의 견 서

1. 배경 설명
   A. 현재 iCAS 표준안은 특정 업체에서 개발한 기술을 제안한 것으로서, 실제 IPTV 서비스에 접목하여 상용 서비스에 사용할 수 있는 기술인지 공개적으로 검증되지 않음
   B. 현 표준안의 핵심 기술인 SVM에 대한 구현 가능성이 검증되지 않은 상황에서 표준으로 제정되어 효력을 발휘하는 것은 매우 높은 위험성을 내포하고 있음
   C. 지난 2/11 TTA IPTV iCAS 표준안 설명회에서 여러 업체에서 지적한 우려 사항으로
      i. **SVM의 성능**,
      ii. SVM의 플랫폼 독립성 (CPU/OS)
      이 있었는데, 위 두 가지 사항은 SVM의 CAS 실행 환경으로서의 가능성을 판단하는데 핵심적인 요구 사항임
   D. 표준안 제안사(삼성전자)의 핵심 개발 연구원이 참석하여 밝힌 '성능' 및 '이식성'에 대한 체계적인 검증 방법과 검증 일정이 도출되어 공개적으로 구현 가능성에 대한 검증이 선행되어야 함
   E. SVM의 구현 가능성이 검증될 때까지 한가지 방안에 의존하여 표준화를 추진하면 만약 검증이 실패하였을 경우에 예상되는 위험성이 매우 크기 때문에, 합리적으로 선택할 수 있는 대안을 포함하는 방향으로 표준화를 진행하는 것이 타당하다고 판단함
   F. 본 의견서에 포함된 내용은 현재 표준안의 위험성을 회피할 수 있도록, 단말의 성격에 따라서 이동성에 대한 요구사항이 필수적이지 않은 사업자 전용 단말기에 적용할 수 있는 방안의 틀을 제안하는 것임
   G. 대안으로 제안하는 방식의 구체적인 규격은 본 표준안의 개정 절차에 따라 SVM의 상세 규격이 작성되는 것과 병행하여 여러 업체의 참여를 통해서 구체화될 수 있을 것으로 예상됨

[과제번호 2008-686]

의견 항목	CAS S/W 실행환경 관련
원안	- CAS S/W 의 Runtime Environment 로 SVM 만을 지정함 - 3.8.절 본문 중 "SVM 은 S/W 혹은 별도 H/W 로 구현될 수 있다."라는 표현
대안	- CAS Runtime Environment (CRE) 용어와 개념을 추가로 정의함 - 이동성 단말(Portable Device, PD)과 사업자 공급 단말(Non-Portable Device, NPD)을 구분하여 용어 및 개념을 추가로 정의함 - CRE 로 가능한 방안을 다음과 같이 선택 가능하도록 표준을 확장함 1. CAS 실행환경 (CAS Runtime Environment, CRE) - "CRE 는 S/W 혹은 별도 H/W 로 구현될 수 있다." 1.1. H/W 기반 CRE 1.1.1. Security Processor (SP) - 특별히 높은 보안성이 필요한 경우에 적용 - 인터페이스 및 프로토콜의 구체적인 내용은 추후 제정함 1.2. S/W 기반 CRE 1.2.1. Secure Virtual Machine (SVM) - PD, NPD 의 경우에 모두 적용할 수 있음 - 현 표준안에 정의된 내용을 그대로 적용함 1.2.2. Virtual Security Processor (VSP) - 사업자가 구매하여 가입자에게 직접 배포하는 NPD 에만 적용 - SVM 과 동일한 보안 요구사항을 적용함
사유	CAS S/W 실행환경을 SVM 으로 제한하는 것은 사업자의 현재 사업 모델을 고려했을 때 지나치게 제한적인 측면이 있다. 즉, 사업자가 직접 구매하여 가입자에 제공하는 단말의 경우에는 보통 사업자간 이동성을 필요로 하지 않기 때문에, 이러한 단말의 경우에는 사업자의 선택에 의하여 CAS S/W 실행환경으로 SVM 을 사용하는 대신 동일한 프로토콜과 기능을 수행하는 가상보안프로세서(VSP)를 사용할 수 있도록 허용하는 것이 바람직하다. 또한, 본문 중에 SVM 을 H/W 로 구현하는 경우는 Virtual Machine 이 아니라, Actual Machine 으로 기능을 구현하는 것이기 때문에 "SVM 은 S/W 혹은 별도 H/W 로 구현될 수 있다."라는 표현은 좀더 포괄적으로 수정하여 "CRE 는 S/W 혹은 별도 H/W 로 구현될 수 있다."로 변경하는 것이 바람직하다.

[과제번호 2008-686]

의견 항목	Secure VM 요구사항
원안	**3.8.1. Secure VM 요구사항** 여러 가지 공격에 대응하여 콘텐츠와 서비스를 안전하게 보호하기 위해서 SVM 은 다음의 보안 요구사항을 만족해야만 한다. • **CAS S/W 인증:** SVM 에 적재되어 실행되는 모든 CAS S/W 는 믿을 수 있는 기관이 인증한 코드이어야 한다. (이후 생략)
대안	**3.8.1. Secure VM 요구사항** IPTV 단말의 이동성을 보장하고, 여러 가지 공격에 대응하여 콘텐츠와 서비스를 안전하게 보호하기 위해서 SVM 은 다음의 요구사항을 만족해야만 한다. • **CPU 독립성 :** SVM 에 적재되어 실행되는 CAS S/W 는 단말 CPU 의 종류(예를 들면, RISC 계열 - ARM, MIPS, CISC 계열 - INTEL, AMD 등)에 관계없이 동일한 이미지(바이너리)로 컴파일되고 실행되어야 한다. • **OS 독립성 :** SVM 에 적재되어 실행되는 CAS S/W 는 단말 OS 의 종류(예를 들면, MS Windows 계열 OS, Linux/UNIX, RTOS - vxWorks, UCOS 등)에 관계없이 동일한 이미지(바이너리)로 컴파일되고 실행되어야 한다. • **CAS S/W 인증:** SVM 에 적재되어 실행되는 모든 CAS S/W 는 믿을 수 있는 기관이 인증한 코드이어야 한다. (이후 생략)
사유	지난 2/11 iCAS 설명회에서 제안 업체의 연구원이 밝힌 SVM의 플랫폼 독립성은 표준안에서 단말의 이동성 확보에 가장 중요한 핵심 요구사항이다. (매우 확보하기 어려운 핵심적인 기술이라고 판단되지만, 제안업체(삼성전자)에서 이와 관련된 기술을 이미 확보했다고 밝혔으므로, 검증을 위한 절차가 필요하며, 이를 위해 핵심 노하우가 즉시 공개되어야 할 것으로 판단됨) 그러므로, 원안에 포함되어 있는 Secure VM의 보안 요구사항에 추가하여, 가상머신으로서의 기본적 요구사항이 명시적으로 포함되어야 한다. 플랫폼 독립성은 단말에서 사용하는 CPU와 OS에 대한 독립성을 의미하므로 위와 같이 두 가지 항목을 추가할 것을 제안한다.

[과제번호 2008-686]

의견 항목	CAS S/W API 관련
원안	**3.8.5. System Call** (중간생략) 본 규격에서는 기본적인 System Call 들에 대해서만 정의하고, 개별 CAS S/W 서비스를 위해 필요한 System Call 들은 상기에서 정의한 System Call API 에 따라 자유롭게 추가 정의하여 사용하는 것이 가능하며, 이에 대한 구체적인 사항들은 규격의 범위에 포함하지 않는다.
대안	**3.8.5. System Call** (중간생략) 단말의 이동성(Portability)을 보장하며 CAS S/W 서비스를 제공하기 위해 필요한 System Call(들)을 다음과 같이 정의한다. 본 규격은, CAS S/W 의 호환성 보장을 위해, 본 규격에서 정의하는 API 를 제외한 추가 API 의 사용을 권장하지 않는다. 3.8.5.1. (이후 구체적인 System Call API 정의)
사유	단말의 이동성을 보장하기 위해 가상머신을 도입하기로 하면서 CAS S/W API 를 자유롭게 추가가능하도록 한 부분은 모순이다. 이를 허용하게 되면 SVM for A-CAS, SVM for B-CAS 와 같이 호환성을 보장할 수 없기 때문이다. 참여하는 CAS 벤더의 모든 의견을 모아서 CAS S/W API 를 구체적으로 정하는 것이 규격에서 SVM 을 도입한 취지를 제대로 살릴 수 있는 방안으로 생각된다.

2010 년 2 월 22 일

회사(단체)명 : LG 전자

한국정보통신기술협회 회장 귀하