한진정보통신 NGS Protocol 연동 규격서

Version 2.0.1
2023-01-10

한진정보통신

- **제 개정 이력**

Ver No.	날짜	작성자	설명
2.0.0	2022-01-04	김형훈	최초 작성
2.0.1	2023-01-10	김형훈	REPORT.MESSAGE 필드 내용 변경

목차

1 개요

본 문서는 메시지(SMS/LMS/MMS/알림톡/친구톡) 발송을 원하는 파트너에게 한진정보통신㈜의 메시지 발송 서버와 연동을 위한 규격을 제공하기 위한 문서입니다.

1.1 기본 사항

- 상호 연동 이전에 파트너는 계정을 발급 받아야 합니다.
- 계정을 발급 받는 과정에 1초당 전송 가능 건수(TPS) 및 월 발송 가능 건수를 협의 하여야 합니다.
- 연동 시 IP인증을 위하여 파트너의 접속 IP를 등록하여야 합니다.
- 한진정보통신㈜의 발송 서버는 Server가 되고 파트너의 서버는 Client로 동작합니다.

1.2 연동 기본 규약

- TCP/IP 프로토콜을 기본으로 사용 합니다.
- 모든 Data는 NULL(0x00)로 Padding된 버퍼의 앞에서부터 채워 넣습니다.
- 본 규격에서 사용하는 모든 데이터 유형은 Char(String)형 입니다.
- nC : n Byte인 Buffer를 의미합니다.
- Packet을 구성하는 Header와 Body는 한번에 전송합니다.
- Deliver 와 Report 세션은 별도의 Port로 서비스되며, 각각의 Port로 두개의 접속이 이루어 져야 합니다.
- 메시지 본문은 확장형 한글(MS949, EUC-KR)을 기본으로 합니다.
- 암호화는 AES256을 기본으로 합니다.
- 동일한 ID로 중복으로 접속 할 경우 두 접속 모두 종료 됩니다.
- 아래의 Protocol 규격에 정의된 필드의 값에 요구되는 값을 설정하여야 하며 이를 위반시 Server에서 접속을 종료 할 수 있습니다.
- 발급된 계정으로 인증 서버에 인증을 통해 수신된 IP와 Port로 접속을 하여야 합니다.
- Client가 Server에 접속한 뒤 접속이 끊어졌을 경우, 약 5초 이후에 재접속을 시도하여야 하며, 짧은 시간에 과도한 접속 요청 시 해당 계정이 잠금 처리 되어 더 이상 정상적인 접속이 이루어지지 않을 수 있습니다.

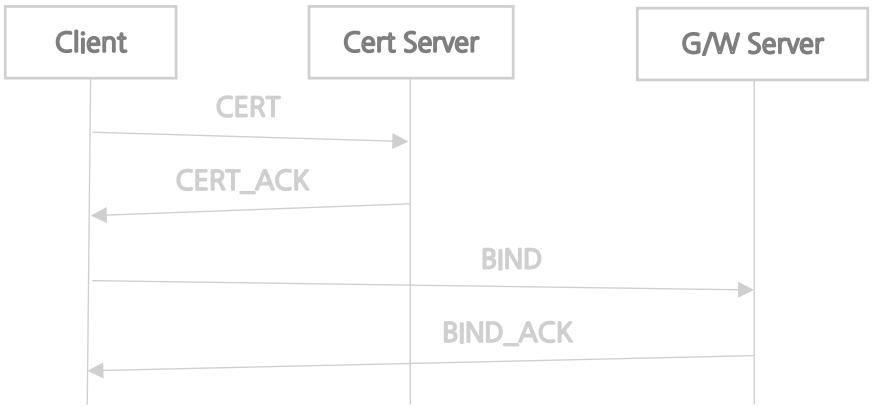
1.3 별첨 문서

- 본 규격의 Error Code 및 알림톡/친구톡 부가 정보는 아래의 별첨 문서를 참고 바랍니다.

  - 별첨_한진정보통신_ErrorCode_Version_yyyymmdd.xlsx
  - 별첨_한진정보통신_Kakao_AddedInfo_yyyymmdd.pdf

2 연동 Flow

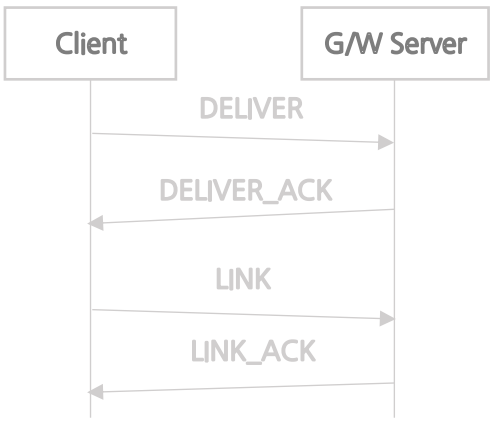
2.1 인증 및 발송 서버 접속



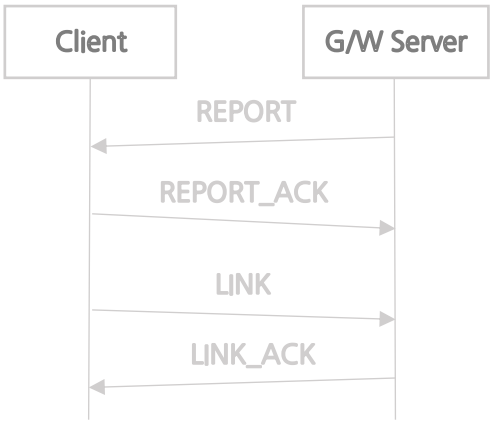
〈 Cert & Bind 〉

- Server로 Connection 후 1초 안에 CERT 및 BIND 요청을 하여야 합니다.
- CERT(인증) 요청에 대한 응답으로 발송 서버 정보(IP, Port, CertKey)를 수신 합니다.
- 수신 받은 발송 서버로 Bind요청을 Deliver 와 Report Port로 각각 수행 하여 연결을 유지 합니다.
- 세션 종료시 인증요청을 다시 수행한후 Bind 요청을 해야 합니다.

2.2 메시지 전송 요청 및 결과 수신



〈 Deliver Session 〉



〈 Report Session 〉

- 메시지 전송 요청은 Deliver 세션을 통해 요청 합니다.
- 요청한 메시지에 대한 전송 결과는 Report 세션을 통해 전달 되므로 반드시 연결 유지 하여야 합니다.
- 각 패킷에 대한 ACK가 10초 이상 수신 되지 않을 경우 접속을 종료하고 다시 접속을 하여야 합니다.
- LINK는 Client에서 전송 요청을 하여야 하며, Server는 그에 대한 응답으로 LINK_ACK를 전송 합니다.
- LINK는 접속 상태 확인을 위한 것으로 마지막 패킷을 수신 후 1분 이내로 전송 하여야 합니다.
- 일정시간 동안 주고 받은 패킷이 없을 경우 Server쪽에서 Connection을 종료 할 수 있습니다.

3 Message Header

Server와 Client 간에 주고 받는 모든 Packet에는 Header 가 Packet 첫 부분에 반드시 존재 하여야 합니다.

3.1 Header 구조

Type	Field	Size	설명	비 고
HEADER (14Byte)	HeadType	4C	Packet Type	3.2 참조
	MsgLeng	10C	Body의 Size	Message Body의 타입별 크기 또는 암호화된 Body 크기

3.2 Packet Type

각 Packet 을 구분하는 Type 으로 기대하지 않은 Type 이 수신되었을 경우 Connection 이 종료 될 수 있다.

HeadType	Value	설 명
CERT	0	인증 및 접속 정보 요청
CERT_ACK	1	인증에 대한 응답
BIND	11	발송 서버 접속 요구
BIND_ACK	12	접속 요구에 대한 응답
DELIVER	21	메시지 전송 요청
DELIVER_ACK	22	메시지 전송 요청에 대한 응답
REPORT	31	전송 결과 전송
REPORT_ACK	32	전송 결과 전송에 대한 응답
LINK	41	세션 상태 확인 요청
LINK_ACK	42	세션 상태 확인 요청에 대한 응답
EVENT	51	Event 전송(Server에서 전송하며 전송에 대한 응답은 불필요)

- LINK 와 LINK_ACK는 Body 없이 Header만 전송합니다.
- EVENT는 EVENT_ACK가 없습니다.

4 Message Body

4.1 인증(CERT)

인증을 통해 메시지 발송 서버의 정보와 인증키를 수신합니다.

[Format]

Type	Field	Size	설명	비 고
CERT (149Byte)	ID	20C	인증 ID	
	PWD	110C	인증 PWD	5.2 Password 암호화 참조
	VERSION	15C	연동 규격 버전	TV_2.0.1 ('TV_' 와 본 문서의 버전을 조합)
	KEYPOS	4C	암호화 Key Offset	PWD를 암호화 할 때 사용한 암호화 Key의 Offset
CERT_ACK (125Byte)	RESULT	4C	결과 코드	"7.1 전송 결과 코드" 참조
	CERT_KEY	65C	Cert Key	64Byte의 문자열 (BIND.CERT_KEY에 설정하여 전송)
	SERVER_IP	40C	연동할 GW IP	인증 실패시 : 실패 사유 메시지
	DELIVER_PORT	8C	Deliver Port	인증 실패시 : NULL
	REPORT_PORT	8C	Report Port	인증 실패시 : NULL

- 3초안에 2번이상의 과도한 요청을 할 경우 정상적인 인증이 되지 않음.

[Example]

➢ CERT

Type	Size	Value
HeadType	4C	0
MsgLeng	10C	149
ID	20C	testid
PWD	110C	ONs0wphSMJDVhzcYvm8hN89/bA4NzZQAYQvMstW8d29nm760R2ujAxD0Izo1iKi85uFKfAcOXfMZicTfMfJ04mvAby03pCF9sbRDorZ9HNM=
VERSION	15C	TV_2.0.1
KEYPOS	4C	12

➢ CERT_ACK

Type	Size	Value
HeadType	4C	1
MsgLeng	10C	125
RESULT	4C	0
CERT_KEY	65C	atK6KYa/iAFM+pdj2tA0tM/poWHkTKlCq6iMHRPXzdlcVJQUlltj8us32qIVL0o
SERVER_IP	40C	111.222.222.222
DELIVER_PORT	8C	4403
REPORT_PORT	8C	4404

4.2 접속 요청 및 인증(BIND)

인증을 통해 수신된 IP와 Port로 '발송 요청 라인'과 '결과 수신 라인'의 접속을 수행합니다.

[Format]

Type	Field	Size	설명	비 고
BIND (220Byte)	ID	20C	인증 ID	
	PWD	110C	인증 PWD	5.2 Password 암호화 참조
	CERT_KEY	65C	Cert Key	64Byte의 문자열 (CERT_ACK 에서 수신한 CERT_KEY 값을 그대로 설정)
	TYPE	2C	연동방식	p - 일반 방식 연동 P - 암호화 방식 연동
	KIND	4C	연결타입 구분	DLV - 메시지 전송 REP - Report 수신
	VERSION	15C	연동 규격 버전	TV_2.0.1 ('TV_' 와 본 문서의 버전을 조합)
	KEYPOS	4C	암호화 Key Offset	PWD를 암호화 할 때 사용한 암호화 Key의 Offset
BIND_ACK (59Byte)	RESULT	4C	결과 코드	"7.1 전송 결과 코드" 참조
	SMS_TPS	5C	1초당 SMS 발송 가능 건수	TPS 초과 건수는 수신 처리 되지 않으며, 전달 받은 TPS를 초과하여 전송 하지 않도록 하여야 한다.
	MMS_TPS	5C	1초당 MMS 발송 가능 건수	
	KKO_TPS	5C	1초당 알림톡/친구톡 발송 가능 건수	
	MESSAGE	40C	결과 메시지	실패시 사유 메시지

- CERT_ACK에서 수신한 CERT_KEY값을 그대로 설정하여야 합니다.
- Deliver Port로 "KIND"의 값을 'REP' 로 설정 후 접속 요청 할 경우 연결이 실패 됩니다..

- Report Port로 “KIND”의 값을 ‘DLV’로 설정 후 접속 요청 할 경우 연결이 실패 됩니다.
- CERT를 수행 후 BIND를 수초 이내에 하지 않으면 연결이 실패 됩니다.

[Example]

➢ BIND

Type	Size	Value
HeadType	4C	11
MsgLeng	10C	220
ID	20C	testid
PWD	110C	ONs0wphSMJDVhzcYvm8hN89/bA4NzZQAYQvMstW8d29nm760R2ujAxD0Izo1iKi85uFKfAcOXfMZicTfMfJ04mvAby03pCF9sbRDorZ9HNM=
CERT_KEY	65C	atK6KYa/iAFM+pdj2tA0tM/poWHkTKlCq6iMHRPXzdIcVJQUllItj8us32qIVL0o
TYPE	2C	p
KIND	4C	DLV
VERSION	15C	TV_2.0.1
KEYPOS	4C	12

➢ BINC_ACK

Type	Size	Value
HeadType	4C	12
MsgLeng	10C	59
RESULT	4C	0
SMS_TPS	5C	80
MMS_TPS	5C	30
KKOMS_TPS	5C	30
MESSAGE	40C	

4.3 메시지 전송(DELIVER)

BIND를 통해 연결된 DLV 세션을 통해 SMS, LMS, MMS, 알림톡, 친구톡 메시지 전송 요청을 할 수 있습니다.

- MSGTYPE에 따라서 가변, 확장 및 대체 필드가 존재하며 타입에 따른 설정을 하여야 합니다.
- MSGTYPE을 잘못 설정 할 경우 전송 실패가 될 수 있습니다.(친구톡, 친구톡 이미지 구분 등)

[Format]

Type	Field	Size	설명	비 고
DELIVER (221Byte ~)	MSGTYPE	2C	메시지 타입	S : SMS L : LMS M : MMS A : 알림톡 a : 알림톡 이미지 F : 친구톡 f : 친구톡 이미지 W : 친구톡 와이드 이미지 (s :국제 SMS, l :국제 LMS, m :국제 MMS) <- 추후 지원 예정
	DA_ADDR	20C	착신번호	
	CALLBACK	20C	회신번호	
	ENCODING	2C	인코딩 타입	TEXT의 인코딩 타입 (KAKAO_INFO의 TITLE) 0 : EUC-KR, 1 : UTF-8
	TEXT	141C	Text (대체 필드)	- SMS : 90Byte이하의 본문 - LMS/MMS : 64Byte이하의 제목 - 알림톡/친구톡 : 발송 정보 [KAKAO_INFO Format] 참조
	SERIAL	20C	Serial Number	고객사 Serial Number 숫자 및 문자 포함 가능
	SENDER_CODE	10C	최초 발신사업자 식별 코드	중앙전파관리소에서 발급받은 9자리의 식별 코드
	MEDIACNT	2C	첨부파일 개수	MEDIA의 개수
	EXT_SIZE	4C	확장 필드 크기	확장 필드를 사용할 경우 EXTENTION 의 크기를 지정한다. (10 : 부서 코드, 16 : 국제 문자)
	EXTENTION	nC	확장 필드	[EXTENTION Format] 참조
	MEDIA	nC	첨부 파일(가변 필드)	[MEDIA Format] 참조
DELIVER_ACK (44Byte)	RESULT	4C	결과 코드	"7.1 전송 결과 코드" 참조
	DA_ADDR	20C	착신 번호	DELIVER.DA_ADDR 의 값
	SERIAL	20C	Serial Number	DELIVER.SERIAL 의 값

[KAKAO_INFO Format]

알림톡/친구톡 전송시 TEXT 영역(141Byte)을 대체 합니다.

Field	Sub Field	Size	설명	비 고
TEXT	SENDERKEY	41C	발신 프로필 Key	
	TEMPLATE	31C	템플릿 코드	알림톡 템플릿 코드
	METHOD	2C	발송 방식	p : push(기본값) r : real P : polling
	FAILOVER	2C	발송 실패 후 처리	0 : 전환/대체 발송 하지 않음 1 : 전환 발송 2 : 대체 발송 3 : 대체 발송 MMS
	TITLE	65C	제목	LMS/MMS 로 전환/대체 발송 할 경우 제목

- 전환 발송 : 전송 실패 시 알림톡/친구톡 본문을 그대로 SMS/LMS/MMS로 변환하여 발송
  * 친구톡 이미지일 경우에는 이미지도 같이 첨부하여야 하며, 첨부 하지 않으면 본문만 전송
- 대체 발송 : 전송 실패 시 알림톡/친구톡 내용 대신 별도로 첨부된 본문을 SMS/LMS로 대체 하여 발송 (첨부 이미지 무시됨)
- 대체 발송 MMS : 대체 발송과 동일하나 첨부된 이미지가 있는 경우 이미지와 같이 MMS로 발송(첨부 이미지 없는 경우 '대체 발송' 과 동일하게 SMS/LMS로 발송)

[EXTENTION Format]

부가적인 서비스 협의가 이루어진 고객에 한하여 아래의 두가지 Type중 하나를 DELIVER의 EXTENTION 영역에 추가 합니다.

Field	Sub Field	Size	설명	비 고
EXTENTION	DPT_CODE	10C	부서 코드	

Field	Sub Field	Size	설명	비 고
EXTENTION	NAT_CODE	16C	국가 번호	

[MEDIA Format]

다음과 같은 첨부파일이 있을 경우 DELIVER의 MEDIACNT 수 만큼 MEDIA영역에 추가 합니다.

- LMS/MMS 의 Text 본문(EUC-KR), 알림톡/친구톡의 본문(EUC-KR, UTF-8)
- MMS의 Image(Binary)

- 알림톡/친구톡의 버튼, 이미지 및 Url 등의 부가 정보(Json포멧, UTF-8)
- 알림톡/친구톡의 대체 발송 대비한 대체 Text 본문(EUC-KR 또는 UTF-8)
- 친구톡 이미지의 전환/대체 발송 대비한 Image(Binary)

Field	Sub Field	Size	설명	비 고
MEDIA	MTYPE	3C	11 - Text : LMS/MMS/알림톡/친구톡 본문 12 - Text : 알림톡/친구톡 실패시 대체 발송 본문 13 - Json : 알림톡/친구톡의 버튼, 이미지등의 정보 21 - JPG 이미지(MMS/친구톡) 22 - JPG 와이드 이미지(친구톡) 23 - PNG 이미지(MMS/친구톡) 24 - PNG 와이드 이미지(친구톡)	MEDIACNT 만큼 반복
	ENCODING	2C	MEDIA의 인코딩 타입 0 : EUC-KR, 1 : UTF-8, 2 : Binary	
	MFILELEN	10C	첨부파일 Size	
	MEDIA	nC	첨부파일 Binary Data	

- 알림톡/친구톡 전송시 ENCODING을 UTF-8로 전송 시 전환/대체 발송 할 경우에는 EUC-KR에서 지원하지 않는 문자가 있을 경우 SMS/LMS/MMS로 전송 성공 하더라도 정상적으로 보이지 않을 수 있습니다.

[Example]

➢ DELIVER - SMS

Type	Size	Value
HeadType	4C	21
MsgLeng	10C	221
MSGTYPE	2C	S
DA_ADDR	20C	01020001234
CALLBACK	20C	15880000
ENCODING	2C	0
TEXT	141C	SMS 테스트 발송 입니다.
SERIAL	20C	202112310012345
SENDER_CODE	10C	101280092
MEDIACNT	2C	0
EXT_SIZE	4C	0

➢ DELIVER - MMS

Type	Size	Value	
HeadType	4C	21	
MsgLeng	10C	23149	
MSGTYPE	2C	M	
DA_ADDR	20C	01020001234	
CALLBACK	20C	15880000	
ENCODING	2C	0	
TEXT	141C	MMS 제목	
SERIAL	20C	202112310012346	
SENDER_CODE	10C	101280092	
MEDIACNT	2C	2	
EXT_SIZE	4C	0	
MTYPE	3C	11	첨부 1
ENCODING	2C	0	
MFILELEN	10C	1965	
MEDIA	1965C	MMS 본문입니다. ..... 본문끝 ←텍스트 본문 첨부	
MTYPE	3C	21	첨부 2
ENCODING	2C	2	
MFILELEN	10C	20933	
MEDIA	20933C	d8ffe0ff1000464a4649010000019000 ..... ff0300d9 ←이미지 Binary Data 첨부	

➢ DELIVER - 알림톡(전환 발송)

Type	Size	Value	
HeadType	4C	21	
MsgLeng	10C	1260	
MSGTYPE	2C	A	
DA_ADDR	20C	01020001234	
CALLBACK	20C	15880000	
ENCODING	2C	0	
SENDERKEY	41C	cf1060fa976a7875eafae84083649af24f6ad3db	TEXT 대신
TEMPLATE	31C	temp_code_01	
METHOD	2C	p	

Type	Size	Value	
FAILOVER	2C	1	
TITLE	65C	Replace Title ← 전환 발송시 제목	
SERIAL	20C	202112310012347	
SENDER_CODE	10C	123456789	
MEDIACNT	2C	2	
EXT_SIZE	4C	0	
MTYPE	3C	11	첨부 1
ENCODING	2C	0	
MFILELEN	10C	909	
MEDIA	909C	알림톡 본문입니다. ← 알림톡 본문 첨부	
MTYPE	3C	13	첨부 2
ENCODING	2C	1	
MFILELEN	10C	100	
MEDIA	100C	{"button_cnt":3,"button1": … .} ←Button정보 Json파일	

➢ DELIVER - 친구톡(대체 발송)

Type	Size	Value	
HeadType	4C	21	
MsgLeng	10C	3716	
MSGTYPE	2C	A	
DA_ADDR	20C	01020001234	
CALLBACK	20C	15880000	
ENCODING	2C	0	
SENDERKEY	41C	cf1060fa976a7875eafae84083649af24f6ad3db	TEXT 대신
TEMPLATE	31C		
METHOD	2C	p	
FAILOVER	2C	2	
TITLE	65C	Replace Title. ← 대체 발송시 제목	
SERIAL	20C	202112310012348	
SENDER_CODE	10C	123456789	
MEDIACNT	2C	2	
EXT_SIZE	4C	0	
MTYPE	3C	11	첨부 1

Type	Size	Value	
ENCODING	2C	0	
MFILELEN	10C	1965	
MEDIA	1965C	친구톡 본문입니다. ..... 본문끝 ← 친구톡 본문 첨부	
MTYPE	3C	13	첨부 2
ENCODING	2C	0	
MFILELEN	10C	1500	
MEDIA	1500C	친구톡 대체 본문입니다. ..... 본문끝 ← 대체 발송 본문 첨부	

➢ DELIVER_ACK

Type	Size	Value
HeadType	4C	22
MsgLeng	10C	44
RESULT	4C	0
DA_ADDR	20C	01020001234
SERIAL	20C	202112310012348

4.4 결과 수신(REPORT)

DLV 세션을 통해 요청된 메시지의 발송 결과를 REP 세션을 통해 결과를 전달 합니다.

[Format]

Type	Field	Size	설명	비 고
REPORT (94Byte)	RESULT	4C	결과 코드	결과 코드 표 참조
	MESSAGE	15C	결과 메시지	- 통신사의 스팸 성공 여부("SS") - 알림/친구톡 실패 시 에러코드("K" + ErrorCode) - 전환/대체 발송시 최종 메시지 타입("T" + Type) * 위 세가지 값이 설정된 경우 ","로 구분된다. Ex) "K2103,TS" - 2103 에러로 SMS로 전환발송 성공
	DA_ADDR	20C	착신 번호	SMSDELIVER 또는 MMSDELIVER 에 설정한 값
	SERIAL	20C	Serial Number	DELIVER 에 설정한 값
	GWSERIAL	16C	GW Serial Number	GW의 Serial Number
	SENDTIME	15C	전송 완료 시간	YYYYMMDDHH24MISS
	TELCOINFO	4C	발송 이통사 정보	'SK' / 'KT' / 'LG' / 'KKO' / 'ETC'(실패 및 기타 통신사일 경우)
REPORT_ACK (40Byte)	RESULT	4C	결과 코드	"7.1 전송 결과 코드" 참조
	SERIAL	20C	Serial Number	DELIVER 에 설정한 값
	GWSERIAL	16C	GW Serial Number	GW의 Serial Number

- 통신사의 스팸 성공 여부 : 통신사에서 스팸메시지로 처리하였으나 결과는 성공으로 처리됨(Spam Success : SS)
- 전환/대체 발송시 최종 메시지 타입 : 알림/친구톡 실패로 인한 전환/대체 발송이 성공일 경우 최종 전송된 메시지 타입(S : SMS , L : LMS , M : MMS)

[Example]

➢ REPORT

Type	Size	Value
HeadType	4C	31
MsgLeng	10C	94
RESULT	4C	0
MESSAGE	15C	
DA_ADDR	20C	01020001234
SERIAL	20C	202112310012348
GWSERIAL	16C	220121140000164
SENDTIME	15C	20211231142201
TELCOINFO	4C	SK

➢ REPORT_ACK

Type	Size	Value
HeadType	4C	32
MsgLeng	10C	40
RESULT	4C	0
SERIAL	20C	202112310012348
GWSERIAL	16C	220121140000164

4.5 Event 수신

Server에서 접속 종료를 하거나, TPS가 변경이 되는 경우 이벤트 정보를 전달 합니다.

- Client는 EVENT 패킷을 수신만 하고 ACK를 전달 할 필요 없습니다.
- Event에 따라 적절한 처리를 하여야 합니다.

[Format]

Type	Field	Size	설명	비 고
EVENT (90Byte)	TYPE	2C	Event Type	0 : 접속 해지시 1 : TPS 변경시
	DATA	88C	Event에 따른 내용	TYPE=0 : 접속 종료 사유 TYPE=1 : 변경된 TPS 값

[Example]

➢ EVENT

Type	Size	Value
HeadType	4C	51
MsgLeng	10C	90
TYPE	2C	1
DATA	88C	80,30,30

5 암호화

Packet을 암호화 할 경우 Server 와 Client는 암호화 키를 생성하고 BIND 시점에 전달한 Key Offset 위치를 기준으로 한 암호화 Key를 사용하여 데이터 암호화를 합니다.

- 암호화는 AES 256Bit 블록 암호화 알고리즘(CBC 모드/Zero IV/PKCS5Padding)을 사용 합니다.
- BIND의 TYPE을 'P' 로 설정하여야 합니다.

5.1 암호화 Key 생성

32Byte의 Null 로 Padding 된 Buffer이며 Password 및 Body 의 AES 256Bit 암호화에 사용합니다.

- 파트너의 ID 발급 시 설정된 Password를 SHA-256으로 Hash 한 값(Hex String - 64Byte)을 기본으로 합니다.
- 0 ~ 64 사이의 임의의 숫자를 Offset 으로 사용하며, 위 Hash 값에서 Offset 부터 32Byte를 최종 암호화 Key로 사용합니다.
- 위 과정에서 정한 Offset을 BIND 시점에 Server로 전달 하여야 합니다.

testpwd

↓ SHA-256 Hash

a85b6a20813c31a8b1b3f3618da796271c9aa293b3f809873053b21aec501087

↓ Offset : 12

31a8b1b3f3618da796271c9aa293b3f8

* Offset 이 60 일 경우 : 32Byte 의 Buffer를 NULL로 Padding 후 앞 4자리에 "1087"만 설정한 값이 Key

5.2 Password 암호화

CERT 또는 BIND의 PWD 필드 암호화 방법입니다.

1. 설정된 Password 를 SHA-256으로 Hash
2. 5.1에서 정의된 암호화 Key를 사용하여 AES 256Bit 암호화
3. Base64 인코딩 후 설정

testpwd

↓ SHA-256 Hash

a85b6a20813c31a8b1b3f3618da796271c9aa293b3f809873053b21aec501087

↓ AES256 & Base64

ONs0wphSMJDVhzcYvm8hN89/bA4NzZQAYQvMstW8d29nm760R2ujAxD0Izo1iKi85uFKfAcOXfMZi

cTfMfJ04mvAby03pCF9sbRDorZ9HNM=

5.3 Body 데이터 암호화

- Header를 제외한 Body만 암호화 하여 송수신 합니다.
- Body 암호화는 해당 패킷 전체를 암호화합니다..(필드별 암호화가 아님)
- CERT / CERT_ACK / BIND / BIND_ACK / EVENT 는 암호화 하지 않고 송수신 합니다..

➢ 위 예제의 SMS DELIVER 패킷을 암호화 Key(31a8b1b3f3618da796271c9aa293b3f8 : Offset 12)로 Body를 암호화 하면 다음과 같습니다.

Type	Size	Value
HeadType	4C	21
MsgLeng	10C	221
MSGTYPE	2C	S
DA_ADDR	20C	01020001234
CALLBACK	20C	15880000
ENCODING	2C	0
TEXT	141C	SMS 테스트 발송 입니다.
SERIAL	20C	202112310012345
SENDER_CODE	10C	101280092
MEDIACNT	2C	0
EXT_SIZE	4C	0

일반 패킷	암호화된 패킷
32 31 00 00 32 32 31 00 00 00 00 00 00 00 53 00	32 31 00 00 32 32 34 00 00 00 00 00 00 00 55 2a
30 31 30 32 30 30 30 31 32 33 34 00 00 00 00 00	53 57 a4 0c b5 b9 33 e1 bf a3 94 19 2e bd ad 1e
00 00 00 00 31 35 38 38 30 30 30 30 00 00 00 00	14 00 c5 a1 f9 52 54 b7 fa 21 ec 15 69 c5 e7 4f
00 00 00 00 00 00 00 00 30 00 53 4d 53 20 c5 d7	f7 c0 92 9c d0 2b 45 55 4d 7a b9 6a 59 dc d9 cf
bd ba c6 ae 20 b9 df bc db 20 c0 d4 b4 cf b4 d9	9c 68 18 4f c3 98 6b aa e6 b6 e8 5b a7 a2 35 94
2e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	2c 7e 27 84 0e 5c db 80 9b 75 9c 26 56 a5 c2 d2
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	b6 4b 58 57 90 00 62 cd 2a 4e 16 ac dc 26 73 ae
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	91 3f b2 1c ea f2 6d aa b4 ab 26 c0 8d 99 cf 6e
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	7c 13 a5 9a aa 77 89 e1 d7 5c ae 9f 4c 7b 58 5f
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	f8 a2 20 af 9c 1e 99 97 b8 ad 4e 29 f7 ea 5e f7
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	ae 63 e5 8e 03 81 15 3e cb 5c 9c 82 79 3c 02 77
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	9f ae 9d 11 d0 ac 38 3f f7 63 1b 71 d0 cf e2 82
00 00 00 00 00 00 00 32 30 32 31 31 32 33 31 30	d2 cc f4 39 f4 ae 95 02 2d 65 0d f4 e7 5e cf 5e
30 31 32 33 34 35 00 00 00 00 00 31 30 31 32 38	a9 99 a0 19 13 1d 57 d9 9e a2 24 05 d5 80 1d 67
30 30 39 32 00 30 00 30 00 00 00	7c a9 ec bd c0 8d b6 dc 8a 3f e0 2b 03 a5

6 첨부 컨텐츠

- 착신 휴대폰의 지원하는 미디어 또는 사양에 따라서 전송이 실패 될 수 있습니다.
- 전송이 성공 되더라도 해당 휴대폰에서 미디어를 볼 수 없을 수 있습니다.
- 이동 통신사의 사정에 따라 첨부 가능한 미디어 및 규격이 변경 될 수 있습니다.
- 본문 메시지를 포함하여 4개까지의 첨부 파일을 지원합니다.
- 첨부파일은 최대 300KB이하를 권장하며, 권장 사이즈 이상 전송 시 전송에 지연이 발생 할 수 있습니다.

6.1 LMS/MMS 컨텐츠 제약

LMS/MMS 전송 시 첨부 가능한 컨텐츠를 아래와 같이 권고 하고 있습니다.

- 텍스트(본문)

  * 최대 2000byte (한글 1000자, 영문 2000자)
  * 한글은 확장 완성형 한글을 지원 합니다.
  * 텍스트 또한 별도의 첨부파일로 간주합니다.
  * Html은 스마트폰에서는 지원하지 않으며 전송 할 경우 Html 소스 그대로 보여질 수 있으며, 일부 스마트폰으로는 전송 실패 될 수 있습니다.
  * 휴대폰에서 지원하지 않는 일부 문자 또는 특수문자를 전송할 경우 전송 실패 될 수 있으며, 전송이 되더라도 내용 확인이 불가합니다.

- 이미지

  * BMP, JPG(JPEG), PNG, GIF 지원가능
  * 최대 첨부 가능 개수 3개이나 이동 통신사에 따라 다름
  * 176*144해상도에 20KB 미만 권장, 최대 320*240해상도에 300KB 미만 권장

- 오디오/비디오

  * 지원 종료

6.2 알림톡/친구톡 컨텐츠 제약

- 텍스트(본문)

  * 최대 1000자 - 영문/한글 구분 없음
  * 친구톡 이미지 : 400자
  * 친구톡 와이드 이미지 : 76자
  * 한글은 확장 완성형 한글 과 UTF-8 지원

  (전환 발송 시 EUC_KR에서 지원하지 않는 문자가 있을 경우 정상 전송 되더라도 보이지 않을 수 있음)

- 대체 발송 텍스트
  * 전송 실패 시 대체 발송할 본문(EUC-KR)을 첨부 할 수 있음
  * 크기에 따라 SMS/LMS로 자동 구분되어 발송

- 친구톡 이미지
  * JPG(JPEG), PNG 지원가능 / 최대 500KB
  * 권장 사이즈 : 720px * 720px
  * 전송 실패 시 전환/대체 발송을 원하는 경우 사전 등록된 이미지 첨부하여 발송

- 친구톡 와이드 이미지
  * JPG(JPEG), PNG 지원가능 / 최대 2MB
  * 제한 사이즈 : 800px * 600px
  * 전송 실패 시 전환/대체 발송을 원하는 경우 사전 등록된 이미지 첨부하여 발송

- 부가 정보 파일(Json)
  * 알림톡/친구톡의 버튼 정보, 이미지 URL 정보, 강조 등 본문내용을 제외한 부가적인 옵션들의 정보들로 구성된 Json형식의 파일로 별도의 첨부파일로 첨부
  * 전환/대체 발송 시 에는 부가정보는 무시되고 본문 혹은 대체 발송 텍스트만 전송됨

  * 상세 명세는 아래와 같은 파일명으로 된 별첨 문서를 참고하세요.

  ➢ 별첨_한진정보통신_Kakao_AddedInfo_yyyymmdd.pdf

7 Error Code

7.1 전송 결과 코드

Error Code의 상세 명세는 아래와 같은 파일명으로 된 별첨 문서를 참고하세요.

- 별첨_한진정보통신_ErrorCode_Version_yyyymmdd.xlsx

7.2 재전송 결과 코드

- Error Code 문서상의 "재시도" 라고 표시된 코드는 DELIVER_ACK에 수신되는 Error Code로 파트너사에서 재전송 처리를 하여야 하는 코드입니다.
- 그중 E_SYS_FAIL, E_SYS_BUSY, E_NET_FAIL, E_TPS_OVER 4가지 경우는 가능하면 재전송을 하여야 하며, 그 외 결과 코드는 상황에 맞게 처리합니다.
- DELIVER_ACK로 E_OK를 제외한 에러가 발생 하였을 경우에는 메시지가 Server로 인입이 되지 않은 상태이므로 서버에서 조회 할 수 없습니다.