건설근로자 전자카드 단말기

지정 세부기준

2022. 5.

건설근로자공제회

Construction Workers Mutual Aid Association

목 차

제1장 개요

제1절 목적

「건설근로자의 고용개선 등에 관한 법률」 제13조제4항 및 동법 시행령 제12조의2제3항, 「건설근로자 전자카드 단말기 지정제도 운영지침」 제4조 등에 따라 전자카드제의 원활한 운영과 전자카드 단말기 지정 업무를 위한 세부기준을 정하는 것을 목적으로 한다.

제2절 지정대상

지정대상

o 건설근로자의 출·퇴근내역 등의 정보를 전자카드 근무관리시스템에 전송하는 장치
  - 근로자의 전자카드 정보 및 출·퇴근 내역 정보 등을 직접 전자카드 근무관리시스템에 전송하는 장치

제3절 단말기 운영환경

단말기는 건설근로자가 보유하고 있는 전자카드와의 근거리 통신을 통해 수신한 전자카드 번호를 건설근로자의 출·퇴근 시간 등의 정보와 함께 전자카드 근무관리시스템으로 전송한다. 건설근로자공제회(이하 '공제회'라고 한다)의 전자카드 근무관리시스템은 단말기로부터 전달받은 정보를 이용하여 근로자를 식별하고 근로자의 출퇴근 내역을 기록·관리한다. 단말기는 온라인 또는 오프라인 방식으로 단말기 소프트웨어에 대한 업데이트를 진행할 수 있다. 단, 공제회로부터 인증받은 형상을 유지해야 한다.

제4절 주요 보안 위협

단말기와 관련된 주요 보안 위협은 다음과 같다.

<표 1> 주요 보안 위협

보안위협	설명	주요 보안 대책
중요정보 불법접근	메모리 해킹, 탭핑, 스키밍, 악성코드 등의 공격기법*을 사용하여 중요정보(민감한 개인정보 정보 등)를 유출할 수 있는 보안 위협	·중요정보 암호화
암호키 유출	중요정보 암호화 연산을 위해 사용되는 암호키가 유출되어 중요정보가 유출될 수 있는 보안 위협	·안전한 암호키 관리
전송데이터 유출	단말기 구성 요소간 또는 단말기와 공제회 서버 간 전송되는 중요정보를 무단으로 노출, 변경시킬 수 있는 보안 위협	·암호화 통신 제공
보안 기능 우회	악성코드를 통해 단말기 보안기 능과 관련된 실행 파일 또는 설정파일 등이 변조되어 보안기능을 우회할 수 있는 보안 위협	·자체보호 기능 ·안티바이러스 제품 설치·운영
인증 우회	메시지를 복사한 후 나중에 재전송함으로써 정당한 사용자로 가장하거나, 정당한 메시지로 가장하는 보안 위협	·인증 기능 ·타임 스탬프 기능

단말기 보안위협과 관련된 주요 공격기법은 다음과 같다.

<표 2> 주요 공격기법

공격기법	설명
메모리 해킹	이용자가 입력한 데이터 등이 메모리상에 평문으로 처리되는 구간을 포착하여 민감한 개인정보, 암호키를 추출해 내는 공격기법
스키밍(Skimming)	카드입력부(예, 카드리더기) 등에 부착되어 민감한 개인정보 등을 빼내어 카드 정보를 전자적으로 복제하는 공격기법
탭핑(Tapping)	카드입력부(예, 카드리더기)와 단말기 사이의 케이블을 도청하여 민감한 개인정보 등을 절취하고 복제하는 공격기법
재전송 공격	프로토콜상에서 유효 메시지를 골라 복사한 후 나중에 재전송하는 공격기법

제5절 단말기 지정기준

「건설근로자 전자카드 단말기 지정제도 운영지침」 제4조제1항에 따른 단말기 지정기준은 다음과 같다.

<표 3> 단말기 지정기준

구분	정보보호 요구사항	비고
기본 요구사항	전자카드 단말기는 근로자가 소지한 전자카드 또는 지문정보를 이용하여 공제회 서버에 근로자의 출퇴근 시간을 기록할 수 있어야 함	
	전자카드 단말기는 근로자의 출퇴근 시간을 확인할 수 있어야 함	
	전자카드 단말기 관리자 비밀번호는 안전하게 생성 및 관리되어야 함	
기술적 요구사항	근로자의 출퇴근 기록 시에 필요한 민감한 개인정보를 안전하게 보호해야 함	
	민감한 개인정보 암호화를 위해 안전한 암호화 연산 및 암호키 관리(생성, 분배, 폐기) 기능을 제공해야 함	
	전자카드 단말기의 정상적인 동작을 보장하기 위한 자체보호 기능을 제공해야 함	
	전자카드 단말기의 중요 자산(암호키 등)을 보호하기 위한 접근제어 기능을 제공해야 함	
	전자카드 단말기의 안전한 업데이트를 보장해야 함	
관리적 요구사항	안전한 전자카드 단말기의 개발을 위해 소프트웨어 개발 보안을 적용해야 함	
	전자카드 단말기 개발시 형상관리체계를 수립하여 운영해야 함	
	안전한 전자카드 단말기 서비스 제공을 위한 안전한 운영환경을 고려해야 함	
	전자카드 단말기 프로그램 및 운영환경에 대한 보안취약점을 점검하여 조치를 취해야 함	
성능 요구사항	안정적인 전자카드 단말기 운영을 보장할 수 있어야 함	

제2장 지정 세부기준

「건설근로자 전자카드 단말기 지정제도 운영지침」 제4조제2항에 따른 단말기 지정 세부기준은 다음과 같다.

제1절 기본 요구사항

단말기로 건설근로자의 정상적인 출·퇴근 기록을 확인하기 위한 기본 요구사항은 다음과 같다.

1. 단말기는 근로자가 소지한 전자카드 또는 지문정보를 이용하여 공제회 서버에 근로자의 출퇴근 시간을 기록할 수 있어야 함

(세부 요구사항)

- 단말기는 공제회에서 지정한 전자카드로부터 공제회 서버가 처리할 수 있는 형태의 전자카드 정보를 추출할 수 있어야 한다.
- 단말기는 근로자의 지문에서 공제회 서버에서 처리할 수 있는 형태의 지문정보를 추출할 수 있어야 한다.
- 단말기는 전자카드 정보 또는 지문정보와 함께 근로자의 출퇴근 시간 정보를 공제회 서버로 전송할 수 있도록 전자카드 태깅 또는 지문인식 시 시간 정보를 정확하게 생성해야 한다.

2. 전자카드 단말기는 근로자의 출퇴근 시간을 확인할 수 있어야 함

(세부 요구사항)

- 단말기는 전자카드 태깅 또는 지문인식 시, 건설근로자 공제회 서버에서 식별된 근로자의 정보가 처리된 상태를 알 수 있는 디스플레이 기능을 제공하여야 한다.
- 단말기는 전자카드 태깅 또는 지문인식 시, 출퇴근 시간 정보를 디스플레이 등을 이용하여 근로자에게 제공하여야 한다. 단, 민감한 개인정보는 출력해서는 안 된다.
- 단말기는 전자카드 태깅 또는 지문인식 시, 근로자의 출근과 퇴근을 구분할 수 있도

록 하는 기능을 제공하여야 한다.

- 단말기는 정확한 출퇴근 시간 정보 생성을 위해 신뢰 된 수단(OS 등)을 이용하여 시간 정보를 생성해야 한다.
- 부정 사용 방지를 위해 카메라 모듈로 전자카드 태깅 또는 지문인식으로 식별된 근로자의 얼굴을 촬영해야 한다.
- 부정 사용 방지를 위해 촬영된 근로자의 사진은 3개월간 안전한 방법으로 저장되어야 한다.
- 전자카드 태깅 또는 지문인식 시 근로자는 촬영되는 사진을 확인할 수 있어야 한다.
- 저장 기간이 지난 근로자의 사진은 삭제되어야 한다.

3. 전자카드 단말기 관리자 비밀번호는 안전하게 생성 및 관리되어야 함

(세부 요구사항)

- 단말기의 보안 설정 등을 변경하기 위해서는 관리자 비밀번호를 입력하여야 한다. 관리자 비밀번호는 3가지 종류 이상의 문자 구성(영문 대•소문자, 숫자, 특수문자)으로 8자리 이상의 길이 또는 2가지 종류 이상의 문자 구성으로 10자리 이상의 길이를 갖도록 생성하여야 한다.
- 전자카드 단말기의 관리자 비밀번호 설정 및 변경은 최신 버전의 '패스워드 선택 및 이용 안내서(한국인터넷진흥원)'를 참고한다.
- 비밀번호는 하드코딩 되어서는 안 되며, 단말기 최초 구동 시에 설정할 수 있어야 한다.
- 비밀번호 입력 시 비밀번호는 마스킹 등의 방법으로 노출되지 않게 사용되어야 한다.
- 관리자 비밀번호는 사용 기간을 설정하여 갱신을 수행해야 한다.

제2절 기술적 요구사항

단말기로 건설근로자의 정상적인 출·퇴근 기록을 확인하기 위한 기본 요구사항은 다음과 같다.

1. 근로자의 출퇴근 기록 시에 필요한 민감한 개인정보를 안전하게 보호해야 함

(세부 요구사항)

- 고유 식별정보 확인 목적으로 처리되는 민감한 개인정보는 전송구간 전체에서 기밀성이 보장되어야 한다.
- 민감한 개인정보는 단말기 어떠한 형태로도 메모리 및 파일 시스템 등에 저장이 허용되지 않으며 사용 후 메모리 등에서 완전히 삭제되어야 한다.
- 민감한 개인정보는 단말기 화면에 출력되지 않아야 한다.

2. 민감한 개인정보 암호화를 위해 안전한 암호화 연산 및 암호키 관리(생성, 분배, 폐기) 기능을 제공해야 함

(세부 요구사항)

- 기밀성을 제공하기 위해서는 112bit 이상의 보안 강도를 갖는 암호알고리즘 및 암호키가 사용되어야 한다.

< 적용 암호알고리즘 >

① 단말기에 입력된 전자카드 번호나 지문정보, 출퇴근 시간 등이 공제회 서버로 전송되기 위해서는 SEED(128bit)로 암호화되어 공제회 서버로 전송되어야 하며, 전자카드 번호는 단말기 내부에서 복호화(평문으로 저장)되지 않아야 함

② 단말기와 공제회 서버 간의 암호키 교환을 위해서는 RSA (2048bit)를 사용해야 함

- 안전성이 검증된 암호키 생성, 분배 방법이 사용되어야 한다.
- 사용이 만료/종료된 암호키 및 암호키 생성분배를 위해 사용된 모든 정보는 단말기에서 파기 및 삭제되어야 한다.
- 기밀성을 제공하기 위하여 암호알고리즘에 사용되는 암호키는 암호화, 분산 저장 및 난독화 등의 방법으로 안전하게 저장되어야 한다.

- 암호 알고리즘에 사용되는 암호키는 안전성이 검증된 난수발생기 및 키 생성 함수 등의 방법으로 생성되어야 한다.
- 암호키 전송/저장 시 기밀성과 무결성을 보장해야 한다.
- 암호키를 사용하기 전에 무결성 검증을 통해 변조 여부를 확인하고 사용해야 한다.
- 전자카드 단말기에서 사용하는 모든 암호키는 사용 기간을 설정하여 갱신을 수행해야 한다.

3. 전자카드 단말기의 정상적인 동작을 보장하기 위한 자체보호 기능을 제공해야 함

(세부 요구사항)

- 단말기의 정상적인 동작을 보장하기 위하여 보안 기능 실행 코드 및 보안 기능 관련 저장데이터에 대하여 변경 여부에 대하여 탐지하기 위하여 무결성 점검을 해야 한다.
- 무결성 점검은 단말기 시동 시와 주기적 혹은 관리자 요청 시 실행되어야 한다.
- 무결성 점검 결과 변경이 탐지되면 단말기의 동작은 중단되어야 하며, 경고음 또는 화면 출력 등을 통하여 통보해야 할 수 있어야 한다.
- 무결성이 훼손된 암호키는 단말기에서 삭제되어야 한다.

4. 전자카드 단말기의 중요 자산(암호키 등)을 보호하기 위한 접근제어 기능을 제공해야 함

(세부 요구사항)

- 단말기 내부에 저장된 암호키 등 중요정보에 대한 접근 시도를 방지하기 위하여 단말기에 대한 논리적인 비인가 된 접근을 허용하지 않아야 한다.
- 단말기의 외부 인터페이스(USB, JTAG, Serial 등)을 통하여 전자카드 내부에 대한 접근을 제한해야 한다.

5. 전자카드 단말기의 안전한 업데이트를 보장해야 함

(세부 요구사항)

- 관리자를 인증한 이후에 업데이트가 진행되어야 한다.
- 업데이트 파일에 대한 기밀성 및 무결성 검증 방법이 제공되어 악성 업데이트 파일의 업데이트를 방지해야 한다.
- 업데이트 진행 시에 어떠한 정보도 출력되어서는 안 된다.
- 업데이트 실패 시 단말기는 업데이트 실패를 업데이트를 진행하는 대상에게 알려야 한다.
- (온라인 업데이트 경우) 업데이트 서버를 제외한 비 인가된 네트워크 통신 접속을 제한해야 한다.
- (온라인 업데이트 경우) 단말기는 업데이트 서버의 주소(IP 등)에 대한 무결성 검증을 수행하여 무결성 검증 성공 시에만 업데이트가 진행돼야 한다.
- (온라인 업데이트 경우) 단말기의 펌웨어 혹은 소프트웨어 업데이트를 안전하게 진행하기 위해 업데이트 서버에 대한 식별 및 인증 기능을 제공해야 한다.
- (오프라인 업데이트 경우) 업데이트 파일을 전송받기 전 업데이트 파일을 전송하는 외부 객체에 대한 식별 및 인증을 수행해야 한다.
- 대기 화면 등에 버전 정보를 표시해야 하며, 업데이트를 진행하였을 때 전자카드 단말기의 버전 정보가 반드시 변경되어야 한다.

< 업데이트 주의사항 >

- 지정된 단말기의 형상 변경이 발생될 수 있는 업데이트는 지정기관으로부터, 재지정 또는 갱신 이후 승인된 업데이트 사항이 적용되어야 한다. 단, 긴급한 보안패치가 필요한 경우 지정기관과 협의를 통해 선조치 후, 승인(재지정 또는 갱신)을 진행할 수 있다.

제3절 관리적 요구사항

단말기로 건설근로자의 정상적인 출·퇴근 기록을 확인하기 위한 기본 요구사항은 다음과 같다.

1. 안전한 전자카드 단말기의 개발을 위해 소프트웨어 개발 보안을 적용해야 함

(세부 요구사항)

- 안전한 단말기 프로그램 개발을 위해 개발단계부터 취약점의 원인을 배제하도록 소프트웨어 개발 보안 방법론을 채택하여 개발해야 한다.
  - 단말기 개발업체는 전자카드 단말기에 채택하여 이행한 개발 보안 방법론에 관한 문서를 시험기관에 제공해야 하며, 개발환경의 보안, 소스 코드 관리, 개발자 보안 교육 등에 관한 내용을 시험기관에 제공해야 한다.

< 소프트웨어 개발 보안 관련 주요 참고자료 >

① (국내) 소프트웨어 개발 보안 가이드 및 시큐어 코딩 가이드(행정안전부·한국인터넷진흥원)

② (국외) SEI CERT C/C++/Perl/java/Android Coding Standard (카네기멜론대학교 SEI연구소)

③ (국외) OWASP Secure Coding Practices – Quick Reference Guide, OWASP

- 단말기 개발단계에서 식별된 취약점에 대하여 위험평가를 해야 한다.

2. 전자카드 단말기 개발시 형상관리체계를 수립하여 운영해야 함

(세부 요구사항)

- 단말기 개발 시 형상관리 체계를 수립하고 형상 관리 계획에 따라 운영 및 관리하여야 한다.
- 형상 관리 체계에서 모든 형상 항목은 유일하게 식별되어야 한다.
- 형상 항목의 변경은 인가된 변경만 허용해야 하며 변경사항은 추적할 수 있어야 한다.

3. 안전한 전자카드 단말기 서비스 제공을 위한 안전한 운영환경을 고려해야 함

(세부 요구사항)

- 단말기가 일반 범용 운영체제에서 동작할 경우, 시스템 제공 및 관리 업체에서 운영체제의 기본 보안 설정을 구성해야 한다.
- 운영체제, 방화벽, 안티바이러스 제품 등에 대해 필수 보안패치를 적용할 수 있는 관리 수단을 제공해야 한다.
- 단말기 관련 소프트웨어(개인정보처리/공제회 서버 통신프로그램) 및 원격제어 소프트웨어 등의 프로그램 이용 및 설치 시 신뢰할 수 있는 특정 구간의 IP주소, 포트, 프로토콜 등만 허용하도록 설정되어야 하며, 불필요한 서비스는 제거하거나 비활성화 되어야 한다.
- 단말기의 신규 운영환경 구성, A/S에 의한 운영환경 재구성 등으로 인하여 단말기 ID를 설정하여야 하는 경우 반드시 건설공제회 서버로부터 단말기 ID 번호를 검증받아 설정하여야 한다.

4. 전자카드 단말기 프로그램 및 운영환경에 대한 보안취약점을 점검하여 조치를 해야 함

(세부 요구사항)

- 단말기 프로그램에서 보안취약점 발견 시, 관련사항을 지정가관에 신고하고 보안취약점을 조치하여 보안패치를 먼저 배포하고 지정시험 대행기관에 보안패치 프로그램에 대한 시험을 의뢰해야 한다.
- 단말기 운영환경에 대한 보안취약점 발견 시 단말기가 설치된 건설 현장 등에 해당 내용을 공지하여 보안패치를 적용할 수 있도록 해야 한다.
- 단말기가 손상되었으면 서비스를 복구하기 위한 복구 계획을 세워야 한다.
- 단말기의 프로그램 및 운영환경의 보안취약점에 대해서 상시적 점검체계를 구축해야 한다.

제4절 성능 요구사항

안정적인 전자카드 단말기 운영을 보장하기 위한 성능 요구사항은 다음과 같다.

1. 안정적인 전자카드 단말기 운영을 보장할 수 있어야 함

(세부 요구사항)

- 단말기는 다음과 같은 전자파 인증을 획득해야 한다.
  - 국립전파연구원 “방송통신기자재등의 적합성평가”에 따른 요구사항 충족 및 인증획득
    ※ 전자파에 대하여 KC인증을 제출해야 한다.
- 현장 설치 단말기는 건설현장의 운영환경(온·습도, 방수 등)에서 안전하게 정상 동작함을 보증하기 위해 KC인증 또는 관련 성능의 시험성적서를 제출해야 한다.
- 단말기는 공제회 서버에 근로자의 출퇴근 시간을 전송할 수 있는 유선 또는 무선 통신 기능을 제공해야 한다.