ETSI ES 202 488-3 V1.1.1 (2003-09)

ETSI Standard

Access and Terminals (AT);
Second Generation Transmission Systems for Interactive Cable Television Services - IP Cable Modems;
Part 3: Baseline privacy plus interface specification

Reference

DES/AT-020043-03

Keywords

access, broadband, cable, data, IP, IPcable,
modem

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

Contents

Intellectual Property Rights 8

Foreword 8

1 Scope 9
1.1 Requierements 9

2 References 10

3 Abbreviations 11

4 Purpose 12
4.1 Void 12
4.2 Background 12
4.2.1 Service goals 12
4.2.2 Statement of compatibility 13

5 Baseline privacy plus overview 13
5.1 Architectural overview 13
5.1.1 Packet Data Encryption 13
5.1.2 Key management protocol 14
5.1.3 BPI+ security associations 14
5.1.4 QoS SIDs and BPI+ SAIDs 15
5.2 Operational overview 15
5.2.1 Cable Modem initialization 15
5.2.2 Cable Modem key update mechanism 16

6 Data Over Cable System MAC frame formats 17
6.1 Variable-length packet data PDU MAC frame format 17
6.2 Fragmentation MAC Frame Format 19
6.3 Requirements on usage of BP extended header element in MAC header 21

7 Baseline Privacy Key Management (BPKM) protocol 21
7.1 State models 21
7.1.1 Introduction 21
7.1.1.1 Preliminary comment on dynamic security associations and dynamic SA mapping 24
7.1.1.2 Security capabilities selection 24
7.1.2 Authorization state machine 25
7.1.2.1 States 27
7.1.2.1.1 Start 27
7.1.2.1.2 Authorize Wait (Auth Wait) 27
7.1.2.1.3 Authorized 27
7.1.2.1.4 Reauthorize Wait (Reauth Wait) 27
7.1.2.1.5 Authorize Reject Wait (Auth Reject Wait) 27
7.1.2.1.6 Silent 27
7.1.2.2 Messages 27
7.1.2.2.1 Authorization Request (Auth Request) 27
7.1.2.2.2 Authorization Reply (Auth Reply) 27
7.1.2.2.3 Authorization Reject (Auth Reject) 27
7.1.2.2.4 Authorization Invalid (Auth Invalid) 28
7.1.2.2.5 Authentication Information (Authent Info) 28
7.1.2.3 Events 28
7.1.2.3.1 Provisioned 28
7.1.2.3.2 Timeout 28
7.1.2.3.3 Authorization Grace Timeout (Auth Grace Timeout) 28
7.1.2.3.4 Reauthorize (Reauth) 28
7.1.2.3.5 Authorization Invalid (Auth Invalid) 28
7.1.2.3.6 Permanent Authorization Reject (Perm Auth Reject) 29
7.1.2.3.7 Authorization Reject (Auth Reject) 29
7.1.2.3.8 [TEK] Stop 29