dect
wireless technology

DECT Security
Step B&C

DECT Enhanced Security

STEP A	STEP B	STEP C
• Encryption of all calls • Re-keying during a call • Early encryption • Subscription requirements • Behaviour against legacy devices	• Encryption of all calls • Re-keying during a call • Early encryption • Subscription requirements • Behaviour against legacy devices	• Encryption of all calls • Re-keying during a call • Early encryption • Subscription requirements • Behaviour against legacy devices
DSAA	DSAA2	DSAA2
DSC	DSC	DSC2

Security Testing

Test tools required have been developed by Dosch&Amand and Bithium:

- Step A:
  - DA1220-B31: to test the cases for the security features from the original EN 300 444 GAP specification
  - DA1220-B32: to test the cases for the EN 300 444 N.35 features
- Step B:
  - DA1220-B36: to test the cases for the EN 300 444 N.35 features but with DSAA2 algorithm
- Step C:
  - Compliance is verified by using the Security Step C (SSC) tester in development by Bithium

DECT Forum website

- We will continue to use the same logo

- Proposal is to add a column to indicate certification level: A or B&C
- Nemko will carry out the security certification testing
- The program aims to be launched before year end
- More details about the process, costs etc. will be communicated to all the members well in time before the launch

DECT Forum website

Security Certified products

	Company	Product	Product Identification	Date of status achievement	Hardware version	Software version
	ascom	DH8	S-10-21-10091	07-okt-2021	D1	1.1.7
	poly	CB7321 CD/A	S-05-20-10086	13-jan-2021	VB2	V0056
	poly	S7320T/A	S-05-20-10087	13-jan-2021	VB2	V0056
	poly	S7310T/A	S-05-20-10088	13-jan-2021	VB2	V0056
	EPOS	SDW D1 USB	S-09-20-10090	13-okt-2020	N/A	28.0.0
	ascom	IPBS3	S-06-20-10089	10-jun-2020	PB	11.0.0
	spectralink	IP-DECT Server 200	S_02_20_10077	25-feb-2020	10A	18D
	spectralink	IP-DECT Server 6500	S_02_20_10078	25-feb-2020	10A	18D
	spectralink	IP-DECT Base Station	S_02_20_10079	25-feb-2020	10A	18D

dect

wireless technology

Security Step A

Precondition is compliance with security features in the original EN 300 444 GAP specification, below test cases defined in EN 300 494-2 (for the PT) and EN 300 494-3 (for the FT).

A.3.1 PT test cases

Test Case Id	Description	
TC_PT_MM_BV_AU_01	Authentication of PT; IUT(PT) has no stored ZAP value and service class info	
TC_PT_MM_BV_AU_02	Authentication of PT; unacceptable algorithm requested; reject	
TC_PT_MM_BV_AU_03	Authentication of PT; IUT(PT) has stored ZAP value; IUT includes ZAP value in the replay	
TC_PT_MM_BV_AU_04	Authentication of PT; ZAP increment handling	
TC_PT_MM_BV_AU_09	Authentication of PT; IUT(PT) has stored service class info; IUT includes service class info in the reply	
TC_PT_MM_BI_03	Authentication of PT; {AUTHENTICATIONREQUEST} missing <<RAND>>; reject	
TC_PT_MM_BV_KA_01	Key allocation	
TC_PT_MM_BV_KA_02	Key allocation; <<Auth type>> unacceptable; reject	
TC_PT_MM_TI_01	Key allocation; timer P-<MM_auth.1> expiry (± 5% margin)	
TC_PT_ME_BV_13	Obtain access rights interrupted by key allocation	
TC_PT_MM_BV_CH_03	Cipher switching; FT initiated; "cipher-off" to "cipher-on"	
TC_PT_MM_BV_CH_05	Cipher switching; FT initiated; "cipher-off" to "cipher-on"; unacceptable algorithm or key; reject	
TC_PT_MM_BV_CH_12	Cipher switching; FT initiated; "cipher-off" to "cipher-on" fails; release of link	
TC_PT_MM_BV_CH_14	Cipher switching; FT initiated; "cipher-off" to "cipher-on"; successful intra-cell bearer handover	
TC_PT_MM_BI_02	"Cipher off"; {CIPHER-REQUEST}, with invalid <<Cipher info>>; reject	

A.3.2 FT test cases

Test Case Id	Description	
TC_FT_MM_BV_AU_01	Authentication of PT; PT has no stored ZAP value and service class info	
TC_FT_MM_TI_02	Authentication of PT; timer F-<MM_auth.1> expiry (± 5% margin)	
TC_FT_MM_BV_KA_01	Key allocate; IUT initiated	
TC_FT_MM_BV_KA_02	Key allocate; IUT initiated; "implicit PT authentication" failure; IUT rejects	
TC_FT_MM_TI_05	Key allocation; timer F-<MM_key.1> expiry (± 5% margin)	
TC_FT_MM_BV_CH_03	Cipher switching; IUT(FT) initiated; "cipher-off" to "cipher-on"	
TC_FT_MM_BV_CH_08	Cipher switching; IUT(FT) initiated; "cipher-off" to "cipher-on" fails	
TC_FT_MM_BV_CH_14	Cipher switching; IUT(FT) initiated; "cipher-off" to "cipher-on" and intracell handover	
TC_FT_MM_BO_01	Cipher switching; IUT(FT) initiated; ignoring unexpected {IDENTITY-REPLY}	
TC_FT_MM_TI_06	Cipher switching; IUT(FT) initiated; timer F-<MM_cipher.1> expiry (± 5% margin)	

Security Step A

Added to the original EN 300 444 GAP specification as feature N.35, below test cases defined in TS 102 841

A.1 FT Test Case

Test Case Id	Description	
TC_FT_GAP.N.35_BV_101	Verify that FT enables encryption for incoming call within timer < MM_encryption_check.1 >	
TC_FT_GAP.N.35_BV_102	Verify that FT enables encryption for outgoing call within timer < MM_encryption_ check.1 >	
TC_FT_GAP.N.35_BV_105	Release of unencrypted call in case of wrong answer to authentication request	
TC_FT_GAP.N.35_BV_106	Release of unencrypted call in case of missing answer to authentication request	
TC_FT_GAP.N.35_BV_107	Release of unencrypted call in case of PP sending {AUTHENTICATION-REJECT} message	
TC_FT_GAP.N.35_BV_108	Release of unencrypted call in case of cipher rejects.	
TC_FT_GAP.N.35_BV_109	Release of unencrypted call in case of missing encryption activation on MAC layer.	
TC_FT_GAP.N.35_BV_201	Verify indication of Support of 'Re-keying' and 'early encryption' in extended higher layer capabilities part 2	
TC_FT_GAP.N.35_BV_202	Usage and frequency of re-keying procedure	
TC_FT_GAP.N.35_BV_203	Abnormal release if encryption for re-keying is not activated in MAC layer	
TC_FT_GAP.N.35_BV_204	Abnormal release if PP does not answer to {AUTHENTICATION-REQUEST} message for re-keying procedure	
TC_FT_GAP.N.35_BV_205	Abnormal release if PP answers to {AUTHENTICATION-REQUEST} message for re-keying procedure with { AUTHENTICATION-REJECT}	
TC_FT_GAP.N.35_BV_206	Abnormal release if PP answers to {CIPHER_REQUEST} message for re-keying procedure with { CIPHER_REJECT}	
TC_FT_GAP.N.35_BV_301	Assignment of default cipher key and usage of early encryption during incoming call.	
TC_FT_GAP.N.35_BV_302	Usage of early encryption during outgoing call	
TC_FT_GAP.N.35_BV_303	Usage of early encryption for MM procedure	
TC_FT_GAP.N.35_BV_401	Duration of registration window	
TC_FT_GAP.N.35_BV_402	Closing of registration window after successful registration.	

A.2 PT Test Case

Test Case Id	Description	
TC_PT_GAP.N.35_BV_101	Encryption of all calls	
TC_PT_GAP.N.35_BV_201	Indication of Support of 'Re-keying' and 'early encryption' in terminal capabilities during registration	
TC_PT_GAP.N.35_BV_202	Indication of Support of 'Re-keying' and 'early encryption' in terminal capabilities during location registration	
TC_PT_GAP.N.35_BV_203	Re-keying procedure	
TC_PT_GAP.N.35_BV_301	Assignment of default cipher key and usage of early encryption during incoming call	
TC_PT_GAP.N.35_BV_302	Usage of early encryption during outgoing call	
TC_PT_GAP.N.35_BV_303	Usage of early encryption for MM procedure	
TC_PT_GAP.N.35_BV_304	Overwriting a default cipher key by assigning a new default cipher key with the same index	
TC_PT_GAP.N.35_BV_305	Assign two default cipher keys with different indices.	
TC_PT_GAP.N.35_BV_306	PP releases connection in case FP rejects early encryption on MAC layer	
TC_PT_GAP.N.35_BV_501	Release of unexpectedly unencrypted outgoing call in call proceeding state	
TC_PT_GAP.N.35_BV_502	Release of unexpectedly unencrypted outgoing call in connect state	
TC_PT_GAP.N.35_BV_503	Release of unexpectedly unencrypted incoming call in alerting state	
TC_PT_GAP.N.35_BV_504	Release of unexpectedly unencrypted incoming call in connect state.	
TC_PT_GAP.N.35_BV_505	Release of unexpectedly unencrypted outgoing call in connect state after switching encryption support in FT off	
TC_PT_GAP.N.35_BV_506	Release of unexpectedly unencrypted outgoing call in connect state despite of successful authentication	
TC_PT_GAP.N.35_BV_507	Release of unexpectedly unencrypted incoming call in connect state despite of successful authentication	

Security Step B

Added to the original EN 300 444 GAP specification as feature N.36. No new test cases were defined but compliance is tested using same test cases as for Step A with DSAA2 as algorithm.

A.1 FT Test Case

Test Case Id	Description	
TC_FT_GAP.N.35_BV_101	Verify that FT enables encryption for incoming call within timer < MM_encryption_check.1 >	
TC_FT_GAP.N.35_BV_102	Verify that FT enables encryption for outgoing call within timer < MM_encryption_ check.1 >	
TC_FT_GAP.N.35_BV_105	Release of unencrypted call in case of wrong answer to authentication request	
TC_FT_GAP.N.35_BV_106	Release of unencrypted call in case of missing answer to authentication request	
TC_FT_GAP.N.35_BV_107	Release of unencrypted call in case of PP sending {AUTHENTICATION-REJECT} message	
TC_FT_GAP.N.35_BV_108	Release of unencrypted call in case of cipher rejects.	
TC_FT_GAP.N.35_BV_109	Release of unencrypted call in case of missing encryption activation on MAC layer.	
TC_FT_GAP.N.35_BV_201	Verify indication of Support of 'Re-keying' and 'early encryption' in extended higher layer capabilities part 2	
TC_FT_GAP.N.35_BV_202	Usage and frequency of re-keying procedure	
TC_FT_GAP.N.35_BV_203	Abnormal release if encryption for re-keying is not activated in MAC layer	
TC_FT_GAP.N.35_BV_204	Abnormal release if PP does not answer to {AUTHENTICATION-REQUEST} message for re-keying procedure	
TC_FT_GAP.N.35_BV_205	Abnormal release if PP answers to {AUTHENTICATION-REQUEST} message for re-keying procedure with { AUTHENTICATION-REJECT}	
TC_FT_GAP.N.35_BV_206	Abnormal release if PP answers to {CIPHER_REQUEST} message for re-keying procedure with { CIPHER_REJECT}	
TC_FT_GAP.N.35_BV_301	Assignment of default cipher key and usage of early encryption during incoming call.	
TC_FT_GAP.N.35_BV_302	Usage of early encryption during outgoing call	
TC_FT_GAP.N.35_BV_303	Usage of early encryption for MM procedure	
TC_FT_GAP.N.35_BV_401	Duration of registration window	
TC_FT_GAP.N.35_BV_402	Closing of registration window after successful registration.	

A.2 PT Test Case

Test Case Id	Description	
TC_PT_GAP.N.35_BV_101	Encryption of all calls	
TC_PT_GAP.N.35_BV_201	Indication of Support of 'Re-keying' and 'early encryption' in terminal capabilities during registration	
TC_PT_GAP.N.35_BV_202	Indication of Support of 'Re-keying' and 'early encryption' in terminal capabilities during location registration	
TC_PT_GAP.N.35_BV_203	Re-keying procedure	
TC_PT_GAP.N.35_BV_301	Assignment of default cipher key and usage of early encryption during incoming call	
TC_PT_GAP.N.35_BV_302	Usage of early encryption during outgoing call	
TC_PT_GAP.N.35_BV_303	Usage of early encryption for MM procedure	
TC_PT_GAP.N.35_BV_304	Overwriting a default cipher key by assigning a new default cipher key with the same index	
TC_PT_GAP.N.35_BV_305	Assign two default cipher keys with different indices.	
TC_PT_GAP.N.35_BV_306	PP releases connection in case FP rejects early encryption on MAC layer	
TC_PT_GAP.N.35_BV_501	Release of unexpectedly unencrypted outgoing call in call proceeding state	
TC_PT_GAP.N.35_BV_502	Release of unexpectedly unencrypted outgoing call in connect state	
TC_PT_GAP.N.35_BV_503	Release of unexpectedly unencrypted incoming call in alerting state	
TC_PT_GAP.N.35_BV_504	Release of unexpectedly unencrypted incoming call in connect state.	
TC_PT_GAP.N.35_BV_505	Release of unexpectedly unencrypted outgoing call in connect state after switching encryption support in FT off	
TC_PT_GAP.N.35_BV_506	Release of unexpectedly unencrypted outgoing call in connect state despite of successful authentication	
TC_PT_GAP.N.35_BV_507	Release of unexpectedly unencrypted incoming call in connect state despite of successful authentication	

Security Step B

- There has been discussion about the need to re-test also the original GAP security features with DSAA2
- Neither specific test cases nor tester are available for this
- Current understanding is though that these cases are either covered implicitly by the tests from the previous slide or they are not relevant
- Therefore the CWG considers that it is acceptable to not run the below test cases with DSAA2 provided that they have actually been run for Step A in DSAA mode

A.3.1 PT test cases

Test Case Id	Description	
TC_PT_MM_BV_AU_01	Authentication of PT; IUT(PT) has no stored ZAP value and service class info	
TC_PT_MM_BV_AU_02	Authentication of PT; unacceptable algorithm requested; reject	
TC_PT_MM_BV_AU_03	Authentication of PT; IUT(PT) has stored ZAP value; IUT includes ZAP value in the replay	
TC_PT_MM_BV_AU_04	Authentication of PT; ZAP increment handling	
TC_PT_MM_BV_AU_09	Authentication of PT; IUT(PT) has stored service class info; IUT includes service class info in the reply	
TC_PT_MM_BI_03	Authentication of PT; {AUTHENTICATIONREQUEST} missing <<RAND>>; reject	
TC_PT_MM_BV_KA_01	Key allocation	
TC_PT_MM_BV_KA_02	Key allocation; <<Auth type>> unacceptable; reject	
TC_PT_MM_TI_01	Key allocation; timer P-<MM_auth.1> expiry (± 5% margin)	
TC_PT_ME_BV_13	Obtain access rights interrupted by key allocation	
TC_PT_MM_BV_CH_03	Cipher switching; FT initiated; "cipher-off" to "cipher-on"	
TC_PT_MM_BV_CH_05	Cipher switching; FT initiated; "cipher-off" to "cipher-on"; unacceptable algorithm or key; reject	
TC_PT_MM_BV_CH_12	Cipher switching; FT initiated; "cipher-off" to "cipher-on" fails; release of link	
TC_PT_MM_BV_CH_14	Cipher switching; FT initiated; "cipher-off" to "cipher-on"; successful intra-cell bearer handover	
TC_PT_MM_BI_02	"Cipher off"; {CIPHER-REQUEST}, with invalid <<Cipher info>>; reject	

A.3.2 FT test cases

Test Case Id	Description	
TC_FT_MM_BV_AU_01	Authentication of PT; PT has no stored ZAP value and service class info	
TC_FT_MM_TI_02	Authentication of PT; timer F-<MM_auth.1> expiry (± 5% margin)	
TC_FT_MM_BV_KA_01	Key allocate; IUT initiated	
TC_FT_MM_BV_KA_02	Key allocate; IUT initiated; "implicit PT authentication" failure; IUT rejects	
TC_FT_MM_TI_05	Key allocation; timer F-<MM_key.1> expiry (± 5% margin)	
TC_FT_MM_BV_CH_03	Cipher switching; IUT(FT) initiated; "cipher-off" to "cipher-on"	
TC_FT_MM_BV_CH_08	Cipher switching; IUT(FT) initiated; "cipher-off" to "cipher-on" fails	
TC_FT_MM_BV_CH_14	Cipher switching; IUT(FT) initiated; "cipher-off" to "cipher-on" and intracell handover	
TC_FT_MM_BO_01	Cipher switching; IUT(FT) initiated; ignoring unexpected {IDENTITY-REPLY}	
TC_FT_MM_TI_06	Cipher switching; IUT(FT) initiated; timer F-<MM_cipher.1> expiry (± 5% margin)	