . . 314e9bec8c906df589f5d404d40eea311f39a1d6447d9a887d423ed1c9242899
. . . . e3d71f19f4be19583421410636f18d1b3c9b37446a1e4150693d40ae09cd87ce
. . . . eab5c18ea7f793020103

. . cert_tbs->subjectUI: pointer was NULL

. . cert_tbs->validity:
. . . notBefore:  21.03.2002 10:00:17
. . . notAfter: . 10.03.2004 10:00:16
. . cert_tbs->extensions:
. . . extensions->extensions[ 0 ]:
. . . . extension describer: no extension describer available
. . . . extension->extnID: 2 16 840 1 113730 1 1
. . . . extension->critical: 0
. . . . extension->extnValue: 03020080
. . . extensions->extensions[ 1 ]:
. . . . extension describer:
. . . . . subjectKeyIdentifier
. . . . extension->extnID: 2 5 29 14
. . . . extension->critical: 0
. . . . extension->extnValue: 0414570a9d020b22b1acf32446dc30669b80fe211d76
. . . extensions->extensions[ 2 ]:
. . . . extension describer:
. . . . . authorityKeyIdentifier
. . . . extension->extnID: 2 5 29 35
. . . . extension->critical: 0
. . . . extension->extnValue: 301680140678875c340e658267674f24f49331a9134f58b4
. cert->signature:
. . signature->signAI:
. . . algid->algorithm: 1 2 840 113549 1 1 5
. . . algid->parameters: 0500 ( NULL )
. . signature->signBS
. . . 1f5387a3bd36a2f5980c6c84550c40666c61fd4da0d954502478b2a71a601692
. . . 9e8b51f669fe7567bdd3fd0f219380fad7f2e6076c89b23759671625a52ba11d
. . . 288462a3df58272f0a94ffc5771a238dec6e77b81f0928597bf55d13aca1f397
. . . f4b4f1513b5d2cb5d0b48306994eb5a36c77c951fb2b4f22aa24f806c3c19c6e
```

6.10 Test Configurations

6.10.1 Gatekeeper and Terminal

Clauses 6.2, 6.3, 6.4 and 6.5 correlate to a test configuration of a Terminal and a Gatekeeper.

6.10.2 Gatekeeper and Gateway

Annex F of H.235 [2] does not cover this configuration. It is recommended to deploy annex D of H.235 [2] for that scenario, see clause 5.6.2.

6.10.3 Gatekeeper and Gatekeeper

The Gatekeeper-to-Gatekeeper communications according to Annex F H.235 [2] is very similar to the terminal Gatekeeper communication, with the exception that different private/public keys, certificates are used and that the call signalling messages are being digitally signed.

7 Global Service Providers

For further study.

History

Document history		
V4.1.1	May 2002	Publication as TS 101 888-2
V4.2.1	December 2003	Publication