

시험 성적서

한국정보통신기술협회

주소: 경기도 성남시 분당구 분당로 47
전화: 031-780-9189 Fax: 031-724-0169

성적서번호 : TTA-21-0982-01



1. 의뢰자

- 기관명 : (주)지에스티엘
- 주소 : 경기도 이천시 신둔면 경충대로3233번길

2. 시료 : 특정소출력 무선기기(모델명: BFX-UA300)

3. 시험기간 : 2021. 7. 30.

4. 시험방법 : 시험 내용 및 결과 참조

5. 시험결과 : 시험 내용 및 결과 참조

이 성적서의 시험 결과는 의뢰자에 의해 제공된 시료에 한하며 용도 이외의 사용을 금합니다.

확 인

작성자

성명 : 홍성욱

홍성욱

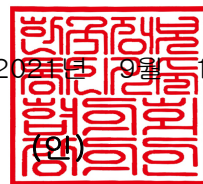
승인자

성명 : 김지명

김지명

2021년 9월 13일

한국정보통신기술협회 회장



※ You can verify the forgery and authenticity by the barcode at the end of this document.

(주)지에스티엘

특정소출력 무선기기(모델명: BFX-UA300)

TTA Tested 시험



본 문서는 한국정보통신기술협회(TTA) 방송통신인프라단의 시험 성적서로서 누구든지 TTA의 사전승인 없이는 문서의 일부분만을 발췌하거나 인용하여 사용하거나 배포할 수 없습니다.



목 차

1. 개요	4
가. 시험 목적	4
나. 시험 대상 기술기준	4
다. 시험 절차	4
라. 시험 대상 장비	4
마. 시험 장비	5
바. 시험 구성도	5
2. 시험 내용 및 결과	6
가. CA Token 요청 메시지 확인	6
나. 제한수신 모듈 요청 및 Acknowledgement 메시지 확인	7
다. 동적 ID(Dynamic ID) 갱신 저장 확인	8
라. SVM 시스템콜(System Call) 동작 확인	8
마. 다운로드한 제한수신 모듈을 이용한 스크램블(암호화) 콘텐츠 시청 확인	9
바. 다운로드 받은 제한수신 모듈 ID를 이용한 스크램블(암호화) 콘텐츠 시청 확인	9
사. 서로 다른 제한수신 모듈과의 호환성 확인	10
3. 시험 결과 요약	11



한국정보통신기술협회(TTA) 방송통신인프라단에서는 (주)지에스티엘에서 시험 의뢰한 특정소출력 무선 기기(BFX-UA300)의 IPTV 가입자 단말장치 제한수신 규격(iCAS) 적합성평가 시험에 대한 시험 성적서를 제출한다. 시험 결과는 본 성적서의 시험환경 및 의뢰제품 모델에만 국한된다.

1. 개요

가. 시험 목적

본 시험은 IPTV 가입자 단말장치에 대하여 유선설비의 적합성평가 처리방법, 제 9조, 『별표 7. 인터넷 멀티미디어 방송용 가입자 단말장치 시험방법』 (전파연구소공고 제2015-104호, 2015.11.24)의 “10. 인터넷 멀티미디어 방송 가입자 단말장치의 제한수신 규격” 및 “IPTV 용 교환 가능한 CAS(iCAS)”(TTAK.KO-08.0023/R2) 표준의 적합 여부를 확인한다.

나. 시험 대상 기술기준

『인터넷 멀티미디어 방송사업의 방송통신설비에 관한 기술기준』 (전파연구소고시 제2016-28호, 2016.12.19), 제 3장 가입자 단말장치 기술기준이다.

다. 시험 절차

유선설비의 적합성평가 처리방법, 제 9조, 『별표 7. 인터넷 멀티미디어 방송용 가입자 단말장치 시험방법』의 “10. 인터넷 멀티미디어 방송 가입자 단말장치의 제한수신 규격” 및 “IPTV 용 교환 가능한 CAS(iCAS)”(TTAK.KO-08.0023/R2)에 따라 시험한다.

라. 시험 대상 장비

본 IPTV 가입자 단말장치 제한수신 규격(iCAS) 적합성평가 시험은 (주)지에스티엘에서 의뢰한 시험 대상 장비는 <그림 1>과 같으며 제품 정보는 다음과 같다.

- 제조사: 주식회사 에이엘티
- 모델명: BFX-UA300
- 전원 어댑터(모델명): Weihai Sunlin Electronics Co., Ltd.(LA-B271KS)



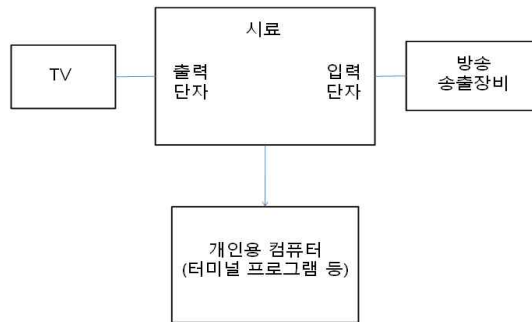
※ You can verify the forgery and authenticity by the barcode at the end of this document.

마. 시험 장비

- 스크램블(암호화)되어 있는 인터넷 멀티미디어 방송 서비스용 콘텐츠
- 인터넷 멀티미디어 방송 송출장비(다음의 장비 혹은 기능을 포함함)
 - 제한수신 서버(Conditional Access System, CAS)
 - 가입자 관리 시스템(Subscriber Management System, SMS)
 - 제한수신 모듈(CAS S/W) 다운로드 서버
- 디지털 텔레비전
- 제한수신 모듈(S/W)

바. 시험 구성도

IPTV 가입자 단말장치 제한수신 규격(iCAS) 적합성평가 시험환경 구성은 <그림 2>와 같다. 방송 송출장비는 스크램블(암호화)된 방송스트림을 계속적으로 송출하고 있으며, 시험시료의 동작 결과는 TV 화면, 방송 송출장비의 데이터 분석 화면, 컴퓨터의 로그 분석 화면 등을 통해 확인한다.



<그림 2> 시험구성도



2. 시험 내용 및 결과

가. CA Token 요청 메시지 확인

(1) 개요

가입자 단말장치가 전송하는 CA Token 요청 메시지 형식이 “IPTV용 교환 가능한 CAS(iCAS)” (TTAK.KO-08.0023/R1) 및 “IPTV용 교환 가능한 CAS(iCAS)” (TTAK.KO-08.0023/R2) 표준에서 정의하고 있는 SSL/TLS 통신방식 혹은 전자봉투 방식의 CA Token 요청 메시지 형식인지 확인한다.

(2) 시험 절차

- (가) 가입자 단말장치가 콘텐츠 시청을 시도하도록 설정하여 콘텐츠 시청 권한 획득을 위한 CA To-ken(Content Access Token)을 요청하도록 한다.
- (나) 가입자 단말장치가 가입자 관리 시스템으로 전달한 CA Token 요청 메시지의 내용을 확인한다.

(3) 판정 기준

가입자 단말장치가 전송하는 CA Token 요청 메시지는 SSL/TLS 통신방식인 경우 다음과 같이 구성되어 있어야 한다.

```
Version (1byte)
Type (1byte)
Command (2bytes)
Length (4bytes)
Device ID (32bytes)
Number of ContentID (4bytes)
(CID 1 || ... || CID N) (N * 4bytes)
```

가입자 단말장치가 전송하는 CA Token 요청 메시지는 전자봉투 방식인 경우 다음과 같이 구성되어 있어야 한다.

```
Version (1byte)
Type (1byte)
Command (2bytes)
Length (4bytes)
Cert length (4bytes)
Cert(w bytes)
Encryption Algorithm (1byte)
SMS_CERT_PUB Encrypted Data Length (3bytes)
E{SMS_CERT_PUB, (CEK Type || CEK)} (x bytes)
Number of ContentID (4bytes)
E{CEK, (CID 1 || CID2 || .... || CID N) || Device ID || Nc} (y bytes)
Signature Algorithm (1byte)
```



Signature Length (3bytes) Signature (z bytes)
--

(4) 시험 결과

가입자 단말장치가 전송하는 CA Token 요청 메시지는 SSL/TLS 통신방식인 경우 다음과 같이 구성되어 있어야 한다.

시험기	판정
가입자 단말장치가 SSL/TLS 통신방식의 CA Token 요청 메시지를 판정 기준의 메시지 형식대로 전송함	적합

나. 제한수신 모듈 요청 및 Acknowledgement 메시지 확인**(1) 개요**

가입자 단말장치가 전송하는 제한수신 모듈 요청 메시지 형식이 “IPTV용 교환 가능한 CAS(iCAS)”(TTAK.KO-08.0023/R1) 및 “IPTV용 교환 가능한 CAS(iCAS)”(TTAK.KO-08.0023/R2) 표준에서 정의하고 있는 제한수신 모듈 요청 메시지 형식인지 확인한다.

(2) 시험 절차

- (가) 가입자 단말장치가 콘텐츠 시청을 위한 제한수신 모듈 요청을 시도하도록 설정한다.
(나) 가입자 단말장치가 제한수신 모듈 다운로드 서버로 전달한 제한수신 모듈 요청 메시지의 내용을 확인한다.

(3) 판정 기준

가입자 단말장치는 다음의 제한수신 모듈 요청 메시지 형식으로 제한수신 모듈 요청 메시지를 전송하는지 확인한다.

Version (1byte) Type (1byte) Command (2bytes) Length (4bytes) Device ID (32bytes) DynID (32bytes) Number of CAS SW (=n) (4bytes) (CAS SW ID 1 CAS SW ID2 CAS SW IDn) (n*4bytes) CA Token Length (=y) (4bytes) CA Token (y bytes)

또한, 다음의 Acknowledgement 메시지 형식으로 Acknowledgement 메시지를 전송하는지 확인한다.



Version (1byte)
 Type (1byte)
 Command (2bytes)
 Length (4bytes)
 Result(1byte)
 Reason(3bytes)
 Device ID (32bytes)
 New DynID (32bytes)

(4) 시험 결과

시험기	판정
가입자 단말장치가 판정 기준의 제한수신 모듈 요청 메시지 형식 및 Acknowledgement 메시지 형식대로 메시지를 전송함	적합

다. 동적 ID(Dynamic ID) 갱신 저장 확인**(1) 개요**

가입자 단말장치가 전송하는 매회 제한수신 모듈 요청 메시지마다 갱신된 동적 ID를 포함하고 있어야 한다.

(2) 시험 절차

- (가) 가입자 단말장치가 최소 3회 이상 제한수신 모듈을 다운로드 받도록 설정한다.
 (나) 매 회마다 제한수신 모듈 요청 메시지 내용을 확인한다.

(3) 판정 기준

매회 제한수신 모듈 요청 메시지마다 갱신된 동적 ID를 포함하고 있어야 한다.

(4) 시험 결과

시험기	판정
가입자 단말장치의 매회 제한수신 요청 메시지마다 갱신된 동적 ID를 포함하고 있음	적합

라. SVM(Secure Virtual Machine) 시스템콜(System Call) 동작 확인**(1) 개요**

SVM 시스템콜이 각 기능에 맞게 지원되어야 한다.



※ You can verify the forgery and authenticity by the barcode at the end of this document.

(2) 시험 절차

- (가) 가입자 단말장치의 SVM 시스템콜을 호출하는 제한수신 모듈이 가입자 단말장치로 다운로드 되어 실행되도록 설정한다.
- (나) 가입자 단말장치가 SVM 시스템콜을 지원하는지 확인한다.

(3) 판정 기준

SVM 시스템콜이 정의된 기능을 지원해야 한다.

(4) 시험 결과

시험기	판정
가입자 단말장치의 SVM 시스템콜이 정의된 기능대로 동작함	적합

마. 다운로드한 제한수신 모듈을 이용한 스크램블(암호화) 콘텐츠 시청 확인

(1) 개요

다운로드한 제한수신 모듈을 이용한 스크램블(암호화) 콘텐츠 시청이 지원되어야 한다.

(2) 시험 절차

- (가) 인터넷 멀티미디어 방송 송출장비로부터 스크램블(암호화)된 콘텐츠를 송출한다.
- (나) 가입자 단말장치가 해당 콘텐츠를 시청할 수 있도록 제한수신 모듈 요청(검증) 및 다운로드를 완료하도록 설정한다.
- (다) 다운로드 받은 제한수신 모듈로 콘텐츠의 시청 여부를 확인한다.

(3) 판정 기준

스크램블(암호화)된 콘텐츠의 시청이 가능해야 한다.

(4) 시험 결과

시험기	판정
가입자 단말장치에서 스크램블(암호화)된 콘텐츠의시청이 가능함	적합

바. 다운로드 받은 제한수신 모듈 ID를 이용한 스크램블(암호화) 콘텐츠 시청 확인

(1) 개요

다운로드 받은 제한수신 모듈 ID를 이용한 스크램블(암호화) 콘텐츠 시청이 지원되어야 한다.



※ You can verify the forgery and authenticity by the barcode at the end of this document.

(2) 시험 절차

- (가) 위 2.마. 시험을 완료한 상태에서 콘텐츠 시청을 중단하고, 해당 콘텐츠에 대한 시청을 재시도하여 가입자 단말장치가 제한수신 모듈을 재요청하도록 설정한다.
- (나) 제한수신 모듈 다운로드 서버에서 제한수신 모듈 요청에 대한 응답 메시지로 콘텐츠의 시청이 가능한 제한수신 모듈 ID를 송출한다.
- (다) 가입자 단말장치가 수신한 제한수신 모듈 ID에 해당하는 제한수신 모듈로 콘텐츠의 시청이 가능한지 확인한다.

(3) 판정 기준

스크램블(암호화)된 콘텐츠의 시청이 가능해야 한다.

(4) 시험 결과

시험기	판정
가입자 단말장치가 응답으로 받은 제한수신 모듈 ID로 해당 제한수신 모듈을 실행시켜 스크램블(암호화)된 콘텐츠의 시청이 가능함	적합

사. 서로 다른 제한수신 모듈과의 호환성 확인

(1) 개요

서로 다른 제한수신 모듈과의 호환성이 지원되어야 한다.

(2) 시험 절차

- (가) 제한수신 모듈 다운로드 서버에 2개 이상의 서로 다른 제조사의 제한수신 모듈을 준비한다.
- (나) 인터넷 멀티미디어 방송 송출장비로부터 서로 다른 제한수신 모듈로 시청할 수 있는 스크램블(암호화)된 콘텐츠를 송출한다.
- (다) 가입자 단말장치는 각 스크램블(암호화)된 콘텐츠의 시청을 시도하여, 각 콘텐츠에 따른 제한수신 모듈을 다운로드 받고, 이를 이용하여 해당 콘텐츠의 시청이 가능한지 확인한다.

(3) 판정 기준

스크램블(암호화)된 콘텐츠의 시청이 가능해야 한다.

(4) 시험 결과

시험기	판정
가입자 단말장치에서 스크램블(암호화)된 콘텐츠의 시청이 가능함	적합



3. 시험 결과 요약

업체명	(주)지에스티엘		
제조사/모델명	제조사: 주식회사 에이엘티 / 모델명: BFX-UA300		
시험 절차	유선설비의 적합성평가 처리방법, 제 9조, 『별표 7. 인터넷 멀티미디어 방송용 가입자 단말장치 시험방법』의 “10. 인터넷 멀티미디어 방송 가입자 단말장치의 제한수신 규격” 및 “IPTV 용 교환 가능한 CAS(iCAS)”(TTAK.KO-08.0023/R2) 표준을 적용함		
시험 항목	No.	시험항목	적합/부적합
	1	CA Token 요청 메시지 확인	적합
	2	제한수신 모듈 요청 및 Acknowledgement 메시지 확인	적합
	3	동적 ID(Dynamic ID) 갱신 저장 확인	적합
	4	SVM 시스템콜(System Call) 동작 확인	적합
	5	다운로드한 제한수신 모듈을 이용한 스크램블(암호화) 콘텐츠 시청 확인	적합
	6	다운로드 받은 제한수신 모듈 ID를 이용한 스크램블(암호화) 콘텐츠 시청 확인	적합
	7	서로 다른 제한수신 모듈과의 호환성 확인	적합
시험 결과	(주)지에스티엘에서 의뢰한 특정소출력 무선기기(BFX-UA300)는 유선 설비의 적합성평가 처리방법, 제9조, 『별표 7. 인터넷 멀티미디어 방송용 가입자 단말장치 시험방법』의 “10. 인터넷 멀티미디어 방송 가입자 단말장치의 제한수신 규격”에서 요구하는 모든 시험 항목을 통과하였음		



※ You can verify the forgery and authenticity by the barcode at the end of this document.