



**E**UROPEAN  
**T**ELECOMMUNICATION  
**S**TANDARD

**ETS 300 759**

October 1997

---

Source: DECT

Reference: DE/DECT-060019

ICS: 33.020

**Key words:** DAM, DECT, radio, testing

**Digital Enhanced Cordless Telecommunications (DECT);  
DECT Authentication Module (DAM);  
Test specification for DAM**

**ETSI**

European Telecommunications Standards Institute

**ETSI Secretariat**

**Postal address:** F-06921 Sophia Antipolis CEDEX - FRANCE

**Office address:** 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE

**X.400:** c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

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

---

**Copyright Notification:** No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 1997. All rights reserved.



## Contents

Foreword .....	11
1 Scope .....	13
2 Normative references .....	13
3 Definitions and abbreviations .....	13
3.1 Definitions .....	13
3.2 Abbreviations .....	14
4 Test environment .....	14
4.1 Test equipment .....	14
4.1.1 PE simulator .....	14
4.1.2 Signal generation device .....	14
4.1.3 Precision force-inducing contacting device .....	14
4.1.4 Temperature controllable environment .....	14
4.1.5 Temperature measuring device .....	15
4.1.6 Voltage Measuring Device .....	15
4.1.7 Precision measuring device .....	15
4.1.8 Current measuring device .....	15
4.2 IUT default conditions .....	15
4.3 Default data formatting .....	15
4.4 Test procedure.....	15
4.5 Test requirement.....	16
5 Test group hierarchy .....	17
5.1 Test groups under DAM.....	17
5.2 Test groups under PHY .....	18
5.3 Test groups under ELEC .....	18
5.4 Test groups under LOG .....	19
5.5 Test groups under SEC .....	19
5.6 Test groups under CMD .....	20
5.7 Test groups under CEF .....	20
6 Test procedure .....	21
6.1 Physical characteristics.....	21
6.1.1 Format and layout .....	21
6.1.1.1 ID-1 card.....	21
6.1.1.1.1 Definition and applicability.....	21
6.1.1.1.2 Conformance requirement.....	21
6.1.1.1.3 Test purpose.....	22
6.1.1.1.4 Method of test .....	22
6.1.1.1.5 Test requirement.....	22
6.1.1.2 Plug-in card.....	22
6.1.1.2.1 Definition and applicability.....	22
6.1.1.2.2 Conformance requirement.....	23
6.1.1.2.3 Test purpose.....	23
6.1.1.2.4 Method of test .....	23
6.1.1.2.5 Test requirement.....	23
6.1.2 Temperature range for card operation .....	24
6.1.2.1 Definition and applicability .....	24
6.1.2.2 Conformance requirement.....	24
6.1.2.3 Test purpose.....	24
6.1.2.4 Method of test .....	24
6.1.2.5 Test requirement .....	25
6.1.3 Contacts .....	25
6.1.3.1 Definition and applicability .....	25

	6.1.3.2	Conformance requirement .....	25
	6.1.3.3	Test purpose .....	25
	6.1.3.4	Method of test .....	25
	6.1.3.5	Test requirement .....	25
6.2	Electronic signals and transmission protocols .....		26
	6.2.1	Supply voltage Vcc (contact C1) .....	26
	6.2.1.1	Voltage limits .....	26
	6.2.1.1.1	Definition and applicability .....	26
	6.2.1.1.2	Conformance requirement .....	26
	6.2.1.1.3	Test purpose .....	26
	6.2.1.1.4	Method of test .....	26
	6.2.1.1.5	Test requirement .....	27
	6.2.1.2	Current limits .....	27
	6.2.1.2.1	Definition and applicability .....	27
	6.2.1.2.2	Conformance requirement .....	27
	6.2.1.2.3	Test purpose .....	27
	6.2.1.2.4	Method of test .....	27
	6.2.1.2.5	Test requirement .....	28
	6.2.1.3	Idle current limits .....	28
	6.2.1.3.1	Definition and applicability .....	28
	6.2.1.3.2	Conformance requirement .....	28
	6.2.1.3.3	Test purpose .....	28
	6.2.1.3.4	Method of test .....	28
	6.2.1.3.5	Test requirement .....	29
	6.2.1.4	Current limits at all frequencies .....	29
	6.2.1.4.1	Definition and applicability .....	29
	6.2.1.4.2	Conformance requirement .....	29
	6.2.1.4.3	Test purpose .....	29
	6.2.1.4.4	Method of test .....	29
	6.2.1.4.5	Test requirement .....	29
	6.2.2	Reset RST (contact C2) .....	30
	6.2.2.1	Static operation .....	30
	6.2.2.1.1	Definition and applicability .....	30
	6.2.2.1.2	Conformance requirement .....	30
	6.2.2.1.3	Test purpose .....	30
	6.2.2.1.4	Method of test .....	30
	6.2.2.1.5	Test requirement .....	31
	6.2.2.2	Dynamic operation .....	31
	6.2.2.2.1	Definition and applicability .....	31
	6.2.2.2.2	Conformance requirement .....	31
	6.2.2.2.3	Test purpose .....	31
	6.2.2.2.4	Method of test .....	31
	6.2.2.2.5	Test requirement .....	31
	6.2.3	Clock CLK (contact C3) .....	32
	6.2.3.1	Frequency and duty cycle .....	32
	6.2.3.1.1	Definition and applicability .....	32
	6.2.3.1.2	Conformance requirement .....	32
	6.2.3.1.3	Test purpose .....	32
	6.2.3.1.4	Method of test .....	32
	6.2.3.1.5	Test requirement .....	33
	6.2.3.2	Voltage and current .....	33
	6.2.3.2.1	Definition and applicability .....	33
	6.2.3.2.2	Conformance requirement .....	33
	6.2.3.2.3	Test purpose .....	33
	6.2.3.2.4	Method of test .....	33
	6.2.3.2.5	Test requirement .....	34
	6.2.3.3	Dynamic operation .....	34
	6.2.3.3.1	Definition and applicability .....	34
	6.2.3.3.2	Conformance requirement .....	35
	6.2.3.3.3	Test purpose .....	35
	6.2.3.3.4	Method of test .....	35
	6.2.3.3.5	Test requirement .....	35
	6.2.4	I/O (contact C7) .....	35

6.2.4.1	Voltage and current .....	35
6.2.4.1.1	Definition and applicability.....	35
6.2.4.1.2	Conformance requirement.....	36
6.2.4.1.3	Test purpose.....	36
6.2.4.1.4	Method of test.....	36
6.2.4.1.5	Test requirement.....	36
6.2.4.2	Dynamic operation.....	36
6.2.4.2.1	Definition and applicability.....	36
6.2.4.2.2	Conformance requirement.....	37
6.2.4.2.3	Test purpose.....	37
6.2.4.2.4	Method of test.....	37
6.2.4.2.5	Test requirement.....	37
6.2.5	States .....	37
6.2.5.1	Definition and applicability .....	37
6.2.5.2	Conformance requirement.....	37
6.2.5.3	Test purpose.....	38
6.2.5.4	Method of test.....	38
6.2.5.5	Test requirement .....	38
6.2.6	Answer To Reset (ATR) .....	38
6.2.6.1	ATR content.....	38
6.2.6.1.1	Definition and applicability.....	38
6.2.6.1.2	Conformance requirement.....	39
6.2.6.1.3	Test purpose.....	39
6.2.6.1.4	Method of test.....	39
6.2.6.1.5	Test requirement.....	40
6.2.6.2	PTS procedure .....	40
6.2.6.2.1	Definition and applicability.....	40
6.2.6.2.2	Conformance requirement.....	40
6.2.6.2.3	Test purpose.....	40
6.2.6.2.4	Method of test.....	41
6.2.6.2.5	Test requirement.....	41
6.2.7	Major Capabilities .....	41
6.2.7.1	Definition and applicability .....	41
6.2.7.2	Conformance requirement.....	41
6.2.7.3	Test purpose.....	41
6.2.7.4	Method of test.....	42
6.2.7.5	Test requirement .....	42
6.3	Logical model.....	42
6.3.1	File identifier .....	42
6.3.1.1	File-type identification .....	42
6.3.1.1.1	Definition and applicability.....	42
6.3.1.1.2	Conformance requirement.....	42
6.3.1.1.3	Test purpose.....	42
6.3.1.1.4	Method of test.....	42
6.3.1.1.5	Test requirement.....	43
6.3.1.2	File ID assignments .....	43
6.3.1.2.1	Definition and applicability.....	43
6.3.1.2.2	Conformance requirement.....	43
6.3.1.2.3	Test purpose.....	43
6.3.1.2.4	Method of test.....	43
6.3.1.2.5	Test requirement.....	43
6.3.2	Dedicated files.....	44
6.3.2.1	Definition and applicability .....	44
6.3.2.2	Conformance requirement.....	44
6.3.2.3	Test purpose.....	44
6.3.2.4	Method of test.....	44
6.3.2.5	Test requirement .....	45
6.3.3	Elementary Files.....	45
6.3.3.1	Definition and applicability .....	45
6.3.3.2	Conformance requirement.....	45
6.3.3.3	Test purpose.....	46
6.3.3.4	Method of test.....	46
6.3.3.5	Test requirement .....	46

6.3.4	Methods for selecting the DECT application.....	46
6.3.4.1	Definition and applicability.....	46
6.3.4.2	Conformance requirement.....	47
6.3.4.3	Test purpose.....	47
6.3.4.4	Method of test.....	47
6.3.4.5	Test requirement.....	47
6.3.5	Methods for selecting a file.....	48
6.3.5.1	Definition and applicability.....	48
6.3.5.2	Conformance requirement.....	48
6.3.5.3	Test purpose.....	48
6.3.5.4	Method of test.....	49
6.3.5.5	Test requirement.....	50
6.3.6	Reservation of file IDs.....	50
6.3.6.1	Definition and applicability.....	50
6.3.6.2	Conformance requirement.....	50
6.3.6.3	Test purpose.....	50
6.3.6.4	Method of test.....	51
6.3.6.5	Test requirement.....	51
6.4	Security services and facilities.....	51
6.4.1	Algorithms and processes.....	51
6.4.2	Authentication.....	52
6.4.3	UAK allocation.....	52
6.4.4	File access control.....	52
6.4.4.1	ALWAYS, CHV1, FT-AUT and NEVER.....	52
6.4.4.1.1	Definition and applicability.....	52
6.4.4.1.2	Conformance requirement.....	53
6.4.4.1.3	Test purpose.....	53
6.4.4.1.4	Method of test.....	53
6.4.4.1.5	Test requirement.....	54
6.4.4.2	CHV2.....	54
6.4.4.2.1	Definition and applicability.....	54
6.4.4.2.2	Conformance requirement.....	54
6.4.4.2.3	Test purpose.....	54
6.4.4.2.4	Method of test.....	55
6.4.4.2.5	Test requirement.....	55
6.4.5	Subscription registration maintenance.....	55
6.5	Description of the functions.....	55
6.5.1	SELECT function.....	55
6.5.1.1	Definition and applicability.....	55
6.5.1.2	Conformance requirement.....	56
6.5.1.3	Test purpose.....	56
6.5.1.4	Method of test.....	56
6.5.1.5	Test requirement.....	57
6.5.2	STATUS function.....	58
6.5.2.1	Definition and applicability.....	58
6.5.2.2	Conformance requirement.....	58
6.5.2.3	Test purpose.....	58
6.5.2.4	Method of test.....	59
6.5.2.5	Test requirement.....	59
6.5.3	READ BINARY function.....	59
6.5.3.1	Definition and applicability.....	59
6.5.3.2	Conformance requirement.....	60
6.5.3.3	Test purpose.....	60
6.5.3.4	Method of test.....	60
6.5.3.5	Test requirement.....	61
6.5.4	UPDATE BINARY function.....	61
6.5.4.1	Definition and applicability.....	61
6.5.4.2	Conformance requirement.....	61
6.5.4.3	Test purpose.....	61
6.5.4.4	Method of test.....	62
6.5.4.5	Test requirement.....	62
6.5.5	READ RECORD function.....	62
6.5.5.1	Definition and applicability.....	62

	6.5.5.2	Conformance requirement.....	63
	6.5.5.3	Test purpose.....	63
	6.5.5.4	Method of test.....	64
	6.5.5.5	Test requirement .....	65
6.5.6		UPDATE RECORD function.....	65
	6.5.6.1	Definition and applicability .....	65
	6.5.6.2	Conformance requirement.....	65
	6.5.6.3	Test purpose.....	66
	6.5.6.4	Method of test.....	66
	6.5.6.5	Test requirement .....	67
6.5.7		SEEK function .....	68
	6.5.7.1	Definition and applicability .....	68
	6.5.7.2	Conformance requirement.....	68
	6.5.7.3	Test purpose.....	68
	6.5.7.4	Method of test.....	69
	6.5.7.5	Test requirement .....	70
6.5.8		INCREASE function .....	70
	6.5.8.1	Definition and applicability .....	70
	6.5.8.2	Conformance requirement.....	71
	6.5.8.3	Test purpose.....	71
	6.5.8.4	Method of test.....	71
	6.5.8.5	Test requirement .....	71
6.5.9		VERIFY CHV function .....	71
	6.5.9.1	Definition and applicability .....	71
	6.5.9.2	Conformance requirement.....	72
	6.5.9.3	Test purpose.....	72
	6.5.9.4	Method of test.....	72
	6.5.9.5	Test requirement .....	73
6.5.10		CHANGE CHV function.....	73
	6.5.10.1	Definition and applicability .....	73
	6.5.10.2	Conformance requirement.....	74
	6.5.10.3	Test purpose.....	74
	6.5.10.4	Method of test.....	74
	6.5.10.5	Test requirement .....	75
6.5.11		DISABLE CHV function .....	75
	6.5.11.1	Definition and applicability .....	75
	6.5.11.2	Conformance requirement.....	76
	6.5.11.3	Test purpose.....	76
	6.5.11.4	Method of test.....	76
	6.5.11.5	Test requirement .....	77
6.5.12		ENABLE CHV function .....	77
	6.5.12.1	Definition and applicability .....	77
	6.5.12.2	Conformance requirement.....	77
	6.5.12.3	Test purpose.....	78
	6.5.12.4	Method of test.....	78
	6.5.12.5	Test requirement .....	79
6.5.13		UNBLOCK CHV function.....	79
	6.5.13.1	Definition and applicability .....	79
	6.5.13.2	Conformance requirement.....	79
	6.5.13.3	Test purpose.....	79
	6.5.13.4	Method of test.....	80
	6.5.13.5	Test requirement .....	80
6.5.14		INVALIDATE function.....	81
	6.5.14.1	Definition and applicability .....	81
	6.5.14.2	Conformance requirement.....	81
	6.5.14.3	Test purpose.....	81
	6.5.14.4	Method of test.....	81
	6.5.14.5	Test requirement .....	82
6.5.15		REHABILITATE function .....	82
	6.5.15.1	Definition and applicability .....	82
	6.5.15.2	Conformance requirement.....	82
	6.5.15.3	Test purpose.....	82
	6.5.15.4	Method of test.....	83

	6.5.15.5	Test requirement.....	83
6.5.16	ASK RANDOM function .....		83
	6.5.16.1	Definition and applicability.....	83
	6.5.16.2	Conformance requirement .....	84
	6.5.16.3	Test purpose .....	84
	6.5.16.4	Method of test .....	84
	6.5.16.5	Test requirement.....	84
6.5.17	PT AUTHENTICATION function.....		84
	6.5.17.1	Definition and applicability.....	84
	6.5.17.2	Conformance requirement .....	85
	6.5.17.3	Test purpose .....	85
	6.5.17.4	Method of test .....	85
	6.5.17.5	Test requirement.....	86
6.5.18	FT AUTHENTICATION function .....		86
	6.5.18.1	Definition and applicability.....	86
	6.5.18.2	Conformance requirement .....	87
	6.5.18.3	Test purpose .....	87
	6.5.18.4	Method of test .....	87
	6.5.18.5	Test requirement.....	88
6.5.19	USER AUTHENTICATION function .....		88
	6.5.19.1	Definition and applicability.....	88
	6.5.19.2	Conformance requirement .....	88
	6.5.19.3	Test purpose .....	88
	6.5.19.4	Method of test .....	89
	6.5.19.5	Test requirement.....	89
6.5.20	UAK ALLOCATION function.....		89
	6.5.20.1	Definition and applicability.....	89
	6.5.20.2	Conformance requirement .....	90
	6.5.20.3	Test purpose .....	90
	6.5.20.4	Method of test .....	90
	6.5.20.5	Test requirement.....	91
6.6	Description of the commands .....		91
6.6.1	Mapping principles.....		92
	6.6.1.1	Definition and applicability.....	92
	6.6.1.2	Conformance requirement .....	92
	6.6.1.3	Test purpose .....	92
	6.6.1.4	Method of test .....	92
	6.6.1.5	Test requirement.....	94
6.6.2	Coding of the commands.....		94
	6.6.2.1	SELECT command .....	94
		6.6.2.1.1	Definition and applicability.....
		6.6.2.1.2	Conformance requirement .....
		6.6.2.1.3	Test purpose .....
		6.6.2.1.4	Method of test .....
		6.6.2.1.5	Test requirement.....
	6.6.2.2	STATUS command.....	98
	6.6.2.3	READ BINARY command.....	98
	6.6.2.4	UPDATE BINARY command .....	98
	6.6.2.5	READ RECORD command.....	98
	6.6.2.6	UPDATE RECORD command.....	98
	6.6.2.7	SEEK command.....	98
	6.6.2.8	INCREASE command.....	98
	6.6.2.9	VERIFY CHV command.....	98
	6.6.2.10	CHANGE CHV command .....	98
	6.6.2.11	DISABLE CHV command .....	99
	6.6.2.12	ENABLE CHV command .....	99
	6.6.2.13	UNBLOCK CHV command .....	99
	6.6.2.14	INVALIDATE command .....	99
	6.6.2.15	REHABILITATE command .....	99
	6.6.2.16	ASK RANDOM command.....	99
	6.6.2.17	PT AUTHENTICATION command.....	99
	6.6.2.18	FT AUTHENTICATION command.....	99
	6.6.2.19	USER AUTHENTICATION command .....	99



	6.6.2.20	UAK ALLOCATION command .....	99
	6.6.2.21	GET RESPONSE command .....	99
		6.6.2.21.1 Definition and applicability.....	99
		6.6.2.21.2 Conformance requirement.....	100
		6.6.2.21.3 Test purpose.....	100
		6.6.2.21.4 Method of test.....	100
		6.6.2.21.5 Test requirement.....	100
6.6.3		Definitions and coding .....	101
	6.6.3.1	Definition and applicability .....	101
	6.6.3.2	Conformance requirement.....	101
	6.6.3.3	Test purpose.....	101
	6.6.3.4	Method of test.....	101
	6.6.3.5	Test requirement .....	101
6.6.4		Status conditions returned by the DAM.....	102
	6.6.4.1	Coding of the status words .....	102
		6.6.4.1.1 Definition and applicability.....	102
		6.6.4.1.2 Conformance requirement.....	102
		6.6.4.1.3 Test purpose.....	103
		6.6.4.1.4 Method of test.....	103
		6.6.4.1.5 Test requirement.....	104
	6.6.4.2	Commands versus possible status responses.....	105
		6.6.4.2.1 Definition and applicability.....	105
		6.6.4.2.2 Conformance requirement.....	105
		6.6.4.2.3 Test purpose.....	105
		6.6.4.2.4 Method of test.....	105
		6.6.4.2.5 Test requirement.....	105
6.7		Contents of the Elementary Files.....	106
	6.7.1	Contents of the EFs at the MF level .....	106
		6.7.1.1 Definition and applicability .....	106
		6.7.1.2 Conformance requirement.....	106
		6.7.1.3 Test purpose.....	107
		6.7.1.4 Method of test.....	107
		6.7.1.5 Test requirement .....	108
	6.7.2	Contents of the EFs at the parent level of the DECT application.....	108
		6.7.2.1 Definition and applicability .....	108
		6.7.2.2 Conformance requirement.....	109
		6.7.2.3 Test purpose.....	109
		6.7.2.4 Method of test.....	109
		6.7.2.5 Test requirement .....	109
	6.7.3	Contents of the EFs at the DECT application level .....	110
		6.7.3.1 Definition and applicability .....	110
		6.7.3.2 Conformance requirement.....	110
		6.7.3.3 Test purpose.....	110
		6.7.3.4 Method of test.....	111
		6.7.3.5 Test requirement .....	111
	6.7.4	Contents of the EFs at the subscription registration level .....	111
		6.7.4.1 Definition and applicability .....	111
		6.7.4.2 Conformance requirement.....	112
		6.7.4.3 Test purpose.....	113
		6.7.4.4 Method of test.....	113
		6.7.4.5 Test requirement .....	114
		History.....	115

Blank page

## Foreword

This European Telecommunication Standard (ETS) has been produced by the Digital Enhanced Cordless Telecommunications (DECT) Project of the European Telecommunications Standards Institute (ETSI).

NOTE: This ETS was submitted for Public Enquiry as part 1 of a 2 part ETS. Part 2 has since been deleted.

<b>Transposition dates</b>	
Date of adoption:	3 October 1997
Date of latest announcement of this ETS (doa):	31 January 1998
Date of latest publication of new National Standard or endorsement of this ETS (dop/e):	31 July 1998
Date of withdrawal of any conflicting National Standard (dow):	31 July 1998

Blank page

## 1 Scope

This European Telecommunication Standard (ETS) provides the test specification for the Digital Enhanced Cordless Telecommunications (DECT) authentication module defined in ETS 300 331 [1]. An Implementation Conformance Statement (ICS) proforma specification for the DECT Authentication Module (DAM) is given in ETS 300 760 [2].

## 2 Normative references

This ETS incorporates by dated and undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this ETS only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

- [1] ETS 300 331 (1995): "Digital European Cordless Telecommunications (DECT); DECT Authentication Module (DAM)".
- [2] ETS 300 760: "Digital Enhanced Cordless Telecommunications (DECT); DECT Authentication Module (DAM); Implementation Conformance Statement (ICS) proforma specification".
- [3] ISO/IEC 7816-1: "Identification cards - Integrated circuit(s) with contacts - Part 1: Physical characteristics".
- [4] ISO/IEC 7816-2: "Identification cards - Integrated circuit(s) cards with contacts - Part 2: Dimensions and location of the contacts".
- [5] ISO/IEC 7816-3: "Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols".
- [6] ISO/IEC 7811-1: "Identification cards - Recording technique - Part 1: Embossing".
- [7] ISO/IEC 7811-3: "Identification cards - Recording technique - Part 3: Location of embossed characters on ID-1 cards".
- [8] ISO/IEC 8859-1: "Information processing - 8-bit single-byte coded graphic character sets - Part 1: Latin alphabet No. 1".

## 3 Definitions and abbreviations

### 3.1 Definitions

For the purposes of this ETS, the following definitions apply:

- terms defined in ETS 300 331 [1]; and

**Implementation Conformance Statement (ICS):** A statement made by the supplier of an implementation or system claimed to conform to a given specification, stating which capabilities have been implemented. The ICS can take several forms: protocol ICS, profile ICS, profile specific ICS, information object ICS, etc.

**ICS proforma:** A document, in the form of a questionnaire, which when completed for an implementation or system becomes an ICS.

### 3.2 Abbreviations

For the purposes of this ETS, the following abbreviations apply:

CRn	Conformance Requirement "n"
DAM	DECT Authentication Module
FT	Fixed radio Termination
ICS	Implementation Conformance Statement
IUT	Implementation Under Test
PE	Portable Equipment
PT	Portable radio Termination

## 4 Test environment

This clause specifies several requirements which shall be met, and a number of rules which shall be adhered to before testing can proceed.

### 4.1 Test equipment

This subclause recommends a minimum specification for each of the items of test equipment referenced in the tests.

#### 4.1.1 PE simulator

This item of equipment shall allow T=0 protocol communications to take place on both ID-1 and plug-in DECT Authentication Module (DAM) cards. It shall be able to generate and send any command APDU and receive any of the possible responses. These commands may be generated manually, one at a time, or automatically from a predefined batch procedure containing one or more commands.

The voltage level for Vcc (contact C1) of the DAM shall be adjustable between 0 V and 6,0 V to an accuracy of 0,1 V. The voltage level for I/O (contact C7) when sending data to the DAM shall be adjustable between 0 V and 6,0 V to an accuracy of 0,1 V.

The Portable Equipment (PE) Simulator shall be able to source current in the range -2 mA to +12 mA.

The PE Simulator shall be able to support clock stop modes.

The PE simulator shall be able to accept an external clock signal to drive RST (contact C3) of the DAM.

It shall be possible to access all the DAM contacts either directly or through test points.

#### 4.1.2 Signal generation device

This item of equipment shall be able to generate square-wave signals for the DAM, any of which can be a signal-shot or continuous signal, in the range 1 MHz to 5 MHz. The voltage levels for both high and low states shall be adjustable between 0 V and 5,50 V to an accuracy of 0,1 V. The duty cycle of the clock signal shall be adjustable between 40 % and 60 % to an accuracy of 1 %. It will also provide control over the following parameters:

- rise and fall time to an accuracy of 10  $\mu$ s;
- overshoot/undershoot voltage to  $\pm 0,3$  V to an accuracy of 0,1 V.

#### 4.1.3 Precision force-inducing contacting device

This item of equipment shall be able to apply a prescribed and maintained level of force onto one or more contacts of a DAM. The range shall be between 0 N and 0,5 N and accurate to 0,01 N.

#### 4.1.4 Temperature controllable environment

This item of equipment shall be able to control the temperature of a chamber large enough to enclose a DAM and card reader. The range of temperature control required is between -25°C and +85°C to an accuracy of 0,5°C.

#### 4.1.5 Temperature measuring device

This item of equipment shall be able to measure the temperature of the DAM to within 0,5°C. The range of this device shall allow measurement of temperatures between -25°C and +85°C.

#### 4.1.6 Voltage Measuring Device

This item of equipment shall be able to measure static and transient voltages on any one of the contacts of the DAM. The measurable voltage range shall be between -10 V to +10 V (to an accuracy of 50 mV) with a timebase accuracy of 100 ns.

#### 4.1.7 Precision measuring device

This item of equipment shall be able to measure both linear and radius of curvature dimensions to an accuracy of 0,01 mm.

#### 4.1.8 Current measuring device

This item of equipment shall be able to measure current levels for any one of the contacts of the DAM. The measurable current range shall be between -2 mA to +12 mA to an accuracy of 1 µA.

### 4.2 IUT default conditions

Unless otherwise stated, the following is default:

- the voltage level for Vcc (contact C1) is set to 5,0 V;
- the voltage levels for CLK (contact C3) are set to 0,7 V and 5,0 V for low and high respectively;
- the clock frequency CLK (contact C3) is set to 5 MHz with duty cycle 50 %;
- the PE simulator generated voltage levels for I/O (contact C7) are set to 0,7 V and 5,0 V for low and high respectively.

### 4.3 Default data formatting

All numeric data enclosed in single quotes (e.g. '8C') in this ETS are hexadecimal data.

Where "X" is used in place of a hexadecimal digit, X ranges from '0' to 'F'. For example, the data '6X' ranges from '60' to '6F' inclusive.

Where data is expressed as a group of bytes, it shall be in the following format: 'XX XX XX... XX', indicating first byte, second byte, third byte etc. in that order.

### 4.4 Test procedure

The following statements are applicable to the test procedure subclause for all test purposes contained within this ETS:

- unless otherwise stated, all steps with the test procedure are to be carried out in order;
- where steps indicate that a PE simulator shall select a particular DF or EF using an unspecified number SELECT commands, the PE simulator is to send the correct sequence of SELECT commands in order to select the required file ID from the current file ID (this may be achieved most easily by selecting from the MF down each time).

The procedure to select DF<sub>DECT</sub> is defined below:

- a) the PE simulator sends a SELECT command to the DAM to select EF<sub>ICC</sub>;
- b) the PE simulator sends a READ BINARY command to the DAM with a length of 1 and an offset of 18. If byte 19 does not exist in the response data, then proceed to step d);
- c) if byte 19 does exist in the response data and bit 4 is set, then the PE simulator sends a SELECT command with the application ID to select the DF<sub>DECT</sub>. Proceed to step i);

- d) the PE simulator sends a SELECT command to the DAM to select  $EF_{DIR}$ ;
- e) if step d) is successful, the PE simulator gains the correct ADM access conditions to read  $EF_{DIR}$ . Otherwise, proceed to step h);
- f) the PE simulator sends a READ BINARY command to the DAM;
- g) the PE simulator sends as many SELECT commands as are required to select the  $DF_{DECT}$  by file ID as given in  $EF_{DIR}$ . Proceed with step i);
- h) the PE simulator sends a SELECT command with the application ID to the DAM to select  $DF_{DECT}$ ;
- i) the PE simulator sends a GET RESPONSE command to the DAM.

The procedure to select the relevant  $EF_{CHV1}$  for the DAM is defined below:

- a) the PE simulator select  $DF_{DECT}$ , as defined above;
  - b) the PE simulator sends a SELECT command to the DAM to select  $EF_{CHV1}$ ;
  - c) if the status condition returned by the DAM is SW1='94', SW2='04', "file not found", then the PE simulator sends a SELECT command to select the parent directory using file ID;
  - d) repeat steps b) and c) until  $EF_{CHV1}$  is found;
- unless otherwise stated, the length (P3) for all READ RECORD and UPDATE RECORD commands sent by the PE simulator is to be that of the length of the EF currently selected. In the case where an EF is not currently selected, the length sent is to be 1 unless otherwise stated;
  - unless otherwise stated, the offset for all READ BINARY, UPDATE BINARY and SEEK commands sent by the PE simulator is to be '00 00';
  - unless otherwise stated, the length (P3) for all STATUS and GET RESPONSE commands sent by the PE simulator is to be such that all available data is read;
  - unless otherwise stated, the CHV and UNBLOCK CHV presented for VERIFY CHV, CHANGE CHV, DISABLE CHV, ENABLE CHV and UNBLOCK CHV commands sent by the PE simulator is to be correct;
  - unless otherwise stated, the "CHV No." (P2) for VERIFY CHV, CHANGE CHV, DISABLE CHV, ENABLE CHV and UNBLOCK CHV commands sent by the PE simulator is to be 1;
  - unless otherwise stated, all CHV1 on the DAM are activated and enabled and sufficient VERIFY CHV1 and UNBLOCK CHV1 attempts remain.

#### 4.5 Test requirement

Where steps within a test procedure involve a PE simulator sending one or more commands to the DAM, these commands are required to be correctly executed, with the DAM responding with status conditions of '90 00' or '9F XX', unless otherwise stated in the test requirements subclause for the test.



## 5 Test group hierarchy

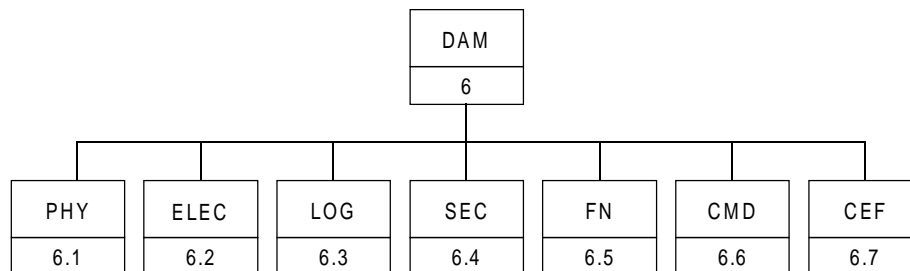
This clause contains the test group hierarchy diagrams which provide a structure for the test purposes and also a correlation between the base specification, Implementation Conformance Statement (ICS) and this ETS.

The information contained in each node for each of the diagrams is as follows:

mnemonic for test group
reference to subclause in test specification

As the test group hierarchy for the DAM is large, it has been broken into subclauses to aid presentation.

### 5.1 Test groups under DAM



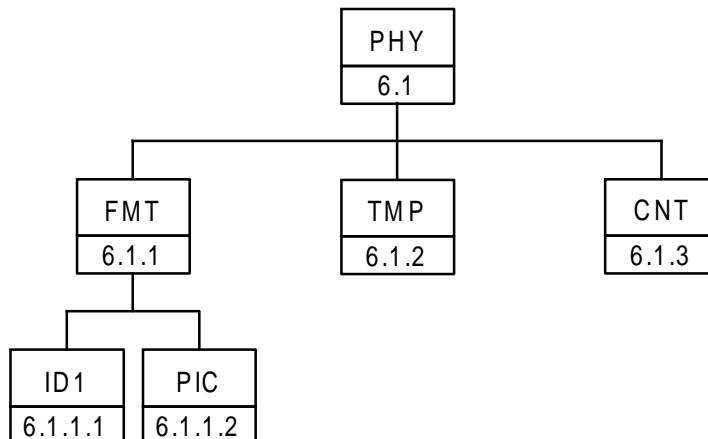
**Figure 1: Top level test group hierarchy**

The mnemonics chosen for this test group are as follows:

- PHY: Physical characteristics - ETS 300 331 [1], clause 4;
- ELEC: Electronic signals and transmission protocols - ETS 300 331 [1], clause 5;
- LOG: Logical Model - ETS 300 331 [1], clause 6;
- SEC: Security services and facilities - ETS 300 331 [1], clause 7;
- FN: Description of the functions - ETS 300 331 [1], clause 8;
- CMD: Description of the commands - ETS 300 331 [1], clause 9;
- CEF: Contents of the Elementary Files - ETS 300 331 [1], clause 10.

The test groups "PHY", "ELEC", "LOG", "SEC", "CMD" and "CEF", shown in figure 1, are broken down further, as shown in the following figures.

## 5.2 Test groups under PHY

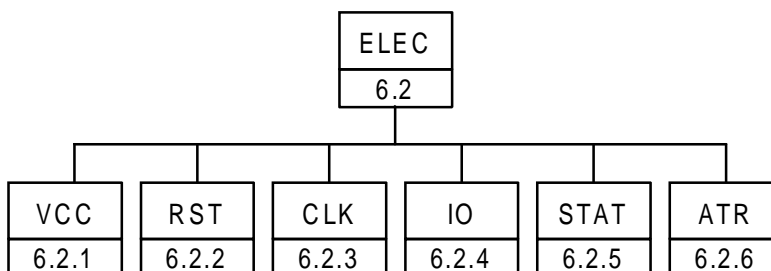


**Figure 2: Breakdown of "PHY" test group**

The mnemonics chosen for this test group are as follows:

- FMT: Format and layout - ETS 300 331 [1], subclause 4.1;
- ID1: ID-1 card - ETS 300 331 [1], subclause 4.1.1;
- PIC: Plug-in card - ETS 300 331 [1], subclause 4.1.2;
- TMP: Temperature range for card operation - ETS 300 331 [1], subclause 4.2;
- CNT: Contacts - ETS 300 331 [1], subclause 4.3.

## 5.3 Test groups under ELEC

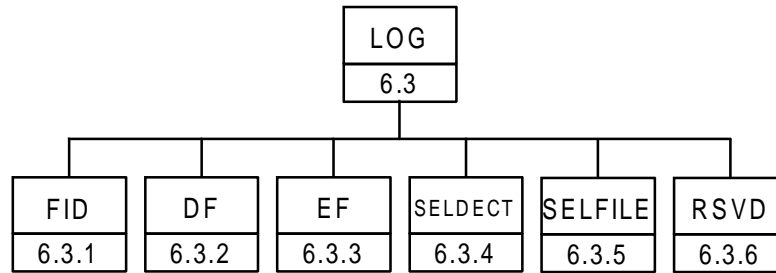


**Figure 3: Breakdown of "ELEC" test group**

The mnemonics chosen for this test group are as follows:

- VCC: Supply voltage Vcc (contact C1) - ETS 300 331 [1], subclause 5.1;
- RST: Reset RST (contact C2) - ETS 300 331 [1], subclause 5.2;
- CLK: Clock CLK (contact C3) - ETS 300 331 [1], subclause 5.3;
- IO: I/O (contact C7) - ETS 300 331 [1], subclause 5.5;
- STAT: States - ETS 300 331 [1], subclause 5.6;
- ATR: Answer To Reset (ATR) - ETS 300 331 [1], subclause 5.8.

#### 5.4 Test groups under LOG

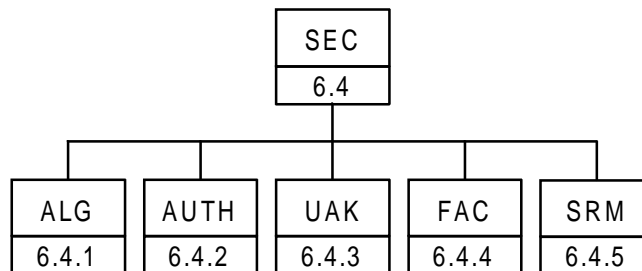


**Figure 4: Breakdown of "LOG" test group**

The mnemonics chosen for this test group are as follows:

- FID: File identifier - ETS 300 331 [1], subclause 6.2;
- DF: Dedicated Files - ETS 300 331 [1], subclause 6.3;
- EF: Elementary Files - ETS 300 331 [1], subclause 6.4;
- SELDECT: Methods for selecting the DECT application - ETS 300 331 [1], subclause 6.5;
- SELFILE: Methods for selecting a file - ETS 300 331 [1], subclause 6.6;
- RSVD: Reservation of file IDs - ETS 300 331 [1], subclause 6.7.

#### 5.5 Test groups under SEC

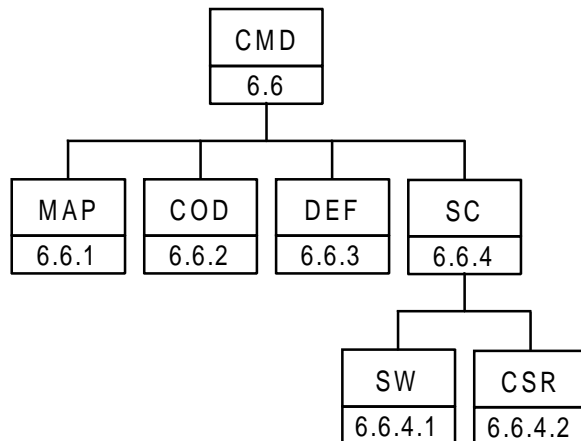


**Figure 5: Breakdown of "SEC" test group**

The mnemonics chosen for this test group are as follows:

- ALG: Algorithms and processes - ETS 300 331 [1], subclause 7.1.3;
- AUTH: Authentication - ETS 300 331 [1], subclause 7.2;
- UAK: UAK allocation - ETS 300 331 [1], subclause 7.3;
- FAC: File access control - ETS 300 331 [1], subclause 7.6;
- SRM: Subscription registration maintenance - ETS 300 331 [1], subclause 7.8.

## 5.6 Test groups under CMD

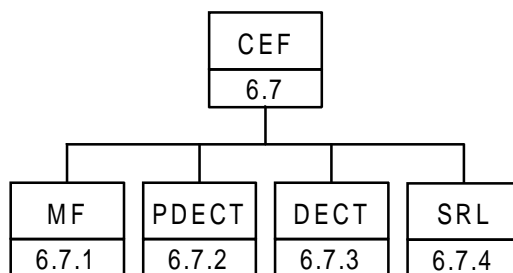


**Figure 6: Breakdown of "CMD" test group**

The mnemonics chosen for this test group are as follows:

- MAP: Mapping principles - ETS 300 331 [1], subclause 9.1;
- COD: Coding of the commands - ETS 300 331 [1], subclause 9.2;
- DEF: Definitions and coding - ETS 300 331 [1], subclause 9.3;
- SC: Status conditions returned by the DAM - ETS 300 331 [1], subclause 9.4;
- SW: Coding of the status words- ETS 300 331 [1], subclause 9.4.1-5;
- CSR: Commands versus possible status responses - ETS 300 331 [1], subclause 9.4.6.

## 5.7 Test groups under CEF



**Figure 7: Breakdown of "CEF" test group**

The mnemonics chosen for this test group are as follows:

- MF: Contents of the EFs at the MF level - ETS 300 331 [1], subclause 10.1;
- PDECT: Contents of EFs at the parent level of the DECT application - ETS 300 331 [1], subclause 10.2;
- DECT: Contents of EFs at the DECT application level - ETS 300 331 [1], subclause 10.3;
- SRL: Contents of the EFs at the Subscription Registration level - ETS 300 331 [1], subclause 10.4.

## 6 Test procedure

This clause details each of the tests in each of the test groups within the Test Group Hierarchy. This test suite allows testing of the Implementation Under Test (IUT) against the base specification with respect to:

- physical characteristics;
- electronic signals and transmission protocols;
- logical model;
- security services and facilities;
- functions;
- commands;
- contents of the Elementary Files.

The numbering of this clause correlates with the numbering of the accompanying ICS to allow for referencing between the documents.

### 6.1 Physical characteristics

The tests in this subclause ensure that the IUT conforms to the specification for both format and layout and contacts.

#### 6.1.1 Format and layout

##### 6.1.1.1 ID-1 card

###### 6.1.1.1.1 Definition and applicability

The format and layout characteristics shall be adhered to, in order to ensure proper operation in the DECT environment.

This test applies to ID-1 DAM cards.

###### 6.1.1.1.2 Conformance requirement

- 1) Format and layout of the ID-1 card shall be in accordance with ISO/IEC 7816-1 [3] and ISO/IEC 7816-2 [4], unless otherwise specified.
- 2) The identification number, as defined in  $EF_{ID}$ , shall be present on the exterior of the ID-1 card.
- 3) The card shall have a polarization mark which indicates how the user should insert the card into the PE.
- 4) The card shall be embossed (optional).
- 5) The embossing shall be in accordance with ISO/IEC 7811-1 [6] and ISO/IEC 7811-3 [7] (conditional).
- 6) The contacts shall be located on either the front (embossed face) or the back of the card.

Reference: ETS 300 331 [1], clause 4, subclauses 4.1, 4.1.1.

Test Group Reference (TGR): TGR\_DAM\_PHY\_FMT\_ID1.

Test Procedure Reference (TPR): TPR\_DAM\_PHY\_FMT\_ID1.

#### 6.1.1.1.3 Test purpose

To verify that the DAM conforms to the above requirements.

NOTE 1: The testing of Conformance Requirement One (CR1) is outside the scope of this ETS. Please refer to the test specification for ISO/IEC 7816-1 [3] and ISO/IEC 7816-2 [4].

NOTE 2: The testing of CR5 is outside the scope of this ETS. Please refer to the test specification for ISO/IEC 7811-1 [6] and ISO/IEC 7811-3 [7].

#### 6.1.1.1.4 Method of test

##### Initial conditions

None.

##### Test procedure

- a) The card is examined for the following:
  - identification number;
  - polarization mark;
  - contact location.
- b) Connect the DAM to the PE Simulator.
- c) The PE simulator resets the DAM.
- d) The PE simulator sends a SELECT command to the DAM to select EF<sub>ID</sub>.
- e) The PE simulator sends a READ BINARY command to the DAM with a length of 10 and an offset of 0 to read the identification number.

#### 6.1.1.1.5 Test requirement

- 1) After step a), the card shall have been observed to exhibit the following:
  - identification number located on the exterior of the card;
  - polarization mark indicating how the user should insert the card into the PE;
  - contact location on the front or the back of the card.
- 2) After step e), the identification number read from EF<sub>ID</sub> shall be identical with that on the exterior of the card.

#### 6.1.1.2 Plug-in card

##### 6.1.1.2.1 Definition and applicability

The format and layout characteristics shall be adhered to, in order to ensure proper operation in the DECT environment.

This test applies to plug-in DAM cards.

#### 6.1.1.2.2 Conformance requirement

- 1) Format and layout of the plug-in card shall be in accordance with ISO/IEC 7816-1 [3] and ISO/IEC 7816-2 [4], unless otherwise specified.
- 2) The information on the exterior of the plug-in card shall include at least the individual account identifier and the check digit.
- 3) The plug-in card shall have a width of 25 mm, a height of 15 mm, a thickness the same as an ID-1 card and a feature for orientation.

Reference: ETS 300 331 [1], clause 4, subclauses 4.1 and 4.1.2.

Test Group Reference (TGR): TGR\_DAM\_PHY\_FMT\_PIC.

Test Procedure Reference (TPR): TPR\_DAM\_PHY\_FMT\_PIC.

#### 6.1.1.2.3 Test purpose

To verify that the DAM conforms to the above requirements.

NOTE 1: The testing of CR1 is outside the scope of this ETS. Please refer to the test specification for ISO/IEC 7816-1 [3] and ISO/IEC 7816-2 [4].

#### 6.1.1.2.4 Method of test

##### Initial conditions

None.

##### Test procedure

- a) The card is examined for the following:
  - individual account identifier and check digit;
  - width;
  - height;
  - thickness;
  - feature for orientation.
- b) Connect the DAM to the PE Simulator.
- c) The PE simulator resets the DAM.
- d) The PE simulator sends a SELECT command to the DAM to select EF<sub>ID</sub>.
- e) The PE simulator sends a READ BINARY command to the DAM with a length of 10 and an offset of 0 to read the identification number.

#### 6.1.1.2.5 Test requirement

- 1) After step a), the card shall have been observed to exhibit the following:
  - at least the individual account identifier and check digit located on the exterior of the card;
  - correct width, height and thickness over the full surface area;
  - feature for orientation.
- 2) After step e), the account identifier and check digit read from EF<sub>ID</sub> shall be identical with that on the exterior of the card.

## 6.1.2 Temperature range for card operation

### 6.1.2.1 Definition and applicability

The temperature range for full operational use shall be adhered to, in order to ensure proper operation in the DECT environment.

This test applies to both plug-in and ID-1 DAM cards.

### 6.1.2.2 Conformance requirement

- 1) The temperature range for full operational use shall be between  $-25^{\circ}\text{C}$  and  $+70^{\circ}\text{C}$  with occasional peaks of up to  $+85^{\circ}\text{C}$ , where "occasional" means not more than 4 hours each time and not over 100 times during the life time of the card.

Reference: ETS 300 331 [1], subclause 4.2.

Test Group Reference (TGR): TGR\_DAM\_PHY\_TMP.

Test Procedure Reference (TPR): TPR\_DAM\_PHY\_TMP.

### 6.1.2.3 Test purpose

To verify that the DAM conforms to the above requirements.

### 6.1.2.4 Method of test

#### Initial conditions:

- 1) the DAM is placed in a temperature-controllable environment and connected to a PE simulator;
- 2) a temperature measuring device is connected to the surface of the DAM;
- 3) the DAM shall have passed the Format and Layout tests in subclause 6.1.1.

#### Test procedure:

- a) the temperature of the DAM is set to  $+25^{\circ}\text{C}$ ;
- b) the PE simulator resets the DAM;
- c) the PE simulator performs the DAM initialization procedure, as defined in ETS 300 331 [1], subclause 11.2.1;
- d) the temperature of the DAM is reduced to  $-25^{\circ}\text{C}$ ;
- e) steps b) and c) are repeated;
- f) the temperature of the DAM is increased to  $+70^{\circ}\text{C}$ ;
- g) steps b) and c) are repeated;
- h) the temperature of the DAM is increased to  $+85^{\circ}\text{C}$ ;
- i) steps b) and c) are repeated for a period of 4 hours;
- j) the temperature of the DAM is reduced to  $+25^{\circ}\text{C}$ ;
- k) steps h), i) and j) are repeated a further 99 times;
- l) carry out the tests in subclause 6.1.1 again.



#### **6.1.2.5 Test requirement**

- 1) The DAM shall operate successfully during steps c), e), g), i) and k).
- 2) After step l), the DAM shall have satisfied the test requirements within subclause 6.1.1.

#### **6.1.3 Contacts**

##### **6.1.3.1 Definition and applicability**

The shape, robustness and provision of contacts shall be adhered to, in order to maintain good electrical contact with the PE, ensuring proper operation in the DECT environment.

##### **6.1.3.2 Conformance requirement**

- 1) Contact C4 shall be provided (optional).
- 2) Contact C6 shall not be bonded in the DAM for any function other than supplying Vpp.
- 3) Contact C8 shall be provided (optional).
- 4) The contact force shall not be greater than 0,5 N per contact.

Reference: ETS 300 331 [1], subclause 4.3.1.

Test Group Reference (TGR): TGR\_DAM\_PHY\_CNT.

Test Procedure Reference (TPR): TPR\_DAM\_PHY\_CNT.

##### **6.1.3.3 Test purpose**

To verify that the DAM conforms to the above requirements.

NOTE: As the contacts specified in CR1 and CR3 are optional, the tests specified here shall only be performed on those contacts when the contacts are present.

##### **6.1.3.4 Method of test**

###### **Initial conditions:**

- 1) the DAM shall have passed the contacts tests in subclause 6.1.1.

###### **Test procedure**

- a) the bonding of contact C6 is examined;
- b) a precision force-inducing contacting device is used to apply a maximum pressure of 0,5 N per contact to the DAM;
- c) the DAM is connected to a PE simulator;
- d) the PE simulator resets the DAM.

##### **6.1.3.5 Test requirement**

- 1) After step a), it shall have been observed that contact C6 is bonded only to supply Vpp.
- 2) After step e), the DAM shall have been reset successfully.

## 6.2 Electronic signals and transmission protocols

The tests in this subclause ensure that the IUT conforms to the electrical specification for each of the contacts and also the protocol.

### 6.2.1 Supply voltage Vcc (contact C1)

#### 6.2.1.1 Voltage limits

##### 6.2.1.1.1 Definition and applicability

In addition to the electronic signals and transmission protocols defined in ISO/IEC 7816-3 [5], the DAM shall operate within the following supply voltage conditions to ensure proper operation in the DECT environment.

This test applies to all DAM implementations with 5 V interface.

##### 6.2.1.1.2 Conformance requirement

- 1) The DAM shall operate when the supply voltage on contact C1 (Vcc) is in the range 4,5 V and 5,5 V.

Reference: ETS 300 331 [1], subclause 5.1.

Test Group Reference (TGR): TGR\_DAM\_ELEC\_VCC.

Test Procedure Reference (TPR): TPR\_DAM\_ELEC\_VCC\_V.

##### 6.2.1.1.3 Test purpose

To verify that the DAM conforms to the above requirements.

##### 6.2.1.1.4 Method of test

###### Initial conditions:

- 1) the DAM is connected to a PE simulator;
- 2) the CHV value is 4 zeroes.

###### Test procedure:

- a) the voltage source for contact C1 (Vcc) is set to 4,5 V;
- b) the PE simulator resets the DAM;
- c) the PE Simulator sends an UPDATE CHV command to the DAM with new CHV value of 8 zeroes;
- d) the PE Simulator sends an UPDATE CHV command to the DAM to return the CHV to its original value;
- e) the voltage source for contact C1 (Vcc) is set to 5,5 V;
- f) the PE simulator resets the DAM;
- g) the PE Simulator sends an UPDATE CHV command to the DAM with new CHV value of 8 zeroes;
- h) the PE Simulator sends an UPDATE CHV command to the DAM to return the CHV to its original value.

#### **6.2.1.1.5 Test requirement**

- 1) After step b), the DAM shall send the correct ATR sequence.
- 2) After step f), the DAM shall send the correct ATR sequence.

#### **6.2.1.2 Current limits**

##### **6.2.1.2.1 Definition and applicability**

In addition to the electronic signals and transmission protocols defined in ISO/IEC 7816-3 [5], the current consumption shall not exceed the specified limit under normal operating conditions to ensure proper operation in the DECT environment.

This test applies to all DAM implementations with 5 V interface.

##### **6.2.1.2.2 Conformance requirement**

- 1) The current consumption of the DAM shall not exceed 10 mA at any frequency accepted by the DAM.

Reference: ETS 300 331 [1], subclause 5.1.

Test Group Reference (TGR): TGR\_DAM\_ELEC\_VCC.

Test Procedure Reference (TPR): TPR\_DAM\_ELEC\_VCC\_I.

##### **6.2.1.2.3 Test purpose**

To verify that the DAM conforms to the above requirements.

##### **6.2.1.2.4 Method of test**

###### **Initial conditions:**

- 1) the DAM is connected to a PE simulator;
- 2) a current measuring device is connected to the DAM;
- 3) the CHV value is 4 zeroes.

###### **Test procedure:**

- a) the frequency of the clock source is set to 1 MHz;
- b) the PE simulator resets the DAM;
- c) the PE simulator performs the DAM initialization procedure during which time the current consumption is measured;
- d) the PE simulator sends an UPDATE CHV command to the DAM with new CHV value of 8 zeroes;
- e) the PE simulator sends an UPDATE CHV command to the DAM to return the CHV to its original value;
- f) the frequency of the clock source is set to 3 MHz;
- g) the PE simulator resets the DAM;
- h) the PE simulator performs the DAM initialization procedure during which time the current consumption is measured;

- i) the PE simulator sends an UPDATE CHV command to the DAM with new CHV value of 8 zeroes;
- j) the PE simulator sends an UPDATE CHV command to the DAM to return the CHV to its original value;
- k) the frequency of the clock source is set to 5 MHz;
- l) the PE simulator resets the DAM;
- m) the PE simulator performs the DAM initialization procedure during which time the current consumption is measured;
- n) the PE simulator sends an UPDATE CHV command to the DAM with new CHV value of 8 zeroes;
- o) the PE simulator sends an UPDATE CHV command to the DAM to return the CHV to its original value.

#### **6.2.1.2.5 Test requirement**

- 1) During steps b), c), d, e), g), h), i), j), l), m), n) and o), the current consumption of the DAM shall not have exceeded 10 mA, excluding spikes up to a maximum charge of 40 nAs with no more than 400 nS duration and an amplitude of at most 200 mA.

#### **6.2.1.3 Idle current limits**

##### **6.2.1.3.1 Definition and applicability**

In addition to the electronic signals and transmission protocols defined in ISO/IEC 7816-3 [5], the current consumption shall not exceed the specified limit under idle conditions to ensure proper operation in the DECT environment.

This test applies to all DAM implementations with 5 V interface.

##### **6.2.1.3.2 Conformance requirement**

- 1) The idle current consumption of the DAM shall not exceed 200  $\mu$ A at 1 MHz and +25°C.

Reference: ETS 300 331 [1], subclause 5.1.

Test Group Reference (TGR): TGR\_DAM\_ELEC\_VCC.

Test Procedure Reference (TPR): TPR\_DAM\_ELEC\_VCC\_IDLE.

##### **6.2.1.3.3 Test purpose**

To verify that the DAM conforms to the above requirements.

##### **6.2.1.3.4 Method of test**

###### **Initial conditions:**

- 1) the DAM is connected to a PE simulator;
- 2) the frequency of the clock source is set to 1 MHz;
- 3) the temperature of the DAM is +25°C.

###### **Test procedure:**

- a) the PE simulator resets the DAM;
- b) the idle current consumption is measured over a period of 10 s.

#### **6.2.1.3.5 Test requirement**

- 1) During step b), the current consumption of the DAM shall not exceed 200  $\mu$ A.

#### **6.2.1.4 Current limits at all frequencies**

##### **6.2.1.4.1 Definition and applicability**

In addition to the electronic signals and transmission protocols defined in ISO/IEC 7816-3 [5], the current consumption shall not exceed the specified limit under idle conditions to ensure proper operation in the DECT environment.

This test applies to all DAM implementations with 5 V interface.

##### **6.2.1.4.2 Conformance requirement**

- 1) The idle current consumption of the DAM shall not exceed 1 mA at any frequency accepted by the DAM.

Reference: ETS 300 331 [1], subclause 5.1.

Test Group Reference (TGR): TGR\_DAM\_ELEC\_VCC.

Test Procedure Reference (TPR): TPR\_DAM\_ELEC\_VCC\_IF.

##### **6.2.1.4.3 Test purpose**

To verify that the DAM conforms to the above requirements.

##### **6.2.1.4.4 Method of test**

###### **Initial conditions:**

- 1) the DAM is connected to a PE simulator;
- 2) the CHV value is 4 zeroes.

###### **Test procedure:**

- a) the frequency of the clock source is set to 1 MHz;
- b) the PE simulator resets the DAM;
- c) the current consumption is measured over a period of 10 s;
- d) the frequency of the clock source is set to 3 MHz;
- e) the PE simulator resets the DAM;
- f) the current consumption is measured over a period of 10 s;
- g) the frequency of the clock source is set to 5 MHz;
- h) the PE simulator resets the DAM;
- i) the current consumption is measured over a period of 10 s.

##### **6.2.1.4.5 Test requirement**

- 1) After steps c), f) and i), the current consumption of the DAM shall not exceed 1 mA.

## 6.2.2 Reset RST (contact C2)

### 6.2.2.1 Static operation

#### 6.2.2.1.1 Definition and applicability

In addition to the electronic signals and transmission protocols defined in ISO/IEC 7816-3 [5], the DAM shall operate within the following limits regarding the reset RST signal to ensure proper operation in the DECT environment.

This test applies to all DAM implementations with 5 V interface.

#### 6.2.2.1.2 Conformance requirement

- 1) The DAM shall operate within the following limits for RST:
  - $V_{OH}$  between  $V_{CC} - 0,7$  V and  $V_{CC}$  for  $I_{OHmax}$  of  $+20$   $\mu$ A;
  - $V_{OL}$  between 0 V and 0,6 V for  $I_{OLmax}$  of  $-200$   $\mu$ A;
  - $t_R$  and  $t_F$  not exceeding 400  $\mu$ s, with  $C_{out}$  and  $C_{in}$  equal to 30 pF.

Reference: ETS 300 331 [1], subclause 5.2.

Test Group Reference (TGR): TGR\_DAM\_ELEC\_RST.

Test Procedure Reference (TPR): TPR\_DAM\_ELEC\_RST\_ST.

#### 6.2.2.1.3 Test purpose

To verify that the DAM conforms to the above requirements.

#### 6.2.2.1.4 Method of test

##### Initial conditions:

- 1) the DAM is connected to a PE simulator;
- 2) a current measuring device is connected to RST (contact C2) of the DAM;
- 3) the capacitance,  $C_{out}$  and  $C_{in}$ , of RST (contact C2) is measured to be 30 pF.

##### Test procedure:

- a) the following parameters are set for RST:
  - $V_{OH}$  of the RST signal is set to  $V_{CC} - 0,7$  V;
  - $V_{OL}$  of the RST signal is set to 0 V;
  - $t_R$  and  $t_F$  are set to 400  $\mu$ s;
- b) the PE simulator resets the DAM;
- c) the following parameters are set for RST:
  - $V_{OH}$  of the RST signal is set to  $V_{CC}$ ;
  - $V_{OL}$  of the RST signal is set to 0,6 V;
  - $t_R$  and  $t_F$  are set to 400  $\mu$ s;
- d) the PE simulator resets the DAM.

#### 6.2.2.1.5 Test requirement

- 1) After steps b) and d), the following shall be true:
  - $I_{OHmax}$  is measured to be less than or equal to +20  $\mu$ A;
  - $I_{OLmax}$  is measured to be less than or equal to -200  $\mu$ A.

#### 6.2.2.2 Dynamic operation

##### 6.2.2.2.1 Definition and applicability

In addition to the electronic signals and transmission protocols defined in ISO/IEC 7816-3 [5], the DAM shall operate within the following limits regarding the reset RST signal to ensure proper operation in the DECT environment.

This test applies to all DAM implementations with 5 V interface.

##### 6.2.2.2.2 Conformance requirement

- 1) The voltage on RST shall remain between -0,3 V and  $V_{cc} + 0,3$  V during dynamic operation.

Reference: ETS 300 331 [1], subclause 5.2.

Test Group Reference (TGR): TGR\_DAM\_ELEC\_RST.

Test Procedure Reference (TPR): TPR\_DAM\_ELEC\_RST\_DY.

##### 6.2.2.2.3 Test purpose

To verify that the DAM conforms to the above requirements.

##### 6.2.2.2.4 Method of test

###### Initial conditions:

- 1) the DAM is connected to a PE simulator;
- 2) the following parameters are set for signal RST:
  - $V_{OH}$  of the RST signal is set to  $V_{cc}$ ;
  - $V_{OL}$  of the RST signal is set to 0,0 V;
  - $t_R$  and  $t_F$  are set to 400  $\mu$ s;
  - set the overshoot voltage to be  $V_{cc} + 0,3$  V;
  - set the undershoot voltage to be -0,3 V.

###### Test procedure:

- a) The PE simulator resets the DAM.

##### 6.2.2.2.5 Test requirement

- 1) After step a), the DAM shall send the correct ATR.

### 6.2.3 Clock CLK (contact C3)

#### 6.2.3.1 Frequency and duty cycle

##### 6.2.3.1.1 Definition and applicability

In addition to the electronic signals and transmission protocols defined in ISO/IEC 7816-3 [5], the DAM shall operate within the following limits regarding the reset RST signal to ensure proper operation in the DECT environment.

This test applies to all DAM implementations with 5 V interface.

##### 6.2.3.1.2 Conformance requirement

- 1) The DAM shall support clock frequencies between 1 MHz and 5 MHz.
- 2) The DAM shall **not** support an internal clock.
- 3) The DAM shall support a duty cycle between 40 % and 60 % of the period during stable operation.

Reference: ETS 300 331 [1], subclause 5.4.

Test Group Reference (TGR): TGR\_DAM\_ELEC\_CLK.

Test Procedure Reference (TPR): TPR\_DAM\_ELEC\_CLK\_FREQ.

##### 6.2.3.1.3 Test purpose

To verify that the DAM conforms to the above requirements.

##### 6.2.3.1.4 Method of test

###### Initial conditions:

- 1) the DAM is connected to a PE simulator.

###### Test procedure:

- a) the frequency of the clock source is set to 1 MHz;
- b) the duty cycle of the clock source is set to 40 % high;
- c) the PE simulator resets the DAM;
- d) the duty cycle of the clock source is set to 60 % high;
- e) the PE simulator resets the DAM;
- f) the frequency of the clock source is set to 5 MHz;
- g) the duty cycle of the clock source is set to 40 % high;
- h) the PE simulator resets the DAM;
- i) the duty cycle of the clock source is set to 60 % high;
- j) the PE simulator resets the DAM.



#### 6.2.3.1.5 Test requirement

- 1) After steps c), e), h) and j), the DAM shall send the correct ATR sequence.
- 2) The DAM shall not support an internal clock.

#### 6.2.3.2 Voltage and current

##### 6.2.3.2.1 Definition and applicability

In addition to the electronic signals and transmission protocols defined in ISO/IEC 7816-3 [5], the DAM shall operate within the following limits regarding the clock CLK signal to ensure proper operation in the DECT environment.

This test applies to all DAM implementations with 5 V interface.

##### 6.2.3.2.2 Conformance requirement

- 1) The DAM shall operate within the following limits for CLK:
  - $V_{OH}$  between  $V_{CC} - 0,7\text{ V}$  and  $V_{CC}$  for  $I_{OHmax}$  of  $+20\text{ }\mu\text{A}$ ;
  - $V_{OL}$  between  $0\text{ V}$  and  $0,5\text{ V}$  for  $I_{OLmax}$  of  $-200\text{ }\mu\text{A}$ ;
  - $t_R$  and  $t_F$  not exceeding 9 % of the clock period ( $0,5\text{ }\mu\text{s}$  maximum), with  $C_{out}$  and  $C_{in}$  equal to  $30\text{ pF}$ .

Reference: ETS 300 331 [1], subclause 5.2.

Test Group Reference (TGR): TGR\_DAM\_ELEC\_CLK.

Test Procedure Reference (TPR): TPR\_DAM\_ELEC\_CLK\_VI.

##### 6.2.3.2.3 Test purpose

To verify that the DAM conforms to the above requirements.

##### 6.2.3.2.4 Method of test

###### Initial conditions:

- 1) the DAM is connected to a PE simulator;
- 2) a current measuring device is connected to CLK (contact C3) of the DAM;
- 3) the capacitance,  $C_{out}$  and  $C_{in}$ , of CLK (contact C3) is measured to be  $30\text{ pF}$ .

###### Test procedure:

- a) the clock signal is set to  $1\text{ MHz}$ ;
- b) the following parameters are set for CLK:
  - $V_{OH}$  at  $V_{CC} - 0,7\text{ V}$ ;
  - $V_{OL}$  at  $0\text{ V}$ ;
- c) the PE simulator resets the DAM;
- d) the following parameters are set for CLK:
  - $V_{OH}$  at  $V_{CC} - 0,7\text{ V}$ ;
  - $V_{OL}$  at  $0,5\text{ V}$ ;
- e) the PE simulator resets the DAM;

- f) the following parameters are set for CLK:
- $V_{OH}$  at  $V_{CC}$ ;
  - $V_{OL}$  at 0 V;
- g) the PE simulator resets the DAM;
- h) the following parameters are set for CLK:
- $V_{OH}$  at  $V_{CC}$ ;
  - $V_{OL}$  at 0,5 V;
- i) the PE simulator resets the DAM;
- j) the clock signal is set to 5 MHz;
- k) the following parameters are set for CLK:
- $V_{OH}$  at  $V_{CC} - 0,7$  V;
  - $V_{OL}$  at 0 V;
- l) the PE simulator resets the DAM;
- m) the following parameters are set for CLK:
- $V_{OH}$  at  $V_{CC} - 0,7$  V;
  - $V_{OL}$  at 0,5 V;
- n) the PE simulator resets the DAM;
- o) the following parameters are set for CLK:
- $V_{OH}$  at  $V_{CC}$ ;
  - $V_{OL}$  at 0 V;
- p) the PE simulator resets the DAM;
- q) the following parameters are set for CLK:
- $V_{OH}$  at  $V_{CC}$ ;
  - $V_{OL}$  at 0,5 V;
- r) the PE simulator resets the DAM.

#### 6.2.3.2.5 Test requirement

- 1) After steps c), e), g), i), l), n), p) and r) the following shall be true:
- $I_{OHmax}$  is measured to be less than or equal to +20  $\mu$ A;
  - $I_{OLmax}$  is measured to be less than or equal to -200  $\mu$ A;
  - $t_R$  and  $t_F$  is measured and shall not exceed 9 % of the clock period (0,5  $\mu$ s maximum), with  $C_{out}$  and  $C_{in}$  equal to 30 pF.

#### 6.2.3.3 Dynamic operation

##### 6.2.3.3.1 Definition and applicability

In addition to the electronic signals and transmission protocols defined in ISO/IEC 7816-3 [5], the DAM shall operate within the following limits regarding the clock CLK signal to ensure proper operation in the DECT environment.

This test applies to all DAM implementations with 5 V interface.

#### 6.2.3.3.2 Conformance requirement

- 1) The voltage on CLK shall remain between -0,3 V and  $V_{cc} + 0,3$  V during dynamic operation.

Reference: ETS 300 331 [1], subclause 5.4.

Test Group Reference (TGR): TGR\_DAM\_ELEC\_CLK.

Test Procedure Reference (TPR): TPR\_DAM\_ELEC\_CLK\_DY.

#### 6.2.3.3.3 Test purpose

To verify that the DAM conforms to the above requirements.

#### 6.2.3.3.4 Method of test

##### Initial conditions

- 1) The DAM is connected to a PE simulator.
- 2) The following parameters are set for signal CLK:
  - $V_{OH}$  of the RST signal is set to  $V_{cc}$ ;
  - $V_{OL}$  of the RST signal is set to 0,0 V;
  - $t_R$  and  $t_F$  are set to 400  $\mu$ s;
  - set the overshoot voltage to be  $V_{cc} + 0,3$  V;
  - set the undershoot voltage to be -0,3 V.

##### Test procedure

- a) The PE simulator resets the DAM.

#### 6.2.3.3.5 Test requirement

- 1) During step a), the DAM shall send the correct ATR sequence.

### 6.2.4 I/O (contact C7)

#### 6.2.4.1 Voltage and current

##### 6.2.4.1.1 Definition and applicability

In addition to the electronic signals and transmission protocols defined in ISO/IEC 7816-3 [5], the DAM shall operate within the following limits regarding the I/O signal to ensure proper operation in the DECT environment.

This test applies to all DAM implementations with 5 V interface.

#### 6.2.4.1.2 Conformance requirement

- 1) The DAM shall operate within the following limits for I/O:
  - $V_{IH}$  between  $0,7 \times V_{CC}$  and  $V_{CC} + 0,3$  V for  $I_{IHmax}$  of  $+20 \mu A$ ;
  - $V_{IL}$  between  $-0,3$  V and  $0,8$  V for  $I_{ILmax}$  of  $+1$  mA;
  - $V_{OH}$  between  $3,8$  V and  $V_{CC}$  for  $I_{OHmax}$  of  $+20 \mu A$ ;
  - $V_{OL}$  between  $0$  V and  $0,4$  V for  $I_{OLmax}$  of  $-1$  mA;
  - $t_R$  and  $t_F$  not exceeding  $1 \mu s$ , with  $C_{out}$  and  $C_{in}$  equal to  $30$  pF.

Reference: ETS 300 331 [1], subclause 5.5.

Test Group Reference (TGR): TGR\_DAM\_ELEC\_IO.

Test Procedure Reference (TPR): TPR\_DAM\_ELEC\_IO\_VI.

#### 6.2.4.1.3 Test purpose

To verify that the DAM conforms to the above requirements.

#### 6.2.4.1.4 Method of test

##### Initial conditions:

- 1) the DAM is connected to a PE simulator;
- 2) a current measuring device is connected to I/O (contact C7) of the DAM;
- 3) the capacitance,  $C_{out}$  and  $C_{in}$ , of I/O (contact C7) is measured to be  $30$  pF.

##### Test procedure:

- a)  $V_{OH}$  and  $V_{OL}$  on the PE simulator are set to the minimum ranges allowed by the DAM ( $V_{IH}$  and  $V_{IL}$ );
- b) the PE simulator resets the DAM;
- c) the PE simulator sends a STATUS command to the DAM;
- d)  $V_{OH}$  and  $V_{OL}$  on the PE simulator are set to the maximum ranges allowed by the DAM ( $V_{IH}$  and  $V_{IL}$ );
- e) the PE simulator resets the DAM;
- f) the PE simulator sends a STATUS command to the DAM.

#### 6.2.4.1.5 Test requirement

- 1) During steps b), c), e) and f), the DAM conforms to the above requirements.

#### 6.2.4.2 Dynamic operation

##### 6.2.4.2.1 Definition and applicability

In addition to the electronic signals and transmission protocols defined in ISO/IEC 7816-3 [5], the DAM shall operate within the following limits regarding the I/O signal to ensure proper operation in the DECT environment.

This test applies to all DAM implementations with  $5$  V interface.

#### 6.2.4.2.2 Conformance requirement

- 1) The voltage on I/O shall remain between -0,3 V and  $V_{cc} + 0,3$  V during dynamic operation.

Reference: ETS 300 331 [1], subclause 5.5.

Test Group Reference (TGR): TGR\_DAM\_ELEC\_IO.

Test Procedure Reference (TPR): TPR\_DAM\_ELEC\_IO\_DY.

#### 6.2.4.2.3 Test purpose

To verify that the DAM conforms to the above requirements.

#### 6.2.4.2.4 Method of test

##### Initial conditions:

- 1) the DAM is connected to a PE simulator;
- 2) the following parameters are set for signal I/O:
  - $V_{OH}$  of the I/O signal is set to  $V_{cc}$ ;
  - $V_{OL}$  of the I/O signal is set to 0,0 V;
  - $t_R$  and  $t_F$  are set to 1  $\mu$ s;
  - set the overshoot voltage to be  $V_{cc} + 0,3$  V;
  - set the undershoot voltage to be -0,3 V.

##### Test procedure:

- a) the PE simulator resets the DAM;
- b) the PE simulator sends a STATUS command to the DAM.

#### 6.2.4.2.5 Test requirement

- 1) After step a), the DAM shall send the correct ATR.

### 6.2.5 States

#### 6.2.5.1 Definition and applicability

There are two states for the while the power supply is on, operating state when the DAM is executing a command, and idle state at any other time.

This test applies to both plug-in and ID-1 DAM cards.

#### 6.2.5.2 Conformance requirement

- 1) The DAM shall support exactly one of these items:
  - clock stop allowed, no preferred level;
  - clock stop allowed, high level preferred;
  - clock stop allowed, low level preferred;
  - clock stop not allowed;
  - clock stop only allowed on high level;
  - clock stop only allowed on low level.

2) When the DAM is in idle state, all pertinent data shall be retained.

Reference: ETS 300 331 [1], subclauses 5.6 and 10.1.1.

Test Group Reference (TGR): TGR\_DAM\_ELEC\_STAT.

Test Procedure Reference (TPR): TPR\_DAM\_ELEC\_STAT.

### 6.2.5.3 Test purpose

To verify that the DAM conforms to the above requirements.

### 6.2.5.4 Method of test

#### Initial conditions:

1) the DAM is connected to a PE simulator.

#### Test procedure:

- a) the PE simulator resets the DAM;
- b) the PE simulator sends a SELECT command to the DAM to select EF<sub>ICC</sub>;
- c) the PE simulator sends a READ BINARY command using a length of 1 byte to the DAM;
- d) the PE simulator sends a SELECT command to the DAM to select EF<sub>ICC</sub>;
- e) the PE Simulator stops the clock according to the clock stop mode read in step c);
- f) the PE Simulator pauses for 10 s, then starts the clock;
- g) the PE Simulator sends a GET RESPONSE command to the DAM.

### 6.2.5.5 Test requirement

1) After step c), the coding of bits 1, 2 and 3 shall be one of the following only:

Bit 3	Bit 2	Bit 1	Clock stop mode
1	0	0	Clock stop allowed, no preferred level
1	1	0	Clock stop allowed, high level preferred
1	0	1	Clock stop allowed, low level preferred
0	0	0	Clock stop not allowed
0	1	0	Clock stop only allowed on high level
0	0	1	Clock stop only allowed on low level

2) After step g), the response data read shall be that indicating EF<sub>ICC</sub>.

### 6.2.6 Answer To Reset (ATR)

#### 6.2.6.1 ATR content

##### 6.2.6.1.1 Definition and applicability

The ATR is information presented by the DAM to the PE at the beginning of the card session and gives operational requirements.

This test applies to both plug-in and ID-1 DAM cards.

#### 6.2.6.1.2 Conformance requirement

- 1) The ATR consists of at the most 33 characters.
- 2) Initial character TS is sent by the DAM.
- 3) Format character T0 is sent by the DAM.
- 4) Interface character (global) TA1 is sent by the DAM (optional).
- 5) Interface character (global) TB1 is sent by the DAM (optional).
- 6) Interface character (global) TC1 is sent by the DAM (optional).
- 7) Interface character TD1 is sent by the DAM (optional).
- 8) Interface character (specific) TA2 is sent by the DAM (optional).
- 9) Interface character (global) TB2 is **never** sent by the DAM.
- 10) Interface character (specific) TC2 is sent by the DAM (optional).
- 11) Interface character TD<sub>i</sub> is sent by the DAM (optional).
- 12) Interface characters TA<sub>i</sub>, TB<sub>i</sub>, TC<sub>i</sub> ( $i > 2$ ) are sent by the DAM (optional).
- 13) Historical characters T1,...,TK are sent by the DAM (optional).
- 14) Check character TCK is sent by the DAM (conditional).

Reference: ETS 300 331 [1], subclauses 5.8.1 and 5.8.2.

Test Group Reference (TGR): TGR\_DAM\_ELEC\_ATR.

Test Procedure Reference (TPR): TPR\_DAM\_ELEC\_ATR\_CON.

#### 6.2.6.1.3 Test purpose

To verify that the DAM conforms to the above requirements.

#### 6.2.6.1.4 Method of test

##### Initial conditions:

- 1) the DAM is connected to a PE simulator.

##### Test procedure:

- a) the PE simulator resets the DAM.

#### 6.2.6.1.5 Test requirement

- 1) After step a), the DAM shall send the ATR sequence.
- 2) The total length of the ATR sequence shall not be more than 33 characters.
- 3) The following characters shall be present and in the following order:
  - initial character TS;
  - format character T0;
  - interface character (global) TA1, if its presence is indicated by T0;
  - interface character (global) TB1, if its presence is indicated by T0;
  - interface character (global) TC1, if its presence is indicated by T0;
  - interface character TD1, if its presence is indicated by T0;
  - interface character (specific) TA2, if its presence is indicated by TD1;
  - interface character (specific) TC2, if its presence is indicated by TD1;
  - interface character TD<sub>i</sub>, if its presence is indicated by TD<sub>(i-1)</sub>,  $i > 1$ ;
  - interface characters TA<sub>i</sub>, TB<sub>i</sub>, TC<sub>i</sub> if their presence is indicated by TD<sub>(i-1)</sub>,  $i > 2$ ;
  - historical characters T1, ... , TK, if their presence is indicated by T0;
  - check character TCK, if an additional protocol type to T=0 is indicated by TD1.
- 4) PI1 shall equal 0 if TB1 is sent.
- 5) TC1 shall be either 0 or 255, if sent.
- 6) The DAM shall never send interface character (global) TB2.

#### 6.2.6.2 PTS procedure

##### 6.2.6.2.1 Definition and applicability

The ATR indicates which protocols are available for use during a session. The PTS procedure allows one of the available protocol types to be selected.

This test applies to both plug-in and ID-1 DAM cards.

##### 6.2.6.2.2 Conformance requirement

- 1) The DAM shall respond to a PTS-Request from the PE with a PTS-Response.

Reference: ETS 300 331 [1], subclauses 5.8.1 and 5.8.2.

Test Group Reference (TGR): TGR\_DAM\_ELEC\_ATR.

Test Procedure Reference (TPR): TPR\_DAM\_ELEC\_ATR\_PTS.

##### 6.2.6.2.3 Test purpose

To verify that the DAM conforms to the above requirements.



#### 6.2.6.2.4 Method of test

##### Initial conditions:

- 1) The DAM is connected to a PE simulator.

##### Test Procedure:

- a) the PE simulator resets the DAM;
- b) the PE simulator sends a PTS-Request to the DAM, selecting T=0 protocol.

#### 6.2.6.2.5 Test requirement

- 1) After step a), the DAM shall send the correct ATR sequence.
- 2) After step b), the DAM shall send a valid PTS-Response.

### 6.2.7 Major Capabilities

#### 6.2.7.1 Definition and applicability

The DAM shall adhere to the electronic signals and transmission protocols defined in ETS 300 331 [1] and ISO/IEC 7816-3 [5] to ensure proper operation in the DECT environment.

This test applies to both plug-in and ID-1 DAM cards.

#### 6.2.7.2 Conformance requirement

- 1) Electronic signals and transmission protocols shall be in accordance with ISO/IEC 7816-3 [5] unless otherwise specified.
- 2) The choice of the transmission protocol(s), to be used to communicate between the PE and the DAM, shall at least include that specified and denoted by T=0 in ISO/IEC 7816-3 [5].
- 3) The baud rate for all communications shall be: (clock frequency) / 372.
- 4) The bit/character duration and sampling time specified in ISO/IEC 7816-3 [5], subclauses 6.1.1 and 6.1.2, are valid for all communications.
- 5) Error detection and character repetition is mandatory for the DAM for all communications.

Reference: ETS 300 331 [1], clause 5, subclauses 5.7, 5.9 and 5.10.

Test Group Reference (TGR): TGR\_DAM\_ELEC\_MAJOR.

Test Procedure Reference (TPR): TPR\_DAM\_ELEC\_MAJOR.

#### 6.2.7.3 Test purpose

To verify that the DAM conforms to the above requirements.

NOTE: The testing of CR1, CR2, CR3, CR4 and CR5 is outside the scope of this ETS. Please refer to the test specification for ISO/IEC 7816-3 [5].

#### 6.2.7.4 Method of test

##### Initial conditions

N/A.

##### Test procedure

N/A.

#### 6.2.7.5 Test requirement

N/A.

### 6.3 Logical model

The tests in this subclause ensure that the IUT is tested against the specification of the logical structure, for a DAM, the code associated with it, and the structure of the files used.

#### 6.3.1 File identifier

##### 6.3.1.1 File-type identification

###### 6.3.1.1.1 Definition and applicability

A file identifier is used to address or identify each specific file.

This test applies to both plug-in and ID-1 DAM cards.

###### 6.3.1.1.2 Conformance requirement

- 1) For DECT, the Master File shall be coded as '3F 00'.
- 2) For DECT, file type '7F' shall be used to identify Dedicated Files.
- 3) For DECT, file types '00', '01' and '2F' shall be used to identify Elementary Files under the MF.
- 4) For DECT, file type '6F' shall be used to identify Elementary Files under a Dedicated File.

Reference: ETS 300 331 [1], subclause 6.2.

Test Group Reference (TGR): TGR\_DAM\_LOG\_FID.

Test Procedure Reference (TPR): TPR\_DAM\_LOG\_FID\_FT1.

###### 6.3.1.1.3 Test purpose

To verify that the DAM conforms to the above requirements.

###### 6.3.1.1.4 Method of test

##### Initial conditions:

- 1) The DAM is connected to a PE simulator.

##### Test procedure:

- a) the PE simulator resets the DAM;
- b) for every possible file ID in the file structure for the DECT application, the PE Simulator sends SELECT commands to the DAM to select the file ID and, if selected successfully, the PE Simulator sends a GET RESPONSE command to the DAM.

### 6.3.1.1.5 Test requirement

- 1) After each successful SELECT and GET RESPONSE in step b), byte 7 of the response data shall conform to the following table:

File ID	Type of File
'3F 00'	'01'
'7F 50'	'03'
'7F XX'	'02'
'6F XX'	'04'
'00 XX'	'04'
'01 XX'	'04'
'2F XX'	'04'

### 6.3.1.2 File ID assignments

#### 6.3.1.2.1 Definition and applicability

A file identifier is used to address or identify each specific file. There are a number of rules regarding file ID assignment.

This test applies to both plug-in and ID-1 DAM cards.

#### 6.3.1.2.2 Conformance requirement

- 1) A file ID is assigned at the time of creation of the file concerned.
- 2) Two files under the same parent shall never have the same ID.
- 3) A child and any parent in the direct hierarchy shall never have the same ID.

Reference: ETS 300 331 [1], subclause 6.2.

Test Group Reference (TGR): TGR\_DAM\_LOG\_FID.

Test Procedure Reference (TPR): TPR\_DAM\_LOG\_FID\_FIA.

#### 6.3.1.2.3 Test purpose

To verify that all files within the DAM structure conform to the above requirements.

NOTE 1: CR1 cannot be tested as the SELECT function requires the file ID in order to select files.

NOTE 2: CR2 and CR3 cannot be tested due to the operation of the SELECT function which can only ever select a single file for a given file ID.

#### 6.3.1.2.4 Method of test

##### Initial conditions

N/A.

##### Test procedure

N/A.

#### 6.3.1.2.5 Test requirement

N/A.

### 6.3.2 Dedicated files

#### 6.3.2.1 Definition and applicability

Dedicated files provide a functional grouping of both Elementary and Dedicated Files. In this way a structured hierarchy of files can be established on the DAM.

This test applies to both plug-in and ID-1 DAM cards.

#### 6.3.2.2 Conformance requirement

- 1) The identifier for and the path to DF<sub>DECT</sub> shall be given in the Elementary File EF<sub>DIR</sub> (optional).
- 2) The DFs for registrations shall be placed as immediate children under DF<sub>DECT</sub>.
- 3) Each registration shall be placed in its own DF.

Reference: ETS 300 331 [1], subclause 6.3.

Test Group Reference (TGR): TGR\_DAM\_LOG\_DF.

Test Procedure Reference (TPR): TPR\_DAM\_LOG\_DF.

#### 6.3.2.3 Test purpose

To verify that the Dedicated Files within the DAM file structure conform to the above requirements.

#### 6.3.2.4 Method of test

##### Initial conditions:

- 1) The DAM is connected to a PE simulator.

##### Test procedure:

- a) the PE simulator resets the DAM;
- b) the PE simulator sends a SELECT command to the DAM to select EF<sub>DIR</sub>;
- c) if step b) is successful, the PE simulator gains the correct ADM access conditions to read EF<sub>DIR</sub>. Otherwise, proceed to step g);
- d) the PE simulator sends a READ BINARY command to the DAM;
- e) the PE simulator sends as many SELECT commands as are required to select the DF<sub>DECT</sub> by file ID as given in EF<sub>DIR</sub>;
- f) the PE simulator sends a SELECT command to select the master file;
- g) the PE simulator sends a single SELECT command to the DAM to select DF<sub>SR1</sub>;
- h) the PE simulator sends SELECT commands to the DAM to select DF<sub>DECT</sub>;
- i) the PE simulator sends a SELECT command to the DAM to select EF<sub>LSR</sub>;
- j) the PE simulator sends a GET RESPONSE command to the DAM;
- k) the PE simulator sends a SELECT command to the DAM to select DF<sub>SR1</sub>;

- l) the PE simulator sends a SELECT command to the DAM to select each of the following files in sequence:
- EF<sub>SR</sub>;
  - EF<sub>IPIU</sub>;
  - EF<sub>PARK</sub>;
  - EF<sub>DCK</sub>;
  - EF<sub>UAK</sub>;
  - EF<sub>AC</sub>;
  - EF<sub>ST</sub>;
- m) steps k) and l) are repeated for all registrations on the DAM.

#### 6.3.2.5 Test requirement

- 1) After step g) the status condition returned by the DAM shall be SW1='94', SW2='04' - file ID not found.
- 2) After step i) the number of records in EF<sub>LSR</sub> shall be noted for use in step m).

#### 6.3.3 Elementary Files

##### 6.3.3.1 Definition and applicability

Elementary Files structure the way in which information is held on the DAM and provide security on how this information is accessed.

This test applies to both plug-in and ID-1 DAM cards.

##### 6.3.3.2 Conformance requirement

- 1) The total data length of the body of an EF with transparent structure shall be indicated in the header of the EF.
- 2) The record length of an EF with linear fixed structure shall be indicated in the header of the EF.
- 3) The record length multiplied by the number of records of an EF with linear fixed structure shall be indicated in the header of the EF.
- 4) For an EF with cyclic structure, when all the records have been used for storage, then the next storage of data shall overwrite the oldest information.
- 5) The record length of an EF with cyclic structure shall be indicated in the header of the EF.
- 6) The record length multiplied by the number of records of an EF with cyclic structure shall be indicated in the header of the EF.
- 7) The DAM shall be able to access records within a linear fixed EF using all of the methods given in subclause 6.4.2.

Reference: ETS 300 331 [1], subclauses 6.4.1, 6.4.2 and 6.4.3.

Test Group Reference (TGR): TGR\_DAM\_LOG\_EF.

Test Procedure Reference (TPR): TPR\_DAM\_LOG\_EF.

### 6.3.3.3 Test purpose

To verify that the EFs within the DAM file structure conform to the above requirements.

NOTE 1: CR4, CR5 and CR6 cannot be tested as there are no cyclic EFs within the DAM structure.

NOTE 2: CR7 is tested in subclauses 6.5.5 and 6.5.6.

### 6.3.3.4 Method of test

#### Initial conditions:

- 1) The DAM is connected to a PE simulator.

#### Test procedure:

- a) the PE simulator resets the DAM;
- b) for all EFs in the file structure on the DAM, the PE simulator sends SELECT commands to the DAM to select each EF in sequence;
- c) for all EFs successfully selected, the PE simulator sends a GET RESPONSE command to the DAM;
- d) for all transparent EFs, the PE simulator sends a READ BINARY command to the DAM. The length used shall be that of bytes 3 and 4 of the response data in step c);
- e) for all transparent EFs, the PE simulator sends a READ BINARY command with offset '00 01' to the DAM. The length used shall be that of bytes 3 and 4 of the response data in step c);
- f) for all linear fixed EFs, the PE simulator sends a READ RECORD using FIRST mode to the DAM. The length used shall be that of byte 15 of the response data in step c);
- g) for all linear fixed EFs, the PE simulator sends a READ RECORD using ABSOLUTE mode to the DAM. The record length used shall be that of byte 15 of the response data in step c) and the record number shall be that of bytes 3 and 4 of the response data in step c) divided by the record length;
- h) for all linear fixed EFs, the PE simulator sends a READ RECORD using ABSOLUTE mode to the DAM. The record length used shall be that of byte 15 of the response data in step c) and the record number shall be that of bytes 3 and 4 of the response data in step c) divided by the record length, plus 1.

### 6.3.3.5 Test requirement

- 1) After steps e) and h) the status condition returned by the DAM shall be SW1='94', SW2='02' - out of range (invalid address).

## 6.3.4 Methods for selecting the DECT application

### 6.3.4.1 Definition and applicability

In addition to the method of selecting files by file ID, the direct selection method allows selection of the DECT application, or other application on a multi-application card, using an application identifier. Alternatively, DF<sub>DECT</sub> may be selected using the file identifiers in EF<sub>DIR</sub>.

This test applies to both plug-in and ID-1 DAM cards.

#### 6.3.4.2 Conformance requirement

- 1) Of the two methods available for selecting the DECT application, the DAM shall support at least one method.

Reference: ETS 300 331 [1], subclause 6.5.

Test Group Reference (TGR): TGR\_DAM\_LOG\_SELDECT.

Test Procedure Reference (TPR): TPR\_DAM\_LOG\_SELDECT.

#### 6.3.4.3 Test purpose

To verify that the DAM conforms to the above requirements.

#### 6.3.4.4 Method of test

##### Initial conditions:

- 1) The DAM is connected to a PE simulator.

##### Test procedure

- a) the PE simulator resets the DAM;
- b) the PE simulator sends a SELECT command to the DAM to select EF<sub>ICC</sub>;
- c) the PE simulator sends a READ BINARY command to the DAM with a length of 1 and an offset of 18. If byte 19 does not exist in the response data, then proceed to step f);
- d) if byte 19 does exist in the response data and bit 4 is set, then make a direct selection of DF<sub>DECT</sub>. Otherwise, proceed to step f);
- e) the PE simulator sends a SELECT command to select the master file;
- f) the PE simulator sends a SELECT command to the DAM to select EF<sub>DIR</sub>;
- g) if step f) is successful, the PE simulator gains the correct ADM access conditions to read EF<sub>DIR</sub>. Otherwise, proceed to step k);
- h) the PE simulator sends a READ BINARY command to the DAM;
- i) the PE simulator sends as many SELECT commands as are required to select the DF<sub>DECT</sub> by file ID as given in EF<sub>DIR</sub>;
- j) the PE simulator sends a SELECT command to select the master file;
- k) the PE simulator sends SELECT commands to the DAM to select DF<sub>DECT</sub>.

#### 6.3.4.5 Test requirement

- 1) After step i) or step k) or both, DF<sub>DECT</sub> shall be selected.
- 2) After step k), if bit 4 of byte 19 of the response data from step c) is present and not set, then the status condition returned by the DAM shall be SW1='6B', SW2='XX'.

### 6.3.5 Methods for selecting a file

#### 6.3.5.1 Definition and applicability

The PE accesses information on the DAM navigating around the file structure by selecting DFs and EFs as required. There are a number of rules regarding which file elements may be selected from a given DF or EF.

This test applies to both plug-in and ID-1 DAM cards.

#### 6.3.5.2 Conformance requirement

- 1) Selection of a DF or MF shall set the current Directory on the DAM.
- 2) After a selection of a DF or MF there shall be no current EF.
- 3) After a selection of an EF, the current EF shall be set to this EF and the current Directory shall remain the DF or MF which is the parent of this EF.
- 4) The current EF shall always be the child of the current Directory.
- 5) Any application specific command shall only be operable if it is specific to the current Directory.
- 6) It shall be possible to select the following from the last selected file:
  - any file which is an immediate child of the current Directory;
  - any DF which is an immediate child of the parent of the current DF;
  - the parent of the current Directory;
  - the current DF;
  - the MF.

NOTE: Reselection of the last selected file is allowed.

- 7) It shall be possible to select any of the "valid selections" in table 6, subclause 6.6 of ETS 300 331 [1] for each of the "last selected file" entries.

Reference: ETS 300 331 [1], subclause 6.6.

Test Group Reference (TGR): TGR\_DAM\_LOG\_SELFILE

Test Procedure Reference (TPR): TPR\_DAM\_LOG\_SELFILE

#### 6.3.5.3 Test purpose

To verify that the DAM conforms to the above requirements with regard to file selection.

NOTE 1: CR4 cannot be tested as it is not possible to select an EF from another directory directly.

NOTE 2: CR5 is tested for each of the functions in subclause 6.5.

NOTE 3: Selections to and from 'DF1' and 'EF3' in CR7 cannot be tested as these files do not exist within the DAM structure.



**6.3.5.4 Method of test**

**Initial conditions:**

- 1) The DAM is connected to a PE simulator.

**Test procedure:**

- a) the PE simulator resets the DAM;
- b) the PE simulator sends SELECT commands to the DAM to select DF<sub>DECT</sub>;
- c) the PE simulator sends a STATUS command to the DAM;
- d) the PE simulator sends a SELECT command to the DAM to select DF<sub>SR1</sub>;
- e) the PE simulator sends a STATUS command to the DAM;
- f) the PE simulator sends a READ BINARY command using a length of 1 byte to the DAM;
- g) the PE simulator sends a SELECT command to the DAM to select EF<sub>SR</sub>;
- h) the PE simulator sends a GET RESPONSE command to the DAM;
- i) the PE simulator sends a STATUS command to the DAM;
- j) step k) is carried out for each line in table 6, subclause 6.6 of ETS 300 331 [1];
- k) step l) is carried out for each one of the "valid selections" in that line of the table;
- l) steps m) then n) are carried out in turn;
- m) the PE simulator sends SELECT commands to the DAM to select the "last selected file";
- n) the PE simulator sends a SELECT command to the DAM to select the "valid selection".

The following file IDs are used to represent the IDs in the table:

Table	Actual
MF	MF
DF1	N/A
DF2	DF <sub>DECT</sub>
DF3	DF <sub>SR1</sub>
DF4	DF <sub>SR2</sub>
EF1	EF <sub>ID</sub>
EF2	EF <sub>ICC</sub>
EF3	N/A
EF4	EF <sub>LSR</sub>
EF5	EF <sub>DCK</sub>
EF6	EF <sub>PARK</sub>
EF7	EF <sub>DCK</sub>

NOTE: As there is no corresponding 'DF1' and 'EF3' on the DAM, all selections from and all selections to these two files are not to be carried out.

### 6.3.5.5 Test requirement

- 1) After step c), bytes 5 and 6 of the response data shall indicate that DF<sub>DECT</sub> is the currently selected directory.
- 2) After step e), bytes 5 and 6 of the response data shall indicate that DF<sub>SR1</sub> is the currently selected directory.
- 3) After step f) the status condition returned by the DAM shall be SW1='94', SW2='00' - no EF selected.
- 4) After step h) the response data shall indicate that EF<sub>SR</sub> is the currently selected EF.
- 5) After step i) bytes 5 and 6 of the response data shall indicate that DF<sub>SR1</sub> is the currently selected directory.

### 6.3.6 Reservation of file IDs

#### 6.3.6.1 Definition and applicability

In order to accommodate planned and possible future requirements, certain file IDs are considered reserved, and may not be used in the DAM file structure.

This test applies to both plug-in and ID-1 DAM cards.

#### 6.3.6.2 Conformance requirement

- 1) The following Dedicated File IDs are reserved for use by DECT:

'7F 60';  
'7F 7X';  
'7F 50';  
'7F 51';  
'7F 52'.

- 2) The following Elementary File IDs are reserved for use by DECT:

'2F 1X' under MF;  
'2F DX' under MF;  
'6F XX' under DFs '7F 50', '7F 51', '7F 52' and '7F 7X'.

- 3) The coding 'FF FF' shall not be used.

Reference: ETS 300 331 [1], subclause 6.7.

Test Group Reference (TGR): TGR\_DAM\_LOG\_RSVD.

Test Procedure Reference (TPR): TPR\_DAM\_LOG\_RSVD.

#### 6.3.6.3 Test purpose

To verify that the DAM conforms to the above requirements.

#### 6.3.6.4 Method of test

##### Initial conditions:

- 1) the DAM is connected to a PE simulator.

##### Test procedure:

- a) the PE simulator resets the DAM;
- b) for all possible EFs on the DAM, the PE simulator sends SELECT commands to the DAM to select each EF in sequence;
- c) at every DF level (including MF) within the file structure on the DAM, the PE simulator sends a SELECT command to the DAM to select the file 'FF FF'.

#### 6.3.6.5 Test requirement

- 1) For all successful selections in step b), the ID of the selected file shall be one of those in figure 7, clause 10 of ETS 300 331 [1] or shall not be one of those listed as reserved.
- 2) The status conditions returned by the DAM After step c) shall be SW1='94', SW2='04' - file ID not found.

### 6.4 Security services and facilities

The tests in this subclause ensure that the IUT conforms with the security aspects which are related to the DAM.

#### 6.4.1 Algorithms and processes

Individual testing of specific algorithms and processes within the DAM is not possible in practice due to the nature of the encapsulation and sequential use of the algorithms and processes within the DAM. However, it is possible to test all of the algorithms and processes inherently, through the testing of procedures and functions which employ these algorithms and processes. Therefore, in order to test the algorithms and processes within the DAM, the test procedures within the subclauses referenced below should be executed:

- processes B1, A11 and A12 shall be employed in the DAM after receiving a PT AUTHENTICATION command from the PE, during the authentication of a Portable radio Termination (PT) by the Fixed radio Termination (FT). Refer to subclause 6.5.17 of this ETS for an associated test procedure to inherently test processes B1, A11 and A12;
- processes B1, A21 and A22 shall be employed in the DAM after receiving an FT AUTHENTICATION command from the PE, during the authentication of a PT by the FT. Refer to subclause 6.5.18 of this ETS for the associated test procedure to inherently test processes B1, A21 and A22;
- processes B2, A11 and A12 shall be employed in the DAM after receiving a USER AUTHENTICATION command from the PE, during user authentication by the FT. Refer to subclause 6.5.19 of this ETS for an associated test procedure to inherently test processes B2, A11 and A12.

#### **6.4.2 Authentication**

The authentication mechanisms employed in the DECT system between the FT and PT to authenticate a PT, an FT or a user, result in finite interactions with the DAM, mainly through the use of the functions PT AUTHENTICATION, ASK RANDOM, FT AUTHENTICATION and USER AUTHENTICATION. In order to test the behaviour of the DAM during these authentication mechanisms, it is sufficient to test the functions which operate on the DAM during the authentication mechanisms. The test procedures for the functions themselves shall be executed, as defined in the subclauses referenced below:

- for authentication of a PT, see to subclause 6.5.17 ("PT AUTHENTICATION function");
- for authentication of a FT, see to subclause 6.5.18 ("FT AUTHENTICATION function");
- for user authentication, see to subclause 6.5.19 ("USER AUTHENTICATION function");
- for mutual authentication, see to subclause 6.5.17 ("PT AUTHENTICATION function") followed by subclause 6.5.18 ("FT AUTHENTICATION function") or subclause 6.5.19 ("USER AUTHENTICATION function") followed by subclause 6.5.18 ("FT AUTHENTICATION function").

#### **6.4.3 UAK allocation**

The UAK allocation mechanism, employed in the DECT system between the FT and PT, to provide initial allocation of a UAK, results in finite interactions with the DAM, mainly through the use of the functions PT AUTHENTICATION, ASK RANDOM and UAK ALLOCATION. In order to test the behaviour of the DAM during this mechanism, it will be sufficient to test the functions which operate on the DAM during the mechanism. The test procedures for the functions themselves shall be executed, as defined in the subclauses referenced below:

- for the UAK ALLOCATION function, refer to subclause 6.5.20 ("UAK ALLOCATION function");
- for the PT AUTHENTICATION function, refer to subclause 6.5.17 ("PT AUTHENTICATION function");
- for the ASK RANDOM function, refer to subclause 6.5.16 ("ASK RANDOM function").

#### **6.4.4 File access control**

##### **6.4.4.1 ALWAYS, CHV1, FT-AUT and NEVER**

###### **6.4.4.1.1 Definition and applicability**

Every file has its own specific access condition for each command which shall be fulfilled before the command can take place.

This test applies to both plug-in and ID-1 DAM cards.

#### 6.4.4.1.2 Conformance requirement

- 1) For access condition ALWAYS, the command can be performed without any restriction;
- 2) For access condition CHV1, the command shall only be possible if one of the following three conditions is fulfilled:
  - a correct CHV1 value has already been presented to the DAM during the current session;
  - the CHV1 enabled/disabled indicator is set to "disabled";
  - UNBLOCK CHV1 has been successfully performed during the current session.
- 3) For access condition FT-AUT, the command shall only be possible after a successful authentication of an FT by the DAM.
- 4) For access condition NEVER, the command shall not be possible over the DAM/PE interface.

NOTE 1: Allocation of ADM levels and the respective requirements for their fulfilment are the responsibility of the appropriate administrative authority.

NOTE 2: Bullet points 2) and 3) of CR2 are tested in subclauses 6.5.11, 6.5.12 and 6.5.13.

Reference: ETS 300 331 [1], subclause 7.6.

Test Group Reference (TGR): TGR\_DAM\_SEC\_FAC.

Test Procedure Reference (TPR): TPR\_DAM\_SEC\_FAC.

#### 6.4.4.1.3 Test purpose

To verify that the DAM conforms to the above requirements.

#### 6.4.4.1.4 Method of test

##### Initial conditions:

- 1) the DAM is connected to a PE simulator;
- 2) CHV1 on the DAM is enabled and three VERIFY CHV1 attempts remain;
- 3) EF<sub>ICC</sub> is not currently invalidated;
- 4) a DF<sub>SR</sub> exists on the DAM.

##### Test procedure:

- a) the PE simulator resets the DAM;
- b) the PE simulator sends a SELECT command to the DAM to select EF<sub>ICC</sub>;
- c) the PE simulator sends a READ BINARY command to the DAM to read the first 1 byte in EF<sub>ICC</sub>;
- d) the PE simulator sends an UPDATE BINARY command to the DAM to update the byte in EF<sub>ICC</sub> with the byte read in step c);
- e) the PE simulator sends SELECT commands to the DAM to select DF<sub>DECT</sub>;
- f) the PE simulator sends a SELECT command to the DAM to select DF<sub>SR1</sub>;
- g) the PE simulator sends a SELECT command to the DAM to select EF<sub>IPUJ</sub>;
- h) the PE simulator sends a READ BINARY command to the DAM to read all bytes in EF<sub>IPUJ</sub>;
- i) the PE simulator gains CHV1 security access;

- j) the PE simulator sends a READ BINARY command to the DAM to read all bytes in EF<sub>IPUI</sub>;
- k) the PE simulator sends an UPDATE BINARY command to the DAM to update all bytes in EF<sub>IPUI</sub> with the actual data read in step j);
- l) the PE simulator gains FT-AUT security access;
- m) the PE simulator sends an UPDATE BINARY command to the DAM to update all bytes in EF<sub>IPUI</sub> with the actual data read in step j);
- n) the PE simulator sends an INVALIDATE command to the DAM to invalidate EF<sub>ICC</sub>;
- o) the PE simulator gains the security access condition(s) specified by the administrative authority for both INVALIDATE and REHABILITATE on EF<sub>ICC</sub>;
- p) if step o) is successful, the PE simulator sends an INVALIDATE command to the DAM to invalidate EF<sub>ICC</sub>;
- q) if step o) is successful, the PE simulator sends an REHABILITATE command to the DAM to rehabilitate EF<sub>ICC</sub>.

#### 6.4.4.1.5 Test requirement

- 1) After steps d), h), k) and n) the status condition returned by the DAM shall be SW1='98', SW2='04' - access condition not fulfilled.

#### 6.4.4.2 CHV2

##### 6.4.4.2.1 Definition and applicability

Every file has its own specific access condition for each command which shall be fulfilled before the command can take place.

This test applies to both plug-in and ID-1 DAM cards.

##### 6.4.4.2.2 Conformance requirement

- 1) For access condition CHV2, the command shall only be possible if one of the following three conditions is fulfilled:
  - a correct CHV2 value has already been presented to the DAM during the current session;
  - the CHV2 enabled/disabled indicator is set to "disabled";
  - UNBLOCK CHV2 has been successfully performed during the current session.

NOTE 1: CR1 can only be tested if the DAM structure contains an EF whose ADM policy is CHV2.

NOTE 2: Bullet points 2) and 3) of CR1 are tested in subclauses 6.5.11, 6.5.12 and 6.5.13.

Reference: ETS 300 331 [1], subclause 7.6.

Test Group Reference (TGR): TGR\_DAM\_SEC\_FAC.

Test Procedure Reference (TPR): TPR\_DAM\_SEC\_FAC\_CHV2.

##### 6.4.4.2.3 Test purpose

To verify that the DAM conforms to the above requirements.

#### 6.4.4.2.4 Method of test

##### Initial conditions:

- 1) the DAM is connected to a PE simulator;
- 2) CHV2 exists on the DAM, is enabled and three VERIFY CHV2 attempts remain;
- 3) the location of a transparent EF, whose UPDATE access condition is CHV2, is known.

##### Test procedure:

- a) the PE simulator resets the DAM;
- b) the PE simulator sends a SELECT command to the DAM to select the EF identified in Initial condition 3);
- c) the PE simulator sends a READ BINARY command to the DAM to read the first byte in the EF;
- d) the PE simulator sends an UPDATE BINARY command to the DAM to update the first byte in the EF with the byte read in step c);
- e) the PE simulator gains CHV2 security access;
- f) the PE simulator sends an UPDATE BINARY command to the DAM to update the first byte in the EF with the byte read in step c).

#### 6.4.4.2.5 Test requirement

- 1) After steps d), h), k) and n) the status condition returned by the DAM shall be SW1='98', SW2='04' - access condition not fulfilled.

#### 6.4.5 Subscription registration maintenance

The mechanisms employed in the DECT system between the FT, PE and DAM while entering, updating or terminating subscription registrations, results in finite interactions with the DAM through the use of functions to select, read and update EFs on the DAM, allocate an initial UAK and obtain mutual authentication. In order to test the behaviour of the DAM during the subscription registration mechanisms, it is sufficient to test the functions which operate on the DAM during these mechanisms. The test procedures for the functions themselves should be executed, as defined in subclause 6.5.

#### 6.5 Description of the functions

The tests in this subclause ensure that the IUT conforms to the functional specification for all the commands and their respective responses.

##### 6.5.1 SELECT function

###### 6.5.1.1 Definition and applicability

It shall be mandatory for all cards complying with ETS 300 331 [1] to support all functions described therein.

This test applies to both plug-in and ID-1 DAM cards.

### 6.5.1.2 Conformance requirement

- 1) The SELECT function shall select a file according to the methods described in clause 6 of ETS 300 331 [1].
- 2) The function shall accept as an input, a file ID.
- 3) The function shall accept as an input, an application identifier (for direct selection).
- 4) If the selected file is the MF or a DF, then the function shall output the file ID, total memory space available, CHV enabled/disabled indicator and CHV status. For further details, see subclause 9.2.1.
- 5) If the selected file is an EF, then the function shall output the file ID, access conditions, invalidation indicator, indication as to whether the file is readable even if invalidated, structure of EF and the length of the records in the case of linear fixed or cyclic structure. For further details, see subclause 9.2.1.
- 6) If the selected file is EF<sub>CHV</sub>, the function shall output all the information described for the EF, plus the number of remaining CHV attempts. For further details, see subclause 9.2.1.
- 7) After a successful selection, the record pointer in a linear fixed file shall be undefined.
- 8) The record pointer in a cyclic file shall address the last record which has been updated or increased.

Reference: ETS 300 331 [1], subclauses 8.1 and 9.2.1

Test Group Reference (TGR): TGR\_DAM\_FN.

Test Procedure Reference (TPR): TPR\_DAM\_FN\_SEL.

### 6.5.1.3 Test purpose

To verify that the SELECT function conforms to the above requirements for the different file types available.

NOTE 1: CR1 is tested in subclause 6.3.5.

NOTE 2: CR3 can only be tested if EF<sub>DIR</sub> contains a valid application ID for DECT assigned by ETSI.

NOTE 3: CR8 cannot be tested as there are no cyclic EFs in the DAM file structure.

### 6.5.1.4 Method of test

#### Initial conditions:

- 1) the DAM is connected to a PE simulator;
- 2) CHV1 on the DAM is enabled and three VERIFY CHV1 attempts and ten UNBLOCK CHV1 attempts remain;
- 3) the first two records in EF<sub>LSR</sub> contain the following data:
  - record 1: '7F 70 30 31 32 33 34 35 36 37 38 39 3A 3B';
  - record 2: '7F 71 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F'.

The data for all other records (if any) is 'FF'.



**Test procedure:**

- a) the PE simulator resets the DAM;
- b) the PE simulator selects DF<sub>DECT</sub> as defined in subclause 4.4;
- c) the PE simulator sends a VERIFY CHV command with **incorrect** CHV1 to the DAM;
- d) the PE simulator sends a DISABLE CHV command to the DAM;
- e) the PE simulator sends a SELECT command using the file ID to the DAM to re-select DF<sub>DECT</sub>;
- f) the PE simulator sends a GET RESPONSE command to the DAM;
- g) the PE simulator selects the relevant EF<sub>CHV1</sub> using the file ID as defined in subclause 4.4;
- h) the PE simulator sends a GET RESPONSE command to the DAM;
- i) the PE simulator selects DF<sub>DECT</sub> as defined in subclause 4.4;
- j) the PE simulator gains the security access condition(s) specified by the administrative authority for both INVALIDATE and REHABILITATE on EF<sub>LSR</sub>;
- k) the PE simulator sends a SELECT command to the DAM to select EF<sub>LSR</sub>;
- l) the PE simulator sends a GET RESPONSE command to the DAM;
- m) the PE simulator sends an INVALIDATE command to the DAM;
- n) the PE simulator sends a SELECT command to the DAM to re-select EF<sub>LSR</sub>;
- o) the PE simulator sends a GET RESPONSE command to the DAM;
- p) the PE simulator sends a REHABILITATE command to the DAM;
- q) the PE simulator sends a READ RECORD command using PREVIOUS mode to the DAM.

**6.5.1.5 Test requirement**

- 1) After steps b) and f) bytes 5 and 6 of the response data shall indicate that DF<sub>DECT</sub> is the currently selected file.
- 2) After step b) the following shall be true of the response data:
  - bit 8 of byte 14 shall be 0 indicating that CHV1 is enabled;
  - bits 1 through 4 of byte 19 shall indicate three VERIFY CHV1 attempts remaining;
  - bits 1 through 4 of byte 20 shall indicate ten UNBLOCK CHV1 attempts remaining.
- 3) After step f) the following shall be true of the response data:
  - bit 8 of byte 14 shall be 0 indicating that CHV1 is disabled;
  - bits 1 through 4 of byte 19 shall indicate two VERIFY CHV1 attempts remaining.

- 4) After step h) the following shall be true of the response data:
  - bytes 9 through 11 shall state the access conditions in subclause 10.2.1 of ETS 300 331 [1];
  - bit 1 of byte 12 shall be 1 indicating that the file is not invalidated;
  - bit 2 of byte 12 shall indicate whether the file is readable even if invalidated;
  - byte 14 shall be '00' indicating transparent structure;
  - byte 15 shall indicate two VERIFY CHV1 attempts remaining.
- 5) After step l) the following shall be true of the response data:
  - bytes 5 and 6 shall indicate that EF<sub>LSR</sub> is the currently selected file;
  - bytes 9 through 11 shall state the access conditions in subclause 10.3.1 of ETS 300 331 [1];
  - bit 1 of byte 12 shall be 1 indicating that the file is not invalidated;
  - bit 2 of byte 12 shall indicate whether the file is readable even if invalidated;
  - byte 14 shall be '01' indicating linear fixed structure;
  - byte 15 shall indicate the length of the records.
- 6) After step o) the response data shall indicate the following:
  - bit 1 of byte 12 shall be 0 indicating that the file is invalidated.
- 7) After step q) the response data shall be the same as that of the last record indicating that the current pointer was undefined.

## 6.5.2 STATUS function

### 6.5.2.1 Definition and applicability

It shall be mandatory for all cards complying with ETS 300 331 [1] to support all functions described therein.

This test applies to both plug-in and ID-1 DAM cards.

### 6.5.2.2 Conformance requirement

- 1) The STATUS function shall output the file ID, total memory space available, CHV enabled/disabled indicator and CHV status of the currently selected MF or DF. For further details, see subclause 9.2.2.

Reference: ETS 300 331 [1], subclauses 8.2 and 9.2.2

Test Group Reference (TGR): TGR\_DAM\_FN.

Test Procedure Reference (TPR): TPR\_DAM\_FN\_STATUS.

### 6.5.2.3 Test purpose

To verify that the DAM conforms to the above requirements.

#### 6.5.2.4 Method of test

##### Initial conditions:

- 1) the DAM is connected to a PE simulator;
- 2) CHV1 on the DAM is enabled and three VERIFY CHV1 attempts and ten UNBLOCK CHV1 attempts remain.

##### Test procedure:

- a) the PE simulator resets the DAM;
- b) the PE simulator selects DF<sub>DECT</sub> as defined in subclause 4.4;
- c) the PE simulator sends a STATUS command to the DAM;
- d) the PE simulator sends a VERIFY CHV command with **incorrect** CHV1 to the DAM;
- e) the PE simulator sends a DISABLE CHV command to the DAM;
- f) the PE simulator sends a STATUS command to the DAM.

#### 6.5.2.5 Test requirement

- 1) After steps c) and f) bytes 5 and 6 of the response data shall indicate that DF<sub>DECT</sub> is the currently selected file.
- 2) After step c) the following shall be true of the response data:
  - bit 8 of byte 14 shall be 0 indicating that CHV1 is enabled;
  - bits 1 through 4 of byte 19 shall indicate three VERIFY CHV1 attempts remaining;
  - bits 1 through 4 of byte 20 shall indicate ten UNBLOCK CHV1 attempts remaining.
- 3) After step f) the following shall be true of the response data:
  - bit 8 of byte 14 shall be 0 indicating that CHV1 is disabled;
  - bits 1 through 4 of byte 19 shall indicate two VERIFY CHV1 attempts remaining.

#### 6.5.3 READ BINARY function

##### 6.5.3.1 Definition and applicability

It shall be mandatory for all cards complying with ETS 300 331 [1] to support all functions described therein.

This test applies to both plug-in and ID-1 DAM cards.

### 6.5.3.2 Conformance requirement

- 1) The READ BINARY function shall read a string of bytes from the current transparent EF.
- 2) The function shall accept as an input, the relative address (offset) and the length (in bytes) of the string.
- 3) The function shall output the string of bytes.
- 4) The function shall only be performed if the READ access condition for the current EF is satisfied.

Reference: ETS 300 331 [1], subclauses 8.3 and 9.2.3

Test Group Reference (TGR): TGR\_DAM\_FN.

Test Procedure Reference (TPR): TPR\_DAM\_FN\_RDBIN.

### 6.5.3.3 Test purpose

To verify that the READ BINARY function conforms to the above requirements.

### 6.5.3.4 Method of test

#### Initial conditions:

- 1) the DAM is connected to a PE simulator;
- 2) EF<sub>LCSR</sub> contains the data string: '7F 70';
- 3) CHV1 is enabled.

#### Test procedure:

- a) the PE simulator resets the DAM;
- b) the PE simulator sends SELECT commands to the DAM to select EF<sub>LCSR</sub> under DF<sub>DECT</sub>;
- c) the PE simulator sends a READ BINARY command using a length of 2 bytes to the DAM;
- d) the PE simulator sends a VERIFY CHV command to the DAM;
- e) the PE simulator sends a READ BINARY command using a length of 2 bytes to the DAM;
- f) the PE simulator sends a READ BINARY command using a length of 1 byte to the DAM;
- g) the PE simulator sends a READ BINARY command using an offset of '00 01' and length 1 byte to the DAM;
- h) the PE simulator sends a READ BINARY command using an offset of '00 01' and length 3 byte to the DAM;
- i) the PE simulator sends a READ BINARY command using an offset of '00 02' and length 1 byte to the DAM.

#### **6.5.3.5 Test requirement**

- 1) After step c) the status condition returned by the DAM shall be SW1='98', SW2='04' - access condition not fulfilled;
- 2) after step e) the data string returned shall be '7F 70';
- 3) after step f) the data string returned shall be '7F';
- 4) after step g) the data string returned shall be '70'.
- 5) After step h) the status condition returned by the DAM shall be SW1='67', SW2='XX' - incorrect parameter P3;
- 6) After step i) the status condition returned by the DAM shall be SW1='6B', SW2='XX' - incorrect parameter P1 or P2.

#### **6.5.4 UPDATE BINARY function**

##### **6.5.4.1 Definition and applicability**

It shall be mandatory for all cards complying with ETS 300 331 [1] to support all functions described therein.

This test applies to both plug-in and ID-1 DAM cards.

##### **6.5.4.2 Conformance requirement**

- 1) The UPDATE BINARY function shall update the current transparent EF with a string of bytes.
- 2) The function shall accept as an input, the relative address (offset), the length (in bytes) of the string, and the string of bytes.
- 3) The function shall only be performed if the UPDATE access condition for the current EF is satisfied.

Reference: ETS 300 331 [1], subclauses 8.4 and 9.2.4

Test Group Reference (TGR): TGR\_DAM\_FN.

Test Procedure Reference (TPR): TPR\_DAM\_FN\_UPBIN.

##### **6.5.4.3 Test purpose**

To verify that the UPDATE BINARY function conforms to the above requirements.

#### 6.5.4.4 Method of test

##### Initial conditions:

- 1) the DAM is connected to a PE simulator;
- 2) EF<sub>LCSR</sub> contains the data string: 'FF FF';
- 3) CHV1 is enabled.

##### Test procedure:

- a) the PE simulator resets the DAM;
- b) the PE simulator sends SELECT commands to the DAM to select EF<sub>LCSR</sub> under DF<sub>DECT</sub>;
- c) the PE simulator sends an UPDATE BINARY command using a length of 2 bytes, and data string '7F 70' to the DAM;
- d) the PE simulator sends a READ BINARY command to the DAM using a length of 2 bytes and an offset of '00 00';
- e) the PE simulator sends a VERIFY CHV command to the DAM;
- f) the PE simulator sends an UPDATE BINARY command using a length of 2 bytes, and data string '7F 70' to the DAM;
- g) the PE simulator sends a READ BINARY command using a length of 2 bytes to the DAM;
- h) the PE simulator sends an UPDATE BINARY command using a length of 1 byte, and data string 'FF' to the DAM;
- i) the PE simulator sends a READ BINARY command using a length of 2 bytes to the DAM;
- j) the PE simulator sends an UPDATE BINARY command using an offset of '00 01', a length 1 byte, and data string 'FF' to the DAM;
- k) the PE simulator sends a READ BINARY command using a length of 2 bytes to the DAM.

#### 6.5.4.5 Test requirement

- 1) After step c) the status condition returned by the DAM shall be SW1='98', SW2='04' - access condition not fulfilled;
- 2) after step d) the data string returned shall be 'FF FF';
- 3) after step g) the data string returned shall be '7F 70';
- 4) after step i) the data string returned shall be 'FF 70';
- 5) after step k) the data string returned shall be 'FF FF'.

#### 6.5.5 READ RECORD function

##### 6.5.5.1 Definition and applicability

It shall be mandatory for all cards complying with ETS 300 331 [1] to support all functions described therein.

This test applies to both plug-in and ID-1 DAM cards.

### 6.5.5.2 Conformance requirement

- 1) The READ RECORD function shall read one complete record in the current linear fixed or cyclic EF.
- 2) The function shall accept as an input, the mode, record number if absolute mode, and the length of the record.
- 3) The function shall output the record specified by the mode.
- 4) The function shall only be performed if the READ access condition for the current EF is satisfied.
- 5) If the mode is CURRENT, the current record is read, the record pointer is not affected.
- 6) If the mode is ABSOLUTE, the record given by the record number is read, the record pointer is not affected.
- 7) If the mode is NEXT, the record pointer is incremented before the function is performed and the pointed record is read.
- 8) If the mode is NEXT, and the record pointer has not been previously been set within the selected EF, the **first** record shall be read and the record pointer set to this record.
- 9) If the mode is NEXT, and the record pointer addresses the last record in a linear fixed EF, the record pointer shall not change and no data shall be read.
- 10) If the mode is NEXT, and the record pointer addresses the last record in a cyclic EF, the **first** record shall be read and the record pointer set to this record.
- 11) If the mode is PREVIOUS, the record pointer is decremented before the function is performed and the pointed record is read.
- 12) If the mode is PREVIOUS, and the record pointer has not been previously been set within the selected EF, the **last** record shall be read and the record pointer set to this record.
- 13) If the mode is PREVIOUS, and the record pointer addresses the first record in a linear fixed EF, the record pointer shall not change and no data shall be read.
- 14) If the mode is PREVIOUS, and the record pointer addresses the first record in a cyclic EF, the **last** record shall be read and the record pointer set to this record.
- 15) If the mode is FIRST, the **first** record shall be read and the record pointer set to this record.
- 16) If the mode is LAST, the **last** record shall be read and the record pointer set to this record.
- 17) The record pointer shall not be changed if the function is unsuccessful.

Reference: ETS 300 331 [1], subclauses 8.5 and 9.2.5

Test Group Reference (TGR): TGR\_DAM\_FN.

Test Procedure Reference (TPR): TPR\_DAM\_FN\_RDREC.

### 6.5.5.3 Test purpose

To verify that the READ RECORD function conforms to the above requirements for the different modes available.

NOTE: CR10 and CR14 cannot be tested as there are no cyclic EFs in the DAM file structure.

#### 6.5.5.4 Method of test

##### Initial conditions:

- 1) the DAM is connected to a PE simulator;
- 2) the record in EF<sub>DCK</sub> contains '00' for all bytes of data;
- 3) the first two records in EF<sub>LSR</sub> contain the following data:
  - record 1: '7F 70 30 31 32 33 34 35 36 37 38 39 3A 3B';
  - record 2: '7F 71 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F'.

The data for all other records (if any) is 'FF'.

- 4) CHV1 is enabled.

##### Test procedure:

- a) the PE simulator resets the DAM;
- b) the PE simulator sends SELECT commands to the DAM to select EF<sub>DCK</sub> under DF<sub>SR1</sub>;
- c) the PE simulator sends a READ RECORD command using ABSOLUTE mode with record 1 to the DAM;
- d) the PE simulator sends a VERIFY CHV command to the DAM;
- e) the PE simulator sends a READ RECORD command using ABSOLUTE mode with record 1 to the DAM;
- f) the PE simulator sends SELECT command to the DAM to select EF<sub>LSR</sub> under DF<sub>DECT</sub>;
- g) the PE simulator sends a READ RECORD command using ABSOLUTE mode with record 2 to the DAM;
- h) the PE simulator sends a READ RECORD command using NEXT mode to the DAM;
- i) the PE simulator sends a READ RECORD command using CURRENT mode to the DAM;
- j) the PE simulator sends a READ RECORD command using NEXT mode to the DAM;
- k) the PE simulator sends a READ RECORD command using PREVIOUS mode to the DAM;
- l) the PE simulator sends a READ RECORD command using PREVIOUS mode to the DAM;
- m) the PE simulator sends a SELECT command to the DAM to select EF<sub>LSR</sub> once more;
- n) the PE simulator sends a READ RECORD command using PREVIOUS mode to the DAM;
- o) the PE simulator sends a READ RECORD command using NEXT mode to the DAM;
- p) the PE simulator sends a READ RECORD command using CURRENT mode to the DAM;
- q) the PE simulator sends a READ RECORD command using FIRST mode to the DAM;
- r) the PE simulator sends a READ RECORD command using LAST mode to the DAM.



#### 6.5.5.5 Test requirement

- 1) After step c) the status condition returned by the DAM shall be SW1='98', SW2='04' - access condition not fulfilled;
- 2) after step e) the record data returned shall be that of the first record in EF<sub>DCK</sub>;
- 3) after steps g) and j) the record data returned shall be that of the second record in EF<sub>LSR</sub>;
- 4) after steps h), i), k) and q) the record data returned shall be that of the first record in EF<sub>LSR</sub>;
- 5) after steps l) and o) the status condition returned by the DAM shall be SW1='94', SW2='02' - out of range (invalid address);
- 6) after steps n), p) and r) the record data returned shall be that of the last record in EF<sub>LSR</sub>.

#### 6.5.6 UPDATE RECORD function

##### 6.5.6.1 Definition and applicability

It shall be mandatory for all cards complying with ETS 300 331 [1] to support all functions described therein.

This test applies to both plug-in and ID-1 DAM cards.

##### 6.5.6.2 Conformance requirement

- 1) The UPDATE RECORD function shall update one complete record in the current linear fixed or cyclic EF.
- 2) The function shall accept as an input, the mode, record number if absolute mode, the length of the record, and the data used for updating the record.
- 3) The function shall only be performed if the UPDATE access condition for the current EF is satisfied.
- 4) For cyclic files, only PREVIOUS mode is allowed.
- 5) If the mode is CURRENT, the current record is updated, the record pointer is not affected.
- 6) If the mode is ABSOLUTE, the record given by the record number is updated, the record pointer is not affected.
- 7) If the mode is NEXT, the record pointer is incremented before the function is performed and the pointed record is updated.
- 8) If the mode is NEXT, and the record pointer has not been previously been set within the selected EF, the **first** record shall be updated and the record pointer set to this record.
- 9) If the mode is NEXT, and the record pointer addresses the last record, the record pointer shall not change and no record shall be updated.
- 11) If the mode is PREVIOUS, the record pointer is decremented before the function is performed and the pointed record is updated.
- 12) If the mode is PREVIOUS, and the record pointer has not been previously been set within the selected EF, the **last** record shall be updated and the record pointer set to this record.
- 13) If the mode is PREVIOUS, and the record pointer addresses the first record, the record pointer shall not change and no record shall be updated.
- 14) If the mode is PREVIOUS and the EF is a cyclic file, the oldest record is updated, the record pointer set to this record, and this record shall become the first record.

- 15) If the mode is FIRST, the **first** record shall be updated and the record pointer set to this record.
- 16) If the mode is LAST, the **last** record shall be updated and the record pointer set to this record.
- 17) The record pointer shall not be changed if the function is unsuccessful.

Reference: ETS 300 331 [1], subclauses 8.6 and 9.2.6

Test Group Reference (TGR): TGR\_DAM\_FN.

Test Procedure Reference (TPR): TPR\_DAM\_FN\_UPREC.

### 6.5.6.3 Test purpose

To verify that the UPDATE RECORD function conforms to the above requirements for the different modes available.

NOTE: CR14 cannot be tested as there are no cyclic EFs in the DAM file structure.

### 6.5.6.4 Method of test

#### Initial conditions:

- 1) the DAM is connected to a PE simulator;
- 2) each record in EF<sub>DCK</sub> contains '00' for all bytes of data;
- 3) each record in EF<sub>LSR</sub> contains 'FF' for all bytes of data;
- 4) CHV1 is enabled.

#### Test procedure:

- a) the PE simulator resets the DAM;
- b) the PE simulator sends SELECT commands to the DAM to select EF<sub>DCK</sub> under DF<sub>SR1</sub>;
- c) the PE simulator sends a UPDATE RECORD command using ABSOLUTE mode with record 1 to the DAM. The data used is 'E2' for all bytes;
- d) the PE simulator sends a VERIFY CHV command to the DAM;
- e) the PE simulator sends a UPDATE RECORD command using ABSOLUTE mode with record 1 to the DAM. The data used is 'E2' for all bytes;
- f) the PE simulator sends a READ RECORD command using FIRST mode to the DAM;
- g) the PE simulator sends SELECT commands to the DAM to select EF<sub>LSR</sub> under DF<sub>DECT</sub>;
- h) the PE simulator sends a UPDATE RECORD command using ABSOLUTE mode with record 2 to the DAM. The data used is 'E3' for all bytes;
- i) the PE simulator sends a READ RECORD command using ABSOLUTE mode with record 2 to the DAM;
- j) the PE simulator sends an UPDATE RECORD command using PREVIOUS mode to the DAM. The data used is 'E4' for all bytes;
- k) the PE simulator sends a READ RECORD command using FIRST mode to the DAM;
- l) the PE simulator sends a UPDATE RECORD command using CURRENT mode to the DAM. The data used is 'E5' for all bytes;

- m) the PE simulator sends a READ RECORD command using FIRST mode to the DAM;
- n) the PE simulator sends an UPDATE RECORD command using NEXT mode to the DAM. The data used is 'E6' for all bytes;
- o) the PE simulator sends a READ RECORD command using ABSOLUTE mode with record 2 to the DAM;
- p) the PE simulator sends an UPDATE RECORD command using PREVIOUS mode to the DAM. The data used is 'E7' for all bytes;
- q) the PE simulator sends a READ RECORD command using FIRST mode to the DAM;
- r) the PE simulator sends an UPDATE RECORD command using PREVIOUS mode to the DAM. The data used is 'E8' for all bytes;
- s) the PE simulator sends a SELECT command to the DAM to select EF<sub>LSR</sub> once more;
- t) the PE simulator sends an UPDATE RECORD command using PREVIOUS mode to the DAM. The data used is 'E9' for all bytes;
- u) the PE simulator sends a READ RECORD command using LAST mode to the DAM;
- v) the PE simulator sends an UPDATE RECORD command using NEXT mode to the DAM. The data used is 'EA' for all bytes;
- w) the PE simulator sends an UPDATE RECORD command using FIRST mode to the DAM. The data used is 'EB' for all bytes;
- x) the PE simulator sends a READ RECORD command using FIRST mode to the DAM;
- y) the PE simulator sends an UPDATE RECORD command using LAST mode to the DAM. The data used is 'EC' for all bytes;
- z) the PE simulator sends a READ RECORD command using LAST mode to the DAM.

#### 6.5.6.5 Test requirement

- 1) After step c) the status condition returned by the DAM shall be SW1='98', SW2='04' - access condition not fulfilled.
- 2) After step f) the record data returned shall be 'E2' for all bytes.
- 3) After step i) the record data returned shall be 'E3' for all bytes.
- 4) After step k) the record data returned shall be 'E4' for all bytes.
- 5) After steps r) and v) the status condition returned by the DAM shall be SW1='94', SW2='02' - out of range (invalid address).
- 6) After step m) the record data returned shall be 'E5' for all bytes.
- 7) After step o) the record data returned shall be 'E6' for all bytes.
- 8) After step q) the record data returned shall be 'E7' for all bytes.
- 9) After step u) the record data returned shall be 'E9' for all bytes.
- 10) After step x) the record data returned shall be 'EB' for all bytes.
- 11) After step z) the record data returned shall be 'EC' for all bytes.

## 6.5.7 SEEK function

### 6.5.7.1 Definition and applicability

It shall be mandatory for all cards complying with ETS 300 331 [1] to support all functions described therein.

This test applies to both plug-in and ID-1 DAM cards.

### 6.5.7.2 Conformance requirement

- 1) The SEEK function shall search through the current linear fixed EF to find a record containing the given pattern.
- 2) The function shall accept as an input, the type and mode, pattern, length of pattern and offset.
- 3) The SEEK function shall support both type 1 and type 2.
- 4) For a type 2 SEEK, the function shall output the record number.
- 5) The SEEK function shall support the following modes:
  - from the beginning forwards;
  - from the end backwards;
  - from the next location forwards;
  - from the previous location backwards.
- 6) The function shall only be performed if the READ access condition for the current EF is satisfied.
- 7) If the parameter P3 indicates a pattern-length greater than the record length, the DAM shall send the status information "incorrect parameter P3".
- 8) If the record length is shorter than pattern length and offset, then the response from the DAM shall be "offset out of range".
- 9) The DAM shall be able to accept any pattern length from 1 to 16 bytes inclusive.
- 10) For a SEEK function of next location forwards, if the record pointer has not been previously set within the selected linear fixed EF, the search begins with the **first** record.
- 11) For a SEEK function of previous location backwards, if the record pointer has not been previously set within the selected linear fixed EF, the search begins with the **last** record.
- 12) After a successful SEEK function, the record pointer shall be set to the record in which the pattern was found.
- 13) The record pointer shall not be changed by an unsuccessful SEEK function.

Reference: ETS 300 331 [1], subclauses 8.7 and 9.2.7

Test Group Reference (TGR): TGR\_DAM\_FN

Test Procedure Reference (TPR): TPR\_DAM\_FN\_SEEK

### 6.5.7.3 Test purpose

To verify that the SEEK function conforms to the above requirements for the different modes available.

#### 6.5.7.4 Method of test

##### Initial conditions:

- 1) the DAM is connected to a PE simulator;
- 2) each record in EF<sub>DCK</sub> contains '00' for all bytes of data;
- 3) the first two records in EF<sub>LSR</sub> contain the following data:
  - record 1: '7F 70 30 31 32 33 34 35 36 37 4C 4D 4E 4F';
  - record 2: '7F 71 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F'.

The data for all other records (if any) is 'FF';

- 4) CHV1 is enabled.

##### Test procedure:

- a) the PE simulator resets the DAM;
- b) the PE simulator sends SELECT commands to the DAM to select EF<sub>DCK</sub> under DF<sub>SR1</sub>;
- c) the PE simulator sends a type 1 SEEK command using the "from the beginning forwards" mode, a pattern-length of 1, and pattern '00' to the DAM;
- d) the PE simulator sends a VERIFY CHV command to the DAM;
- e) the PE simulator sends a type 1 SEEK command using the "from the beginning forwards" mode, a pattern-length of 1, and pattern '00' to the DAM;
- f) the PE simulator sends SELECT commands to the DAM to select EF<sub>LSR</sub> under DF<sub>DECT</sub>;
- g) the PE simulator sends a type 2 SEEK command using the "from the beginning forwards" mode, a pattern-length of 1, and pattern '7F' to the DAM;
- h) the PE simulator sends a GET RESPONSE command to the DAM;
- i) the PE simulator sends a type 2 SEEK command using the "from the beginning forwards" mode, an offset of '0C', a pattern-length of 3, and pattern '4C 4D 4E' to the DAM;
- j) the PE simulator sends a GET RESPONSE command to the DAM;
- k) the PE simulator sends a type 2 SEEK command using the "from the end backwards" mode, an offset of '0C', a pattern-length of 3, and pattern '4C 4D 4E' to the DAM;
- l) the PE simulator sends a GET RESPONSE command to the DAM;
- m) the PE simulator sends a type 2 SEEK command using the "from the previous location backwards" mode, a pattern-length of 16, and the following pattern to the DAM:
  - '7F 70 30 31 32 33 34 35 36 37 4C 4D 4E 4F ';
- n) the PE simulator sends a GET RESPONSE command to the DAM;
- o) the PE simulator sends a type 2 SEEK command using the "from the next location forwards" mode, an offset of '0C', a pattern-length of 3, and pattern '4C 4D 4E' to the DAM;
- p) the PE simulator sends a GET RESPONSE command to the DAM;
- q) the PE simulator sends a SELECT command to the DAM to select EF<sub>LSR</sub> again;

- r) the PE simulator sends a type 2 SEEK command using the "from the next location forwards" mode, an offset of '0C', a pattern-length of 3, and pattern '4C 4D 4E' to the DAM;
- s) the PE simulator sends a GET RESPONSE command to the DAM to retrieve the single byte of response data;
- t) the PE simulator sends a SELECT command to the DAM to select EF<sub>LSR</sub> again;
- u) the PE simulator sends a type 2 SEEK command using the "from the previous location backwards" mode, an offset of '0C', a pattern-length of 3, and pattern '4C 4D 4E' to the DAM;
- v) the PE simulator sends a GET RESPONSE command to the DAM;
- w) the PE simulator sends a type 2 SEEK command using the "from the beginning forwards" mode, a pattern-length of 5, and pattern 'E0 E1 E2 E3 E4' to the DAM;
- x) the PE simulator sends a READ RECORD command using CURRENT mode to the DAM;
- y) the PE simulator sends SELECT commands to the DAM to select EF<sub>DCK</sub> under DF<sub>SR1</sub>;
- z) the PE simulator sends a type 2 SEEK command using the "from the beginning forwards" mode, a pattern-length of 9, and 'FF' for all 9 bytes to the DAM;
- aa) the PE simulator sends a type 2 SEEK command using the "from the beginning forwards" mode, an offset of '02', a pattern-length of 7, and 'FF' for all pattern bytes to the DAM.

#### 6.5.7.5 Test requirement

- 1) After step c) the status condition returned by the DAM shall be SW1='98', SW2='04' - access condition not fulfilled.
- 2) After steps e), j), n) and s) the response data shall indicate that the first record has been found.
- 3) After steps h), l), p) and v) the response data shall indicate that the second record has been found.
- 4) After step w) the status condition returned by the DAM shall be SW1='94', SW2='04' - pattern not found.
- 5) After step x) the record data returned shall be that of the second record in EF<sub>LSR</sub>.
- 6) After step z) the status condition returned by the DAM shall be SW1='67', SW2='00' - incorrect parameter P3.
- 7) After step aa) the status condition returned by the DAM shall be SW1='94', SW2='02' - out of range.

#### 6.5.8 INCREASE function

##### 6.5.8.1 Definition and applicability

It shall be mandatory for all cards complying with ETS 300 331 [1] to support all functions described therein.

This test applies to both plug-in and ID-1 DAM cards.

#### **6.5.8.2 Conformance requirement**

- 1) This function shall add the value given to the value of the last increased/updated record of the current cyclic EF and store the result into the oldest record.
- 2) The record pointer shall be set to this record and this record becomes the first record.
- 3) The function shall accept as an input, the value to be added.
- 4) The function shall output the value of the increased record and the value which has been added.
- 5) The DAM shall not perform the INCREASE if the result would exceed the maximum value of the record (represented by all bytes set to 'FF').

Reference: ETS 300 331 [1], subclauses 8.8 and 9.2.8

Test Group Reference (TGR): TGR\_DAM\_FN

Test Procedure Reference (TPR): TPR\_DAM\_FN\_INC

#### **6.5.8.3 Test purpose**

To verify that the INCREASE function conforms to the above requirements.

NOTE: This function cannot be tested as there are no cyclic EFs in the DAM file structure.

#### **6.5.8.4 Method of test**

##### **Initial conditions:**

- N/A.

##### **Test procedure:**

- N/A.

#### **6.5.8.5 Test requirement**

N/A.

### **6.5.9 VERIFY CHV function**

#### **6.5.9.1 Definition and applicability**

It shall be mandatory for all cards complying with ETS 300 331 [1] to support all functions described therein.

This test applies to both plug-in and ID-1 DAM cards.

### 6.5.9.2 Conformance requirement

- 1) This function shall verify the CHV presented for the current directory by comparing it with the one stored in the relevant EF<sub>CHV</sub>.
- 2) The function shall accept as input, an indication of CHV1/CHV2 and the CHV.
- 3) The verification process shall be subject to the following conditions being fulfilled:
  - CHV is not disabled;
  - CHV is not blocked.
- 4) If the access condition for a function to be performed on a file is CHV1 or CHV2, then a successful verification of the relevant CHV shall be required prior to the use of the function on this file unless the CHV is disabled.
- 5) If the CHV presented is correct, the number of remaining CHV attempts for that CHV shall be reset to its initial value 3.
- 6) If the CHV presented is false, the number of remaining CHV attempts for that CHV shall be decremented.
- 6) After 3 consecutive false CHV attempts, not necessarily in the same card session, the respective CHV shall be blocked and the access condition never fulfilled until the UNBLOCK CHV function has been successfully performed on the respective CHV.

Reference: ETS 300 331 [1], subclauses 8.9 and 9.2.9

Test Group Reference (TGR): TGR\_DAM\_FN

Test Procedure Reference (TPR): TPR\_DAM\_FN\_VERCHV

### 6.5.9.3 Test purpose

To verify that the VERIFY CHV function conforms to the above requirements.

### 6.5.9.4 Method of test

#### Initial conditions:

- 1) the DAM is connected to a PE simulator;
- 2) CHV1 on the DAM is enabled and three VERIFY CHV1 attempts and ten UNBLOCK CHV1 attempts remain.

#### Test procedure:

- a) the PE simulator resets the DAM;
- b) the PE simulator sends SELECT commands to the DAM to select EF<sub>LCSR</sub> under DF<sub>DECT</sub>;
- c) the PE simulator sends a READ BINARY command using a length of 2 bytes to the DAM;
- d) the PE simulator sends a VERIFY CHV command to the DAM. If the status condition returned by the DAM is SW1='98', SW2='02' then the following steps do not apply;
- e) the PE simulator sends a READ BINARY command using a length of 2 bytes to the DAM;
- f) the PE simulator sends a VERIFY CHV command with **incorrect** CHV1 to the DAM;
- g) the PE simulator sends a STATUS command to the DAM;
- h) the PE simulator sends a VERIFY CHV command to the DAM;



- i) the PE simulator sends a STATUS command to the DAM;
- j) the PE simulator sends a VERIFY CHV command with **incorrect** CHV1 to the DAM;
- k) the PE simulator sends a VERIFY CHV command with **incorrect** CHV1 to the DAM;
- l) the PE simulator resets the DAM;
- m) the PE simulator sends a VERIFY CHV command with **incorrect** CHV1 to the DAM;
- n) the PE simulator resets the DAM;
- o) the PE simulator sends a VERIFY CHV command to the DAM;
- p) the PE simulator sends an UNBLOCK CHV command to the DAM;
- q) the PE simulator sends a DISABLE CHV command to the DAM;
- r) the PE simulator resets the DAM;
- s) the PE simulator sends a VERIFY CHV command to the DAM.

#### **6.5.9.5 Test requirement**

- 1) After steps c), f), j) and k), the status condition returned by the DAM shall be SW1='98', SW2='04' - access condition not fulfilled.
- 2) After step g) the following shall be true of the response data:
  - bits 1 through 4 of byte 19 shall indicate two VERIFY CHV1 attempts remaining.
- 3) After step i) the following shall be true of the response data:
  - bits 1 through 4 of byte 19 shall indicate three VERIFY CHV1 attempts remaining.
- 4) After steps o) and m), the status condition returned by the DAM shall be SW1='98', SW2='40' - CHV blocked.
- 5) After step s) the status condition returned by the DAM shall be SW1='98', SW2='08' - in contradiction with CHV status.

#### **6.5.10 CHANGE CHV function**

##### **6.5.10.1 Definition and applicability**

It shall be mandatory for all cards complying with ETS 300 331 [1] to support all functions described therein.

This test applies to both plug-in and ID-1 DAM cards.

### 6.5.10.2 Conformance requirement

- 1) This function shall assign a new value to the relevant CHV, subject to the following conditions being fulfilled:
  - CHV is not disabled;
  - CHV is not blocked.
- 2) The function shall accept as input, an indication of CHV1/CHV2 and the old and new CHV.
- 3) If the old CHV presented is correct, the number of remaining CHV attempts for that CHV shall be reset to its initial value 3 and the new value for the CHV shall become valid.
- 4) If the old CHV presented is false, the number of remaining CHV attempts for that CHV shall be decremented and the value of the CHV shall remain unchanged.
- 5) After 3 consecutive false CHV presentations, not necessarily in the same card session, the respective CHV shall be blocked and the access condition never fulfilled until the UNBLOCK CHV function has been successfully performed on the respective CHV.

Reference: ETS 300 331 [1], subclauses 8.10, 9.2 and clause 10

Test Group Reference (TGR): TGR\_DAM\_FN

Test Procedure Reference (TPR): TPR\_DAM\_FN\_CHCHV

### 6.5.10.3 Test purpose

To verify that the CHANGE CHV function conforms to the above requirements.

### 6.5.10.4 Method of test

#### Initial conditions:

- 1) the DAM is connected to a PE simulator;
- 2) CHV1 on the DAM is enabled and set to '0000';
- 3) three VERIFY CHV1 attempts and ten UNBLOCK CHV1 attempts remain.

#### Test procedure:

- a) the PE simulator resets the DAM;
- b) the PE simulator sends a CHANGE CHV command with an **incorrect** old CHV1 of '11 11' and new CHV1 of '3333' to the DAM;
- c) the PE simulator sends a STATUS command to the DAM;
- d) the PE simulator sends a CHANGE CHV command with an old CHV1 of '00 00' and new CHV1 of '33 33' to the DAM;
- e) the PE simulator sends a STATUS command to the DAM;
- f) the PE simulator sends a CHANGE CHV command with an **incorrect** old CHV1 of '00 00' and new CHV1 of '55 55' to the DAM;
- g) the PE simulator sends a CHANGE CHV command with an **incorrect** old CHV1 of '00 00' and new CHV1 of '55 55' to the DAM;
- h) the PE simulator resets the DAM;

- i) the PE simulator sends a CHANGE CHV command with an **incorrect** old CHV1 of '00 00' and new CHV1 of '55 55' to the DAM;
- j) the PE simulator resets the DAM;
- k) the PE simulator sends a CHANGE CHV command with an old CHV1 of '33 33' and new CHV1 of '55 55' to the DAM;
- l) the PE simulator sends an UNBLOCK CHV command with CHV1 of '55 55' to the DAM;
- m) the PE simulator sends a DISABLE CHV command to the DAM;
- n) the PE simulator resets the DAM;
- o) the PE simulator sends a CHANGE CHV command with an old CHV1 '55 55' and new CHV1 of '77 77' to the DAM.

#### **6.5.10.5 Test requirement**

- 1) After step b), f), and g), the status condition returned by the DAM shall be SW1='98', SW2='04' - access condition not fulfilled.
- 2) After step c) the following shall be true of the response data:
  - bits 1 through 4 of byte 19 shall indicate two VERIFY CHV1 attempts remaining.
- 3) After step e) the following shall be true of the response data:
  - bits 1 through 4 of byte 19 shall indicate three VERIFY CHV1 attempts remaining.
- 4) After steps i) and k) the status condition returned by the DAM shall be SW1='98', SW2='40' - CHV blocked.
- 5) After step o) the status condition returned by the DAM shall be SW1='98', SW2='08' - in contradiction with CHV status.

#### **6.5.11 DISABLE CHV function**

##### **6.5.11.1 Definition and applicability**

It shall be mandatory for all cards complying with ETS 300 331 [1] to support all functions described therein.

This test applies to both plug-in and ID-1 DAM cards.

#### 6.5.11.2 Conformance requirement

- 1) The successful execution of this function shall have the effect that files protected by the respective CHV are now accessible as if they were marked "ALWAYS".
- 2) The function shall accept as input, an indication of CHV1/CHV2.
- 3) This function shall not be executed by the DAM when the respective CHV is already disabled or blocked.
- 4) If the CHV presented is correct, the number of remaining CHV attempts for that CHV shall be reset to its initial value 3 and that CHV shall be disabled.
- 5) If the CHV presented is false, the number of remaining CHV attempts for that CHV shall be decremented and that CHV shall remain enabled.
- 6) After 3 consecutive false CHV presentations, not necessarily in the same card session, the respective CHV shall be blocked and the access condition never fulfilled until the UNBLOCK CHV function has been successfully performed on the respective CHV.

Reference: ETS 300 331 [1], subclauses 8.11 and 9.2.11

Test Group Reference (TGR): TGR\_DAM\_FN

Test Procedure Reference (TPR): TPR\_DAM\_FN\_DISCHV

#### 6.5.11.3 Test purpose

To verify that the DISABLE CHV function conforms to the above requirements.

#### 6.5.11.4 Method of test

##### Initial conditions:

- 1) the DAM is connected to a PE simulator;
- 2) CHV1 on the DAM is enabled;
- 3) three VERIFY CHV1 attempts and ten UNBLOCK CHV1 attempts remain.

##### Test procedure:

- a) the PE simulator resets the DAM;
- b) the PE simulator sends SELECT commands to the DAM to select EF<sub>LCSR</sub> under DF<sub>DECT</sub>;
- c) the PE simulator sends a READ BINARY command using a length of 2 bytes to the DAM;
- d) the PE simulator sends a DISABLE CHV command with **incorrect** CHV1 to the DAM;
- e) the PE simulator sends a STATUS command to the DAM;
- f) the PE simulator sends a DISABLE CHV command to the DAM;
- g) the PE simulator sends a STATUS command to the DAM;
- h) the PE simulator sends an ENABLE CHV command to the DAM;
- i) the PE simulator sends a READ BINARY command using a length of 2 bytes to the DAM;
- j) the PE simulator sends a DISABLE CHV command with **incorrect** CHV1 to the DAM;
- k) the PE simulator sends a DISABLE CHV command with **incorrect** CHV1 to the DAM;

- l) the PE simulator resets the DAM;
- m) the PE simulator sends a DISABLE CHV command with **incorrect** CHV1 to the DAM;
- n) the PE simulator resets the DAM;
- o) the PE simulator sends a DISABLE CHV command to the DAM;
- p) the PE simulator sends an UNBLOCK CHV command to the DAM;
- q) the PE simulator sends a DISABLE CHV command to the DAM;
- r) the PE simulator sends a DISABLE CHV command to the DAM.

#### **6.5.11.5 Test requirement**

- 1) After steps c), d), j) and k), the status condition returned by the DAM shall be SW1='98', SW2='04' - access condition not fulfilled.
- 2) After step e), the following shall be true of the response data:
  - Bits 1 through 4 of byte 19 shall indicate two VERIFY CHV1 attempts remaining.
- 3) After step g), the following shall be true of the response data:
  - Bits 1 through 4 of byte 19 shall indicate three VERIFY CHV1 attempts remaining.
- 4) After steps m) and o), the status condition returned by the DAM shall be SW1='98', SW2='40' - CHV blocked.
- 5) After step r), the status condition returned by the DAM shall be SW1='98', SW2='08' - in contradiction with CHV status.

#### **6.5.12 ENABLE CHV function**

##### **6.5.12.1 Definition and applicability**

It shall be mandatory for all cards complying with ETS 300 331 [1] to support all functions described therein.

This test applies to both plug-in and ID-1 DAM cards.

##### **6.5.12.2 Conformance requirement**

- 1) The successful execution of this function shall have the effect that files are now protected by the respective CHV.
- 2) The function shall accept as input, an indication of CHV1/CHV2.
- 3) This function shall not be executed by the DAM when the respective CHV is already enabled or blocked.
- 4) If the CHV presented is correct, the number of remaining CHV attempts for that CHV shall be reset to its initial value 3 and that CHV shall be enabled.
- 5) If the CHV presented is false, the number of remaining CHV attempts for that CHV shall be decremented and that CHV shall remain disabled.
- 6) After 3 consecutive false CHV presentations, not necessarily in the same card session, the respective CHV shall be blocked and the access condition never fulfilled until the UNBLOCK CHV function has been successfully performed on the respective CHV.

Reference: ETS 300 331 [1], subclauses 8.12 and 9.2.12

Test Group Reference (TGR): TGR\_DAM\_FN

Test Procedure Reference (TPR): TPR\_DAM\_FN\_ENCHV

### 6.5.12.3 Test purpose

To verify that the ENABLE CHV function conforms to the above requirements.

### 6.5.12.4 Method of test

#### Initial conditions:

- 1) The DAM is connected to a PE simulator;
- 2) CHV1 on the DAM is disabled;
- 3) Three VERIFY CHV1 attempts and ten UNBLOCK CHV1 attempts remain.

#### Test procedure:

- a) the PE simulator resets the DAM;
- b) the PE simulator sends SELECT commands to the DAM to select EF<sub>LCSR</sub> under DF<sub>DECT</sub>;
- c) the PE simulator sends a READ BINARY command using a length of 2 bytes to the DAM;
- d) the PE simulator sends a ENABLE CHV command with **incorrect** CHV1 to the DAM;
- e) the PE simulator sends a STATUS command to the DAM;
- f) the PE simulator sends a ENABLE CHV command to the DAM;
- g) the PE simulator sends a STATUS command to the DAM;
- h) the PE simulator sends a READ BINARY command using a length of 2 bytes to the DAM;
- i) the PE simulator sends a DISABLE CHV command to the DAM;
- j) the PE simulator sends a ENABLE CHV command with **incorrect** CHV1 to the DAM;
- k) the PE simulator sends a ENABLE CHV command with **incorrect** CHV1 to the DAM;
- l) the PE simulator resets the DAM;
- m) the PE simulator sends a ENABLE CHV command with **incorrect** CHV1 to the DAM;
- n) the PE simulator resets the DAM;
- o) the PE simulator sends a ENABLE CHV command to the DAM;
- p) the PE simulator sends an UNBLOCK CHV command to the DAM;
- q) the PE simulator sends a ENABLE CHV command to the DAM;
- r) the PE simulator sends a DISABLE CHV command to the DAM;
- s) the PE simulator sends a ENABLE CHV command to the DAM.

#### 6.5.12.5 Test requirement

- 1) After step e) the following shall be true of the response data:
  - bits 1 through 4 of byte 19 shall indicate two VERIFY CHV1 attempts remaining.
- 2) After step g) the following shall be true of the response data:
  - bits 1 through 4 of byte 19 shall indicate three VERIFY CHV1 attempts remaining.
- 3) After steps d), j) and k), the status condition returned by the DAM shall be SW1='98', SW2='04' - access condition not fulfilled.
- 4) After steps m) and o), the status condition returned by the DAM shall be SW1='98', SW2='40' - CHV blocked.
- 5) After step q) the status condition returned by the DAM shall be SW1='98', SW2='08' - in contradiction with CHV status.

#### 6.5.13 UNBLOCK CHV function

##### 6.5.13.1 Definition and applicability

It shall be mandatory for all cards complying with ETS 300 331 [1] to support all functions described therein.

This test applies to both plug-in and ID-1 DAM cards.

##### 6.5.13.2 Conformance requirement

- 1) This function shall unblock a CHV which has been blocked by 3 consecutive wrong CHV presentations.
- 2) The function shall accept as input, an indication of CHV1/CHV2, the UNBLOCK CHV and the new CHV.
- 3) This function shall be performed regardless of whether or not the relevant CHV is blocked.
- 4) If the UNBLOCK CHV presented is correct, the new CHV value, presented together with the UNBLOCK CHV is stored in the relevant EFCHV, the number of remaining UNBLOCK CHV attempts for that UNBLOCK CHV is reset to its initial value 10 and the number of remaining CHV attempts for that CHV is reset to its initial value 3.
- 5) After a successful unblocking attempt, the CHV shall be enabled, and the relevant access condition level satisfied.
- 6) If the presented UNBLOCK CHV is false, the number of remaining UNBLOCK CHV attempts for that UNBLOCK CHV shall be decremented.
- 7) After 10 consecutive false UNBLOCK CHV presentations, not necessarily in the same card session, the respective UNBLOCK CHV shall be blocked.
- 8) A false UNBLOCK CHV shall have no effect on the status of the respective CHV itself.

Reference: ETS 300 331 [1], subclauses 8.13 and 9.2.13

Test Group Reference (TGR): TGR\_DAM\_FN

Test Procedure Reference (TPR): TPR\_DAM\_FN\_UNCHV

##### 6.5.13.3 Test purpose

To verify that the UNBLOCK CHV function conforms to the above requirements.

#### 6.5.13.4 Method of test

##### Initial conditions:

- 1) the DAM is connected to a PE simulator;
- 2) CHV1 on the DAM is enabled;
- 3) three VERIFY CHV1 attempts and ten UNBLOCK CHV1 attempts remain.

##### Test procedure:

- a) the PE simulator resets the DAM;
- b) the PE simulator sends SELECT commands to the DAM to select  $EF_{LCSR}$  under  $DF_{DECT}$ ;
- c) the PE simulator sends a VERIFY CHV command to the DAM;
- d) the PE simulator sends an UNBLOCK CHV command with **incorrect** UNBLOCK CHV1 and CHV1 to the DAM;
- e) the PE simulator sends a STATUS command to the DAM;
- f) the PE simulator sends a READ BINARY command using a length of 2 bytes to the DAM;
- g) the PE simulator sends a DISABLE CHV command to the DAM;
- h) the PE simulator sends an UNBLOCK CHV command to the DAM;
- i) the PE simulator sends a STATUS command to the DAM;
- j) the PE simulator sends a READ BINARY command using a length of 2 bytes to the DAM;
- k) the PE simulator sends an UNBLOCK CHV command to the DAM.

#### 6.5.13.5 Test requirement

- 1) After step d), the status condition returned by the DAM shall be SW1='98', SW2='04' - access condition not fulfilled.
- 2) After step e) the following shall be true of the response data:
  - bit 8 of byte 14 shall be 0 indicating that CHV1 is enabled;
  - bits 1 through 4 of byte 19 shall indicate three VERIFY CHV1 attempts remaining;
  - bits 1 through 4 of byte 20 shall indicate nine UNBLOCK CHV1 attempts remaining.
- 3) After step i) the following shall be true of the response data:
  - bit 8 of byte 14 shall be 0 indicating that CHV1 is enabled;
  - bits 1 through 4 of byte 19 shall indicate three VERIFY CHV1 attempts remaining;
  - bits 1 through 4 of byte 20 shall indicate ten UNBLOCK CHV1 attempts remaining.



## 6.5.14 INVALIDATE function

### 6.5.14.1 Definition and applicability

It shall be mandatory for all cards complying with ETS 300 331 [1] to support all functions described therein.

This test applies to both plug-in and ID-1 DAM cards.

### 6.5.14.2 Conformance requirement

- 1) This function shall invalidate the current EF.
- 2) After an INVALIDATE function the respective flag in the file status shall be changed accordingly.
- 3) The function shall only be performed if the INVALIDATE access condition for the current EF is satisfied.
- 4) An invalidated file shall no longer be available within the application for any function except for the SELECT and REHABILITATE functions.
- 5) The function READ may be performed when "readable when invalidated" is indicated in the file status.

Reference: ETS 300 331 [1], subclauses 8.14 and 9.2.14

Test Group Reference (TGR): TGR\_DAM\_FN

Test Procedure Reference (TPR): TPR\_DAM\_FN\_INVALID

### 6.5.14.3 Test purpose

To verify that the INVALIDATE function conforms to the above requirements.

### 6.5.14.4 Method of test

#### Initial conditions:

- 1) The DAM is connected to a PE simulator;
- 2) EF<sub>AC</sub> on the DAM is not invalidated.

#### Test procedure:

- a) The PE simulator resets the DAM;
- b) The PE simulator sends SELECT commands to the DAM to select EF<sub>LCSR</sub> under DF<sub>DECT</sub>;
- c) The PE simulator sends an INVALIDATE command to the DAM;
- d) The PE simulator gains the security access condition(s) specified by the administrative authority for both INVALIDATE and REHABILITATE on EF<sub>AC</sub>;
- e) The PE simulator sends a SELECT command to the DAM to select EF<sub>AC</sub> once more;
- f) The PE simulator sends a GET RESPONSE command to the DAM;
- g) The PE simulator sends an INVALIDATE command to the DAM;
- h) The PE simulator sends a SELECT command to the DAM to select EF<sub>AC</sub> again;
- i) The PE simulator sends a GET RESPONSE command to the DAM;

- j) The PE simulator sends a VERIFY CHV command to the DAM;
- k) The PE simulator sends a UPDATE BINARY command using a length of 1 byte and data 'C1' to the DAM;
- l) The PE simulator sends an INVALIDATE command to the DAM;
- m) The PE simulator sends a READ RECORD command to the DAM with mode FIRST and length of 5 bytes;
- n) The PE simulator sends a REHABILITATE command to the DAM.

#### 6.5.14.5 Test requirement

- 1) After step c) the status condition returned by the DAM shall be SW1='98', SW2='04' - access condition not fulfilled.  
  
NOTE: The assumption is made that the access condition is not ALW.
- 2) After step f) the following shall be true of the response data:
  - bit 1 of byte 12 shall be 1 indicating that the file is **not** invalidated.
- 3) After step i) the following shall be true of the response data:
  - bit 1 of byte 12 shall be 1 indicating that the file **is** invalidated.
- 4) After steps k) and l) the status condition returned by the DAM shall be SW1='98', SW2='10' - in contradiction with invalidation status.
- 5) After step m), if bit 2 of byte 12 in the response data after step f) and i) is set to '1' then the status condition returned by the DAM shall be SW1='98', SW2='10', in contradiction with invalidation status. Otherwise, the DAM shall return the data of the first record in EF<sub>AC</sub>.

#### 6.5.15 REHABILITATE function

##### 6.5.15.1 Definition and applicability

It shall be mandatory for all cards complying with ETS 300 331 [1] to support all functions described therein.

This test applies to both plug-in and ID-1 DAM cards.

##### 6.5.15.2 Conformance requirement

- 1) This function shall rehabilitate an invalidated current EF.
- 2) After a REHABILITATE function the respective flag in the file status byte shall be changed accordingly.
- 3) The function shall only be performed if the REHABILITATE access condition for the current EF is satisfied.

Reference: ETS 300 331 [1], subclauses 8.15 and 9.2.15

Test Group Reference (TGR): TGR\_DAM\_FN

Test Procedure Reference (TPR): TPR\_DAM\_FN\_REHAB

##### 6.5.15.3 Test purpose

To verify that the REHABILITATE function conforms to the above requirements.

#### 6.5.15.4 Method of test

##### Initial conditions:

- 1) the DAM is connected to a PE simulator;
- 2) EF<sub>AC</sub> on the DAM is invalidated.

##### Test procedure:

- a) the PE simulator resets the DAM;
- b) the PE simulator sends SELECT commands to the DAM to select EF<sub>AC</sub> under DF<sub>DECT</sub>;
- c) the PE simulator sends a REHABILITATE command to the DAM;
- d) the PE simulator gains the security access condition(s) specified by the administrative authority for both INVALIDATE and REHABILITATE on EF<sub>AC</sub>;
- e) the PE simulator sends a SELECT command to the DAM to select EF<sub>AC</sub> once more;
- f) the PE simulator sends a GET RESPONSE command to the DAM;
- g) the PE simulator sends a REHABILITATE command to the DAM;
- h) the PE simulator sends a SELECT command to the DAM to select EF<sub>AC</sub> again;
- i) the PE simulator sends a GET RESPONSE command to the DAM;
- j) the PE simulator sends a VERIFY CHV command to the DAM;
- k) the PE simulator sends a UPDATE BINARY command using a length of 1 byte and data 'D1' to the DAM.

#### 6.5.15.5 Test requirement

- 1) After step c) the status condition returned by the DAM shall be SW1='98', SW2='04' - access condition not fulfilled.

NOTE: The assumption is made that the access condition is not ALW.

- 2) After step f) the following shall be true of the response data:
  - bit 1 of byte 12 shall be 1 indicating that the file is invalidated.
- 3) After step i) the following shall be true of the response data:
  - bit 1 of byte 12 shall be 1 indicating that the file is no longer invalidated.

#### 6.5.16 ASK RANDOM function

##### 6.5.16.1 Definition and applicability

It shall be mandatory for all cards complying with ETS 300 331 [1] to support all functions described therein.

This test applies to both plug-in and ID-1 DAM cards.

**6.5.16.2 Conformance requirement**

- 1) This function shall cause the DAM to return a random number.
- 2) The random number returned shall be used in the subsequent FT AUTHENTICATION command.

Reference: ETS 300 331 [1], subclauses 8.16. and 9.2.16

Test Group Reference (TGR): TGR\_DAM\_FN

Test Procedure Reference (TPR): TPR\_DAM\_FN\_RAND

**6.5.16.3 Test purpose**

To verify that the DAM conforms to the above requirements.

NOTE: CR2 is tested in subclause 6.5.18, "FT AUTHENTICATION function".

**6.5.16.4 Method of test**

**Initial conditions:**

- 1) the DAM is connected to a PE simulator.

**Test procedure:**

- a) the PE simulator resets the DAM;
- b) the PE simulator sends one hundred ASK RANDOM commands to the DAM in sequence.

**6.5.16.5 Test requirement**

- 1) After step b) the hundred random numbers returned shall be random.

**6.5.17 PT AUTHENTICATION function**

**6.5.17.1 Definition and applicability**

It shall be mandatory for all cards complying with ETS 300 331 [1] to support all functions described therein.

This function is employed by the PE during the authentication of a PT mechanism by the FT to authenticate the DAM when placed in the PE with respect to a selected subscription registration.

This test applies to both plug-in and ID-1 DAM cards.

#### 6.5.17.2 Conformance requirement

- 1) When the PE sends a PT AUTHENTICATION command to the DAM, the DAM shall run the specified algorithm and reply with RES1, DCK and, if calculated, the ZAP.
- 2) The function shall accept as input, a key number, algorithm identifier, INC, RS and RAND\_F.
- 3) The function shall not be executable unless a DF<sub>SR</sub> has been selected as the current directory and a successful CHV1 verification procedure has been performed.
- 4) A key file shall be selected before executing the PT AUTHENTICATION function.

Reference: ETS 300 331 [1], subclauses 8.17, 9.2.17, 7.2.1 and 11.4.1.

Test Group Reference (TGR): TGR\_DAM\_FN

Test Procedure Reference (TPR): TPR\_DAM\_FN\_PTA

#### 6.5.17.3 Test purpose

To verify that the PT AUTHENTICATION function conforms to the above requirements.

#### 6.5.17.4 Method of test

##### Initial conditions:

- 1) the DAM is connected to a PE simulator.

##### Test procedure:

- a) the PE simulator resets the DAM;
- b) the PE simulator selects DF<sub>DECT</sub> as defined in subclause 4.4;
- c) the PE simulator send a SELECT command to the DAM to select DF<sub>SR1</sub> under DF<sub>DECT</sub>;
- d) the PE simulator gains CHV1 security access;
- e) the PE simulator sends a SELECT command to the DAM to select EF<sub>UAK</sub>;
- f) the PE simulator sends a PT AUTHENTICATION command to the DAM containing valid data, including a key number, an algorithm identifier, INC, RS and RAND\_F;
- g) the PE simulator sends a GET RESPONSE command to the DAM;
- h) the PE simulator resets the DAM;
- i) the PE simulator selects DF<sub>DECT</sub> as defined in subclause 4.4;
- j) the PE simulator sends a SELECT command to the DAM to select DF<sub>SR1</sub>;
- k) the PE simulator gains CHV1 security access;
- l) the PE simulator sends a SELECT command to the DAM to select EF<sub>AC</sub>;
- m) the PE simulator sends a PT AUTHENTICATION command to the DAM using valid data, including a key number, an algorithm identifier, INC, RS and RAND\_F;
- n) the PE simulator sends a GET RESPONSE command to the DAM;
- o) the PE simulator resets the DAM;
- p) the PE simulator selects DF<sub>DECT</sub> as defined in subclause 4.4;

- q) the PE simulator sends a SELECT command to the DAM to select DF<sub>SR1</sub>;
- r) the PE simulator sends a PT AUTHENTICATION command to the DAM using valid data, including a key number, an algorithm identifier, INC, RS and RAND\_F;
- s) the PE simulator sends a SELECT command to the DAM to select EF<sub>AC</sub>;
- t) the PE simulator sends a PT AUTHENTICATION command to the DAM using valid data, including a key number, an algorithm identifier, INC, RS and RAND\_F;
- u) the PE simulator resets the DAM;
- v) the PE simulator sends a SELECT command to the DAM to select the MF;
- w) the PE simulator gains CHV1 security access;
- x) the PE simulator sends a PT AUTHENTICATION command to the DAM using valid data, including a key number, an algorithm identifier, INC, RS and RAND\_F.

#### 6.5.17.5 Test requirement

- 1) After step g) the DAM shall have sent RES1, DCK and, if calculated, the ZAP to the PE simulator. The following shall be true of the response data:
  - bytes 1 to 4 shall contain RES1;
  - bytes 5 to 12 shall contain DCK;
  - if calculated, byte 13 shall contain ZAP.
- 2) After step n) the DAM shall have sent RES1, DCK and, if calculated, the ZAP to the PE simulator. The following shall be true of the response data:
  - bytes 1 to 4 shall contain RES1;
  - bytes 5 to 12 shall contain DCK;
  - if calculated, byte 13 shall contain ZAP.
- 3) After step r), the status condition returned by the DAM shall be SW1='94', SW2='08' - file type is inconsistent with the command.
- 4) After step t) the status condition returned by the DAM shall be SW1='98', SW2='04' - access condition not fulfilled, authentication failed.
- 5) After step x) the status condition returned by the DAM shall be SW1='98', SW2='04' - authentication failed.

#### 6.5.18 FT AUTHENTICATION function

##### 6.5.18.1 Definition and applicability

It shall be mandatory for all cards complying with ETS 300 331 [1] to support all functions described therein.

This function is employed by the PE during the authentication of a FT mechanism by the DAM to authenticate the FT with respect to the selected registration in the DAM.

This test applies to both plug-in and ID-1 DAM cards.

### 6.5.18.2 Conformance requirement

- 1) When the PE sends an FT AUTHENTICATION command to the DAM, the DAM shall run the specified algorithm to produce an authentication parameter XRES2 which it will compare with RES2, which it obtained in the FT AUTHENTICATION command.
- 2) FT authentication shall only be successful if the verification by the DAM is positive.
- 3) The function shall accept as input, a key number, algorithm identifier, RS and RES2.
- 4) The ASK RANDOM function shall immediately precede the FT AUTHENTICATION function.
- 5) A key file shall be selected before executing the FT AUTHENTICATION function.

Reference: ETS 300 331 [1], subclauses 8.18, 9.2.18, 7.2.2 and 11.4.2.

Test Group Reference (TGR): TGR\_DAM\_FN

Test Procedure Reference (TPR): TPR\_DAM\_FN\_FTA

### 6.5.18.3 Test purpose

To verify that the FT AUTHENTICATION function conforms to the above requirements.

### 6.5.18.4 Method of test

#### Initial conditions:

- 1) the DAM is connected to a PE simulator.

#### Test procedure:

- a) the PE simulator resets the DAM;
- b) the PE simulator selects DF<sub>DECT</sub> as defined in subclause 4.4;
- c) the PE simulator sends a SELECT command to the DAM to select DF<sub>SR1</sub>;
- d) the PE simulator gains CHV1 security access;
- e) the PE simulator sends a SELECT command to the DAM to select EF<sub>IPUI</sub>;
- f) the PE simulator sends a READ BINARY command to the DAM to read all data in EF<sub>IPUI</sub>;
- g) the PE simulator sends an UPDATE BINARY command to the DAM to update all bytes in EF<sub>IPUI</sub> with the actual data read in step f);
- h) the PE simulator sends a SELECT command to the DAM to select EF<sub>SR</sub>;
- i) the PE simulator sends a GET RESPONSE command to the DAM;

NOTE: This is to determine the size of EF<sub>SR</sub>;

- j) the PE simulator sends a READ BINARY command to the DAM to read all data in EF<sub>SR</sub>;
- k) the PE simulator sends an ASK RANDOM command to the DAM;
- l) the PE simulator sends an FT AUTHENTICATION command to the DAM containing random data for the key number, algorithm identifier, RS and RES2 parameters;
- m) the PE simulator sends a SELECT command to the DAM to select EF<sub>UAK</sub>;

- n) the PE simulator sends an FT AUTHENTICATION command to the DAM containing random data for the key number, algorithm identifier, RS and RES2 parameters;
- o) the PE simulator sends an ASK RANDOM command to the DAM;
- p) the PE simulator sends an FT AUTHENTICATION command to the DAM containing valid data, including a key number, an algorithm identifier, RS and RES2;
- q) the PE simulator sends a SELECT command to the DAM to select EF<sub>IPUI</sub>;
- r) the PE simulator sends an UPDATE BINARY command to the DAM to update all bytes in EF<sub>IPUI</sub> with the actual data read in step f);
- s) repeat steps a) to p), but this time select EF<sub>AC</sub> instead of EF<sub>UAK</sub>, in step k).

#### 6.5.18.5 Test requirement

- 1) After step g) the status condition returned by the DAM shall be SW1='98', SW2='04' - access condition not fulfilled, authentication failed.
- 2) After step l), the status condition returned by the DAM shall be SW1='94', SW2='08' - file type is inconsistent with the command.
- 3) After step n) the status condition returned by the DAM shall be SW1='98', SW2='35' - ASK RANDOM has not been executed.
- 4) After step o) the DAM shall have sent RAND\_P to the PE simulator. The following shall be true of the response data:
  - bytes 1 to 8 shall contain RAND\_P.

#### 6.5.19 USER AUTHENTICATION function

##### 6.5.19.1 Definition and applicability

It shall be mandatory for all cards complying with ETS 300 331 [1] to support all functions described therein.

This function is employed by the PE during the user authentication mechanism by the FT to authenticate the DAM when placed in the PE with respect to the selected registration.

This test applies to both plug-in and ID-1 DAM cards.

##### 6.5.19.2 Conformance requirement

- 1) When the PE sends a USER AUTHENTICATION command to the DAM, the DAM shall run the specified algorithm and reply with RES1 and DCK.
- 2) The function shall accept as input, a key number, algorithm identifier, RS, RAND\_F and UPI.
- 3) A key file shall be selected before executing the USER AUTHENTICATION function.

Reference: ETS 300 331 [1], subclauses 8.19, 9.2.19, 7.2.3 and 11.4.3.

Test Group Reference (TGR): TGR\_DAM\_FN

Test Procedure Reference (TPR): TPR\_DAM\_FN\_USRA

##### 6.5.19.3 Test purpose

To verify that the USER AUTHENTICATION function conforms to the above requirements.



#### 6.5.19.4 Method of test

##### Initial conditions:

- 1) the DAM is connected to a PE simulator.

##### Test procedure:

- a) the PE simulator resets the DAM;
- b) the PE simulator selects  $DF_{DECT}$  as defined in subclause 4.4;
- c) the PE simulator sends a SELECT command to the DAM to select  $DF_{SR1}$ ;
- d) the PE simulator sends a USER AUTHENTICATION command to the DAM containing valid data, including a key number, an algorithm identifier, RS, RAND\_F and UPI;
- e) the PE simulator sends a SELECT command to the DAM to select  $EF_{UAK}$ ;
- f) the PE simulator sends a USER AUTHENTICATION command to the DAM containing valid data, including a key number, an algorithm identifier, RS, RAND\_F and UPI;
- g) the PE simulator sends a GET RESPONSE command to the DAM.

#### 6.5.19.5 Test requirement

- 1) After step d), the status condition returned by the DAM shall be SW1='94', SW2='08' - file type is inconsistent with the command.
- 2) After step g) the DAM shall have sent RES1 and DCK to the PE simulator. The following shall be true of the response data:
  - bytes 1 to 4 shall contain RES1;
  - bytes 5 to 12 shall contain DCK.

#### 6.5.20 UAK ALLOCATION function

##### 6.5.20.1 Definition and applicability

It shall be mandatory for all cards complying with ETS 300 331 [1] to support all functions described therein.

This function is employed by the PE during the UAK allocation mechanism for the initial allocation of a UAK for a selected registration.

This test applies to both plug-in and ID-1 DAM cards.

#### 6.5.20.2 Conformance requirement

- 1) When the PE sends a UAK ALLOCATION command to the DAM, the DAM shall run the specified algorithm and produce an authentication parameter XRES2 and the UAK.
- 2) The DAM shall compare XRES2 with RES2, which it obtained in the UAK ALLOCATION command. If the two values are equal, the UAK is stored in EF<sub>UAK</sub> under the UAK number identified in the UAK ALLOCATION command.
- 3) The function shall accept as input, a key number, UAK number, algorithm identifier, RS and RES2.
- 4) The function shall not be executable unless a successful PT authentication procedure has already been performed.
- 5) A key file shall be selected before executing the UAK ALLOCATION function.

Reference: ETS 300 331 [1], subclauses 8.20, 9.2.20, 7.3 and 11.5.

Test Group Reference (TGR): TGR\_DAM\_FN

Test Procedure Reference (TPR): TPR\_DAM\_FN\_UAK

#### 6.5.20.3 Test purpose

To verify that the UAK ALLOCATION function conforms to the above requirements.

#### 6.5.20.4 Method of test

##### Initial conditions:

- 1) the DAM is connected to a PE simulator;
- 2) the DAM supports the authentication algorithm and contains the AC which are identified in the Allocation-type element in the KEY-ALLOCATE message.

##### Test procedure:

- a) the PE simulator resets the DAM;
- b) the PE simulator selects DF<sub>DECT</sub> as defined in subclause 4.4;
- c) the PE simulator sends a SELECT command to the DAM to select DF<sub>SR1</sub>;
- d) the PE simulator sends a SELECT command to the DAM to select EF<sub>SR</sub>;
- e) the PE simulator sends a GET RESPONSE command to the DAM;  
NOTE 1: This is to determine the size of EF<sub>SR</sub>.
- f) the PE simulator sends a READ BINARY command to the DAM to read all data in EF<sub>SR</sub>;
- g) the PE simulator sends an UAK ALLOCATION command to the DAM containing random data for the key number, UAK number, algorithm identifier, RS and RES2 parameters;
- h) the PE simulator sends a SELECT command to the DAM to select EF<sub>AC</sub>;
- i) the PE simulator sends an UAK ALLOCATION command to the DAM containing valid data for the key number, UAK number, algorithm identifier, RS and RES2 parameters;
- j) the PE simulator resets the DAM;
- k) the PE simulator selects DF<sub>DECT</sub> as defined in subclause 4.4;

- l) the PE simulator sends a SELECT command to the DAM to select DF<sub>SR1</sub>;
- m) the PE simulator sends a SELECT command to the DAM to select EF<sub>SR</sub>;
- n) the PE simulator sends a GET RESPONSE command to the DAM;  
NOTE 2: This is to determine the size of EF<sub>SR</sub>.
- o) the PE simulator sends a READ BINARY command to the DAM to read all data in EF<sub>SR</sub>;
- p) the PE simulator sends a SELECT command to the DAM to select EF<sub>AC</sub>;
- q) the PE simulator sends a PT AUTHENTICATION command to the DAM using valid data, including a key number, an algorithm identifier, INC, RS and RAND<sub>F</sub>;
- r) the PE simulator sends a GET RESPONSE command to the DAM;
- s) the PE simulator sends an ASK RANDOM command to the DAM;
- t) the PE simulator sends a UAK ALLOCATION command to the DAM using valid data, including a key number, UAK number, an algorithm identifier, INC, RS and RES2.

#### 6.5.20.5 Test requirement

- 1) After step g), the status condition returned by the DAM shall be SW1='94', SW2='08' - file type is inconsistent with the command.
- 2) After step i) the status condition returned by the DAM shall be SW1='98', SW2='04' - access condition not fulfilled, authentication failed.
- 3) After step r) the DAM shall have sent RES1, DCK and, if calculated, the ZAP to the PE simulator. The following shall be true of the response data:
  - bytes 1 to 4 shall contain RES1;
  - bytes 5 to 12 shall contain DCK;
  - if calculated, byte 13 shall contain ZAP.
- 4) After step s) the DAM shall have sent RAND<sub>P</sub> to the PE simulator. The following shall be true of the response data:
  - bytes 1 to 8 shall contain RAND<sub>P</sub>.
- 5) After step t) the DAM shall have stored the new UAK in EF<sub>UAK</sub> under the UAK number identified in the UAK ALLOCATION command.

#### 6.6 Description of the commands

The tests in this subclause ensure that the IUT conforms to the specification for the mapping of functions onto Application Protocol Data Units (APDUs) which are used by the transmission protocol.

## 6.6.1 Mapping principles

### 6.6.1.1 Definition and applicability

The transmission protocol requires that the command and response Application Protocol Data Units (APDUs) are mapped using certain principles, in order to ensure correct operation in the DECT environment.

NOTE: The testing of the commands do only follow the normal path, and some specific error conditions. To ensure proper execution of the commands under all circumstances especially under more specific error conditions, the DAM should be tested for this too. For the time being no relevant test document for this purpose exists.

This test applies to both plug-in and ID-1 DAM cards.

### 6.6.1.2 Conformance requirement

- 1) The command APDU shall have format (CLA, INS, P1, P2, P3 {, data}).
- 2) The response APDU shall have format ({data,} SW1, SW2).
- 3) The class of instruction (CLA) shall be in the range 'A0' - 'A3'.

Reference: ETS 300 331 [1], subclause 9.1.

Test Group Reference (TGR): TGR\_DAM\_CMD\_MAP

Test Procedure Reference (TPR): TPR\_DAM\_CMD\_MAP

### 6.6.1.3 Test purpose

To verify that the DAM conforms to the above requirements.

### 6.6.1.4 Method of test

#### Initial conditions:

- 1) the DAM is connected to a PE simulator.

#### Test procedure:

- a) the PE simulator resets the DAM;
- b) the PE simulator selects  $DF_{DECT}$  as defined in subclause 4.4;
- c) the PE simulator gains the security access condition(s) specified by the administrative authority for both INVALIDATE and REHABILITATE on  $EF_{DCK}$ ;
- d) the PE simulator sends a STATUS command to the DAM.

[bytes sent: CLA='A0', INS='F2', P1='00', P2='00', P3='00'];

[bytes received: SW1, SW2<sub>0</sub>];

- e) the PE simulator sends a GET RESPONSE command to the DAM.

[bytes sent: CLA='A0', INS='C0', P1='00', P2='00', P3=SW2<sub>0</sub>];

[bytes received: data, SW1, SW2];

- f) the PE simulator sends a VERIFY CHV command to the DAM:  
[bytes sent: CLA='A0', INS='20', P1='00', P2='01', P3='08', data=valid CHV1 code];  
[bytes received: SW1, SW2];
- g) the PE simulator sends a SELECT command to the DAM to select EF<sub>DCK</sub>:  
[bytes sent: CLA='A0', INS='A4', P1='00', P2='00', P3='02', data='6F 82'];  
[bytes received: SW1, SW2<sub>1</sub>];
- h) the PE simulator sends a GET RESPONSE command to the DAM, requesting all of the available response data, as indicated by SW2<sub>1</sub>:  
[bytes sent: CLA='A0', INS='C0', P1='00', P2='00', P3=SW2<sub>1</sub>];  
[bytes received: data, SW1, SW2];
- i) the PE simulator sends a READ BINARY command to the DAM to read all 8 bytes:  
[bytes sent: CLA='A0', INS='B0', P1='00', P2='00', P3='08'];  
[bytes received: data, SW1, SW2];
- j) the PE simulator sends an UPDATE BINARY command to the DAM to update EF<sub>DCK</sub> with the 8 bytes read in step g):  
[bytes sent: CLA='A0', INS='D6', P1='00', P2='00', P3='08', data];  
[bytes received: SW1, SW2];
- k) the PE simulator sends the following five command APDUs in sequence, where CLA='A0', 'A1', 'A2' then 'A3':  
[bytes sent: CLA, INS='00', P1='00', P2='00', P3='00'];  
[bytes received: SW1, SW2];
- l) the PE simulator sends an INVALIDATE command to the DAM:  
[bytes sent: CLA='A0', INS='04', P1='00', P2='00', P3='00'];  
[bytes received: SW1, SW2];
- m) the PE simulator sends a REHABILITATE command to the DAM:  
[bytes sent: CLA='A0', INS='44', P1='00', P2='00', P3='00'];  
[bytes received: SW1, SW2].

#### 6.6.1.5 Test requirement

- 1) After step d), the DAM shall have sent SW1='9F' and SW2='lgth'.
- 2) After step e), the DAM shall have sent 'lgth' bytes followed by SW1='90' and SW2='00'.
- 3) After step g), the DAM shall have sent SW1='9F' and SW2='lgth'.
- 4) After step h), the DAM shall have sent 'lgth' bytes followed by SW1='90' and SW2='00'.
- 5) After step i), the DAM shall have sent 8 bytes followed by SW1='90' and SW2='00'.
- 6) After step j), the DAM shall have sent SW1='98' and SW2='04'.
- 7) After step k), the DAM shall have sent SW1='6D' and SW2='XX'.
- 8) After steps l) and m), the DAM shall have sent SW1='90' and SW2='00'.

#### 6.6.2 Coding of the commands

The test procedures defined in subclause 6.5 of this ETS, intrinsically test most the coding of the associated commands. Therefore, test purposes exist in this subclause only to cover areas of testing not already covered by subclause 6.5.

##### 6.6.2.1 SELECT command

###### 6.6.2.1.1 Definition and applicability

It shall be mandatory for all cards complying with ETS 300 331 [1] to support all functions described therein.

This test applies to both plug-in and ID-1 DAM cards.

###### 6.6.2.1.2 Conformance requirement

- 1) The SELECT command shall provide the response data described in ETS 300 331 [1], subclause 9.2.1.

Reference: ETS 300 331 [1], subclause 9.2.1.

Test Group Reference (TGR): TGR\_DAM\_CMD

Test Procedure Reference (TPR): TPR\_DAM\_CMD\_SEL

###### 6.6.2.1.3 Test purpose

To verify that the coding of the SELECT command conforms to the above requirements.

#### 6.6.2.1.4 Method of test

##### Initial conditions:

- 1) the DAM is connected to a PE simulator.

##### Test procedure:

- a) the PE simulator resets the DAM;
- b) the PE simulator sends a SELECT command to the DAM to select MF:  
[bytes sent: CLA='A0', INS='A4', P1='00', P2='00', P3='02', data='3F 00'];  
[bytes received: SW1, SW2<sub>1</sub>];
- c) the PE simulator sends a GET RESPONSE command to the DAM:  
[bytes sent: CLA='A0', INS='C0', P1='00', P2='00', P3=SW2<sub>1</sub>];  
[bytes received: data, SW1, SW2];
- d) the PE simulator selects DF<sub>DECT</sub> as defined in subclause 4.4;
- e) the PE simulator sends SELECT commands to the DAM to select DF<sub>SR1</sub>:  
[example bytes sent: CLA='A0', INS='A4', P1='00', P2='00', P3='02', data='7F 70'];  
[bytes received: SW1, SW2<sub>2</sub>];
- f) the PE simulator sends a GET RESPONSE command to the DAM:  
[bytes sent: CLA='A0', INS='C0', P1='00', P2='00', P3=SW2<sub>2</sub>];  
[bytes received: data, SW1, SW2];
- g) the PE simulator sends a SELECT command to the DAM to select EF<sub>PARK</sub>:  
[bytes sent: CLA='A0', INS='A4', P1='00', P2='00', P3='02', data='6F 12'];  
[bytes received: SW1, SW2<sub>3</sub>];
- h) the PE simulator sends a GET RESPONSE command to the DAM:  
[bytes sent: CLA='A0', INS='C0', P1='00', P2='00', P3=SW2<sub>3</sub>];  
[bytes received: data, SW1, SW2];
- i) the PE simulator sends a SELECT command to the DAM to select EF<sub>UAK</sub>:  
[bytes sent: CLA='A0', INS='A4', P1='00', P2='00', P3='02', data='6F 22'];  
[bytes received: SW1, SW2<sub>4</sub>];
- j) the PE simulator sends a GET RESPONSE command to the DAM:  
[bytes sent: CLA='A0', INS='C0', P1='00', P2='00', P3=SW2<sub>4</sub>];  
[bytes received: data, SW1, SW2];
- k) the PE simulator selects the relevant EF<sub>CHV1</sub> as defined in subclause 4.4;
- l) the PE simulator sends a SELECT command to the DAM to re-select EF<sub>CHV1</sub>:

[bytes sent: CLA='A0', INS='A4', P1='00', P2='00', P3='02', data='00 00'];

[bytes received: SW1, SW2<sub>5</sub>];

m) the PE simulator sends a GET RESPONSE command to the DAM:

[bytes sent: CLA='A0', INS='C0', P1='00', P2='00', P3=SW2<sub>5</sub>];

[bytes received: data, SW1, SW2].

#### 6.6.2.1.5 Test requirement

1) After step c) the following shall be true of the response data:

- bytes 3 and 4 shall contain information about the total memory amount under the MF that is not allocated by any of the DFs or EFs under the MF;
- bytes 5 and 6 shall contain the file ID for the MF, '3F 00';
- byte 7 shall contain '01' for MF;
- bytes 9 - 11 shall give the access conditions for the MF;
- byte 12 shall contain the binary code X000001Y, where X indicates the frequency required for running the authentication algorithm, and Y gives the invalidation status, which should be 1 otherwise the card has become mute;
- byte 13 shall give the number of bytes that follow in the response information;
- byte 14 shall give the current directory characteristics as specified in ETS 300 331 [1];
- byte 15 shall indicate the correct number of DFs which are a direct child of the MF;
- byte 16 shall indicate the correct number of EFs which are a direct child of the MF;
- bytes 19 - 22 shall give information about the CHVs under the MF. For details see ETS 300 331 [1].

2) After step f) the following shall be true of the response data:

- bytes 3 and 4 shall contain information about the total memory amount under DF<sub>DECT</sub> that is not allocated by any of the DFs or EFs under DF<sub>DECT</sub>;
- bytes 5 and 6 shall contain the file ID for DF<sub>DECT</sub>. The recommended value is '7F 50';
- byte 7 shall contain '02' for DF or '03' in a multi-application card indicating that an ASC is linked to the application;
- bytes 9 - 11 shall give the access conditions for DF<sub>DECT</sub>;
- byte 12 shall contain the binary code X000001Y, where X indicates the frequency required for running the authentication algorithm and Y gives the invalidation status which should be 1 otherwise the card has become mute;
- byte 13 shall give the number of bytes that follow in the response information;
- byte 15 shall indicate the correct number of DFs which are a direct child of DF<sub>DECT</sub>;
- byte 16 shall indicate the correct number of EFs which are a direct child of DF<sub>DECT</sub>;
- bytes 19 - 22 shall give information about the CHVs under DF<sub>DECT</sub>. For details see ETS 300 331 [1].



- 3) After step h) the following shall be true of the response data:
- bytes 3 and 4 shall contain information about the file size for EF<sub>PARK</sub>. The size shall be at least 6 and shall always be divisible by 6;
  - bytes 5 and 6 shall contain the file ID for EF<sub>PARK</sub> '6F 12';
  - byte 7 shall contain '04' for EF;
  - bytes 9 - 11 shall give the access conditions for EF<sub>PARK</sub>. Byte 9 shall have the value '14' and byte 10 the value '00';
  - byte 12 shall contain the binary code 000000XY, where X indicates whether it is possible to read the file when it is invalidated, and Y gives the invalidation status, which should be 1 otherwise the subscription is not valid;
  - byte 13 shall give the number of bytes that follow in the response information;
  - byte 14 gives the structure of the EF and in this case it shall contain '00' indicating transparent structure;
  - byte 15, if present, shall be '00'.
- 4) After step j) the following shall be true of the response data:
- bytes 3 and 4 shall contain information about the file size for EF<sub>UAK</sub>. The size shall be at least 17 and at most 136 and shall always be divisible by 17;
  - bytes 5 and 6 shall contain the file ID for EF<sub>UAK</sub>, '6F 22';
  - byte 7 shall contain '04' for EF;
  - bytes 9 - 11 shall give the access conditions for EF<sub>UAK</sub>. Byte 9 shall have the value 'FF' and byte 10 the value '00';
  - byte 12 shall contain the binary code 000000XY, where X indicates whether it is possible to read the file when it is invalidated, and Y gives the invalidation status, which should be 1 otherwise the subscription is not valid;
  - byte 13 shall give the number of bytes that follow in the response information;
  - byte 14 gives the structure of the EF and in this case it shall be '01' indicating linear fixed structure;
  - byte 15 shall be '11'.
- 5) After step m) the following shall be true of the response data:
- bytes 3 and 4 shall be '00 17';
  - bytes 5 and 6 shall contain the file ID for EF<sub>CHV1</sub>, '00 00';
  - byte 7 shall contain '04' for EF;
  - bytes 9 - 11 shall give the access conditions for EF<sub>UAK</sub>. Byte 9 shall have the value 'Fx', where x is the assigned access condition for update, and byte 10 shall have the value '00';
  - byte 12: bit 2 shall be 1 and bit 3 shall be 0;
  - byte 13 shall give the number of bytes that follow and shall be coded '07';

- byte 14 gives the structure of the EF and in this case it shall be '00' indicating transparent structure;
- byte 15 shall indicate the number of remaining CHV attempts and shall be in the range '00' to '03';
- byte 16 shall be '01' indicating CHV verification;
- byte 17 bits 1, 2 and 3 shall be 0;
- bytes 18 and 20 shall be 'FF';
- byte 19 shall indicate the number of remaining UNBLOCK CHV attempts and shall be in the range '00' to '0A'.

#### **6.6.2.2 STATUS command**

The test procedure defined in subclause 6.5.2 intrinsically tests the coding of this command and so is not replicated here.

#### **6.6.2.3 READ BINARY command**

The test procedure defined in subclause 6.5.3 intrinsically tests the coding of this command and so is not replicated here.

#### **6.6.2.4 UPDATE BINARY command**

The test procedure defined in subclause 6.5.4 intrinsically tests the coding of this command and so is not replicated here.

#### **6.6.2.5 READ RECORD command**

The test procedure defined in subclause 6.5.5 intrinsically tests the coding of this command and so is not replicated here.

#### **6.6.2.6 UPDATE RECORD command**

The test procedure defined in subclause 6.5.6 intrinsically tests the coding of this command and so is not replicated here.

#### **6.6.2.7 SEEK command**

The test procedure defined in subclause 6.5.7 intrinsically tests the coding of this command and so is not replicated here.

#### **6.6.2.8 INCREASE command**

This command cannot be tested as there are no cyclic EFs in the DAM file structure.

#### **6.6.2.9 VERIFY CHV command**

The test procedure defined in subclause 6.5.9 intrinsically tests the coding of this command and so is not replicated here.

#### **6.6.2.10 CHANGE CHV command**

The test procedure defined in subclause 6.5.10 intrinsically tests the coding of this command and so is not replicated here.

**6.6.2.11 DISABLE CHV command**

The test procedure defined in subclause 6.5.11 intrinsically tests the coding of this command and so is not replicated here.

**6.6.2.12 ENABLE CHV command**

The test procedure defined in subclause 6.5.12 intrinsically tests the coding of this command and so is not replicated here.

**6.6.2.13 UNBLOCK CHV command**

The test procedure defined in subclause 6.5.13 intrinsically tests the coding of this command and so is not replicated here.

**6.6.2.14 INVALIDATE command**

The test procedure defined in subclause 6.5.14 intrinsically tests the coding of this command and so is not replicated here.

**6.6.2.15 REHABILITATE command**

The test procedure defined in subclause 6.5.15 intrinsically tests the coding of this command and so is not replicated here.

**6.6.2.16 ASK RANDOM command**

The test procedure defined in subclause 6.5.16 intrinsically tests the coding of this command and so is not replicated here.

**6.6.2.17 PT AUTHENTICATION command**

The test procedure defined in subclause 6.5.17 intrinsically tests the coding of this command and so is not replicated here.

**6.6.2.18 FT AUTHENTICATION command**

The test procedure defined in subclause 6.5.18 intrinsically tests the coding of this command and so is not replicated here.

**6.6.2.19 USER AUTHENTICATION command**

The test procedure defined in subclause 6.5.19 intrinsically tests the coding of this command and so is not replicated here.

**6.6.2.20 UAK ALLOCATION command**

The test procedure defined in subclause 6.5.20 intrinsically tests the coding of this command and so is not replicated here.

**6.6.2.21 GET RESPONSE command**

**6.6.2.21.1 Definition and applicability**

It shall be mandatory for all cards complying with ETS 300 331 [1] to support all functions described therein.

This test applies to both plug-in and ID-1 DAM cards.

#### 6.6.2.21.2 Conformance requirement

- 1) The GET RESPONSE command shall provide response data after the execution of commands SELECT, SEEK (type 2), PT AUTHENTICATION and USER AUTHENTICATION.
- 2) It is required that the GET RESPONSE command is executed immediately after the command it is related to (no other command shall come between the command/response pair and the command GET RESPONSE). If this sequence is not respected, the DAM shall send the Status Information "technical problem with no diagnostic given" as a reaction to the GET RESPONSE.
- 3) Since the MF is implicitly selected after the activation of the DAM, GET RESPONSE shall be allowed as the first command after activation.

Reference: ETS 300 331 [1], subclause 9.2.21.

Test Group Reference (TGR): TGR\_DAM\_CMD

Test Procedure Reference (TPR): TPR\_DAM\_CMD\_GET

#### 6.6.2.21.3 Test purpose

To verify that the coding of the GET RESPONSE command conforms to the above requirements.

NOTE: CR1 is tested in subclauses 6.5.1, 6.5.7, 6.5.17 and 6.5.19.

#### 6.6.2.21.4 Method of test

##### Initial conditions:

- 1) the DAM is connected to a PE simulator.

##### Test procedure:

- a) the PE simulator resets the DAM;
- b) the PE simulator sends a GET RESPONSE command to the DAM:  
[bytes sent: CLA='A0', INS='C0', P1='00', P2='00', P3='16'];  
[bytes received: P3 bytes of data, SW1, SW2];
- c) the PE simulator sends a STATUS command to the DAM with the correct P3;
- d) the PE simulator sends a GET RESPONSE command to the DAM:  
[bytes sent: CLA='A0', INS='C0', P1='00', P2='00', P3='16'];  
[bytes received: SW1, SW2].

#### 6.6.2.21.5 Test requirement

- 1) After step b) bytes 5 and 6 of the response data shall indicate that MF is the currently selected file.
- 2) After step d) the status condition returned by the DAM shall be SW1='6F', SW2='XX' - technical problem with no diagnostic given.

### **6.6.3 Definitions and coding**

#### **6.6.3.1 Definition and applicability**

Certain definitions and coding are used in the response parameters/data of the commands.

This test applies to both plug-in and ID-1 DAM cards.

#### **6.6.3.2 Conformance requirement**

- 1) In a DECT specific card, all bytes which are RFU shall be set to '00'.
- 2) In a DECT specific card, all bits which are RFU shall be set to 0.
- 3) The file structure indicator byte shall be one of the following values: '00', '01' or '03'.
- 4) The file type indicator byte shall be one of the following values: '01', '02', '03' or '04'.

Reference: ETS 300 331 [1], subclause 9.3.

Test Group Reference (TGR): TGR\_DAM\_CMD\_DEF

Test Procedure Reference (TPR): TPR\_DAM\_CMD\_DEF

#### **6.6.3.3 Test purpose**

To verify that the response parameters/data conform to the above requirements for all file IDs on the DAM.

NOTE: CR4 is covered in subclause 6.3.1.1, "File-type identification".

#### **6.6.3.4 Method of test**

##### **Initial conditions:**

- 1) the DAM is connected to a PE simulator.

##### **Test procedure:**

- a) the PE simulator resets the DAM;
- b) for every possible file ID in the file structure, the PE simulator sends SELECT commands to select the file ID. When a file is selected successfully, the PE simulator sends a GET RESPONSE command to the DAM.

#### **6.6.3.5 Test requirement**

- 1) After step b) for the MF and all DFs found, the following shall be true of the response data:
  - byte 1, 2, 8 and 18 shall be '00';
  - bits 3 to 7 of byte 12 shall be 0;
  - bits 5 to 7 of byte 14 shall be 0;
  - bits 5, 6 and 7 of bytes 19 through 22 of the response data shall be 0.

- 2) After step b) for all EFs found (except for EF<sub>CHV</sub>), the following shall be true of the response data:
  - bytes 1 and 2 shall be '00';
  - byte 8 shall be '00' if the EF is either Transparent or Linear Fixed;
  - byte 14 shall be coded as follows:
    - '00' = Transparent;
    - '01' = Linear Fixed;
    - '03' = Cyclic;
  - if present, byte 15 shall be '00' if the EF is Transparent;
  - if present, bytes 16 and following shall be '00';
  - bits 3 through 8 of byte 12 shall be 0.
- 3) After step b) for EF<sub>CHV</sub> files, the following shall be true of the response data:
  - bytes 1, 2 and 8 shall be '00';
  - byte 14 shall be '00';
  - bytes 21 and following shall be '00';
  - bits 6 through 8 of byte 12 shall be 0.

#### 6.6.4 Status conditions returned by the DAM

##### 6.6.4.1 Coding of the status words

###### 6.6.4.1.1 Definition and applicability

The status words SW1 and SW2 provide the method with which the DAM can respond to the PE after executing a command.

This test applies to both plug-in and ID-1 DAM cards.

###### 6.6.4.1.2 Conformance requirement

- 1) The DAM shall respond with the correct SW1 and SW2 status words for commands which are correctly executed.
- 2) The DAM shall respond with the correct SW1 and SW2 status words for commands which produce memory management errors.
- 3) The DAM shall respond with the correct SW1 and SW2 status words for commands which produce referencing management errors.
- 4) The DAM shall respond with the correct SW1 and SW2 status words for commands which produce security management errors.
- 5) The DAM shall respond with the correct SW1 and SW2 status words for commands which produce application independent errors.

Reference: ETS 300 331 [1], subclause 9.4.

Test Group Reference (TGR): TGR\_DAM\_CMD\_SC\_SW

Test Procedure Reference (TPR): TPR\_DAM\_CMD\_SC\_SW

#### 6.6.4.1.3 Test purpose

To verify that the DAM conforms to the above requirements when issuing SW1 and SW2 status words.

NOTE 1: CR2 cannot be tested as there is no mechanism to force the DAM to produce memory errors.

NOTE 2: Error code '98 50' in CR4 cannot be tested as there are no cyclic EFs in the DAM file structure.

#### 6.6.4.1.4 Method of test

##### Initial conditions:

- 1) the DAM is connected to a PE simulator;
- 2) EF<sub>LSR</sub> on the DAM is not invalidated;
- 3) CHV1 on the DAM is enabled;
- 4) three VERIFY CHV1 attempts and ten UNBLOCK CHV1 attempts remain.

##### Test procedure:

- a) the PE simulator resets the DAM;
- b) the PE simulator sends a VERIFY CHV command to the DAM;
- c) the PE simulator sends SELECT commands to the DAM to select DF<sub>DECT</sub>;
- d) the PE simulator sends a GET RESPONSE command to the DAM;
- e) the PE simulator sends a READ BINARY command using a length of 1 byte to the DAM;
- f) the PE simulator sends a SELECT command to the DAM to select EF<sub>LSR</sub>;
- g) the PE simulator sends an UPDATE RECORD command using LAST mode to the DAM. The data used is 'E1' for all bytes;
- h) the PE simulator sends an UPDATE RECORD command using NEXT mode to the DAM. The data used is 'E2' for all bytes;
- i) the PE simulator sends a READ BINARY command using a length of 1 byte to the DAM;
- j) the PE simulator sends a VERIFY CHV command with **incorrect** CHV1 to the DAM;
- k) the PE simulator sends an ENABLE CHV command to the DAM;
- l) the PE simulator sends an FP AUTHENTICATION command with valid data to the DAM;
- m) the PE simulator sends VERIFY CHV command with **incorrect** CHV1 to the DAM;
- n) the PE simulator sends VERIFY CHV command with **incorrect** CHV1 to the DAM;
- o) the PE simulator sends an UPDATE RECORD command using FIRST mode to the DAM. Parameter P3 is set to 1 and the data used is 'E3';
- p) the PE simulator sends an UPDATE RECORD command using mode '44' to the DAM. The data used is 'E4' for all bytes;

- q) the PE simulator sends the following APDU to the DAM:  
[bytes sent: CLA='A0', INS='18', P1='00', P2='00', P3='00'];
- r) the PE simulator sends the following APDU to the DAM:  
[bytes sent: CLA='F2', INS='F2', P1='00', P2='00', P3='00'];
- s) the PE simulator gains the security access condition specified by the administrative authority for REHABILITATE on EF<sub>LSR</sub>;
- t) the PE simulator sends a REHABILITATE command to the DAM;
- u) the PE simulator sends a GET RESPONSE command to the DAM.

#### 6.6.4.1.5 Test requirement

- 1) After step c) the status condition returned by the DAM shall be SW1='9F', SW2='XX' - length 'XX' of the response data.
- 2) After step d) the status condition returned by the DAM shall be SW1='90', SW2='00' - normal ending of command.
- 3) After step e) the status condition returned by the DAM shall be SW1='94', SW2='00' - no EF selected.
- 4) After step h) the status condition returned by the DAM shall be SW1='94', SW2='02' - out of range (invalid address).
- 5) After step i) the status condition returned by the DAM shall be SW1='94', SW2='08' - file type inconsistent with the command.
- 6) After steps j) and m) the status condition returned by the DAM shall be SW1='98', SW2='04' - unsuccessful CHV verification, at least one attempt left.
- 7) After step k) the status condition returned by the DAM shall be SW1='98', SW2='08' - in contradiction with CHV status.
- 8) After step l) the status condition returned by the DAM shall be SW1='98', SW2='35' - ASK RANDOM has not been executed.
- 9) After step n) the status condition returned by the DAM shall be SW1='98', SW2='40' - unsuccessful CHV verification, no attempt left.
- 10) After step o) the status condition returned by the DAM shall be SW1='67', SW2='XX' - incorrect parameter P3.
- 11) After step p) the status condition returned by the DAM shall be SW1='6B', SW2='00' - incorrect parameter P1 or P2.
- 12) After step q) the status condition returned by the DAM shall be SW1='6D', SW2='00' - unknown instruction code given in the command.
- 13) After step r) the status condition returned by the DAM shall be SW1='6E', SW2='00' - wrong instruction class given in the command.
- 14) After step t) the status condition returned by the DAM shall be SW1='98', SW2='10' - in contradiction with invalidation status.
- 15) After step u) the status condition returned by the DAM shall be SW1='6F', SW2='XX' - technical problem with no diagnostic given.



## 6.6.4.2 Commands versus possible status responses

### 6.6.4.2.1 Definition and applicability

Limiting the status conditions for each command to a defined set allows the PE to efficiently manage the handling of the status condition.

This test applies to both plug-in and ID-1 DAM cards.

### 6.6.4.2.2 Conformance requirement

- 1) Table 10 in ETS 300 331 [1], subclause 9.4.6 shows for each command the possible status conditions returned (marked by an asterisk \*). The DAM shall not generate status conditions other than those allowed for each command.

Reference: ETS 300 331 [1], subclause 9.4.6.

Test Group Reference (TGR): TGR\_DAM\_CMD\_SC\_CSR

Test Procedure Reference (TPR): TPR\_DAM\_CMD\_SC\_CSR

### 6.6.4.2.3 Test purpose

To verify for each command that the DAM will only generate the allowed status conditions.

NOTE: CR1 cannot be tested as it is not possible to force the DAM to generate all of the allowed status conditions for each command and there is no way of forcing the DAM to generate disallowed status conditions for each command.

### 6.6.4.2.4 Method of test

**Initial conditions:**

- N/A.

**Test procedure:**

- N/A.

### 6.6.4.2.5 Test requirement

N/A.

## 6.7 Contents of the Elementary Files

The subclause provides tests to ensure that the IUT contains all of the EFs needed for a DECT session.

### 6.7.1 Contents of the EFs at the MF level

#### 6.7.1.1 Definition and applicability

The following Elementary Files are required on the DAM card at the MF level in order for a DECT session to be carried out. For each of these EFs, the correct access conditions, data items and coding need to be in place:

- EF<sub>ICC</sub> - general information about manufacturing of the ICC card;
- EF<sub>ID</sub> - unique card identification number and issuing information;
- EF<sub>NAME</sub> (optional) - information about the user;
- EF<sub>IC</sub> (optional) - chip related information;
- EF<sub>DIR</sub> (optional) - path for selecting DECT or other application directories;
- EF<sub>LANG</sub> (optional) - language to be used for displaying messages.

This test applies to both plug-in and ID-1 DAM cards.

#### 6.7.1.2 Conformance requirement

- 1) The ASCII coding of the data items shall be in accordance with ISO/IEC 8859-1 [8].
- 2) EFs, records or data items having an unassigned value shall have their bytes and bits set to 'FF' and 1, respectively.
- 3) After the administrative phase, all data items shall have a defined value or have their bits set to 1.
- 4) All implemented EFs have a file size greater than zero shall contain all mandatory items.
- 5) Optional data items shall be filled with 'F', or if located at the end of the EF need not exist.
- 6) EF<sub>ICC</sub> shall contain the following data items for bytes 1 to 15:
  - clock stop mode;
  - IC card serial number;
  - IC card manufacturing references;
  - card personalizer ID;
  - embedder/IC assembler ID.
- 7) EF<sub>ICC</sub> shall contain the following data items for bytes 16 to 19 (optional):
  - IC identifier;
  - card profile;
  - type of selection.
- 8) Byte 19 of EF<sub>ICC</sub> (optional) shall be coded such that either "Selection by file ID" or "Selection by application ID" is supported.
- 9) EF<sub>ID</sub> shall contain the following data items for bytes 1 to 10:
  - identification number.
- 10) EF<sub>ID</sub> shall contain the following data items for bytes 10 to 19 (optional):
  - date of activation;
  - card expiry date;
  - card sequence number;
  - country code.

- 11) EF<sub>NAME</sub> (optional) shall contain the following data items for bytes 1 to X (optional):
  - card holder name.
- 12) The coding of the "card holder name" data item in EF<sub>NAME</sub> shall be left justified and padded with 'FF' (optional).
- 13) EF<sub>IC</sub> (optional) shall contain the following data items for bytes 1 to 8:
  - IC serial number;
  - IC manufacturing references.
- 14) EF<sub>DIR</sub> (optional) shall contain the following data items for bytes 1 to X:
  - application identifier tag (shall be coded '4F');
  - application identifier length;
  - application identifier.
- 15) EF<sub>DIR</sub> (optional) shall contain the following data items for bytes X + 1 to Y (optional):
  - application label tag (shall be coded '50');
  - application label length;
  - application label (verbal description).
- 16) EF<sub>DIR</sub> (optional) shall contain the following data items for bytes Y + 1 to end:
  - path tag (shall be coded '51');
  - path length;
  - path.
- 17) All "Path" data items within EF<sub>DIR</sub> shall be coded using the MF as the starting file ID and the file ID of the application as the ending file ID.
- 18) EF<sub>LANG</sub> (optional) shall contain the following data items for bytes 1 to 8 (optional):
  - first language preference;
  - second language preference;
  - third language preference;
  - fourth language preference.

Reference: ETS 300 331 [1], subclause 10.1.

Test Group Reference (TGR): TGR\_DAM\_CEF\_MF

Test Procedure Reference (TPR): TPR\_DAM\_CEF\_MF

### 6.7.1.3 Test purpose

To verify that the DAM conforms to the above requirements.

### 6.7.1.4 Method of test

#### Initial conditions:

- 1) the DAM is connected to a PE simulator.

#### Test procedure:

- a) the PE simulator resets the DAM;
- b) the PE simulator gains the access condition(s) necessary to read EF<sub>NAME</sub> and EF<sub>DIR</sub>;
- c) the PE simulator sends a SELECT command to the DAM to select EF<sub>ICC</sub>;

- d) the PE simulator sends a GET RESPONSE command to the DAM;
- e) the PE simulator sends a READ BINARY command to the DAM to read all available data bytes;
- f) the PE simulator sends a SELECT command to the DAM to select EF<sub>ID</sub>;
- g) the PE simulator sends a GET RESPONSE command to the DAM;
- h) the PE simulator sends a READ BINARY command to the DAM to read all available data bytes;
- i) the PE simulator sends a SELECT command to the DAM to select EF<sub>NAME</sub>;
- j) if step h) is successful, the PE simulator sends a GET RESPONSE command to the DAM;
- k) if step h) is successful, the PE simulator sends a READ BINARY command to the DAM to read all available data bytes;
- l) the PE simulator sends a SELECT command to the DAM to select EF<sub>IC</sub>;
- m) if step k) is successful, the PE simulator sends a GET RESPONSE command to the DAM;
- n) if step k) is successful, the PE simulator sends a READ BINARY command to the DAM to read all available data bytes;
- o) The PE simulator sends a SELECT command to the DAM to select EF<sub>DIR</sub>;
- p) If step n) is successful, the PE simulator sends a GET RESPONSE command to the DAM;
- q) If step n) is successful, the PE simulator sends a READ BINARY command to the DAM to read all available data bytes;
- r) The PE simulator sends a SELECT command to the DAM to select EF<sub>LANG</sub>;
- s) If step q) is successful, the PE simulator sends a GET RESPONSE command to the DAM;
- t) If step q) is successful, the PE simulator sends a READ BINARY command to the DAM to read all available data bytes.

#### 6.7.1.5 Test requirement

- 1) After steps e), h), k), n), and t) the data read shall conform to the requirements above.

#### 6.7.2 Contents of the EFs at the parent level of the DECT application

##### 6.7.2.1 Definition and applicability

The following Elementary Files are required on the DAM card at the parent level of the DECT application in order for a DECT session to be carried out. For each of these EFs, the correct access conditions, data items and coding need to be in place:

- EF<sub>CHV1</sub> - Card holder verification information for CHV1;
- EF<sub>CHV2</sub> (optional) - Card holder verification information for CHV2.

This test applies to both plug-in and ID-1 DAM cards.

### 6.7.2.2 Conformance requirement

- 1) The ASCII coding of the data items shall be in accordance with ISO/IEC 8859-1 [8].
- 2) EFs, records or data items having an unassigned value shall have their bytes and bits set to 'FF' and 1, respectively.
- 3) After the administrative phase, all data items shall have a defined value or have their bits set to 1.
- 4) All implemented EFs have a file size greater than zero shall contain all mandatory items.
- 5) Optional data items shall be filled with 'F', or if located at the end of the EF need not exist.
- 6) EF<sub>CHV</sub> shall contain the following data items for bytes 1 to 23:
  - EF<sub>CHV</sub> activation byte;
  - way to present CHV/UNBLOCK CHV;
  - coded 'FF';
  - CHV;
  - '03' - number of permissible consecutive false CHV attempts;
  - remaining CHV attempts counter;
  - UNBLOCK CHV;
  - remaining UNBLOCK CHV attempts counter;
  - coded 'FF'.
- 7) The CHV shall consist of 4 to 8 ASCII coded decimal digits ('0' to '9') right padded with 'FF'.
- 8) The UNBLOCK CHV shall consist of 8 ASCII coded decimal digits ('0' to '9').

Reference: ETS 300 331 [1], subclause 10.2.

Test Group Reference (TGR): TGR\_DAM\_CEF\_PDECT

Test Procedure Reference (TPR): TPR\_DAM\_CEF\_PDECT

### 6.7.2.3 Test purpose

To verify that the DAM conforms to the above requirements.

NOTE 1: These requirements are already tested in the following subclauses: 6.5.9 (VERIFY CHV), 6.5.10 (CHANGE CHV), 6.5.11 (DISABLE CHV), 6.5.12 (ENABLE CHV), 6.5.13 (UNBLOCK CHV) and 6.6.2.1 (SELECT).

NOTE 2: CHV2 can be tested in the same way.

### 6.7.2.4 Method of test

**Initial conditions:**

- N/A.

**Test procedure:**

- N/A.

### 6.7.2.5 Test requirement

N/A.

### 6.7.3 Contents of the EFs at the DECT application level

#### 6.7.3.1 Definition and applicability

The following Elementary Files are required on the DAM card at the DECT application level in order for a DECT session to be carried out. For each of these EFs, the correct access conditions, data items and coding need to be in place.

- EF<sub>LSR</sub> - list of all subscription registrations;
- EF<sub>LCSR</sub> - file ID of last chosen subscription registration;
- EF<sub>IPDI</sub> - International portable DAM identity.

This test applies to both plug-in and ID-1 DAM cards.

#### 6.7.3.2 Conformance requirement

- 1) The ASCII coding of the data items shall be in accordance with ISO/IEC 8859-1 [8].
- 2) EFs, records or data items having an unassigned value shall have their bytes and bits set to 'FF' and 1, respectively.
- 3) After the administrative phase, all data items shall have a defined value or have their bits set to 1.
- 4) All implemented EFs file a have size greater than zero shall contain all mandatory items.
- 5) Optional data items shall be filled with 'F', or if located at the end of the EF need not exist.
- 6) EF<sub>LSR</sub> shall contain the following data items for each record (14 data bytes):
  - file ID of DF<sub>SR</sub>;
  - name of subscription registration.
- 7) EF<sub>LSR</sub> shall contain at least two records (subscription registrations).
- 8) The "name" data item of EF<sub>LSR</sub> shall be coded in ASCII and padded with 'F'.
- 9) EF<sub>LCSR</sub> shall contain the following data items for bytes 1 to 2:
  - file ID of last chosen subscription registration.
- 10) EF<sub>IPDI</sub> shall contain the following data items for bytes 1 to 5:
  - IPDI.

Reference: ETS 300 331 [1], subclause 10.3.

Test Group Reference (TGR): TGR\_DAM\_CEF\_DECT

Test Procedure Reference (TPR): TPR\_DAM\_CEF\_DECT

#### 6.7.3.3 Test purpose

To verify that the DAM conforms to the above requirements.

#### 6.7.3.4 Method of test

##### Initial conditions:

- 1) the DAM is connected to a PE simulator.

##### Test procedure:

- a) the PE simulator resets the DAM;
- b) the PE simulator selects  $DF_{DECT}$  as defined in subclause 4.4;
- c) the PE simulator sends a SELECT command to the DAM to select  $EF_{LSR}$ ;
- d) the PE simulator sends a GET RESPONSE command to the DAM;
- e) the PE simulator sends READ RECORD commands to the DAM to read the data in all the records. The record length is 14 bytes;
- f) the PE simulator sends a SELECT command to the DAM to select  $EF_{LCSR}$ ;
- g) the PE simulator sends a GET RESPONSE command to the DAM;
- h) the PE simulator sends a READ BINARY command to the DAM to read all available data bytes;
- i) the PE simulator sends a SELECT command to the DAM to select  $EF_{IPDI}$ ;
- j) the PE simulator sends a GET RESPONSE command to the DAM;
- k) the PE simulator sends a READ BINARY command to the DAM to read all available data bytes.

#### 6.7.3.5 Test requirement

- 1) After steps e), h) and k) the data read shall conform to the requirements above.

#### 6.7.4 Contents of the EFs at the subscription registration level

##### 6.7.4.1 Definition and applicability

The following Elementary Files are required on the DAM card at the subscription registration level in order for a DECT session to be carried out. For each of these EFs, the correct access conditions, data items and coding need to be in place:

- $EF_{SR}$  - subscription specific information;
- $EF_{IPUI}$  - International portable user identity;
- $EF_{PARK}$  - Portable access rights key;
- $EF_{TPUI}$  (optional) - temporary portable user identity;
- $EF_{ZAP}$  (optional) - ZAP field;
- $EF_{DCK}$  - Derived cipher key;
- $EF_{UAK}$  - User authentication keys;
- $EF_{AC}$  - Authentication codes;
- $EF_{ST}$  - Service table.

This test applies to both plug-in and ID-1 DAM cards.

#### 6.7.4.2 Conformance requirement

- 1) The ASCII coding of the data items shall be in accordance with ISO/IEC 8859-1 [8].
- 2) EFs, records or data items having an unassigned value shall have their bytes and bits set to 'FF' and 1, respectively.
- 3) After the administrative phase, all data items shall have a defined value or have their bits set to 1.
- 4) All implemented EFs have a file size greater than zero shall contain all mandatory items.
- 5) Optional data items shall be filled with 'F', or if located at the end of the EF need not exist.
- 6) EF<sub>SR</sub> shall contain the following data items for bytes 1 to X:
  - DECT phase;
  - bitmap of available ACs;
  - bitmap of available UAKs;
  - number (0 or 1) of available DCKs;
  - identifiers of available authentication algorithms.
- 7) EF<sub>IPUI</sub> shall contain the following data items for bytes 1 to 13:
  - PUT and leftmost 4 bits of PUN;
  - rightmost bits of PUN.
- 8) EF<sub>PARK</sub> shall contain the following data items for each consecutive group of 6 bytes:
  - PLI of the PARK;
  - "0", ARC, leftmost 4 bits of ARD;
  - rightmost bits of ARD.
- 9) EF<sub>PARK</sub> shall contain at least 6 bytes of data.
- 10) The coding of bytes 2 to 6 of each 6-byte group in EF<sub>PARK</sub> shall be binary, left justified and padded with 1-bits.
- 11) EF<sub>TPUI</sub> (optional) shall contain the following data items for bytes 1 to 3.
  - TPUI.
- 12) EF<sub>ZAP</sub> (optional) shall contain the following data items for byte 1:
  - ZAP field (4 bits).
- 13) The coding of byte 1 in EF<sub>ZAP</sub> shall be binary, left justified and padded with four 1-bits.
- 14) EF<sub>DCK</sub> shall contain the following data items for each record (8 bytes):
  - DCK.
- 15) EF<sub>DCK</sub> shall contain one record for each subscription registration.
- 16) EF<sub>UAK</sub> shall contain the following data items for each record (17 bytes):
  - length of UAK;
  - UAK.
- 17) EF<sub>UAK</sub> shall contain no more than 8 records.
- 18) The coding of bytes 2 to 17 for each record in EF<sub>UAK</sub> shall be binary, left justified and padded with 1-bits.



- 19) EF<sub>AC</sub> shall contain the following data items for each record (5 bytes):
  - length of AC;
  - AC.
- 20) EF<sub>AC</sub> shall contain no more than 8 records.
- 21) The coding of bytes 2 to 5 for each record in EF<sub>AC</sub> shall be binary, left justified and padded with 1-bits.
- 22) EF<sub>ST</sub> shall contain the following data items for byte 1:
  - services No. 1 to No. 4.

Reference: ETS 300 331 [1], subclause 10.4.

Test Group Reference (TGR): TGR\_DAM\_CEF\_SRL

Test Procedure Reference (TPR): TPR\_DAM\_CEF\_SRL

#### **6.7.4.3 Test purpose**

To verify that the DAM conforms to the above requirements.

#### **6.7.4.4 Method of test**

##### **Initial conditions:**

- 1) the DAM is connected to a PE simulator.

##### **Test procedure:**

- a) the PE simulator resets the DAM;
- b) the PE simulator selects DF<sub>DECT</sub> as defined in subclause 4.4;
- c) the PE simulator sends a SELECT command to the DAM to select DF<sub>SR1</sub>;
- d) the PE simulator sends a VERIFY CHV command to the DAM to verify CHV1;
- e) the PE simulator sends a SELECT command to the DAM to select EF<sub>SR</sub>;
- f) the PE simulator sends a GET RESPONSE command to the DAM;
- g) the PE simulator sends a READ BINARY command to the DAM to read all available data bytes;
- h) the PE simulator sends a SELECT command to the DAM to select EF<sub>IPUI</sub>;
- i) the PE simulator sends a GET RESPONSE command to the DAM;
- j) the PE simulator sends a READ BINARY command to the DAM to read all available data bytes;
- k) the PE simulator sends a SELECT command to the DAM to select EF<sub>PARK</sub>;
- l) the PE simulator sends a GET RESPONSE command to the DAM;
- m) the PE simulator sends a READ BINARY command to the DAM to read all available data bytes;
- n) the PE simulator sends a SELECT command to the DAM to select EF<sub>TPUI</sub>;
- o) if step m) is successful, the PE simulator sends a GET RESPONSE command to the DAM;

- p) if step m) is successful, the PE simulator sends a READ BINARY command to the DAM to read all available data bytes;
- q) the PE simulator sends a SELECT command to the DAM to select EF<sub>ZAP</sub>;
- r) if step p) is successful, the PE simulator sends a GET RESPONSE command to the DAM;
- s) if step p) is successful, the PE simulator sends a READ BINARY command to the DAM to read all available data bytes;
- t) the PE simulator sends a SELECT command to the DAM to select EF<sub>DCK</sub>;
- u) the PE simulator sends a GET RESPONSE command to the DAM;
- v) the PE simulator sends READ RECORD commands to the DAM to read the data in all the records. The record length is 8 bytes;
- w) the PE simulator sends a SELECT command to the DAM to select EF<sub>UAK</sub>;
- x) the PE simulator sends a GET RESPONSE command to the DAM;

NOTE 1: The contents of EF<sub>UAK</sub> can never be read but can be implicitly tested by performing the appropriate authentication procedure in subclause 6.5.20.

- y) the PE simulator sends a SELECT command to the DAM to select EF<sub>AC</sub>;
- z) the PE simulator sends a GET RESPONSE command to the DAM;

NOTE 2: The contents of EF<sub>AC</sub> can never be read but can be implicitly tested by performing the appropriate authentication procedure in subclause 6.5.20.

- aa) the PE simulator sends a SELECT command to the DAM to select EF<sub>ST</sub>;
- ab) the PE simulator sends a GET RESPONSE command to the DAM;
- ac) the PE simulator sends a READ BINARY command to the DAM to read all available data bytes;
- ad) the PE simulator sends a SELECT command to the DAM to select DF<sub>SR2</sub>;
- ae) steps e) to ac) are repeated for DF<sub>SR2</sub>;
- af) steps e) to ac) are repeated for the remaining subscriptions on the DAM, if any.

#### 6.7.4.5 Test requirement

- 1) After steps g), j), m), p), s), v), and ac) the data read shall conform to the requirements above.

## History

Document history			
June 1996	Public Enquiry	PE 107:	1996-06-03 to 1996-09-27
July 1997	Vote	V 9739:	1997-07-29 to 1997-09-26
October 1997	First Edition		