

<p>차 량 ICT 기 반</p> <p>긴 급 구 난 체 계 (e-Call)</p> <p>제 5 부 : 데 이 터 보 안 지 침</p> <p>20XX</p>	<div> <div> <div>지능형 교통시스템 표준</div> <div>ITSK-000XX:20XXv2</div> </div> <div> <div>제정일 : 20XX년XX월XX일</div> <div>개정일 : 20XX년XX월XX일</div> </div> </div> <div> <div>차량 ICT 기반</div> <div>긴급구난체계(e-Call)</div> <div>- 제 5 부: 데이터 보안 지침</div> <div>Automotive ICT based</div> <div>e-Call system</div> <div>- Part 5: Guide-line for</div> <div>Data Security</div> </div> <div>2016 (Ver1.0)</div> <div>한국지능형교통체계협회</div>
---	---

표준(안)문서 버전 이력 (작성 예시)

문서 버전	문서변경 일자	문서변경 내용
Ver1.0	2016.07.4	▪ ITS 단체표준 제안
		▪
		▪
		▪
		—

## 머 리 말

본 단체표준은 차량 ICT 기반 긴급구난체계(e-Call) 시스템의 주요 보호대상 데이터를 식별하고 해당 데이터를 다양한 위협으로부터 안전하게 보호하기 위한 방안을 제공하는데 목적이 있다.

본 표준은 미래창조과학부의 「정보통신·방송 연구개발」사업의 지원을 받아 작성되었습니다.

# <목 차>

제1장 서문 .....	1
1. 제정목적 .....	1
2. 적용범위 .....	1
2.1. 표준의 구성 .....	1
3. 정의 .....	1
4. 약어 .....	2
5. 참조표준 .....	2
5.1. 준용표준 .....	3
5.2. 국내·외 참조표준 .....	3
5.3. 준용/참조한 표준과 본 표준의 비교표 .....	3
5.4. 참고 문서 .....	3
6. 지적재산권 관련 사항 .....	3
7. 표준이력 .....	3
7.1. 표준이력 .....	3
7.2. 주요개정사항 .....	3
 제2장 차량 ICT 기반 e-Call 데이터 보안 지침 개요 .....	4
 제3장 e-Call 시스템에서 발생하는 데이터의 종류 .....	5
 제4장 e-Call 시스템 구간 별 데이터 종류 및 위협 .....	7
1. e-Call 단말 내부 구간 .....	7
2. e-Call 단말 - e-Call 센터 간 통신 구간 .....	8
3. e-Call 센터 내부 구간 .....	8
 제5장 e-Call 시스템 구간 별 보안 지침 .....	9
1. e-Call 단말 내부 구간 보안 .....	9
2. e-Call 단말 - e-Call 센터 간 통신 구간 보안 .....	9
3. e-Call 센터 내부 구간 보안 .....	10

# 제1장 서 문

## 1. 제정목적

본 표준은 차량 ICT 기반 긴급구난체계(e-Call) 시스템에서 발생하는 데이터를 안전하게 보호하기 위한 방안을 제시한다.

## 2. 적용범위

본 표준은 e-Call 시스템의 구간별 보호 데이터를 정의하고, 해당 데이터에 발생할 수 있는 위협을 정의한다. 또한 발생 가능 위협에 대한 대응 방안을 제시한다.

### 2.1. 표준의 구성

본 표준의 내용은 e-Call 시스템에서 발생하는 데이터의 종류, e-Call 시스템 구간 별 데이터 종류 및 위협, e-Call 시스템 구간 별 보안 방안으로 구성된다.

#### 2.1.1. e-Call 시스템에서 발생하는 데이터의 종류

e-Call 시스템에서 발생할 수 있는 데이터를 나열하고, 종류 별로 분류한다.

#### 2.1.2. e-Call 시스템 구간 별 데이터 종류 및 위협

e-Call 시스템 구간 별 보호 대상 데이터와 해당 구간에서 발생할 수 있는 위협을 소개한다.

#### 2.1.3. e-Call 시스템 구간 별 보안 지침

e-Call 시스템 구간 별 발생 가능 위협에 대해 제공해야 하는 보안 기능과 권장 사항을 제시한다.

## 3. 정의

- a) e-Call 단말(AECD, Accident Emergency Call Devices) : e-Call 단말은 다음의 기능을 지원하는 장치 또는 장치들의 집합으로 정의
  - 다양한 센서로 부터 사고 판단에 필요한 정보를 수집하거나 SOS 버튼 등에 의한 수동 e-Call 서비스 개시 신호를 수신
  - 다양한 센서로 부터 수신한 정보를 기반으로 사고 발생여부를 판단
  - 차량의 위치 정보를 수신하거나 차량의 위치를 결정
  - e-Call 센터로 사고 정보를 전송

- e-Call 센터의 운영요원과 음성통화 기능을 제공
- b) e-Call 센터(e-Call Center) : e-Call 단말로부터 수신한 사고 정보를 기반으로 사고 발생을 최종적으로 판단하고 구조 기관에 구조 요청을 전달하는 기능을 수행하며, PSAP(Public Safety Answering Point)과 Proxy PSAP 기능으로 구성
- c) e-Call 시스템 : e-Call 서비스 제공을 위해 필요한 모든 기능의 집합으로 e-Call 단말과 e-Call 센터를 포함
- d) 사고 정보(MSD, Minimum Set of Data) : 사고 발생시 e-Call 단말이 e-Call 센터로 전송하는 정보로 사고와 직접적으로 관련된 정보(사고 차량의 위치, 사고 발생 시각 등) 및 부가적인 정보(운전자의 연락처 등)를 포함
- e) PSAP(Public Safety Answering Point) : 탑승자와의 음성통화를 통해 최종 사고 판단을 진행하고, 구조 기관에 출동 요청을 하는 기능을 수행
- f) Proxy PSAP(Proxy Public Safety Answering Point) : e-Call 단말로부터 사고 정보를 수신하고, ARS 기능을 이용하여 차량 탑승자와 음성통화를 진행하고 사고 여부를 판단한다. 대응이 필요한 사고로 추정될 경우 수신한 사고 정보를 PSAP으로 전달하고, 연결 중인 음성통화를 PSAP으로 연결
- g) 차량 센서(Vehicle Sensor) : 차량에 장착된 충돌 센서, 에어백 전개 센서, 가속도 센서 등으로 사고 판단에 필요한 정보를 제공
- h) 외장 센서(External Sensor) : 차량 센서 이외에 e-Call 단말이 사고 판단을 위해 필요한 정보를 제공하는 센서로, AM용 e-Call 단말에 장착 또는 연결된 가속도 센서 등이 해당
- i) 사고 정보(MSD) : 데이터를 기반으로 사고판단 시, e-Call 센터에서 e-Call 단말로 사고 심각도를 판단하기 위한 회신 통화를 정의한다. 사고의 규모와 구급차 등의 출동이 필요 없는 경미한 사고의 신고를 방지하기 위해, e-Call 센터는 e-Call 단말에 음성통화(Callback)을 반드시 시도해야 한다.

## 4. 약어

AECD	Accident Emergency Call Devices, e-Call 단말
MSD	Minimum Set of Data, 사고 정보
PSAP	Public Safety Answering Point, e-Call 센터

## 5. 참조표준 및 문서

### 5.1. 준용표준

해당사항 없음

## 5.2. 국내 · 외 참조 표준

해당사항 없음

## 5.3. 준용/참조한 표준과 본 표준의 비교표

해당사항 없음

## 5.4. 참고 문서

해당사항 없음

# 6. 지적재산권 관련 사항

해당사항 없음

# 7. 표준이력

## 7.1. 표준이력

판수	제정 · 개정일	제정 · 개정 내역

## 7.2. 주요개정사항

해당사항 없음

## 제2장 차량 ICT 기반 e-Call 데이터 보안 지침 개요

e-Call 시스템에서 사용하는 데이터를 분류해 보면, 단말 등록 정보, 차량으로부터 수집하는 정보, MSD 정보, 음성 통화 정보, e-Call 센터 정보, 암호화에 필요한 중요 정보로 나누어 볼 수 있다. 각 정보는 그 종류에 따라 공격자에게 다양한 용도로 악용될 수 있다.

예를 들어, 단말 등록 정보에는 사용자 식별과 단말 식별 등에 필요한 정보가 포함되어 있을 수 있으므로, 해당 정보가 유출되면 공격자가 신분을 위장한 다양한 2차 공격을 감행할 수 있다. 차량으로부터 수집하는 정보는 사고를 판단하는데 핵심이 되는 정보로서, 공격자가 해당 정보를 변조하여 사고가 나지 않았는데도 사고가 난 것처럼 위장할 수 있다. 공격자가 e-Call 센터 접속 정보를 조작한다면, e-Call 단말이 전송한 사고 정보가 공격자가 지정한 서버로 전송되게 할 수 있다.

따라서, e-Call 시스템의 각 구간의 보호 대상이 되는 데이터에 대한 정의와 이와 같은 데이터에 대해 발생할 수 있는 위협에 대한 정의가 선행되어야 하며 이에 따라 각 구간 별 보안 지침을 마련하는 것이 필요하다.



## 제3장 e-Call 시스템에서 발생하는 데이터의 종류

e-Call 시스템에서 발생할 수 있는 데이터는 다음 표와 같이 분류할 수 있다.

식별 번호	데이터 종류	설 명
D-1	단말 등록 정보	e-Call 서비스를 제공받기 위한 사전 등록 절차가 존재하는 경우, 발생하는 정보
D-2	차량으로부터 수집하는 정보	e-Call 단말이 사고판단 및 차량정보 전송을 위해 차량 혹은 내외장 센서로부터 수집한 다양한 정보
D-3	MSD 정보	e-Call 단말이 사고 발생 감지 후 e-Call 센터로 전송하는 사고 정보
D-4	음성 통화 정보	e-Call 센터가 MSD 수신 후 사고 확인을 위해 음성통화를 시도하는데, 이 때 e-Call 단말과 e-Call 센터간 상호간 전송되는 음성 데이터
D-5	e-Call 센터 정보	e-Call 센터 접속을 위한 정보
D-6	암호화에 필요한 중요 정보	e-Call 시스템에 적용할 암호화 알고리즘에 사용할 키 값 등 중요정보

### 1. 단말 등록 정보

e-call 서비스를 제공받기 위한 사전 등록 절차가 존재하는 경우 발생하는 정보로, 다음과 같은 정보가 포함되어 있을 수 있다.

- 사용자 식별 정보 : 사용자 이름, ID, 비밀번호 등
- 단말 식별 정보 : 공장제조번호, e-call에서 부여한 단말 식별 번호 등

### 2. 차량으로부터 수집하는 정보

e-call 단말이 차량, 사고판단 및 차량정보 전송을 위해 차량 혹은 내외장 센서로부터 수집한 다양한 정보로서, 다음과 같은 정보가 포함되어 있을 수 있다.

- 에어백 전개 정보
- 차대 번호
- 연료 종류
- 위치 정보
- 진행 방향 정보

- 탑승 인원
- 적재 화물 종류
- 속도 정보
- 가속도 정보
- 차량 자세 정보
- 바퀴 구름 정보

### 3. MSD 정보

e-call 단말이 사고 발생 감지 후 e-Call 센터로 전송하는 사고 정보로서, 다음과 같은 정보가 포함되어 있다.

- 사고정보버전
- 메시지 식별자
- 제어 종류
- 차량 종류
- 차량 연료
- 사고 발생 시간
- 차량 위치
- 차량 방향
- 폰 번호
- 최근 차량 위치
- 탑승자 수
- OID
- 가속도 값
- 적재화물정보

### 4. 음성 통화 정보

e-call 센터가 MSD 수신 후 사고 확인을 위해 음성통화를 시도하는데, 이 때 e-call 단말과 e-call 센터간 상호간 전송되는 음성 데이터를 뜻한다.

### 5. e-Call 센터 정보

e-Call 단말이 e-Call 센터로 사고 정보를 전송할 수 있으려면, e-Call 센터 접속을 위한 주소 정보 등을 알고 있어야 한다. 다음과 같은 정보가 이에 해당한다.

- e-Call 센터 접속 IP 주소
- e-Call 센터 접속 Port 번호

## 6. 암호화에 필요한 중요 정보

e-Call 시스템에 적용할 암호화 알고리즘에 사용할 키 값 등 중요 정보로서, 다음과 같은 정보를 가질 수 있다.

- 대칭키 암호화 키
- 비대칭키 암호화 키
- e-Call 단말 / e-Call 센터 인증서
- 세션키

## 제4장 e-Call 시스템 구간 별 데이터 종류 및 위협

e-Call 시스템의 구간 별 보호 대상 데이터와 해당 구간에서 발생할 수 있는 위협은 다음의 표와 같다.

식별 번호	구간	보호 대상 데이터	위협
S-1	e-Call 단말 내부 구간	D-1, D-2, D-5, D-6	유출, 변조
S-2	e-Call 단말 - e-Call 센터 간 통신 구간	D-1, D-3, D-4	유출, 변조, 재전송
S-3	e-Call 센터 내부 구간	D-1, D-3, D-6	유출, 변조

### 1. e-Call 단말 내부 구간

e-Call 단말 내부에서는 다음과 같은 데이터가 저장된다.

- e-Call 단말 내에는 서비스 편의를 위해 단말 등록 정보가 저장되어 있을 수 있다.

- e-Call 단말 내에는 사고 판단을 위해 임시로 저장해 놓은 수집 정보가 있을 수 있다.
- e-Call 단말 내에는 e-Call 센터 접속을 위한 정보가 있어야 한다.

위의 정보에 대해 유출 및 변조 공격이 있을 수 있다. 특히 공격자가 단말 등록 정보를 획득하면 이를 이용해 신분 위장 공격을 감행할 수 있다. 또한 사고가 아닌데도 사고 판단 알고리즘이 사고로 판단하도록 수집 정보를 변조할 수 있다. 공격자가 e-Call 센터 접속 정보를 조작한다면, e-Call 단말이 전송한 사고 정보가 공격자가 지정한 서버로 전송되게 할 수 있다.

e-Call 단말 내부 데이터에 대한 위협은 주로 단말 내부에 악성코드를 주입하는 방식으로 이루어질 가능성이 크다.

## 2. e-Call 단말 - e-Call 센터 간 통신 구간

e-Call 단말 - e-Call 센터 간 통신 구간에서는 다음과 같은 데이터가 전송된다.

- 단말 등록이 필요한 경우, 단말 등록 정보가 e-Call 단말로부터 e-Call 센터로 전송될 수 있다.
- 통신 초기화 시 단말 인증을 위해 단말 등록 정보의 일부가 e-Call 단말로부터 e-Call 센터로 전송될 수 있다.
- 사고 발생 시 MSD가 e-Call 단말로부터 e-Call 센터로 전송될 수 있다.
- MSD가 전송된 후 음성 통화 데이터가 e-Call 단말과 e-Call 센터 상호간에 전송될 수 있다.

위의 정보에 대해 유출, 변조, 재전송 공격이 있을 수 있다. 특히 공격자가 단말 등록 정보를 획득하면 이를 이용해 신분 위장 공격을 감행할 수 있다. 또한 MSD 정보가 유출되면 그 안에 속한 전화번호 등 개인정보가 유출되는 것이므로, 프라이버시 침해가 우려된다. MSD 정보가 변조된다면 사고 정보가 바뀌는 것이므로 e-Call 센터는 해당 사고에 대해 잘못된 판단을 하여 그릇된 대처를 할 수 있다. 공격자가 MSD 정보를 갈취했다가 그대로 보내는 재전송 공격을 수행한다면, e-Call 센터를 혼란에 빠뜨릴 수 있다. 공격자가 MSD와 음성 통화 데이터를 모두 변조할 수 있다면, MITM 공격이 가능하다.

e-Call 단말 - e-Call 센터 간 통신 구간에 대한 공격은 다양한 네트워크 기반 공격을 통해 가능하며, 단말 내부에 악성코드를 주입하는 방식으로도 가능하다.

## 3. e-Call 센터 내부 구간

e-Call 센터 내부에서는 다음과 같은 데이터가 저장된다.

- e-Call 센터 내에는 단말 등록 정보가 저장되어 있을 수 있다.
- e-Call 센터 내에는 e-Call 단말로부터 전송된 MSD 정보가 임시 저장되어 있을 수 있다.

위의 정보에 대해 유출, 변조, 재전송 공격이 있을 수 있다. 특히 공격자가 단말 등록 정보를 획득하면 이를 이용해 신분 위장 공격을 감행할 수 있다. 또한 MSD 정보가 유출되면 그 안에 속한 전화번호 등 개인정보가 유출되는 것이므로, 프라이버시 침해가 우려된다.

e-Call 센터 내부 구간에 대한 공격은 다양한 네트워크 기반 공격과 시스템 운영체제의 취약점에 따른 다양한 해킹 공격에 의해 가능하다.

## **제5장 e-Call 시스템 구간 별 보안 지침**

### **1. e-Call 단말 내부 구간 보안**

- e-Call 단말 보안을 위하여 대칭키의 경우 암호강도 112비트 이상의 암호 알고리즘, 공개키의 경우 암호강도 2048비트 이상의 암호 알고리즘을 적용하여 정보 유출을 방지한다.
- 저장된 암호학적 중요 정보 유출 방지를 위해 검증 받은 S/W 보안 모듈 또는 HSM을 사용하여 암호화와 관련된 일련의 과정을 보호한다.
- 단말 내에서 주요 데이터 접근과 관련된 로그를 6개월 이상 저장하거나, 주기적으로 e-Call 센터 서버에 전송한다.
- 해시 함수, 메시지 인증코드, 전자서명 등의 암호 알고리즘 중 하나를 사용하여 저장 정보의 변조 여부를 확인할 수 있는 기능을 제공한다.
- 해시 함수를 사용할 경우 112비트 수준의 암호 강도를 가지는 알고리즘을 사용한다.
- e-Call 단말이 스마트 폰에 해당할 경우, 단말에 e-Call 앱이 설치될 때 안티 바이러스의 설치 여부를 확인하여 설치되어 있지 않을 경우 강제로 설치되도록 한다.

### **2. e-Call 단말 - e-Call 센터 간 통신 구간 보안**

- e-Call 단말 - e-Call 센터 간 통신 시 보안을 위해 대칭키의 경우 암호강도 112비트 이상의 암호 알고리즘, 공개키의 경우 암호강도 2048비트 이상의 암호 알고리즘을 적용하여 정보 유출을 방지한다.
- 저장된 암호학적 중요 정보 유출 방지를 위해 검증 받은 S/W 보안 모듈 또는 HSM을 사용하여 암호화와 관련된 일련의 과정을 보호한다.
- e-Call 센터에서 통신과 관련된 로그를 6개월 이상의 기간동안 저장한다.
- 데이터 전송 시마다 RSA 또는 DSA 암호 알고리즘을 사용한 데이터 서명을 통해 무결성 및 부인방지 기능을 제공한다.

- 데이터 전송 시마다 Timestamp나 nonce 값 등을 이용하여 재전송 공격 방지 기능을 제공한다.
- GMAC, CCM, GCM/GMAC, HMAC 등의 메시지 인증 코드를 사용하여 데이터 위변조 방지 기능을 제공한다.

### 3. e-Call 센터 내부 구간 보안

- e-Call 센터 보안을 위하여 대칭키의 경우 암호강도 112비트 이상의 암호 알고리즘, 공개키의 경우 암호강도 2048비트 이상의 암호 알고리즘을 적용하여 정보 유출을 방지한다.
- 저장된 암호학적 중요 정보 유출 방지를 위해 검증 받은 S/W 보안 모듈 또는 HSM을 사용하여 암호화와 관련된 일련의 과정을 보호한다.
- 단말 내에서 주요 데이터 접근과 관련된 로그를 6개월 이상 저장하거나, 주기적으로 e-Call 센터 서버에 전송한다.
- 해시 함수, 메시지 인증코드, 전자서명 등의 암호 알고리즘 중 하나를 사용하여 저장 정보의 변조 여부를 확인할 수 있는 기능을 제공한다.
- 해시 함수를 사용할 경우 112비트 수준의 암호 강도를 가지는 알고리즘을 사용한다.
- 방화벽과 침입탐지 시스템, 안티 바이러스 등을 구축하여 해킹의 침입 시도를 차단해야 한다.
- 운영체제 취약점에 대한 패치를 주기적으로 수행해야 한다.

**<표준작성 실무자>**

[illegible]