TradeSign

인증업무준칙

(Certification Practice statements)

V 6.2

2022. 12. 23

(주)한국무역정보통신

Document History

Document History		
0.1	2001.3.21	
1.0	2001.7.12	서비스 변경
1.5	2002.8.13	서비스 변경
1.6	2002.10.29	서비스 변경
2.0	2003.6.4	서비스 변경
2.1	2004.4.13	수수료 변경
2.5	2007.2.15	서비스 변경
3.0	2007.5.21	CPS표준 제정 (정보통신부고시 제2007-6호)
3.1	2007.7.6	정보통신부의 변경 요청 (공문: 정보통신부 정보윤리팀-1413 “인증업무준칙 변경요청”)
3.2	2010.6.15	관련기관명 변경, 가입자 의무, 주소 변경, 폐지 요건, 보증 등 변경
3.3	2011.2.28	배경 및 목적 변경, CA/RA/가입자 책임 및 의무사항 추가, 인증서 유효기간 명시, 재발급 수수료 명시, 환불 요건 구체화, 가입자 정보 진정성 확인 명시, 신규발급 절차 구체화, 갱신후 잔존 인증서 유효기간 안내, CRL 공고까지 걸리는 시간, OCSP/TSA 서비스 이용안내, OCSP 서비스 인증서 프로파일, CA전자서명키배포 절차, 인증업무의 휴지 또는 폐지절차, 인증업무의 정지 또는 지정취소 절차, 인증업무관련 공고 구체화, 절차적보호조치, 인적보안, 기록보존 보완, 배상 요건 구체화, 분쟁해결/개인정보보호/감사및점검/CPS 효력 구체화 등
4.0	2011.3.15	118 인증서 긴급 폐지 관련 추가
4.1	2012.8.3	행정안전부 권고에 따른 개정 정기점검 보완사항 개인정보보호법 관련사항 등
4.2	2012.10.30	전자주소 이용목적 추가 등
4.3	2013.5.10	행정안전부 → 미래창조과학부 변경 갱신기간 : 만료1개월 → 만료2개월 주소 및 신청접수처 변경
4.4	2016.3.7	o 인증서 비밀번호 보안수준 강화 o 감사기록의 유형 변경 및 보존기간 늘림 (2년 → 10년) o 보안매체에 발급되는 인증서의 유효기간 연장 (1년 → 5년 미만) o 인증수수료(OCSP) 수수료 인하 500원 à 200원 o 가입자의 책임 및 의무조항 구체화 o 지번주소 → 도로명 주소 변경 o 전자서명법의 용어로 통일 (생성키 → 생성정보 / 검증키 → 검증정보)
4.5	2019.2.7	o 조항항목 명확하게 표시 o 명칭변경 (미래창조과학부→과학기술정보통신부, 재외국민 등록증→재외국민 주민등록증) o 서비스URL 현실화 o 전자서명생성정보 만료시 파기 방법 변경

		o 핵심/부가서비스 시스템 이름 미나열 o 본인확인서비스 주민번호 제공 삭제
4.6	2019.2.22	o 시점확인 서비스 약어 표시 변경 o 핵심 및 부가 서비스 목록 표시 o 본인확인서비스 개인정보 제공 가능 추가
4.7	2020.9.9	o 수수료 관련 항목 수정 o CRL 발행을 최소 일1회 이상으로 수정
4.8	2020.11.20	o 갱신 신청기간 한시적 수정
5.0	2020.12.10	o 전자서명법 개정 반영
5.1	2021.3.26	o 본인확인기관 내용 반영
5.2	2021.4.2	o 인증서 종류 추가
5.2.1	2021.6.23	o 오류 수정 (폐지관련)
5.3	2021.11.2	o 전자서명인증사업자의 역할 o 보유기간 변경 o 신원확인 방법 및 증표 표현의 간소화
5.4	2021.11.4	o 폐지 방법 오류 수정 o 인증업무 휴지 및 폐지시 가입자 보호 방안 구체화 o 전자서명 생성정보의 유출시 처리 방안
5.5	2021.11.9	o 가입철회 내용 추가 o 전자서명 생성정보의 보안 내용 추가 o 방호 관련 내용 추가 o 감사 및 평가 관련 내용 추가
5.6	2021.11.16	o 서비스 내용 추가 o 정보의 제공 내용 명확화 o 시스템 구성 관리 내용 추가 o 전자서명 생성정보 관리 내용 추가
5.6.1	2021.12.1	o 운영기준 준수사실 표기 o 안전한 암호 사용 내용 포함 o 배상 관련 내용 수정
5.6.2	2021.12.6	o 오류수정 및 현행화
5.6.3	2021.12.27	o 배상책임의 면책 부분 삭제
6.0	2022.1.21	o 전자서명인증업무준칙 작성방법의 목차 순으로 변경
6.1	2022.10.31	o 클라우드 공동인증서비스 추가 o 오류 수정
6.2	2022.12.23	o 클라우드 서비스 관련자 및 통지관련 내용 추가 o 전자문서법 관련 사항 포함

차 례

1. 소개

1.1 개요

1.1.1. 인증업무준칙의 배경 및 목적

이 인증업무준칙(CPS : Certification Practice Statements)은 전자서명법(이하 "법"이라 합니다), 전자서명법 시행령(이하 "시행령"이라 합니다), 전자서명법 시행규칙(이하 "시행규칙"이라 합니다) 및 과학기술정보통신부 전자서명인증업무 운영기준(이하 "운영기준"이라 합니다.), 전자서명인증업무준칙 작성방법에 의하여 (주)한국무역정보통신이 전자무역인증센터(이하 "TradeSign"이라 합니다.)를 운영함에 있어 필요한 사항을 정함을 목적으로 합니다.

이 CPS는 TradeSign을 비롯한 인증관련 당사자(등록대행기관, 가입자, 이용자 등)의 책임과 의무사항에 대한 규정도 포함합니다.

1.1.2. 전자서명인증체계

전자서명인증체계는 전자서명인증에 관한 정책의 수립, 시행 및 감독은 과학기술정보통신부가 관장하고 있으며, 한국인터넷진흥원(이하 “인터넷진흥원”이라 한다)을 최상위인증기관으로 구성되어 있습니다.

TradeSign은 가입자의 신원확인 등의 등록업무를 직접 수행하거나, 등록대행기관에 위임할 수 있으며, 인증서를 발급받아 사용하는 전자서명 인증업무의 이용주체로 가입자가 있습니다. 또한, 전자서명인증사업자가 제공하는 전자서명인증서비스를 이용하는 이용자가 있습니다.

1.1.3. TradeSign 소개

(주)한국무역정보통신 Tradesign은 2002년 3월 11일에 공인인증기관으로 처음 지정되었으며, 법에 의하여 전자서명인증사업자로서 인증서비스를 제공합니다.

- 웹사이트 : www.tradesign.net
- 주소 : 경기 성남시 분당구 판교로 338 번지 한국전자무역센터 6 층
- 인증서 신청접수처
  . 경기 성남시 분당구 판교로 338번지 한국전자무역센터 6층
  . 서울시 강남구 영동대로 511 무역센터 트레이드타워 4층
- 전화번호 : 1566-2119

1.1.4. 인증서 정의 및 효력

TradeSign 인증서는 (주)한국무역정보통신이 발급하는 인증서로, 해당 전자서명생성정보에

의한 전자서명은 법 제3조(전자서명의 효력)에 의거 법적인 효력이 있습니다.

법 제3조(전자서명의 효력)

① 전자서명은 전자적 형태라는 이유만으로 서명, 서명날인 또는 기명날인으로서의 효력이 부인되지 아니한다.

② 법령의 규정 또는 당사자 간의 약정에 따라 서명, 서명날인 또는 기명날인의 방식으로 전자서명을 선택한 경우 그 전자서명은 서명, 서명날인 또는 기명날인으로서의 효력을 가진다.

1.2 문서의 명칭

이 인증업무준칙은 "TradeSign 인증업무준칙(CPS)"이라 합니다.

1.3 전자서명인증체계 관련자

1.3.1. 과학기술정보통신부

과학기술정보통신부는 전자서명의 신뢰성을 높이고, 가입자 및 이용자가 합리적으로 전자서명서비스를 선택할 수 있도록 필요한 조치를 수행합니다.

- 전자서명인증업무 운영기준 마련
- 운영기준 준수사실의 인정에 관한 업무를 수행하는 기관(이하 "인정기관"이라 한다)을 지정
- 평가 업무를 수행하는 기관(이하 "평가기관"이라 한다)을 선정하여 고시
- 운영기준에 부합한다고 인정하는 국제적으로 통용되는 평가(이하 "국제통용평가"라 한다)를 정하여 고시

1.3.2. 한국인터넷진흥원(KISA)

한국인터넷진흥원은 법 제9조(인정기관)에 의하여 운영기준 준수사실의 인정에 관한 업무를 수행하는 기관 업무를 수행합니다.

- 전자서명인증 관련 기술개발·보급 및 표준화 연구
- 전자서명인증 관련 제도 연구 및 상호인정 등 국제협력 지원
- 법 제 16 조(검사 등) 제 1 항에 따른 전자서명인증사업자에 대한 검사 지원
- 전자서명인증 최상위 인증기관 (Root CA) 운영
- 그 밖에 전자서명인증 정책의 지원에 필요한 사항

1.3.3. TradeSign(CA)

TradeSign은 법 제8조(운영기준 준수사실의 인정) 등에 의거 정부의 심사를 받아 운영기준

준수사실의 인정을 받은 전자서명인증사업자로 다음의 업무를 수행합니다.

- 인증서비스 신청서 접수 및 처리
- 인증서비스 가입자 신원확인
- 인증서비스의 제공(인증서 발급, 재발급, 갱신, 변경, 효력정지, 효력회복, 폐지 등)
- 등록대행기관(RA)의 지정 및 관리
- 인증서 효력정지 및 폐지목록의 공포
- 시점확인 서비스
- 인증서 유효성 확인 서비스 (이하“OCSP”)
- 본인확인 서비스 (UCPID)
- 기타 전자서명인증사업자로서 필요하다고 인정되는 업무

1.3.3.1. 책임과 의무

1.3.3.1.1. 정확한 정보의 제공

TradeSign은 인정기관(평가기관 포함), 가입자 및 이용자에게 인증서의 신뢰성이나 유효성에 영향을 미칠 수 있는 다음의 정보를 TradeSign 홈페이지 또는 디렉터리시스템에 공고하여 그 사실을 확인할 수 있도록 합니다.

- 전자서명인증업무 운영기준 준수사실의 인정
- 전자서명인증업무 휴지·정지 또는 폐지
- 인증업무준칙(CPS)
- 인증서에 대한 정보 (인증서 및 인증서 폐지 목록(CRL))
- 기타 전자서명인증업무 수행 관련 정보 등

1.3.3.1.2. 전자서명 생성정보의 보호 및 안전조치

신뢰할 수 있는 하드웨어 등을 이용하여 안전한 방법으로 전자서명생성정보를 생성하며 생성된 전자서명생성정보가 분실·훼손 또는 도난·유출되지 않도록 안전하게 관리합니다.

만약, 전자서명생성정보의 분실·훼손, 도난·유출 등 인증서의 신뢰성이나 유효성에 영향을 미치는 사유가 발생한 사실을 인지하는 경우 가입자에게 이를 통보하며 필요한 경우 해당 전자서명생성정보로 발급한 가입자의 인증서를 폐지합니다.

1.3.3.1.3. 신원확인

시행규칙 제5조(실지명의 기준의 신원확인 방법)에서 정하는 신원확인의 기준 및 방법에 따라 신원확인을 수행합니다.

1.3.3.1.4. 가입자 정보의 보호

TradeSign은 가입자의 정보를 기밀정보로 분류하고 임의 접근을 제한하며, 가입자의 동의를 얻어 공개하는 정보라 할지라도 타인에 의한 임의 접근 및 변경 또는 삭제를 불허합니다. 단, TradeSign은 법률에서 정한 규정에 의거 타 기관의 요청이 있는 경우에 이를 공개할 수 있습니다.

1.3.3.1.5. 전자서명생성정보의 올바른 이용

TradeSign은 다음과 같이 이용목적에 따라 여러 가지 전자서명생성정보 및 전자서명검증정보를 만들 수 있습니다. 단, 각 전자서명생성정보 및 전자서명검증정보는 해당 분야에만 이용할 수 있습니다.

- 인증서 발급용으로 만든 전자서명생성정보는 인증서 발급에만 이용한다.
- 시점확인을 위해 만든 전자서명생성정보는 시점확인을 위해서만 이용한다.
- OCSP 서비스용으로 만든 전자서명생성정보는 OCSP 서비스를 위해서만 이용한다.

1.3.3.1.6. 중요 사실에 대한 통보 및 조치

TradeSign은 법 제15조(전자서명인증업무준칙의 준수 등)에 의거하여 운영하여야 하고, 법에 명시된 업무의 폐지 등 중요한 사항은 가입자에게 통보(email, 전화 등)하고 인터넷 홈페이지 등에 게시하여야 합니다.

1.3.3.1.7 안전한 암호 사용

TradeSign은 안전한 암호 알고리즘의 사용 및 국내외 표준적인 보안 기술 규격 준수를 보장합니다. 안전하지 않은 암호 알고리즘 등에 따른 기술적 내용의 결함으로 인해 가입자 또는 이용자에게 손해가 발생한 경우 본 인증업무준칙 9.2(배상)에 따라 그 손해를 배상합니다.

1.3.4. 등록대행기관(RA)

TradeSign은 필요에 따라 하나 이상의 등록대행기관을 지정할 수 있으며, 지정된 등록대행기관은 다음의 업무에 대해 TradeSign을 대신합니다.

- 인증서비스 신청서 접수 및 처리
- 인증서비스 가입자 신원확인
- 인증서비스 가입자 정보의 전산입력

1.3.4.1. 책임과 의무

1.3.4.1.1. 가입자 신원확인

등록대행기관은 법 제14조(신원확인)에 따라 가입자의 신원을 확인합니다.

1.3.4.1.2. 인증서 발급 안내

등록대행기관은 가입자가 신속하고 정확하게 인증서를 발급받을 수 있도록 제반 편의를 제공합니다.

1.3.4.1.3. 가입자 정보의 보호

등록대행기관은 개인정보 보호법 및 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 “정보통신망법”이라 합니다.)에 따라 가입자 정보에 대한 임의 접근을 제한하며, 가입자의 동의를 얻어 공개하는 정보라 할지라도 타인에 의한 임의 접근 및 변경 또는 삭제를 불허합니다.

1.3.5. 가입자

이 인증업무준칙에서 정한 규칙에 따라 TradeSign의 인증서비스에 가입하고, 자신의 전자서명생성정보를 생성하여 전자서명검증정보에 대한 인증서를 발급받은 자(개인, 법인, 단체, 개인사업자 등)를 의미합니다.

1.3.5.1. 책임과 의무

1.3.5.1.1. 정확한 정보의 제공

가입자는 용도에 맞게 인증서를 선택하여 신청하여야 하며, 다음의 각 경우에 정확한 정보를 TradeSign에 제공할 의무가 있습니다.

- 인증서의 발급 (신규발급, 재발급, 갱신발급)
- 인증서의 효력정지 및 효력회복
- 인증서의 폐지
- 가입자의 변경된 정보의 제공

1.3.5.1.2. 전자서명생성정보의 보호 및 관리

가입자는 신뢰할 수 있는 장치를 이용하여 전자서명생성정보를 생성하여야 하며 분실, 훼손, 도난, 유출 당하지 않도록 안전하게 보호, 관리하여야 합니다.

가입자는 전자서명생성정보가 분실, 훼손, 도난, 유출되었음을 인지한 경우, 지체없이 등록대행기관 또는 TradeSign에게 통보하여 해당 인증서를 폐지 또는 효력정지 할 수 있도록 협조하여야 합니다.

가입자의 전자서명생성정보 보호의무 위반으로 인한 결과의 책임은 가입자에게 있습니다.

1.3.5.1.3. 전자서명인증사업자 면책

가입자는 인증서 사용과 공개에 있어 다음의 사유로 인하여 발생되는 모든 책임과 비용에 대하여는 TradeSign의 면책을 보장합니다. 이 의무는 가입자의 인증서비스 신청을 접수한 때부터 시작되며 인증서 만료(폐지 포함)후 5년 동안 지속됩니다.

- 가입자가 그릇되게 제공한 정보
- 가입자가 태만 또는 고의로 제공하지 않은 변경된 정보
- 가입자의 전자서명생성정보 관리 부주의(정보 노출, 분실, 변조 등)

1.3.5.1.4. 가입자 정보 변경의 통보

가입자는 다음의 상황이 발생하면 신속하게 TradeSign 또는 등록대행기관에 해당 사실을 통보하고 적절한 조치를 수행해야 합니다.

- 가입자의 신상정보(성명, 주소, 전자우편 주소, 휴대전화번호 등)가 변경되는 경우
- 가입자의 구속, 사망 등의 이유로 인증서를 이용할 수 없게 된 경우
- 단, 구속이나 사망 등 가입자 자신이 본인임을 증명할 수단이 없을 경우에는 대리인이 사실관계에 대한 입증서류를 지참하여 가입자의 역할을 대행합니다.

1.3.6. 이용자

TradeSign이 가입자에게 발급한 인증서를 이용하여 가입자의 전자서명생성정보와 전자서명 검증정보의 합치성을 확인하려는 자를 의미합니다.

1.3.6.1. 책임과 의무

1.3.6.1.1. 인증서의 용도 내 사용

이용자는 TradeSign의 인증서 이용목적 및 범위를 확인하고 서비스를 제공하여야 하며 이를 위반하여 발생한 손해에 대해서 책임을 져야 합니다.

1.3.6.1.2. 인증서 유효성 확인

이용자는 인증서의 유효성을 확인하기 위해 다음의 조치를 하여야 합니다.

- 인증서가 이용된 시점이 인증서의 유효기간 내에 있어야 한다.
- 인증서가 이용된 시점에 인증서가 정지 또는 폐지된 상태가 아니어야 한다.
- 인증서의 이용범위 또는 용도를 제한하는 경우 이에 관한 사항에 대한 확인하여야 한다.
- 가입자가 제 3 자를 위한 대리권 등을 갖는 경우 또는 직업상 자격 등의 표시를 요청한 경우 이에 관한 사항에 대한 확인하여야 한다.

1.3.6.1.3. 배상 책임

이용자는 인증서 사용과 관련하여 이용자의 고의 또는 과실로 TradeSign 또는 가입자에게 손해를 입힌 경우 TradeSign 또는 가입자에게 그 손해를 배상해야 합니다.

1.3.7. 클라우드 서비스의 공동제공

가입자의 인증서를 클라우드에 저장하고 인터넷을 통해서 쉽게 접근 할 수 있도록 4개의 공동 운영 인증기관 - 한국정보인증, 코스콤, 한국전자인증 및 한국무역정보통신(TradeSign)이 공동으로 제공하는 서비스를 클라우드 서비스라고 합니다.

1.3.7.1. 공동 운영 인증기관의 역할

클라우드 서비스를 사용하는 가입자의 정보를 관리하고, 클라우드 서비스에 접속 할 수 있는 환경을 제공 및 저장서버로 연계해주는 역할을 수행하는 등록서버는 코스콤이 대표로 운영합니다. 가입자의 인증서 및 전자서명생성정보를 보관하는 "저장서버"는 4개의 공동인증기관이 각각 안전하게 운영합니다. TradeSign이 발급한 가입자 인증서와 전자서명생성정보는 TradeSign이 운영하는 저장서버에 보관됩니다.

1.3.7.2. 책임과 의무

TradeSign은 가입자의 인증서와 전자서명생성정보를 안전하게 보관, 관리하여 서비스를 제공할 책임을 가지고 있습니다.

클라우드 서비스의 안전한 제공을 위하여 4개의 공동인증기관은 공동으로 도입한 클라우드 서비스를 지속적으로 유지 관리합니다. 만약, 클라우드 서비스를 제공하는 4개의 공동인증기관 중 서비스 제공을 중단하려는 기관이 있더라도, 클라우드 서비스의 연속성 보장에 지장이 없도록 다른 인증기관의 저장서버로 이전하여 서비스를 제공합니다.

1.4 인증서 종류

TradeSign은 가입자 인증서의 신규발급, 재발급, 갱신발급, 효력정지, 효력회복 및 폐지 등의 업무(이하 "인증서비스"라 합니다)를 수행하며, 인증서 종류는 다음 표와 같습니다.

인증서 유효기간은 최대 3년 입니다.

범용인증서는 인증서가 필요한 모든 분야에서 사용 가능한 인증서입니다.

전자등기용 인증서는 대법원의 전자민원 용도로만 사용이 가능하며, 용도제한용인증서는 정해진 용도 외에 사용할 수 없습니다.

1.4.1. 범용인증서

정책이름	이용기관	용도
전자거래범용(개인)	모든 전자거래이용기관	개인(자연인)의 신원확인, 전자서명 및 암호화
전자거래범용(법인)	모든 전자거래이용기관	개인사업자, 법인사업자 또는 단체의 신원확인, 전자서명 및 암호화
전자거래범용(서버)	모든 전자거래이용기관	개인사업자, 법인사업자 또는 단체의 신원확인, 전자서명 및 암호화 (서버 또는 장치의 사전 설정에 의한 전자서명, 암호화 포함)

※ 서버인증서의 경우 법인 인증서와 동일한 대상에 동일한 방법으로 발급한다.

1.4.1.1. 범용인증서 OID

정책이름	OID(서명용)	OID(암호용)
전자거래범용(개인)	1 2 410 200012 1 1 1	1 2 410 200012 1 1 2
전자거래범용(사업자)	1 2 410 200012 1 1 3	1 2 410 200012 1 1 4
전자거래범용(서버)	1 2 410 200012 1 1 5	1 2 410 200012 1 1 6

1.4.2. 전자등기용 인증서

정책이름	이용기관	용도
전자등기용 인증서	대법원 법원행정처	대법원 전자민원 업무 (인터넷등기소 등)

1.4.3. 용도제한용 인증서

정책이름	이용기관	용도
용도제한용 인증서	특정 전자거래기관 및 (주)한국무역정보통신이 제공하는 서비스	한정된 용도(업무) - (주)한국무역정보통신이 제공하는 서비스 및 전자세금계산서, 정부 전자민원 등

1.5 준칙의 관리

TradeSign의 인증서비스에 관련한 연락처는 다음과 같습니다.

- URL : http://www.tradesign.net/cps.html
- 전자우편 : tradesign@ktnet.co.kr
- 주소 : 경기 성남시 분당구 판교로 338 한국전자무역센터 6 층
- 전화 : 1566-2119
- FAX : (02)6000-2086

이 인증업무준칙의 제·개정권자는 ㈜한국무역정보통신의 대표이사이며, 전자무역인증센터장이 대행할 수 있습니다.

TradeSign은 법 제15조 제1항 각호의 내용이 변경되었거나, 내용의 변경이 필요한 경우 인증업무준칙을 개정할 수 있으며, 인증업무준칙의 개정시에는 홈페이지에 공고합니다.

TradeSign은 최상위인증기관(한국인터넷진흥원)과의 정책 일관성을 위해 준칙제· 개정에 대하여 협의할 수 있습니다.

인증업무준칙이 제·개정된 경우 다음의 내용을 포함한 준칙의 제·개정 관련 기록을 유지·관리하여야 합니다.

- 해당 인증업무준칙 버전
- 제·개정 기록
- 제·개정 내용, 사유 등

가입자는 변경된 준칙이 공고된 후 2주 (공고일 포함) 이내에 서면으로(또는 전자서명생성정보로 전자서명한 전자문서로) 이의를 제기하지 아니한 경우 TradeSign은 가입자가 변경된 인증업무준칙에 동의하는 것으로 간주합니다.

1.6 정의 및 약어

이 인증업무준칙에서 사용되는 용어의 정의는 다음과 같습니다.

1. "전자문서"란 정보처리시스템에 의하여 전자적 형태로 작성되어 송신 또는 수신되거나 저장된 정보를 말한다.
2. "전자서명"이란 다음 각 목의 사항을 나타내는 데 이용하기 위하여 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보를 말한다.
   - 서명자의 신원
   - 서명자가 해당 전자문서에 서명하였다는 사실
3. "전자서명생성정보"란 전자서명을 생성하기 위하여 이용하는 전자적 정보를 말한다.
4. "전자서명수단"이란 전자서명을 하기 위하여 이용하는 전자적 수단을 말한다.
5. "전자서명인증"이란 전자서명생성정보가 가입자에게 유일하게 속한다는 사실을 확인하고 이를 증명하는 행위를 말한다.
6. "인증서"란 전자서명생성정보가 가입자에게 유일하게 속한다는 사실 등을 확인하고 이를 증명하는 전자적 정보를 말한다.
7. "전자서명인증업무"란 전자서명인증, 전자서명인증 관련 기록의 관리 등 전자서명인증서비스를 제공하는 업무를 말한다.
8. "전자서명인증사업자"란 전자서명인증업무를 하는 자를 말한다.
9. "가입자"란 전자서명생성정보에 대하여 전자서명인증사업자로부터 전자서명인증을 받은 자를 말한다.
10. "이용자"란 전자서명인증사업자가 제공하는 전자서명인증서비스를 이용하는 자를 말한다.
11. “CRL(Certificate Revocation List)”이란 공인인증서 효력정지 및 폐지목록을 말한다.
12. “OCSP(Online Certificate Status Protocol)”이란 실시간 인증서 상태확인 프로토콜을 말한다.

13. "클라우드 서비스" 란 가입자의 인증서와 전자서명생성정보를 클라우드에 저장하여 인터넷을 통해 접속하여 이용할 수 있도록 4개의 공동인증기관들이 공동으로 제공하는 서비스 입니다.

2. 전자서명인증업무 관련 정보의 공고

2.1 공고설비

TradeSign은 인증서, 인증서 효력정지 및 폐지목록 등 인증업무와 관련된 정보를 적시성 있도록 공고설비에 공고합니다. TradeSign은 공고하는 설비를 안전하게 운영 및 관리 합니다.

2.2 공고방법

TradeSign은 인증업무관련정보를 본 인증업무준칙 2.1(공고설비)의 정보 저장 위치를 통하여 지체없이 공고하여야 합니다.

TradeSign의 인증서비스에 관련한 정보의 저장위치는 다음과 같습니다.

- TradeSign 인증업무준칙 : https://www.tradesign.net/cps.html
- TradeSign OCSP 서비스 : http://ocsp.tradesign.net:18000/OCSPServer
- 가입자 인증서와 인증서 효력정지 및 폐지목록 : ldap://ldap.tradesign.net:389
- 최상위 인증기관인증서 :
  https://www.rootca.or.kr/kor/accredited/accredited03_01List.jsp
- 인증기관의 인증서 효력정지 및 폐지목록 :
  https://www.rootca.or.kr/kor/accredited/accredited03_02.jsp

2.3 공고 주기

인증서는 발급 즉시 공고하고, 인증서 효력정지 및 폐지목록(CRL)은 최소 일 1회 이상 발행하여 공고합니다.

2.4 공고된 정보에 대한 책임

공고와 관련된 준수사항이 지켜지지 아니하여 이용자에게 손해를 입힌 때에는 법 제20조(손해배상책임)에 따른 책임을 집니다.

3. 신원확인

3.1 가입자 이름 표시 방법

3.1.1. 가입자 이름(DN) 표현방법 및 유일성 보장 방법

가입자 이름(DN) 표현 및 유일성 보장은 인증서 발급 시 가입자 이름을 CN(Common Name)값에 기술하며, 별도의 값을 통해 유일성을 보장합니다.

3.2 인증서 신규 발급 시 신원확인

TradeSign 또는 등록대행기관은 신청자의 신원을 대면으로 확인합니다.

3.2.1. 인증서 발급 신청서에 기재된 가입자 정보 중 그 진정성을 확인하는 사항

TradeSign 및 등록대행기관은 가입자 정보의 진정성을 확인하기 위해 시행규칙 제5조(실지명의 기준의 신원확인 방법)에 의거 인증서를 발급받고자 하는 자의 실지명의를 기준으로 다음 사항을 확인합니다.

3.2.1.1. 개인

- 주민등록표에 기재된 성명 및 주민등록번호
- 외국인의 경우에는 '출입국관리법'에 의한 등록외국인기록표에 기재된 성명 및 등록번호
- 운전면허증에 표시되어 있는 성명 및 주민등록번호
- 여권에 표시되어 있는 성명 및 주민등록번호 (단, 주민번호가 표시되어 있는 여권에 한함)

※ 한국무역정보통신은 방송통신위원회가 지정한 본인확인기관으로 "정보통신망법"에 의거하여 주민번호를 수집 할 수 있습니다.

3.2.1.2. 법인

- 사업자등록증에 기재된 법인명 및 사업자등록번호
- 사업자등록증을 교부받지 아니한 법인의 경우에는 '법인세법'에 의하여 납세번호를 부여받은 문서에 기재된 법인명 및 납세번호

※ 개인사업자의 경우 사업자등록증으로 법인인증서를 발급 받을 수 있습니다.

3.2.1.3. 법인이 아닌 단체 (국세 기본법의 법인격 없는 사단 포함)

- 당해 단체를 대표하는 자의 주민등록표에 기재된 성명 및 주민등록번호 (또는 대표하는 자가 외국인인 경우에는 등록외국인기록표에 기재된 성명 및 등록번호
- '부가가치세법'에 의하여 고유번호를 부여받거나 '소득세법'에 의하여 납세번호를 부여받은 단체의 경우에는 그 문서에 기재된 단체명과 고유번호 또는 납세번호

- 기타 과학기술정보통신부 장관이 정하는 실지명의

3.2.2. 가입자의 전자서명생성정보 소유증명 방법

가입자의 전자서명생성정보 소유증명은 인증서 발급 시 가입자의 전자서명생성정보에 대한 전자서명을 이용한 POP(Proof Of Possession)을 통해 증명합니다.

3.3 인증서 갱신발급, 재발급 및 변경시, 신원확인

3.3.1. 인증서 갱신발급 신청자에 대한 신원확인 방법

인증서 갱신발급 신청자에 대한 신원확인 및 전자서명생성정보의 소유증명은 유효한 가입자 인증서로 수행한 전자서명을 이용하여 신원을 확인할 수 있습니다.

3.3.2. 인증서 재발급 신청자에 대한 신원확인 방법

인증서 재발급 신청자에 대한 신원확인은 인증서 신규발급 절차를 따릅니다.

3.3.3. 가입자 등록정보 변경 신청자에 대한 신원확인 방법

인증서 가입자 등록정보 변경 신청자에 대한 신원확인 방법은 인증서 신규발급 절차를 따릅니다.

3.4 인증서 효력정지.효력회복.폐지 시 신원확인

3.4.1. 인증서 효력정지·효력회복·폐지 신청자에 대한 신원확인 방법

인증서 효력정지, 효력회복, 폐지 신청자에 대한 신원확인은 인증서 신규발급 절차를 따릅니다. 다만 효력정지 또는 폐지의 경우에는 전자서명을 이용하여 신원확인 및 신청내용의 무결성을 확인할 수 있습니다.

4. 인증서 관리

4.1 인증서 발급 신청

4.1.1. 인증서 신청 주체 및 신청 절차

인증서 신청 주체는 개인, 법인 또는 단체이며 이 신청 주체가 직접 혹은 대리인이 TradeSign 또는 등록대행기관에 신원확인 증표를 지참하고 신청서를 제출하여 신청합니다.

TradeSign 또는 등록대행기관은 신청인을 확인하고 발급을 안내합니다.

4.1.2. 등록대행기관 주소 및 연락처

TradeSign은 가입자의 편의를 위해 전국의 각 지역마다 등록대행기관을 두어 운영하고 있으며 자세한 주소 및 연락처 정보는 TradeSign 웹사이트(www.tradesign.net)에서 확인할 수 있습니다. 다만 범용이 아닌 용도제한용 인증서의 신청은 등록대행기관별로 접수가 제한될 수 있으니 사전에 확인하여야 합니다.

4.1.3. 찾아가는서비스

TradeSign 또는 등록대행기관은 가입자를 내방하여 신청접수 및 발급 안내를 제공(찾아가는서비스)할 수 있습니다.

4.2 인증서 발급 신청 처리

4.2.1. 인증서 발급 신청 접수 및 처리 절차

TradeSign은 4.1(인증서 발급 신청)에 따른 발급 신청 접수 시 3.2(인증서 신규 발급 시 신원확인)에 따라 신청인에 대한 식별 및 확인을 진행합니다.

4.2.2. 가입자의 인증서 발급 신청에 대한 승인 또는 거절 기준

가입자의 인증서 발급 신청에 대한 승인 또는 거절은 신원확인과 인증서 신청서를 기준으로 승인하며, 타인 명의로 신청하는 경우, 신청서 내용을 허위로 기재하였거나 허위서류를 첨부하여 신청한 경우, 제출된 서류만으로 가입 신청자의 신원확인이 불가능한 경우, 업무상 또는 기술상 지장이 있다고 인정하는 경우에는 발급 신청을 거절할 수 있습니다.

4.2.3. 인증서 발급 신청 접수에 대한 처리 기간

TradeSign 및 등록대행기관은 인증서 발급 신청이 접수된 시점부터 14일 이내에만 가입자가 인증서를 발급받을 수 있도록 처리하며 전시, 사변, 천재지변 또는 이에 준하는 비상사태가 발생하였을 때는 처리 기간이 변경될 수 있습니다.

4.3 인증서 발급 절차 및 보호조치

4.3.1. 인증서 신규발급 절차

가입자는 TradeSign 및 등록대행기관으로부터 전달받은 인증서 발급과 관련된 정보(참조번호와 인가코드)를 이용하여 TradeSign 홈페이지, 앱 등 TradeSign이 제공하는 인증서 발급 프로그램을 이용하여 인증서를 발급합니다.

4.3.2. 정보통신망을 통해 전송되는 가입자 정보의 전송

가입자 정보는 등록대행기관으로 부터 TradeSign으로 정보통신망을 통하여 직접 전송됩니

다. 이때 전달되어지는 가입자 정보는 암호화 및 전자서명을 적용하여 기밀성과 무결성을 보장합니다.

4.4 인증서 수령

4.4.1. 가입자가 인증서를 수령하는 방법

TradeSign은 가입자에 대한 신원 확인 및 신청서류를 검토한 후, 인증서를 발급 가능한 코드를 제공합니다. 가입자는 TradeSign에 접속하여 해당 코드를 이용하여 인증서를 다운로드 받음으로써 인증서를 수령합니다.

4.5 인증서 이용

인증서는 전자거래 등의 업무에 사용할 수 있습니다. 앞의 전자거래에서의 인증서 사용은 정당한 권한을 가진 가입자가 인증서의 이용범위 및 발급 용도에 맞게 인증서를 사용하는 것을 말합니다.

그러하지 아니한 경우 TradeSign은 기발급된 인증서의 사용을 제한할 수 있습니다.

가입자는 발급받은 인증서의 용도에 따라 유효기간을 확인하여 인증서를 이용 하도록 유의하여야 합니다.

4.6 인증서 갱신발급

4.6.1. 인증서 갱신발급 요건, 신청 주체 및 신청절차

인증서 갱신발급은 인증서 유효기간이 만료되기 2개월 전부터 만료일 사이에 전자서명생성정보와 유효기간이 갱신된 동일한 종류의 새로운 인증서를 발급합니다. 신청 주체는 가입자 본인이며, 신청절차는 TradeSign 홈페이지 또는 TradeSign이 제공하는 앱의 인증서 갱신 발급 메뉴을 이용하여 신청과 발급이 수행됩니다. 반드시 이전에 사용하던 유효한 인증서가 준비되어 있어야 합니다.

4.6.2. 정보통신망을 통해 전송되는 가입자 정보의 전송방법

정보통신망을 통해 전송되는 가입자 정보의 전송은 인증서 신규발급 절차를 따릅니다.

4.6.3. 정보통신망을 통해 전송되는 가입자 정보의 기밀성, 무결성 등에 대한 정보보안 방법

정보통신망을 통해 전송되는 가입자 정보의 기밀성, 무결성 등에 대한 정보보안은 인증서 신규발급 절차를 따릅니다.

4.6.4. 가입자의 전자서명생성정보 소유증명 방법

가입자의 전자서명생성정보 소유증명은 인증서 신규발급 절차를 따릅니다.

4.6.5. 가입자가 갱신발급된 인증서를 수령하는 방법

가입자가 갱신발급 된 인증서를 수령하는 방법은 TradeSign에 접속하여 인증서 갱신 메뉴를 이용하여 인증서를 다운로드 받음으로써 인증서를 수령 합니다.

4.6.6. 갱신 후 유효기간이 남은 기존 인증서의 유효성

갱신발급이 완료되어 새로운 인증서가 발급되어도 기존 인증서는 만료일까지 유효합니다. 따라서 기존 인증서의 폐지가 필요하다면 가입자가 직접 '4.9 인증서의 폐지'에 따라 폐지하여야 합니다.

4.7 인증서 재발급

4.7.1. 인증서 재발급 요건, 신청 주체 및 신청절차

인증서 재발급은 가입자가 자신의 전자서명생성정보가 노출, 분실 또는 변경되었다고 우려되는 경우 인증서를 다시 발급하는 것을 말합니다. 신청 주체는 가입자 본인이며, 신청절차는 4.1 항의 신규 인증서 발급과 동일한 방식으로 TradeSign 및 등록대행 기관에 방문하여 신청합니다.

TradeSign 및 등록대행기관으로부터 전달받은 인증서 발급과 관련된 정보(참조번호와 인가코드)를 이용하여 TradeSign 홈페이지, 앱 등 TradeSign이 제공하는 인증서 발급 프로그램을 이용하여 인증서를 발급합니다.

4.7.2. 정보통신망을 통해 전송되는 가입자 정보의 전송방법

정보통신망을 통해 전송되는 가입자 정보의 전송 방법은 인증서 신규발급 절차를 따릅니다.

4.7.3. 정보통신망을 통해 전송되는 가입자 정보의 기밀성, 무결성 등에 대한 정보보안 방법

정보통신망을 통해 전송되는 가입자 정보의 기밀성, 무결성 등에 대한 정보보안은 인증서 신규발급 절차를 따릅니다.

4.7.4. 가입자의 전자서명생성정보 소유증명 방법

가입자의 전자서명생성정보 소유증명은 인증서 신규발급 절차를 따릅니다.

4.7.5. 가입자가 재발급된 인증서를 수령하는 방법

가입자가 재발급된 인증서를 수령하는 방법은 신규발급 절차를 따릅니다.

4.8 인증서 변경 (가입자 등록정보 변경)

4.8.1. 가입자 등록정보 변경 요건, 신청 주체 및 신청절차

가입자 등록정보 변경은 인증서 내에 반영된 가입자 정보의 변경의 경우는 3.2(인증서 신규 발급 시 신원확인) 절차를 따릅니다.

그 외의 가입자 등록정보(주소, 전화번호, 전자우편 주소 등)가 변경된 경우는 가입자가 홈페이지에서 직접 수정을 하거나 등록정보 변경을 TradeSign에 요청하여 변경시킬 수 있습니다.

4.8.2. 정보통신망을 통해 전송되는 가입자 정보의 전송방법

정보통신망을 통해 전송되는 가입자 정보의 전송은 인증서 신규발급 절차를 따릅니다.

4.8.3. 정보통신망을 통해 전송되는 가입자 정보의 기밀성, 무결성 등에 대한 정보보안 방법

정보통신망을 통해 전송되는 가입자 정보의 기밀성, 무결성 등에 대한 정보보안은 인증서 신규발급 절차를 따릅니다.

4.8.4. 가입자의 전자서명생성정보 소유증명 방법

가입자의 전자서명생성정보 소유증명 방법은 인증서 신규발급 절차를 따릅니다.

4.8.5. 가입자 등록정보가 변경된 인증서를 수령하는 방법

가입자가 가입자 등록정보가 변경된 인증서를 수령하는 방법은 신규발급 절차를 따릅니다.

4.9 인증서 효력정지.효력회복.폐지

4.9.1. 인증서 효력정지·효력회복·폐지 신청요건, 신청 주체 및 신청절차

4.9.1.1. 인증서 효력정지.효력회복.폐지의 정의

- 인증서 효력정지는 인증서의 유효기간 동안 가입자의 신청 등으로 인증서의 효력을 일정기간 동안 정지하는 것을 말합니다.
- 인증서 효력회복은 효력정지된 인증서에 대하여 가입자의 신청 등으로 인증서의 효력을 회복하는 것을 말합니다. 효력회복은 효력정지일부터 6 개월 이내에 가능합니다.
- 인증서 폐지는 가입자의 신청 등으로 인증서의 효력을 영구 정지하는 것을 말합니다.

4.9.1.2. 인증서 효력정지.효력회복.폐지 신청요건

가입자가 인증서 효력정지를 신청한 경우에 TradeSign은 가입자의 인증서를 효력정지 할 수 있습니다.

효력이 정지된 인증서에 대하여 가입자가 효력회복을 신청하였을 경우 TradeSign은 가입자의 인증서를 효력회복 할 수 있습니다. 단, 4.9.7에서 언급한 기간 이내에 효력회복을 신청하여야 합니다.

TradeSign은 다음의 경우에 가입자의 인증서를 폐지할 수 있습니다.

- 가입자가 인증서 폐지를 신청한 경우
- 가입자의 생성정보에 대한 분실, 훼손 또는 도난, 유출된 사실을 인지한 경우
- 가입자의 사망, 실종선고 또는 해산, 법인의 폐업 사실을 인지한 경우
- 가입자의 부정한 방법으로 인증서를 발급받은 사실을 인지한 경우
- 가입자가 준칙의 중요한 의무사항을 위반한 경우
- 가입자의 의무사항 준수가 천재지변 및 기타 원인으로 인해 지연되거나 불가능한 경우
- 가입자의 착오로 인해 인증서를 발급받은 경우

4.9.1.3. 인증서 효력정지.효력회복.폐지의 주체 및 절차

가. 가입자 신청에 의한 효력정지와 폐지 신청 방법은 아래와 같습니다.

- 가입자가 인증서 효력정지·폐지 신청서를 작성하고 신원확인 서류를 첨부하여 TradeSign 에 방문 제출합니다.
- 가입자가 www.tradesign.net 의 효력정지·폐지에서 기존의 유효한 인증서로 신원확인(로그인)을 하고 신청합니다.

나. 가입자 신청에 의한 효력회복 신청 방법은 아래와 같습니다.

- 가입자가 인증서 효력회복 신청서를 작성하고 신원확인 서류를 첨부하여 TradeSign 에 방문 제출합니다. TradeSign 은 동일한 방식으로 신원확인 후 처리 합니다.

다. TradeSign 에 의한 효력정지와 폐지 절차는 다음과 같습니다.

- 가입자에게 폐지, 효력정지 사유를 통보(email, 전화 등)하고 폐지, 효력정지 후, 인증서 폐지대장에 기재합니다.
- 가입자에게 통보할 수 없는 경우, 폐지 또는 효력정지 후, 관련 내용을 TradeSign 게시판에 게재합니다.

4.9.2. 정보통신망을 통해 전송되는 가입자 정보의 전송방법

정보통신망을 통해 전송되는 가입자 정보의 전송은 인증서 신규발급 절차를 따릅니다.

4.9.3. 정보통신망을 통해 전송되는 가입자 정보의 기밀성, 무결성 등에 대한 정보보안 방

법

정보통신망을 통해 전송되는 가입자 정보의 기밀성, 무결성 등에 대한 정보보안은 인증서 신규발급 절차를 따릅니다.

4.9.4. 인증서 효력정지·효력회복·폐지 신청 접수부터 해당 인증서 효력정지·효력회복·폐지까지 소요되는 최대 처리시간

인증서 효력정지, 효력회복, 폐지 신청 접수에 대한 처리시간은 해당 신청이 접수된 시각으로부터 최대 60분 이내이며 인증서비스 이용약관에 나타난 전시, 사변, 천재지변 또는 이에 준하는 비상사태가 발생하였을 때는 처리 시간을 변경합니다.

4.9.5. 인증서 효력정지 및 폐지목록(CRL) 발행주기

인증서 효력정지 및 폐지목록(CRL)은 최소 일 1회 이상 발행합니다.

4.9.6. 인증서 효력정지 및 폐지목록(CRL) 발행 시점부터 해당 인증서 효력정지 및 폐지목록(CRL)을 공고하는데 까지 소요 시간

인증서 효력정지 및 폐지목록(CRL)은 발행시 지체없이 공고하는 것으로 하며, 인증서비스 이용 약관에 나타난 전시, 사변, 천재지변 또는 이에 준하는 비상사태가 발생하였을 때는 처리기간을 변경합니다.

4.9.7. 인증서 효력정지 상태 유지 가능 기간

가입자는 인증서의 효력이 정지된 날로부터 6개월 이내에 그 회복을 신청하여야 합니다. 이 기간 내에 신청하지 않으면 해당 인증서는 자동 폐지됩니다.

4.10 OCSP 서비스

4.10.1. 이용 방법

인증서의 유효 또는 폐지(효력정지포함) 여부를 확인하는 서비스를 OCSP 서비스 하며 OCSP 서비스 신청자는 사전에 TradeSign에 이용계약을 체결하여야 합니다. OCSP 서비스 이용자는 TradeSign 또는 제3자로부터 제공받은 OCSP client 를 통해 서비스를 이용할 수 있습니다.

4.10.2. 이용 조건

OCSP 서비스는 원칙적으로 유료이며 이용요금은 별도 협의를 통해 결정됩니다. TradeSign과 OCSP 서비스 이용자는 RFC2560 표준에 따라 요청 및 응답 전문을 처리하여야 합니다.

4.10.3. 이용계약 해지

OCSP 서비스 이용자가 OCSP 서비스 이용계약을 해지하고자 할 때에는 해지일 한 달 전에 TradeSign으로 통보하여 별도의 절차를 거쳐 계약을 해지할 수 있습니다.

4.11 서비스 가입 철회

가입자의 서비스 가입 철회는 “4.9 인증서 효력정지.효력회복.폐지”의 인증서 폐지 절차를 준용합니다.

이때 제출된 신청서 및 기록들은 관련법인 개인정보 보호법, 전자상거래 등에서의 소비자보호에 관한 법률(이하 “전자상거래법”이라 합니다.) 등에 따라 보존되고 파기 됩니다.

4.12 기타 부가 서비스

4.12.1 시점확인서비스(Time Stamping Service 또는 TSA 서비스 : Time Stamp Authority Service)

4.12.1.1. 이용 방법

전자문서의 작성 시점을 확인할 수 있는 증표를 발급하는 서비스를 시점확인서비스라하며 TSA 서비스 이용자는 사전에 TradeSign에 이용계약을 체결하여야 합니다. TSA 서비스 이용자는 TradeSign 또는 제3자로부터 제공받은 TSA client 를 통해 서비스를 이용할 수 있습니다.

4.12.1.2. 이용 조건

TSA 서비스는 원칙적으로 유료이며 이용요금은 별도 협의를 통해 결정됩니다. TradeSign과 TSA 서비스 이용자는 RFC3161 표준에 따라 요청 및 응답 전문을 처리하여야 합니다.

4.12.1.3. 이용계약 해지

TSA 서비스 이용자가 TSA 서비스 이용계약을 해지하고자 할 때에는 해지일 한 달 전에 TradeSign으로 통보하여 별도의 절차를 거쳐 계약을 해지할 수 있습니다.

4.12.2 클라우드 인증서비스

클라우드 서비스는 4개의 공동인증기관(코스콤, 정보인증, 전자인증, TradeSign)이 함께 제공하는 서비스입니다.

가입자는 클라우드에 가입자 인증서를 보관하고, 등록된 PC, 모바일 등 다양한 매체에서 인증서를 편리하게 사용하는 서비스입니다.

4.12.2.1. 이용 방법

TradeSign의 클라우드 서비스는 가입자가 별도의 이용 신청을 하여야만 사용 가능합니다. 클라우드 서비스 가입시 별도의 신원확인 과정을 수행하며, 가입자는 이를 수행하여야 합니다.

4.12.2.2. 전자서명 생성정보의 보관

TradeSign의 클라우드 서비스는 가입자의 전자서명생성정보를 안전하게 보관합니다.

TradeSign은 가입자의 동의 없이 전자서명 생성정보를 이용하지 않으며, 가입자만 알고 있는 값을 가입자의 전자서명생성정보 암호화 보관시 활용하고 있어서 가입자의 정보제공 없이는 누구도 전자서명 생성정보를 활용할 수 없어 보다 높은 신뢰성을 제공합니다.

4.12.2.3. 이용 조건

TradeSign의 클라우드 서비스는 서비스 이용 수수료, 기타 제공 조건 등 세부사 항은 해당 계약 내용에 따릅니다.

4.12.2.4. 이용계약 해지

TradeSign의 클라우드 서비스는 가입자가 별도의 서비스 해지 신청을 통하여 해지 가능 합니다.

5. 시설 및 운영 관리

5.1 물리적 보호조치

TradeSign은 외부인의 침입이나 불법적 접근 등의 물리적 위협으로부터 인증시스템을 보호하기 위해 보호조치를 합니다.

5.1.1. 시설 위치와 구조에 관한 사항

5.1.1.1. 시설의 위치

TradeSign의 인증시스템을 위한 시설은 아래에 위치 합니다.

무역협회 IDC : 서울특별시 강남구 영동대로 511 코엑스 신관 전시컨벤션센터 B1홀 4층

5.1.1.2. 시설의 구조

인증서비스 전용의 네트워크, 설비 및 전산실을 운영합니다.

5.1.2. 다중출입, 침입감지, 경보 및 감시, 통제

가. 출입통제 시스템은 신원확인카드, 지문인식 및 무게감지 장치 등 다중으로 결합하여 통제구역에 대한 접근을 통제하며, 통제구역 출입 내역을 기록하고, 정기적으로 감사합니다. 또 이상 상황이 발생하는 경우에 대비하여 다음과 같은 시스템을 설치하고 경보 기능을 갖는 감시통제 시스템을 설치, 운영합니다.

- CCTV 카메라 및 모니터링시스템

- 침입감지시스템

나. 하드웨어 보수 등의 업무수행을 위하여 외부인이 핵심 인증시스템실 등에 출입할 경우에 반드시 담당 관리자가 동행합니다.

5.1.3. 물리적 잠금장치

핵심 인증시스템은 물리적 접근통제를 위해 보안캐비닛 내에 설치 운영하며, 보안캐비닛 키는 별도의 열쇠 보관함에 보관합니다.

5.1.4. 방호

인증시스템을 외부 침입으로부터 보호할 수 있도록 시스템실은 다음을 만족하도록 합니다.

- 벽돌, 철근 콘크리트 또는 철골 구조물에 3T 이상의 철판으로 용접된 외벽
- 인증시스템과 타 시스템을 분리할 수 있도록 케이지 설치
- 강화유리 또는 강화필름으로 코팅한 유리를 사용한 창

5.1.5. 화재 및 수재, 정전방지 및 보호설비

가. TradeSign 은 갑작스러운 정전으로 인한 심각한 피해를 방지하기 위하여 무정전 전원공급장치를 이용하며, 별도의 발전기를 설치하여 안정적으로 전원을 공급합니다.

나. TradeSign 은 누수에 대비하여 인증관련 시스템을 안전하게 보호하기 위하여 바닥으로부터 30cm 이상 이격하여 설치합니다.

다. TradeSign 은 화재에 대하여 인증관련 시스템을 보호하기 위하여 화재 탐지기를 설치하고 소화할 때 시스템의 기능에 문제를 야기하지 않는 성분의 휴대용 소화기 및 자동 소화설비 등을 설치합니다.

라. TradeSign 은 제한된 장소의 내화금고에 주요 저장기록 매체를 저장하여 물리적으로 접근을 통제합니다.

5.1.6. 항온항습, 통풍 및 기타 보호설비

Tradesign내 실내온도와 습도를 적정하게 유지하는 설비를 운영합니다. 통풍창은 사람이 통과할 수 있을 경우 차폐막을 설치합니다.

5.1.7. 시설 및 장비의 폐기처리 절차

TradeSign은 시설 및 장비, 문서, 데이터를 폐기하는 경우 보안 관리자가 입회하에 물리적, 논리적으로 복구가 불가능한 방법으로 이를 파기합니다.

5.1.8. 원격지 백업설비 운영

TradeSign은 천재지변 및 기타 재난을 대비하여 10km이상 격리된 원격지 백업설비를 설

치, 운영하며, 물리적으로 접근통제장치와 잠금장치가 있는 보안캐비닛에 보관합니다.

5.2 절차적 보호조치

5.2.1. 인증업무에 대한 업무분장

인증업무의 효율적인 업무수행을 위해 담당자 업무를 지정하고 구분하며 내부 관리 업무분장표에 기재하여 관리합니다.

- 모든 보호조치를 계획, 감독, 통제하는 관리책임자를 지정
- 모든 보호조치의 실행을 담당하는 보안관리자를 지정
- 인증업무 정책을 관리하는 정책관리자를 지정
- 인증업무 고객 및 RA 를 관리하는 고객관리자를 지정
- 인증서 생성/발급/관리, 시점확인 서비스 등 개발, 유지보수하는 개발자를 지정
- 인증센터 시스템 관리, 네트워크 관리, DB 관리 등을 수행하는 운영자를 지정

5.2.2. 인증업무 담당자 인증

물리적 인증방법은 다중결합(신원확인카드, 지문인식, 무게감지)통제 구역을 통과해야 하고, 업무에 맞게 출입 권한을 부여하고 접근 권한있는 자만 허용하고, 시스템 인증방법은 방화벽 시스템과 서버보안 소프트웨어, OTP(One Time Passward)로 승인된 담당자만 접근을 허용합니다.

5.2.3. 동일인에 의해 동시 수행 될 수 없는 인증업무

인증업무 운영의 독립성과 보안성을 감안하여 키 생성 업무는 3인 이상이 공동으로 수행하고, 그 외 인증업무는 각각의 역할에 맞게 2인 이상이 직원이 공동으로 수행하여 동일인이 동시에 수행할 수 없도록 합니다.

5.3 인적 보안

5.3.1. 인증업무 인력 요구사항 및 신원 확인 절차

인증 업무를 운영, 관리하는 인력으로서 12인 이상 확보합니다.

- 정보통신기사, 정보처리기사 및 전자계산기조직응용기사 이상의 국가기술자격 또는 이와 동등 이상의 자격이 있다고 과학기술정보통신부가 인정하는 자격을 갖출 것
- 과학기술정보통신부가 정하여 고시하는 정보보호 또는 정보통신 운영 및 관리 분야에서 2 년 이상 근무한 경력이 있을 것

TradeSign은 인증업무 인력에 대하여 내부규정인 '취업규칙'에 따라 신원확인을 하고 있으

며 이상이 없는 임직원만 관련 업무를 수행하도록 하고 있습니다.

5.3.2. 인증업무 교육 및 업무순환

가. 인증업무를 담당하는 직원은 년 1 회 이상 정보보호관련 내부 또는 외부교육을 이수하도록 합니다.

나. 업무상 취득한 기밀사항의 준수에 관한 보안 서약서를 작성하며, 직원의 업무변경이나 인사이동, 퇴직하는 경우 내부규정에 따라 계정 삭제 및 출입카드를 반납합니다.

5.3.3. 비인가된 행위에 대한 처벌

소속직원의 비인가된 행위를 수행하는 경우 내부 규정이 정하는 바에 따라 해당 직원을 징계합니다

5.4 감사 기록

5.4.1. 감사기록의 유형 및 보존기간

TradeSign은 시스템에서 발생한 모든 이벤트, 사건 등의 세부내역을 감사 기록에 5년 동안 보관합니다.

- 가입자 등록 정보를 입력•접근•변경•삭제
- TradeSign 이 사용하는 전자서명생성정보를 생성•접근•파기
- 인증서의 생성•발급•갱신•효력정지•폐지
- 가입자 인증서의 등록 및 관리
- 전자문서의 시점확인
- 핵심인증시스템의 시작과 종료
- 계정의 추가 및 삭제
- 사용자 권한 변경
- 로그인(login) 및 로그오프(logoff)
- 기타 핵심인증시스템 관리자의 주요 활동

5.4.2. 감사기록 보호조치

TradeSign은 물리적 접근통제와 논리적 접근통제를 통해 감사기록에 대한 접근을 제한하며, 시스템의 각 업무 관리자는 각자의 업무에 대한 감사 기록만 열람할 수 있습니다.

5.4.3. 감사기록의 확인

감사 관리자는 인증시스템에서 생성된 감사기록을 주기적으로 확인하고 검토합니다.

해당 업무는 월 1회 이상 수행됩니다.

5.4.4. 감사기록 백업 주기 및 절차

백업 운영자는 인증시스템의 감사기록을 풀 백업 기준으로 매주 수행하며, 매월 1회 소산지에 보관한다. 백업과 관련한 상세한 절차는 내부 지침 '백업 및 복구 지침'에 따라 실시합니다.

5.5 기록 보존

5.5.1. 보존되는 기록의 유형 및 보존기간

TradeSign은 당해 인증서의 효력이 소멸된 날부터 5년 동안 보관합니다.

- 인증서 발급 및 관리 등 전자서명 인증업무
- TradeSign 의 전자서명인증시스템 등의 운영업무

5.5.2. 보존기록의 보호조치

보존기록은 물리적, 인적통제를 통한 인가된 관리자만이 접근가능 합니다.

- 전자파일은 위·변조 및 훼손 등을 방지하도록 보관합니다.
- 종이문서는 잠금시설이 설치된 서고 또는 잠금장치가 설치된 캐비닛에 보관합니다

5.5.3. 보존기록의 백업주기 및 절차

보존기록은 매 주/월 단위로 백업하여 보존하고, 월 백업본은 보존기록의 손실 및 파괴에 대비하여 원격지 백업설비에 각 1부씩 소산하여 보관합니다.

5.6 전자서명인증사업자의 전자서명생성정보 갱신

TradeSign은 전자서명생성정보가 갱신되면 갱신된 인증서를 디렉토리시스템에 게시함으로써 이용자에게 배포하고, 가입자 인증서 발급, 갱신, 재발급시 인증서를 내려줌으로써 가입자에게 배포합니다.

5.7 장애 및 재난 복구

5.7.1. 인증업무 장애 및 재해 유형별 신고 복구 절차

인증업무 장애 및 재해 시 "전자서명인증사업자 장애 및 비상계획"에 따라 신고 및 복구절차에 따라 복구합니다.

가. 센터 내 정전 – UPS 가동으로 무중단 유지하며, 1 시간 이상 정전의 지속시 무역센터 자가발전기를 사용한 정전 대응을 조치함

나. 센터 통신망 두절 – 기간통신망 서비스 상태를 확인하고, 복구 불가시 제 3 의 회선사업자로 백본망 구축을 수행함

다. DDoS 공격으로 인한 통신 장애 – DDoS 전용장비와 NMS 를 이용하여 네트워크 관문을 감시하고, IPS 등 보안장비와 네트워크 장비로 차단 필터를 적용함

라. 기타 장애 및 재해 – 각 장애 및 재해 상황에 맞도록 복구를 수행함

5.7.2. 인증업무 장애방지 등 연속성 보장 대책

가. 핵심인증시스템 및 서비스 운영과 관련된 시스템은 이중화로 구성하여 주 시스템에 문제가 발생하여도 인증서비스가 가능하도록 구성합니다.

나. 네트워크 회선은 서로 다른 ISP 로부터 제공되도록 이중화하여 구성하며, 하나의 네트워크 회선에 문제가 발생하더라도 다른 회선으로 자동 전환되도록 구성합니다.

다. 가입자 인증서 등의 주요 데이터의 훼손·멸실이 발생하였을 경우 백업된 자료를 이용하여 신속히 복구하여 서비스의 연속성을 보장합니다.

5.8 업무 휴지, 폐지, 종료

5.8.1. 인증업무의 휴지 또는 폐지 사유 및 절차

TradeSign의 사정으로 인하여 인증서비스의 전부 또는 일부를 휴지하거나 폐지할 수 있습니다. 이 절차는 아래와 같습니다. 이 경우 TradeSign은 법 제15조(전자서명인증업무준칙의 준수 등) 제2항 내지 제3항에 의거하여 다음의 사항을 시행합니다.

가. TradeSign 은 휴지 시작일과 종료일 그리고 폐지 종료일을 정합니다.

나. 휴지는 휴지 시작일 30 일 전, 폐지는 종료일 60 일 전에 가입자에게 통보합니다. 통보하는 내용에는 가입자에게의 요금의 반환, 가입자 개인정보의 폐기 등 가입자 보호조치 내용이 포함됩니다. 통보하는 내용에는 가입자에게의 요금의 반환, 가입자 개인정보의 폐기 등 가입자 보호조치 내용이 포함됩니다.

다. TradeSign 은 해당 사실을 홈페이지에 공지하고, 가입자에게 전자우편을 통하여 통보합니다.

라. TradeSign 의 업무가 종료하게 되어도 법으로 정해진 의무를 수행하게 되며, 의무를 수행함에 있어서 필요한 사항에 대하여는 인정기관과 협의하여 진행합니다.

마. 인증서를 사용하고있는 유료 이용자들에 대하여는 이용자들이 인증서를 사용함에 불편하지 않도록 다른 인증수단을 제공하는 것을 인정기관과 협의하여 진행합니다.

5.8.2. 인증업무 인정취소

TradeSign은 시행령 제3조(운영기준 준수사실 인정의 취소)에 따라 인정기관으로 부터 정지명령을 받거나 인정이 취소될 수 있습니다. 이에 대한 사유는 다음과 같습니다.

가. 운영기준준수사실 인정의 취소

- 법 제 17 조(시정명령) 제 1 호에 해당하여 시정명령을 받았으나 이를 정당한 사유 없이 이행하지 아니한 경우

5.8.3 전자서명생성정보의 보안

TradeSign은 전자서명생성정보의 분실.훼손, 도난.유출 등 인증서의 신뢰성이나 유효성에 영향을 미치는 사유가 발생한 사실을 인지하는 경우 한국인터넷진흥원에 해당 사실을 신속하게 신고하고, 가입자에게 이를 통보하며 필요한 경우 당해 전자서명생성정보로 발급한 가입자의 인증서를 폐지합니다.

또한, 즉시 당해 사실을 홈페이지에 공고하고, OCSP, CRL을 갱신 등을 이용하여 확인할 수 있도록 조치합니다.

TradeSign이 제공하는 클라우드 서비스에 보관된 가입자의 전자서명생성정보에 대한 손상, 노출, 파손, 분실, 도난 등 가입자의 인증서의 신뢰도 및 유효성에 중대한 영향을 미치는 사실이 발생할 때, 한국인터넷진흥원에 해당 사실을 신속하게 신고하고, 가입자에게 지체없이 통보합니다.

6. 기술적 보호 조치

6.1 전자서명생성정보 보호

가. 전자서명키(전자서명생성정보, 검증정보) 생성

TradeSign은 인가된 인원만이 내부 및 외부 물리적 침해 등으로부터 안전한 키생성 시스템에서 전자서명키를 생성합니다.

6.2 전자서명생성정보 보호 조치

가. 전자서명생성정보 보호

TradeSign의 전자서명생성정보를 봉인, 접근권한 확인 및 전자서명생성정보의 유출·변경 방지 기능을 갖춘 저장장치에 암호화하여 저장합니다.

전자서명생성정보의 생성 및 사용이 종료된 후 지체 없이 시스템 메모리에서 전자서명생성정보를 삭제합니다.

나. 전자서명생성정보 파기

인증서의 유효기간이 만료되는 경우 해당 전자서명 생성정보 저장매체를 해당 저장장치에서 제공하는 방법을 이용하여 파기하고, 전자서명생성정보가 훼손·유출되었을 경우에 해당 전자서

명생성정보 저장매체를 물리적, 논리적으로 완전히 파기합니다.

다. 전자서명생성정보 백업

전자서명생성정보의 백업본은 2부를 생성하여 1부는 주센터에 보관하고 1부는 원격지에 보관 합니다. 물리적으로 안전한 잠금장치가 있는 캐비넷 등을 이용합니다.

6.3 전자서명생성정보 및 전자서명검증정보의 관리

TradeSign은 전자서명생성정보의 분실·훼손·도난·유출 방지를 위하여 물리적 침해 등으로부터 보호되는 안전한 키 생성시스템에서 인가된 자만이 전자서명생성정보를 생성하여 보관할 수 있도록 합니다.

6.4 데이터 보호 조치

TradeSign은 전자서명생성정보 생성 등에 연관된 데이터의 분실, 훼손, 도난, 유출이 되지 않도록, 해당 기능을 제공하는 하드웨어 보안장치(HSM)를 사용합니다.

6.5 시스템 보안 통제

가. TradeSign 은 서비스를 안전하게 제공하기 위하여, 시스템을 이중화하여 운영합니다.

나. TradeSign 은 인증시스템의 보안 소프트웨어를 설치하여 운영하고 보안 장비를 운영합니다.

다. TradeSign 은 인증시스템에 대한 물리적 접근통제 목록을 문서화하여 접근통제 현황에 대한 주기적인 모니터링을 합니다.

라. TradeSign 은 인증시스템에 설치되는 프로그램의 사용을 제한하고 통제합니다.

마. TradeSign 은 정기적으로 유지보수점검을 시행하며 시스템 추가/폐기/변경에 관한 사항을 관리대장에 기록하여 관리합니다.

6.6 시스템 운영 관리

6.6.1. 인증S/W형상관리

서비스별 설치된 소프트웨어의 추가/변경/삭제 시 사항을 기록하여 버전별 형상을 관리합니다.

6.7 네트워크 보호조치

6.7.1. 네트워크 구성 및 운영

두 개의 ISP에서 회선 서비스를 공급 받아 네트워크를 이중화하여 구성하여 장애에 대비하

고, 침입차단시스템, 침입탐지시스템, 네트워크관리시스템(NMS)을 설치 및 운영하고 있으며, 네트워크 회선을 정기적으로 유지보수하며, 네트워크시스템의 추가/폐기/변경에 관한 사항을 기록•관리합니다.

6.8 시점확인서비스 보호조치

6.8.1. 부가서비스 운영에 대한 보호 조치

TradeSign은 부가서비스 운영과 관련된 주요 시스템을 이중으로 구성하여 운영합니다. 또한, 서비스관리시스템(SMS)과 서버보안 소프트웨어를 설치, 운영하고 정기적으로 유지보수점검을 시행하며 시스템 추가/폐기/변경에 관한 사항을 관리대장에 기록하여 관리합니다.

- 시점확인 시스템
- 클라우드 공동인증 시스템

7. 인증서 형식

7.1 인증서 형식

7.1.1. 가입자 인증서의 구성 및 내용

가입자 인증서의 구성 및 내용은 “전자서명 인증서 프로파일 규격”을 따릅니다.

내용은 다음과 같습니다.

- 기본필드

#	필드명	생성	처리	내용
1	Version	m	m	V3
2	Serial Number	m	m	자동으로 할당되는 일련번호
3	Issuer	m	m	인증서 발급자의 DN
4	Validity	m	m	인증서 유효기간
5	Subject	m	m	인증서 사용자의 DN
6	Subject Public Key Info	m	m	인증서 공개정보 정보
7	Extensions	m	m	확장필드

- 확장필드

#	필드명	C	생성	처리	내용
1	Authority Key Identifier	n	m	m	발급기관 정보 식별자, 디렉토리 주소, 인증기관 인증서 시리얼 번호
2	Subject Key Identifier	n	m	m	주체정보 식별자
3	Key Usage	c	m	m	Digital Signature, non-Repudiation
4	Certificate Policy	c	m	m	인증서 정책, CPS 주소, 인증서 표시규격
5	Policy Mappings	-	-	-	사용안함
6	Subject Alternative Names	n	m	m	가입자 한글실명과 VID
7	Issuer Alternative Names	n	o	m	사용안함
8	Extended Key Usage	n	o	o	보안토큰 사용 시 사용
9	Basic Constraints	-	x	x	사용안함
10	Policy Constraints	-	-	-	사용안함
11	Name Constraints	-	-	-	사용안함
12	CRL Distribution Point	n	m	m	CRL 획득 정보
13	Authority Information Access	n	m	m	OCSP 서버 접근 정보

7.2 인증서 유효성 확인 정보 형식

7.2.1. 가입자 인증서 효력정지 및 폐지목록(CRL)의 구성 및 내용

가입자 인증서 효력정지 및 폐지목록(CRL)의 구성 및 내용은 “전자서명 인증서 효력정지 및 폐지목록 프로파일 규격”을 따릅니다. 내용은 다음과 같습니다.

- 기본필드

#	필드명	생성	처리	내용
1	Version	m	m	V2
2	Signature	m	m	서명 알고리즘
3	Issuer	m	m	발급자의 DN
4	This Update	m	m	개시날짜
5	Next Update	m	m	다음 업데이트
6	Revoked Certificates	m	m	폐지된 인증서 리스트
7	CRL Extensions	m	m	확장필드

- CRL 확장필드

#	필드명	C	생성	처리	내용
1	Authority Key Identifier	n	m	m	기관 키 식별자, 발급자 정보
2	Issuer Alternative Names	n	o	m	사용안함
3	CRL Number	n	m	m	CRL 번호
4	Issuing Distribution Point	c	m	m	디렉토리 주소

- CRL 엔트리 확장필드

#	필드명	C	생성	처리	내용
1	Reason Code	n	m	m	원인코드
2	Hold Instruction Code	n	o	m	사용안함
3	Invalidity Date	n	o	m	폐지날짜
4	Certificate Issuer	c	o	m	사용안함

7.3 OCSP 서비스 형식

7.3.1. OCSP 서비스용 인증서의 구성 및 내용

OCSP 서비스용 인증서의 구성 및 내용은 “실시간 인증서 상태확인 기술규격”을 따릅니다. 사용하는 인증서 프로파일은 다음과 같습니다.

- 기본필드

#	필드명	생성	처리	내용
1	Version	m	m	V3
2	Serial Number	m	m	자동으로 할당되는 일련번호
3	Issuer	m	m	인증서 발급자의 DN
4	Validity	m	m	인증서 유효기간
5	Subject	m	m	인증서 사용자의 DN
6	Subject Public Key Info	m	m	인증서 공개정보 정보
7	Extensions	m	m	확장필드

- 확장필드

#	필드명	C	생성	처리	내용
1	Authority Key Identifier	n	m	m	발급기관 정보 식별자, 디렉토리 주소, 인증기관 인증서 시리얼 번호
2	Subject Key Identifier	n	m	m	사용자의 공개키 hash 값
3	Key Usage	c	m	m	Digital Signature, non-Repudiation
4	Certificate Policy	b	m	m	인증서 정책, CPS 주소, 인증서 표시규격
5	Policy Mappings	-	-	-	사용안함
6	Subject Alternative Names	n	m	m	가입자 한글실명과 VID
7	Issuer Alternative Names	n	o	m	사용안함
8	Extended Key Usage	n	o	o	사용안함
9	Basic Constraints	-	x	x	사용안함
10	Policy Constraints	-	-	-	사용안함
11	Name Constraints	-	-	-	사용안함
12	CRL Distribution Point	n	m	m	CRL 획득 정보
13	Authority Information Access	n	m	m	http://ocsp.tradesign.net:80/OCSPServer
14	OCSP No Check	n	o	m	id-pkix-ocsp-nocheck

8. 감사 및 평가

8.1 감사 및 평가 현황

TradeSign은 법, 시행령 및 시행규칙에 따라 인정기관으로부터 운영기준 준수사실의 인정을 받기 위해 매년 평가기관에 평가를 받습니다.

TradeSign은 정보통신망법 및 정보통신망법 시행령에 따라 본인확인기관으로 지정되었습니다.

8.2 평가자의 신원, 자격

운영기준 준수사실 평가자의 신원 및 자격은 시행령에 따라서 결정됩니다.

방송통신위원회는 본인확인기관 지정 등에 관한 기준 고시에 의거하여 심사위원으로 위촉하여 수행됩니다.

8.3 평가 대상과 평가자의 관계

운영기준 준수사실 평가기관은 시행령에 따라 평가 업무의 독립성, 객관성, 공정성 및 신뢰성을 확보할 수 있는 기관이 지정되며, 이로 인하여 독립성을 유지 할 수 있습니다.

본인확인기관 심사위원은 방송통신위원회에서 직접 위촉하므로 독립성을 유지할 수 있습니다.

8.4 평가 목적 및 내용

운영기준의 준수사실을 인정받기 위하여 평가를 받고 있으며, 평가내용은 과학기술정보통신부가 고시한 전자서명인증업무 운영기준에 의거하여 평가기관이 정한 세부평가기준과 같습니다.

정보통신망법 제23조의2(주민등록번호의 사용 제한) 및 동법 제23조의3(본인확인기관의 지정 등)에 따라 공동인증서를 사용하여 가입자의 주민등록번호를 사용하지 아니하고 본인을 확인하는 방법을 제공하기 위해 본인확인기관으로 지정받고 있습니다.

본인확인기관 심사 항목은 다음과 같습니다.

- 본인확인업무의 안전성 확보를 위한 물리적·기술적·관리적 조치계획
- 본인확인업무의 수행을 위한 기술적·재정적 능력
- 본인확인업무 관련 설비규모의 적정성

8.5 부적합 사항에 대한 조치

운영기준의 준수사실을 인정받고 제17조(시정명령) 각호의 어느 하나에 해당하는 경우, 과학기술정보통신부 장관은 기간을 정하여 시정을 명할 수 있고, 전자서명인증사업자는 기간 내에 시정명령을 이행하여야 합니다.

8.6 결과 보고

평가기관은 운영기준 준수사실에 대해 평가를 하고 그 결과를 인정기관에 제출하여야 합니다.

9. 전자서명인증업무 보증 등 기타사항

9.1 수수료

TradeSign은 서비스 제공에 대하여 수수료를 부과할 수 있습니다. 다만 가입자 또는 이용자와의 계약에 따라 할인 및 부과 시기, 방법 등이 변경될 수 있습니다.

9.1.1. 인증서

구분	발급대상	수수료(1년)
신규발급 / 갱신발급	개인	4,000
	법인/단체/개인사업자	100,000
	서버	1,000,000
재발급	개인	무료
	법인/단체/개인사업자	10,000
	서버	무료

9.1.2. 인증서 조회 및 확인 수수료

TradeSign은 인증서를 조회, 확인하는 이용자에게 수수료를 부과하지 않습니다.

9.1.3. 인증서 유효여부 확인 수수료

구분	수수료(건)
실시간유효확인(OCSP)	200원
효력정지 및 폐지목록(CRL)	무료

9.1.4. 시점확인 (TSA)

구분	수수료(건)
TSA	500원

9.1.5 환불

9.1.5.1 환불사유

TradeSign은 다음과 같은 경우에 대하여 요금을 환불합니다.

가입자가 인증서를 발급받기 전에 TradeSign 또는 등록대행기관에 환불을 요청 하는 경우, 또는 가입자가 TradeSign 또는 등록대행기관의 귀책사유로 인하여 환불을 요청한 경우에 소정의 수수료를 차감한 금액을 환불해 드립니다.

9.1.5.2. 환불수수료

수수료	사유
없음	가입자가 요금을 신용카드로 결제하고 5 영업일 이내에 환불신청을 한 경우 (단 인증서 발급 전이어야 함)
PG수수료 (부가세포함)	가입자가 요금을 계좌이체, 가상계좌, 무통장입금으로 결제하고 환불 신청한 경우 (단 인증서 발급 전이어야 함)
	가입자가 요금을 신용카드로 결제하고 6 영업일 이후에 환불신청을 한 경우 (단 인증서 발급 전이어야 함)
단 찾아가는서비스를 통해 신청서를 제출하시고 환불신청을 한 경우, 위 환불수수료에 찾아가는서비스 이용 수수료가 추가됩니다.	

9.2 배상

9.2.1. 배상책임

TradeSign은 법, 시행령, 시행규칙, 전자서명인증업무 운영기준 및 이 인증업무준칙의 규정을 위반하여 가입자 또는 이용자에게 손해를 입힌 경우 법 제20조(손해배상책임)에 따라 그 손해를 배상합니다. 다만 TradeSign이 고의 또는 과실 없음을 입증한 경우에는 그 배상책임이 면제됩니다

TradeSign은 신뢰할 수 있는 인증을 획득한 암호모듈을 이용하는 것을 원칙으로 합니다. 그렇지 않은 경우 TradeSign은 안정성을 확보하기 위한 충분한 기술적 검증 또는 조취를 취하며, 이에 대한 책임을 부담합니다.

9.2.2. 인증서 유효성 확인 관련 서비스(CRL, OCSP) 책임

가. TradeSign 은 인증서 유효성 확인 관련 서비스에 대해 다음의 배상 책임이 있습니다.

- CRL 의 다음공고시각(Next Update) 이내에 CRL 을 업데이트하지 않음으로써 발생한 가입자, 이용자 손해
- 폐지 또는 효력정지 사실이 CRL 에서 누락됨으로써 발생한 가입자, 이용자 손해
- 가입자의 인증서 폐지 또는 효력정지 신청을 접수하였음에도 불구하고 'OCSP 서비스'를 통해 실시간으로 제공하지 않음으로써 발생한 가입자, 이용자 손해

나. TradeSign 은 인증서 유효성 확인 관련 서비스와 관련하여 발생한 가입자 또는 이용자의 손해에 대해 그 사실이 입증된 경우, 다음의 책임이 없습니다.

- 최신 CRL 이 배포되었음에도 불구하고 가입자, 이용자가 기존 CRL 을 확인함으로써 발생한 손해 (전자서명인증사업자의 과실이 없는 경우)
- 가입자의 인증서 폐지 또는 효력정지 신청시각과 CRL 의 다음공고시각(Next Update)까지의 시간차에 의한 가입자, 이용자의 손해 (전자서명인증사업자의 과실이 없는 경우)

다. TradeSign 은 신뢰성 있는 인증서 유효성 확인을 위해 CRL 보다는 OCSP 를 이용하실 것을 권장합니다.

9.3 영업비밀

TradeSign, 이용자, 가입자 및 등록대행기관은 상호 영업비밀을 보호합니다.

9.4 개인정보 보호

9.4.1. 개인정보처리방침

TradeSign은 개인정보 보호법 및 개인정보처리방침에 따라 가입자 정보를 관리하며 중요 개인정보(주민번호 등)를 암호화하여 DB에 저장하는 것을 원칙으로 합니다.

- 개인정보처리방침 링크 : http://www.tradesign.net/service/policy/privacy

9.4.2. 개인정보의 수집 및 이용 목적

TradeSign은 수집한 개인정보를 다음의 목적을 위하여 활용합니다.

- 인증서 신청, 발급 및 갱신
- 인증서 관리
- 인증서 발급 수수료 결제 및 정산, 환불
- 인증서 유효기간 만료일 안내 (갱신안내)
- 인증서 발급 내역 통보
- 고객문의 상담 및 분쟁 조정을 위한 기록보존 등
- 사용자 이용 통계 (챗봇에 한함)

9.4.3. 개인정보의 제공

TradeSign 전자무역인증센터는 정보주체의 동의, 법률의 특별한 규정 등 개인정보 보호법 제17조 및 제18조에 해당하는 경우에만 개인정보를 제3자에게 제공합니다.

다만, 아래의 경우에는 예외로 합니다.

- 이용자들이 사전에 공개에 동의한 경우
- 법령의 규정에 의거하거나, 수사 목적으로 법령에 정해진 절차와 방법에 따라 수사기관의 요구가 있는 경우

9.5 지식재산권

지식재산권은 저작권법 등 관련 법률에 따라서 TradeSign에 귀속됩니다.

- TradeSign 이 제공하는 서비스 및 솔루션
- TradeSign 이 제공하는 서비스 및 솔루션의 명칭
- TradeSign 이 제공하는 프로그램
- 기타 관련 법에서 명시하고 있는 내용

9.6 보증

TradeSign은 자신이 발급한 인증서와 관련하여 다음의 내용을 보증합니다.

- 발급된 인증서에 포함된 내용이 틀림없다는 사실
- 법, 시행령, 시행규칙, 전자서명인증업무 운영기준 및 인증업무준칙에 의하여 인증서가 발급되었다는 사실
- 인증서 효력정지 및 폐지에 대한 내용이 틀림없다는 사실

9.7 보증 예외 사항

TradeSign은 법, 시행령, 시행규칙, 전자서명인증업무 운영기준 및 이 인증업무준칙에서 정한 사항 이외의 사항 즉, 가입자의 신용 및 가입자 관련 정보의 불변성 등을 보증하지 않습니다.

9.8 보험의 보상 범위

TradeSign은 전자서명인증업무의 수행과 관련하여 고의 또는 과실로 발생하는 사고로 인한 손해배상을 담보하기 위하여 연간 총 보상액 한도가 10억 원인 책임보험에 가입하고 있습니다.

9.9 배상 한계

법 제20조(손해배상책임)에 따라 전자인증업무의 수행과 관련하여 가입자 또는 이용자에게 손해를 입힌 경우에는 그 손해를 배상합니다. 다만, TradeSign이 고의 또는 과실이 없음을 입증하면 그 배상책임이 면제됩니다.

9.10 준칙의 효력

가. 본 인증업무준칙은 2022 년 12 월 23 일부터 시행합니다.

나. 본 인증업무준칙은 새롭게 개정된 준칙이 시행됨과 동시에 효력이 종료됩니다.

9.11 통지 및 의사소통

TradeSign의 전자서명생성정보 및 클라우드 서비스에 보관된 가입자의 전자서명생성정보에 대한 손상, 노출, 파손, 분실, 도난 등 인증서의 신뢰도 및 유효성에 중대한 영향을 미치는 사

실이 발생할 때, 해당 사실을 홈페이지에 공고하는것을 원칙으로하며 필요한 경우 전자우편 또는 전화를 이용하여 통지합니다.

9.12 이력 관리

본 인증업무준칙의 제·개정 주요 이력은 준칙의 앞부분에 포함되어 준칙과 함께 관리됩니다.

9.13 분쟁 해결

9.13.1. 전자서명인증체계 관련자에게 전달되는 문서(또는 전자문서)가 법적 효력을 갖기 위한 요건

"전자문서 및 전자거래 기본법" 제4조(전자문서의 효력)에서 언급하고 있는 전자문서는 전자적 형태로 되어 있다는 이유만으로 법적 효력이 부인되지 아니 합니다.

다음의 요건이 추가적으로 필요 합니다.

가. 인증서에 기초한 전자서명을 포함하며, 법 제 2 조(정의) 제 2 호 각목의 요건을 갖출 것

나. 전자서명에 사용된 인증서가 서명 당시에 유효한 상태이며 정지 또는 폐지 상태가 아니어야 함

9.13.2. 인증업무와 관련된 분쟁을 해결하는 절차

전자서명인증업무와 관련하여 TradeSign과 가입자 또는 이용자간 분쟁이 발생한 경우 법 제22조(분쟁의 조정)에 따라 전자문서·전자거래분쟁조정위원회에 조정을 신청하여 관련 절차에 따라 신속한 방법으로 분쟁을 해결할 수 있습니다.

9.14 관할법원

전자서명인증업무 관련 분쟁이 발생할 경우 그 관할기관은 한국무역정보통신 본사 소재지를 관할하는 지방법원이 됩니다.

9.15 관련 법률 준수

TradeSign 및 전자서명인증체계 관련자는 아래 법률 및 규정을 준수해야 합니다

- 전자서명법, 전자서명법 시행령, 전자서명법 시행규칙
- 개인정보 보호법, 개인정보 보호법 시행령
- 정보통신망법, 정보통신망법 시행령, 정보통신망법 시행규칙

9.16 기타 규정

해당사항 없음