

ENTRUST.NET

SSL 웹 서버인증실무준칙

버전: 2.02

2002년 1월 1일

개정사

발행물	날짜	개정변화
1.0	1999년 5월 26일	초기버전
2.0	2000년 7월 1일	Entrust.net SSL 웹 서버 공개키 기반구조에서 종속 실체를 다루는 조항의 첨가. (예를 들어 제3등록 기관). 기타 다수의 제조조건 개정
2.01	2001년 5월 30일	실질적인 영향없이, 부차적인 개정
2.02	2002년 1월 1일	교차 인증 대체와 관련한 부차적인 개정

목차

1. 소개	6
1.1 개요	6
1.2 확인	6
1.3 공동체 및 적용	6
1.3.1 인증기관	6
1.3.2 등록기관	7
1.3.3 최종실체	7
1.3.4 적용가능성	8
1.4 연락에 관한 주요 사항	8
1.4.1 명세 관리기관	8
1.4.2 담당자	8
2. 일반조항	8
2.1 의무	8
2.1.1 인증기관 의무	8
2.1.2 등록기관 의무	9
2.1.3 가입자 의무	10
2.1.4 신뢰당사자 의무	12
2.1.5 저장소의무	14
2.2 책임	14
2.2.1 인증기관의 책임	14
2.2.2 등록기관의 책임	18
2.3 재정적책임	18
2.3.1 신뢰당사자에 의한 면책	19
2.3.2 신뢰관계	20
2.3.3 관리절차	20
2.4 해석과 시행	20
2.4.1 준거법	20
2.4.2 일부무효, 존속, 통합, 통지	21
2.4.3 분쟁해결 절차	24

2.5 비용	25
2.5.1 인증서 발행과 갱신 비용	25
2.5.2 인증서 접속 비용.....	25
2.5.3 취소 또는 상태정보 접속비용	25
2.5.4 정책정보와 같은 기타 서비스에 대한 비용	26
2.5.5 환불 정책.....	26
2.6 공표와 저장소.....	26
2.6.1 인증기관정보 공표	26
2.6.2 공표 빈도	26
2.6.3 접속 관리	26
2.6.4 저장소.....	27
2.7 준수성 감사	27
2.7.1 실제 준수성 감사 빈도	27
2.7.2 감사관의 자격/신분	27
2.7.3 피감사당사자와 감사와의 관계	27
2.7.4 감사 대상.....	27
2.7.5 부적합한 결과에 따른 시정조치.....	27
2.7.6 결과 통보.....	28
2.8 기밀성	28
2.8.1 기밀로 유지되어야 하는 정보의 형태	28
2.8.2 기밀로 취급되지 않는 정보의 형태	29
2.8.3 인증서 취소/사용 중지 정보의 공개.....	29
2.8.4 법 집행 공무원에 대한 공개.....	29
2.8.5 민사적 발표에 의한 공개.....	29
2.8.6 소유자 요청에 따른 공개	29
2.8.7 기타 정보공개 상황	29
2.9 지적재산권	29
3. 신원확인 과 인증	30
3.1 초기등록	30
3.1.1 명칭유형	31
3.1.2 의미있는 명칭의 필요.....	31
3.1.3 다양한 명칭 형태의 해석 규칙.....	31
3.1.4 명칭의 유일성	32
3.1.5 명칭에 대한 분쟁의 해결절차	32
3.1.6 인지, 인증 및 상표의 역할	32
3.1.7 비밀키 소유 입증방법	34

3.1.8 단체의 신원 확인	34
3.1.9 개인 신원 확인	34
3.2 키 재생성	35
3.3 취소 후 키 재생성	35
3.4 취소 요청	35
4. 운영 조건	36
4.1 인증서 신청	36
4.2 인증서 발행	36
4.3 인증서 승락	36
4.4 인증서 정지 및 취소.....	36
4.4.1 취소 상황	37
4.4.2 인증서 취소 요청을 할 수 있는 자.....	37
4.4.3 인증서 취소 요청 절차	38
4.4.4 취소 요청 유예기간	38
4.4.5 중지 상황	38
4.4.6 중지를 요청할 수 있는 자	38
4.4.7 중지요청 절차	38
4.4.8 중지기간의 한계	38
4.4.9 CRL발행 빈도	38
4.4.10 CRL 확인 요구사항.....	39
4.4.11 온라인 취소/ 상태 확인 가능성	39
4.4.12 온라인 취소 확인 요구사항.....	39
4.4.13 취소 공고의 기타 방식.....	39
4.4.14 취소 공고의 다른 형식에 대한 확인요구사항	39
4.4.15 갱신 키 손상에 대한 특별한 요구사항.....	39
4.5 보안 감사 절차	39
4.6 기록 보관	40
4.7 키 변환	40
4.8 손상, 재해 복구	40
4.9 CA 종료	40
5. 물리적, 절차적 그리고 인적 보안 통제 ...	40
5.1 물리적 통제	40
5.2 절차적 통제	41
5.3 인적 통제	41

6. 기술적 보안 통제	41
6.1 키 쌍 생성과 설치	41
6.1.1 키 쌍 생성	41
6.1.2 개별실체에 대한 비밀키 전달.....	41
6.1.3 인증서 발행인에 대한 공개키 전달.....	41
6.1.4 사용자에게 CA 공개키 전달	41
6.1.5 키 사이즈	42
6.1.6 공개키 매개변수 생성	42
6.1.7 매개변수 품질 확인	42
6.1.8 하드웨어/소프트웨어 키 생성	42
6.1.9 키 사용 목적	42
6.2 비밀 키 보호	42
6.3 키 쌍 관리의 다른 측면	43
6.4 활성화 데이터.....	43
6.5 컴퓨터 보안 통제	43
6.6 인증서 유효기간 기술적 통제	43
6.7 네트워크 보안 통제	43
6.8 암호화 모듈 공학적 통제	43
7. 인증서와 CRL 프로파일	43
7.1 인증서 프로파일	43
7.2 CRL 프로파일	44
8. 내역관리	44
8.1 연락정보	44
8.2 내역 변경절차	44
8.3 발행과 통지 정책	45
8.4 CPS 승인 절차	45
9. 약자	45
10. 정의	46

1. 소개

Entrust.net SSL 웹 서버 인증기관들은 SSL 프로토콜을 사용하는 월드와이드 웹 서버와 브라우저 간의 보다 안전한 통신을 지원하기 위해 Entrust.net SSL 웹 서버인증서를 발행한다. Entrust.net은 온라인 상에서 보다 안전한 온라인 통신을 가능하게 하는 표준 디지털 인증서를 제공하기 위하여 Entrust/PK 소프트웨어가 장착된 Entrust 사의 제품을 사용한다.

1.1 개요

Entrust.net SSL 웹 서버인증실무준칙은 (i) Entrust.net SSL 웹 서버 인증기관과 (ii) Entrust.net SSL 웹 서버 인증기관 산하에서 운영하는 등록기관의 업무와 절차를 설명한다. 또한 Entrust.net SSL 웹 서버인증실무준칙은 Entrust.net SSL 웹 서버인증서와 관련하여 Entrust.net가 인증기관 및 등록기관의 서비스를 이용하도록 하는 조건을 기술한다. Entrust.net SSL 웹 서버인증실무준칙은 (i) Entrust.net SSL 웹 서버인증서 또는 동 인증서에 관련하여 제공된 서비스에 관련하여 Entrust.net 또는 (ii) Entrust.net SSL 웹 서버인증기관 산하에서 운영하는 등록기관, 또는 Entrust.net SSL 웹 서버 인증과 관련하여 서비스를 제공하는 재판매자 또는 공동판매자와 관계를 가지고 있는 모든 신청자, 가입자, 신뢰당사자, 재판매자, 공동판매자를 포함하나 이에 국한되지 않고 모든 사람, 실체 및 기관에 적용할 수 있다. Entrust.net SSL 웹 서버인증실무준칙은 Entrust.net SSL 웹 서버인증기관에 의해 발행되는 Entrust.net SSL 웹 서버인증서에 인용됨으로써 시행된다. Entrust.net SSL 웹 서버인증실무준칙은 신청자, 가입자, 신뢰당사자, 재판매자, 공동판매자 및 기타 사람, 실체 및 조직에게 Entrust.net SSL 웹 서버인증기관 및 동 기관 산하에서 운영하는 등록 기관의 업무준칙을 제공한다. 또한 Entrust.net SSL 웹 서버인증실무준칙은 Entrust.net, Entrust.net SSL 웹 서버인증기관 산하에서 등록기관을 운영하는 제3자, 신청자, 가입자, 신뢰당사자, 재판매자, 공동판매자 및 Entrust.net SSL 웹 서버인증서를 이용하거나 신뢰하거나 Entrust.net SSL 웹 서버 인증기관 또는 동 기관 산하에서 운영하는 등록기관과 관계를 가지고 있는 기타 사람, 실체 또는 조직의 권리 및 의무에 관하여 기술한다.

1.2 확인

이 문서는 Entrust.net SSL 웹 서버인증실무준칙이라 호칭한다.

1.3 공동체 및 적용

Entrust.net SSL 웹 서버인증서의 용도는 SSL 프로토콜을 사용하는 월드와이드 웹 서버로 한정된다. Entrust.net SSL 웹 서버인증서를 다른 용도로 사용하는 것은 금지된다.

1.3.1 인증기관

Entrust.net SSL 웹 서버 공개키 기반구조에서, 인증기관은 Entrust.net에서 운영하는 등록기관 또는 Entrust.net SSL 웹 서버 인증기관 산하에서 운영되는 제3등록 기관에 의하여 검증된 신청자의 CSR과 공개 키를 받아들인다. 만약 Entrust.net SSL 웹 서버인증신청서가 검증되면, 이를 검증한 등록 기관은 Entrust.net SSL 웹 서버인증서 발행요청서를 Entrust.net SSL 웹 서버인증기관에 보낸다. Entrust.net SSL 웹 서버인증기관은 공개 키와 등록기관이 Entrust.net 웹 서버인증기관에 보낸 요청서에 포함된 정보를 포함하고 있는 Entrust.net SSL 웹 서버 인증서를 생성한다. 이와 같이 생성된 Entrust.net SSL 웹 서버인증서는 Entrust.net SSL 웹 서버인증기관에 의해 디지털 서명이 이루어진다.

Entrust.net에 의해 승인된 인증기관만이 Entrust.net SSL 웹 서버인증서를 발행할 수 있다. Entrust.net SSL 웹 서버인증서를 발행할 수 있도록 2 이상의 인증기관이 승인된 경우 Entrust.net은 위와같이 승인된 인증 기관의 목록을 Entrust.net 저장소에 게재한다.

1.3.2 등록기관

Entrust.net SSL 웹 서버 공개키 기반구조에서, Entrust.net SSL 웹 서버인증기관 산하에 있는 등록기관은 신청자로부터 Entrust.net SSL 웹 서버인증신청서를 접수하고 동 신청서에 포함된 정보에 대한 제한된 검증을 이행 할 수 있다. 위 정보가 Entrust.net 정책 기관이 규정한 절차에 따라 검증이 이루어지면, Entrust.net SSL 웹 서버인증기관 산하에서 운영하는 등록기관은 신청자에게 Entrust.net SSL 웹 서버인증서를 발행하도록 Entrust.net SSL 웹 서버인증기관에 요청서를 보낸다.

Entrust.net에 의해 승인된 등록 기관만이 인증서 발행을 위해 Entrust.net SSL 웹 서버인증기관에 요청서를 제출할 수 있다. Entrust.net SSL 웹 서버인증서를 위한 업무를 수행할 수 있도록 2 이상의 등록기관이 승인된 경우 Entrust.net은 승인된 등록 기관의 목록을 Entrust.net 저장소에 게재한다.

1.3.3 최종실체

Entrust.net SSL 웹 서버 공개키 기반구조의 최종실체는 다음으로 구성된다.:

1. 신청자 - 신청자는 Entrust.net SSL 웹 서버인증서를 신청했지만 아직 동 인증서를 발급받지 않은 상태의 사람, 실체 또는 기관이다.
2. 가입자 - 가입자는 Entrust.net SSL 웹 서버인증서가 발행된 상태의 사람, 실체

또는 기관이다.

3. 신뢰당사자 – 신뢰당사자는 가입자의 신원 및 공개키를 검증하거나 암호화된 통신문을 가입자에게 보내거나 가입자로부터 받기 위해 공개키를 사용함에 있어 Entrust.net SSL 웹 서버인증서 또는 Entrust.net 저장소에서 제공되는 다른 정보를 신뢰하거나 이를 사용하는 사람, 실체, 또는 기관이다.

1.3.4 적용가능성

Entrust.net SSL 웹 서버인증실무준칙은 Entrust.net SSL 웹 서버인증기관이 발행한 Entrust.net SSL 웹 서버인증서에 적용할 수 있다. Entrust.net SSL 웹 서버인증서는 SSL 서비스를 제공하는 월드와이드 웹 서버에 의해 사용하기 위해 Entrust.net SSL 웹 서버인증기관이 발행한다. Entrust.net SSL 웹 서버인증서는 SSL 확장자가 있는 X.509v3의 표준을 따른다.

1.4 연락에 관한 주요사항

1.4.1 명세관리기관

Entrust.net SSL 웹 서버인증실무준칙은 Entrust.net 운영 기관이 관리하고 Entrust.net 정책 기관에 의해 수립된 정책에 기초한다.

1.4.2 담당자

Entrust.net SSL 웹 서버 인증서에 대해 질문이 있을 경우 다음으로 연락 할 수 있다:

Entrust.net Inquires
1000 Innovation Drive
Ottawa, Ontario
Canada K2K 3E7
Tel: 1-877-368-7483
Fax: 1-877-839-3538
E-mail: tsite.entrust@Entrust.net

2 일반조항

2.1 의무

2.1.1 인증기관 의무

Entrust.net SSL 웹 서버인증기관은:

- (i) Entrust.net SSL 웹 서버인증실무준칙의 조건에 따라 인증 기관 서비스를 제공한다.
- (ii) Entrust.net SSL 웹 서버인증기관의 산하에서 운영되는 등록기관으로부터 의뢰를 요청 받는 즉시 Entrust.net SSL 웹 서버인증실무준칙의 조건에 따라 Entrust.net SSL 웹 서버 인증서를 발행 한다.
- (iii) Entrust.net SSL 웹 서버인증실무준칙의 조건에 따라 Entrust.net SSL 웹 서버인증서를 발행하고 Entrust.net 저장소에서 Entrust.net SSL 웹 서버 인증 CRL을 발행하고 이용할 수 있게 함으로써 Entrust.net SSL 웹 서버 인증 취소 정보를 이용할 수 있게 한다.
- (iv) Entrust.net SSL 웹 서버인증실무준칙의 조건에 따라 Entrust.net SSL 웹 서버인증서 CRL을 정기적으로 발행 한다.
- (v) Entrust.net SSL 웹 서버인증실무준칙의 조건에 따라 Entrust.net SSL 웹 서버인증기관의 산하에서 운영되는 등록 기관으로부터 취소 요청을 수령하는 즉시 특정 Entrust.net SSL 웹 서버인증서를 취소 한다.

Entrust.net SSL 웹 서버인증기관을 운영할 때 Entrust.net는 Entrust.net SSL 웹 서버인증실무준칙, 가입계약, 또는 신뢰당사자 계약에 따른 의무 수행을 하기 위해 하나 또는 그 이상의 대표자 또는 대리인을 이용 할 수 있다. 단, Entrust.net 은 동 이행에 대한 책임을 진다.

2.1.2 등록기관 의무

Entrust.net SSL 웹 서버인증기관 산하에서 운영되는 등록 기관은:

- (i) Entrust.net SSL 웹 서버인증실무준칙에 따라 Entrust.net SSL 웹 서버 인증신청서를 수령한다.
- (ii) Entrust.net SSL 웹 서버인증서를 신청할 때 신청자가 제출한 정보에 대한 제한된 검증을 수행한다. 만약 검증이 성공적으로 된 경우, Entrust.net SSL 웹 서버인증실무준칙에 따라 Entrust.net SSL 웹 서버인증기관에 인증서 발행요청서를 제출한다.
- (iii) 가입자로부터 Entrust.net SSL 웹 서버인증서의 취소요청서를 수령하고 이를 검증한다. 만약 위 검증이 성공적으로 수행된 경우, Entrust.net SSL 웹 서버인증실무준칙에 따라 Entrust.net SSL 웹 서버인증서의 취소를 위해 Entrust.net SSL 웹 서버인증기관에 요청서를 제출한다.
- (iv) Entrust.net SSL 웹 서버인증실무준칙에 따라 가입자들에게 Entrust.net SSL 웹 서버인증서가 발행 되었다는 것을 통지한다; 그리고
- (v) Entrust.net SSL 웹 서버인증실무준칙에 따라 가입자들에게 발행된 Entrust.net SSL 웹 서버인증서가 취소 되었거나 곧 기간이 만료가 된다는 것을 통지 한다.

Entrust.net은 Entrust.net SSL 웹 서버인증실무준칙, 가입계약서 또는 신뢰당사자 계약서에

따라 Entrust.net이 운영하는 등록기관과 관련된 의무를 수행하기 위해 하나 또는 그 이상의 대표자 또는 대리인을 이용할 수 있다. 단, Entrust.net은 동 준칙과 계약서에 따라 위 대표자 또는 대리인의 이행에 대한 책임을 진다. Entrust.net은 Entrust.net SSL 웹 서버인증기관 산하 등록 기관으로 독립적인 제3기관을 지정할 수 있다. 그러한 제3등록 기관은 Entrust.net SSL 웹 서버인증실무준칙, 가입계약서, 또는 신뢰당사자 계약서에 따른 업무를 수행할 책임이 있다. Entrust.net은 제3등록 기관의 업무 수행에 대한 책임이 없다. 제3등록 기관은 Entrust.net SSL 웹 서버인증기관 산하 등록 기관으로서 그 의무를 수행 함에 있어서 하나 또는 그 이상의 대표자 또는 대리인을 이용 할 수 있다. 제3등록 기관은 Entrust.net SSL 웹 서버인증실무준칙, 가입계약서, 또는 신뢰당사자 계약서에 따라 위 대표자 또는 대리인의 업무수행에 대하여 책임을 진다. Entrust.net은 (i) Entrust.net SSL 웹 서버인증서, 그리고 (ii) Entrust.net SSL 웹 서버인증서와 관련하여 제공된 서비스를 위하여 재판매자와 공동판매자를 지정할 수 있다. 동 재판매자와 공동판매자는 Entrust.net SSL 웹 서버인증실무준칙, 가입계약서, 또는 신뢰당사자계약서에 따라 그들의 업무 수행에 대해 책임을 진다. Entrust.net은 위 재판매자 및 공동판매자의 업무수행에 대하여 책임을 지지 않는다. Entrust.net의 재판매자와 공동판매자는 Entrust.net SSL 웹 서버인증실무준칙, 가입계약서, 또는 신뢰당사자 계약서에 따른 의무 수행을 하기 위해 하나 또는 그 이상의 대표자 또는 대리인을 이용할 수 있다. 재판매자와 공동판매자는 Entrust.net SSL 웹 서버인증실무준칙, 가입계약서, 또는 신뢰당사자 계약에 따라 위 대표자 또는 대리인의 업무 수행에 대하여 책임을 진다. 제3등록기관, 재판매자, 그리고 공동판매자는 (i) 진술, 보증 및 조건의 부인, (ii) 책임의 제한, (iii) 신청자, 가입자 및 신뢰당사자로부터의 진술과 보증, 및 (iv) Entrust.net SSL 웹 서버인증실무준칙, 가입계약서, 및 신뢰당사자 계약서에서 규정하는 신청자, 가입자, 그리고 신뢰당사자로부터의 면책에 따른 이익을 받을 자격이 있다.

2.1.3 가입자 의무

가입자와 신청자는:

- (i) Entrust.net SSL 웹 서버인증서를 포함한 공개키 암호와 인증서의 사용을 이해하고, 필요한 경우 이에 대한 적합한 교육을 받는다.
- (ii) Entrust.net나 독립된 제3등록 기관과의 연락을 통해 실수, 의사표시의 하자, 또는 생략 없이 올바른 정보를 제공한다.
- (iii) 가입자의 Entrust.net SSL 웹 서버인증서나 신청자의 Entrust.net SSL 웹 서버인증신청서에 따라 사용될 새롭고 안전하고 암호화된 키 쌍을 생성한다.
- (iv) Entrust.net SSL 웹 서버인증실무준칙과 가입계약서를 읽고 그 조건에 동의한다.
- (v) Entrust.net SSL 웹 서버인증서의 내용을 수정하지 않는다.
- (vi) Entrust.net SSL 웹 서버인증실무준칙 및 해당 법률의 조건에 따라 합법적이고 인가된 목적으로만 Entrust.net SSL 웹 서버인증서를 사용한다.

- (vii) Entrust.net SSL 웹 서버인증서에 주체(Subject)로 나열된 사람, 실체, 또는 기관을 위하여서만 entrust.net SSL 웹 서버인증서를 사용한다.
- (viii) 가입자나 신청자의 비밀키를 하드웨어 토큰이나 디스크등에 저장하고 보호하고 더 나아가 이를 사용하지 않을 때에는 가입자나 신청자의 컴퓨터와 분리하여 따로 저장하여 보호한다.
- (ix) Entrust.net SSL 웹 서버인증신청서에 포함된 정보의 변경 또는 동 신청서상의 정보를 잘못되거나 부정확하게 만드는 상황이 발생한 경우 그 변경사항을 Entrust.net, 또는 신청자가 Entrust.net SSL 웹 서버인증신청서를 제3등록 기관에 제출했다면, 동 등록기관에 상당한 기간 내에 각 통지한다.
- (x) Entrust.net SSL 웹 서버인증서에 포함된 정보의 변경 또는 동 인증서상의 정보를 잘못되거나 부정확하게 만드는 상황이 발생한 경우 그 변경 사항을 Entrust.net, 또는 가입자가 Entrust.net SSL 웹 서버인증서를 제3등록 기관을 통해 받았다면, 동 등록기관에 상당한 기간 이내에 각 통지한다.
- (xi) 가입자의 Entrust.net SSL 웹 서버인증서에 포함된 정보 또는 인증서 정보를 부정확하거나 잘못되게 만드는 상황이 발생한 경우 Entrust.net SSL 웹 서버인증서의 사용을 즉시 중단한다.
- (xii) 가입자나 신청자의 비밀키에 대하여 현실적인 손상이 발생하였거나 의심되는 경우 Entrust.net, 또는 가입자가 Entrust.net SSL 웹 서버인증서를 제3등록 기관으로부터 받았다면, 동 기관에 통지하고 즉시 동 신청서의 취소를 요청한다.
- (xiii) (a) Entrust.net SSL 웹 서버인증서의 만료 또는 취소시, 또는 (b) Entrust.net SSL 웹 서버인증서 공개 키에 상응하는 비밀키에 대하여 현실적인 손상이 발생하였거나 의심되는 경우, 가입자의 Entrust.net SSL 웹 서버인증서 사용을 즉시 중지 하고 인증서가 설치된 장치나 소프트웨어로부터 동 인증서를 제거한다.
- (xiv) 가입자의 Entrust.net SSL 웹 서버인증서를 주어진 시간에 하나의 월드와이드 웹 서버에서만 사용한다.
- (xv) 다른 인증서에 서명하기 위해 가입자의 Entrust.net SSL 웹 서버인증서의 공개 키와 상응하는 가입자의 비밀 키를 사용하지 않는다.
- (xvi) Entrust.net SSL 웹 서버인증서가 제공하는 보안과 신뢰의 정도에 따라 주어진 상황에서 동 인증서를 사용하는 것이 적합한 지에 대해 가입자 또는 신청자 자신이 판단한다.

Entrust.net SSL 웹 서버인증서와 관련 정보는 수출, 수입, 또는 사용 제한이 있을 수 있다. 가입자는 동 인증서 또는 관련 정보를 수출, 수입하고 사용하는 가입자의 권리에 적용되는 모든 법과 규칙을 준수한다. 가입자는 Entrust.net SSL 웹 서버인증서 또는 관련정보의 수출, 수입, 사용에 필요한 모든 라이선스 및 허가를 획득할 책임을 진다. 동 인증서를 처리하거나 이와 관련하여 사용되는 특정 암호 기술, 소프트웨어, 하드웨어, 그리고 펌웨어("기술")

는 수출, 수입, 또는 사용 제한이 있을 수 있다. 가입자는 동 기술 또는 관련 정보의 수출, 수입 및/또는 사용에 적용되는 모든 법률 및 규정을 준수한다. 가입자는 동 기술 또는 관련 정보의 수출, 수입 및/또는 사용에 적용되는 라이선스 및 허가를 획득할 책임을 진다.

2.1.3.1. 가입자 및 신청자의 진술과 보증

가입자와 신청자는 Entrust.net에 다음과 같이 진술하고 보증한다:

- (i) 가입자나 신청자가 Entrust.net 또는 독립적 제3등록 기관에 제공한 모든 정보는 정확하고 오류, 생략 또는 허위 사실을 포함하고 있지 않다.
- (ii) Entrust.net SSL 웹 서버인증신청서와 관련하여 가입자나 신청자가 제출한 공개 키와 상응하는 비밀키는 건전한 암호기술을 사용하여 생성되었고 손상되지 않았다.
- (iii) 가입자나 신청자가 Entrust.net이나 독립적 제3등록 기관에 Entrust.net SSL 웹 서버인증과 관련하여 제공한 정보는 어느 관할권에 있는 개인, 실체 또는 조직의 지적재산권이나 기타 권리도 침해, 오용, 희석시키고 부당하게 경쟁하거나 위반하지 않는다.
- (iv) 신청자의 Entrust.net SSL 웹 서버인증신청서에 포함된 정보의 변경 또는 동 신청서 상의 정보를 잘못되거나 부정확하게 만드는 상황이 발생한 경우, 그 변경사항을 Entrust.net, 또는 만약 신청자가 Entrust.net SSL 웹 서버인증신청서를 제3등록 기관에 제출했다면, 제3등록기관에 상당한 기간 이내에 각 통지하여야 한다.
- (v) 만약 가입자의 Entrust.net SSL 웹 서버인증서 정보의 변경 또는 동 인증서의 정보를 잘못되거나 부정확하게 만드는 상황이 발생한 경우 Entrust.net SSL 웹 서버인증서의 사용을 즉시 중지한다.
- (vi) 가입자는 (a) Entrust.net SSL 웹 서버인증서의 만료나 취소시, 또는 (b) Entrust.net SSL 웹 서버인증서의 공개 키와 상응하는 비밀키에 대하여 현실적인 손상이 발생하거나 의심되는 경우 가입자의 Entrust.net SSL 웹 서버인증서의 사용을 즉시 중지하고 인증서가 설치된 장치나 소프트웨어로부터 동 인증서를 제거한다.
- (vii) 가입자나 신청자는 Entrust.net SSL 웹 서버인증서를 위험하거나 불법적인 용도 (불법행위 포함)로 사용하지 않는다.

2.1.3.2. 가입자 통지 요구사항

가입자는 아래의 통지를 신뢰 당사자가 볼 수 있도록 가입자 월드와이드 웹 사이트의 중요한 위치에 게재한다 (예를 들어서, 가입자 월드와이드 웹 사이트의 “법” 또는 “부인” 조항에):

“Entrust.net SSL 웹 서버인증서에 대한 신뢰는 Entrust.net SSL 웹 서버인증실무준칙 (www.entrust.net/CPS)의 조건과 신뢰당사자 계약서(www.entrust.net/customer/relyingparty.htm)에 의해 지배된다. Entrust.net SSL 웹 서버인증서에 대한 신뢰는 Entrust.net SSL 웹 서버인증

실무준칙과 신뢰당사자 계약서의 조건을 수락하는 것으로 간주한다.”

2.1.4 신뢰당사자 의무

신뢰당사자는:

- (i) Entrust.net SSL 웹 서버인증서를 포함한 공개키 암호문과 인증서의 사용을 이해하고 필요한 경우 적합한 교육을 받는다.
- (ii) Entrust.net SSL 웹 서버인증실무준칙과 신뢰당사자 계약서의 모든 조건들을 읽고 동의한다.
- (iii) CRL 사용을 포함하여 ITU-T Rec. X509:1997/ISO/IEC 9594-8(1994)에 규정된 인증경로 확인절차에 따라 주요 확장자 및 적합하다고 승인된 전문 정오표를 고려하여 Entrust.net SSL 웹 서버인증서를 검증한다.
- (iv) Entrust.net SSL 웹 서버인증서의 기간이 만료되지 않았거나 취소되지 않고 신뢰 루트를 통하여 적합한 신뢰 관계가 형성되어 있는 경우에만 동 인증서를 신뢰하고 사용한다.
- (v) Entrust.net SSL 웹 서버인증서가 제공하는 보안과 신뢰 및 동 인증서의 사용과 관련된 거래의 가치가 주어진 상황에서 당해 인증서를 신뢰할지 여부에 대한 결정을 포함하여, 스스로 판단하여 주어진 상황에서 그러한 신뢰가 합리적일 경우에 위 인증서를 신뢰한다.

Entrust.net SSL 웹 서버인증서와 관련 정보는 수출, 수입, 또는 사용 제한이 있을 수 있다. 신뢰당사자는 동 인증서 또는 관련 정보를 사용하는 신뢰당사자의 권리에 적용되는 모든 법과 규칙을 준수한다. 신뢰당사자는 Entrust.net SSL 웹 서버인증서 또는 관련정보의 수출, 수입 또는 사용에 필요한 모든 라이선스 및 허가를 획득할 책임을 진다. 동 인증서를 처리하거나 이와 관련하여 사용되는 특정 암호 기술, 소프트웨어, 하드웨어, 그리고 펌웨어("기술")는 수출, 수입, 또는 사용 제한이 있을 수 있다. 신뢰당사자는 동 기술 및 관련 정보의 수출, 수입 및/또는 사용에 적용되는 모든 법률 및 규정을 준수한다. 가입자는 동 기술 또는 관련 정보의 수출, 수입 및/또는 사용에 적용되는 라이선스 및 허가를 획득할 책임을 진다.

2.1.4.1 신뢰당사자의 진술과 보증

신뢰당사자는 Entrust.net에게 다음과 같이 진술하고 보증한다:

- (i) 신뢰당사자는 Entrust.net SSL 웹 서버 인증에 대한 신뢰 여부를 결정 하기 전에 Entrust.net SSL 웹 서버인증서를 올바르게 확인한다. 이는 동 인증서가 만료 또는 취소되지 않고 신뢰 루트를 통하여 적합한 신뢰 관계가 형성될 수 있는지에 대한 확인을 포함한다.
- (ii) 신뢰당사자는 취소되거나 유효기간이 만료된 Entrust.net SSL 웹 서버인증서를 신뢰하지 않는다.

- (iii) 신뢰당사자는 신뢰 루트를 통하여 확인되지 않은 Entrust.net SSL 웹 서버인증서를 신뢰하지 않는다.
- (iv) 신뢰당사자는 Entrust.net SSL 웹 서버인증서가 제공하는 보안과 신뢰 및 동 인증서의 사용과 관련된 거래의 가치가 주어진 상황에서 당해 인증서를 신뢰할지 여부에 대한 결정을 포함하여, 스스로 판단하여 주어진 상황에서 그러한 신뢰가 합리적일 경우에만 위 인증서를 신뢰한다.
- (v) 신뢰당사자는 Entrust.net SSL 웹 서버인증서를 위협하거나 불법적인 용도(불법행위 포함)로 사용하지 않는다.

2.1.5 저장소 의무

Entrust.net 저장소는:

- (i) Entrust.net SSL 웹 서버인증실무준칙 조건에 따라 Entrust.net SSL 웹 서버인증기관이 발행한 Entrust.net SSL 웹 서버 인증 취소 정보를 이용할 수 있도록 해야 한다; 그리고
- (ii) Entrust.net SSL 웹 서버인증실무준칙과 Entrust.net SSL 웹 서버인증기관과 Entrust.net SSL 웹 서버인증기관 산하에서 운영되는 등록기관이 제공하는 제품과 서비스에 관련된 기타 정보 복사본을 이용할 수 있도록 해야 한다.

2.2 책 임

Entrust.net SSL 웹 서버인증서 또는 동 인증서에 관련하여 제공되는 서비스를 사용함으로써 또는 이와 관련하여 발생하는 손실, 비용, 지출, 책임, 손해, 청구 또는 합의금액에 관하여 Entrust.net, Entrust.net SSL 웹 서버인증기관 하에 운영되는 독립적 제3등록기관, 재판매자, 공동판매자, 또는 앞에서 말한 자의 하도급계약자, 판매자, 대행인, 공급자, 고용인, 이사 의 신청자, 가입자, 신뢰당사자 또는 기타 개인, 실체 또는 조직에 대한 총책임의 최대한도는 Entrust.net SSL 웹 서버인증실무준칙에 따라 제한된다. 동 실무준칙은 또한 제한된 보증, 책임제한 및 진술, 보증 및 조건에 대한 부인을 포함하고 있다.

2.2.1 인증기관의 책임

2.2.1.1 보증과 보증에 대한 제한

Entrust.net은 Entrust.net SSL 웹 서버인증기관의 운영과 관련하여 가입자에게 아래와 같이 제한된 보증을 한다:

- (i) Entrust.net SSL 웹 서버인증기관은 Entrust.net SSL 웹 서버인증실무준칙에 규정된 관행 과 절차에 따라 저장소 서비스를 제공한다.

- (ii) Entrust.net SSL 웹 서버인증기관은 Entrust.net SSL 웹 서버인증실무준칙에 규정된 절차에 따라 Entrust.net SSL 웹 서버인증서 발행업무를 수행한다.
- (iii) Entrust.net SSL 웹 서버인증기관은 Entrust.net SSL 웹 서버인증실무준칙에 규정된 절차에 따라 취소업무 서비스를 제공한다.

상기에도 불구하고, 어떠한 경우에도 Entrust.net과 Entrust.net SSL 웹 서버인증기관 하에 운영되는 독립적 제3등록기관, 재판매자, 공동판매자, 또는 앞에서 말한 자의 하도급계약자, 판매자, 대행인, 공급자, 고용인, 이사 누구도 신청자, 가입자, 신뢰당사자 또는 기타 개인, 실체, 조직에 대하여 다음과 같은 사항을 진술, 보증하거나 조건을 제시하지 않는다. (i) Entrust.net SSL 웹 서버인증서에 있는 공개키와 상응하는 비밀 키 생성과 저장에 사용된 기술 (그러한 비밀키가 손상되었거나 올바른 암호 기술을 사용하여 생성이 되었는지에 대한 여부 포함) (ii) 인증서에 관련되거나 이를 사용하는 행위, 거래나 과정을 수행하는데 사용되는 암호기술의 신뢰성 또는 방법, (iii) 소프트웨어, 또는 (iv) Entrust.net SSL 웹 서버인증서 또는 Entrust.net SSL 웹 서버인증서의 사용을 통해 수행된 거래의 부인방지. 왜냐하면, 그러한 결정은 해당법을 적용의 문제이기 때문이다.

신청자, 가입자, 및 신뢰당사자는 Entrust.net SSL 웹 서버 인증과 Entrust.net SSL 웹 서버 인증 신청과 관련된 운영이 인터넷, 통신라인, 네트워크, 서버, 파이어월, 프록시, 라우터, 스위치, 브리지와 같은 통신기반구조("통신장비")를 통한 정보 거래에 의존한다는 것을 인정하고 동의한다. 또한 동 통신장비는 Entrust.net나 Entrust.net SSL 웹 서버인증기관 산하에서 운영되는 독립적 제3등록 기관 또는 재판매자, 공동판매자, 또는 앞에서 말한 자의 하도급 계약자, 판매자, 대행인, 공급자, 고용인, 이사의 통제하에 있지 않음을 인정하고 동의한다. Entrust.net나 Entrust.net SSL 웹 서버인증기관 산하에서 운영되는 독립적 제3등록 기관 또는 재판매자, 공동판매자, 또는 앞에서 말한 자의 하도급계약자, 판매자, 대행인, 공급자, 고용인, 이사는 Entrust.net SSL 웹 서버인증서와 Entrust.net SSL 웹 서버 인증 CRL, 또는 Entrust.net SSL 웹 서버 인증 신청과 관련된 과실, 지연, 장애, 결함, 변조가 동 통신장비로 인한 경우 이에 대한 책임을 지지 않는다.

2.2.1.2 부 인

2.2.1.1항에서 규정된 경우를 제외하고, Entrust.net 및 Entrust.net SSL 웹 서버인증기관 산하에서 운영되는 독립적 제3등록 기관 또는 재판매자, 공동판매자, 또는 앞에서 말한 자의 하도급계약자, 판매자, 대행인, 공급자, 고용인, 이사는 명시적, 묵시적, 법적, 거래상 기타 다른 방법으로 진술 또는 보증을 하거나 조건을 제공하지 아니하며 Entrust.net 및 Entrust.net SSL 웹 서버인증기관 산하에서 운영되는 독립적 제3등록 기관 또는 재판매자, 공동판매자, 또는 앞에서 말한 자의 하도급계약자, 판매자, 대행인, 공급자, 고용인, 이사는 특히 시장성, 법규준수, 자격, 품질에 대한 만족, 또는 특정 목적에 대한 적합성에 대하여 진술하고 보증

하거나 조건을 제시하지 않는다.

2.2.1.3 책임제한

어떠한 경우에도 Entrust.net SSL 웹 서버인증서 및 동 인증서의 사용 또는 이에 대한 신뢰를 포함하는 동 인증서와 관련하여 제공되는 서비스로 인하여 또는 이와 관련하여 발생하는 손해에 관하여 Entrust.net, Entrust.net SSL 웹 서버인증기관 산하에서 운영되는 독립적 제3등록 기관 또는 재판매자, 공동판매자, 또는 앞에서 말한 자의 하도급계약자, 판매자, 대행인, 공급자, 고용인, 이사의 신청자, 가입자, 신뢰당사자 또는 기타 개인, 실체 또는 조직에 대한 총책임의 최대한도는 미화 1,000달러를 초과하지 않는다 (“총 보상한도액”). 동 한도는 거래 횟수 또는 Entrust.net SSL 웹 서버인증서 및 이와 관련되어 제공되는 서비스에 의해 또는 이와 관련하여 발생하는 소송원인의 수와 관련 없이 각 인증서 마다 적용된다. 동 한도는 계약 위반 (기초적 위약 포함), 불법행위 (과실 포함), 법령, 또는 직접적, 간접적, 특별, 법적, 징벌적, 예시적, 결과적, 신뢰적 또는 우발적 피해를 포함하여, 책임에 대한 다른 주장에의 근거여부에 상관 없이 어떠한 책임에도 적용된다.

Entrust.net SSL 웹 서버인증서 또는 동 인증서와 관련하여 제공되는 서비스로 인하여 또는 이와 관련하여 발생하는 책임이 앞에서 말한 총 보상한도액을 초과하는 경우, 한도액 내에 이용할 수 있는 금액은 관할법원의 다른 명령이 있지 않는 한, 먼저 발생한 소송에 관하여 최종 분쟁해결을 위해 우선적으로 할당된다. 어떠한 경우에도 Entrust.net, Entrust.net SSL 웹 서버인증기관 산하에서 운영되는 독립적 제3등록 기관 또는 재판매자, 공동판매자, 또는 앞에서 말한 자의 하도급계약자, 판매자, 대행인, 공급자, 고용인, 이사는 손해배상 청구인간의 할당과 상관 없이, Entrust.net SSL 웹 서버인증서와 동 인증서와 관련되어 제공되는 서비스에 대한 총 보상한도액을 초과하여 지불할 의무는 없다.

어떠한 경우에도 Entrust.net 또는 Entrust.net SSL 웹 서버인증기관 산하에서 운영되는 독립적 제3등록 기관 또는 재판매자, 공동판매자, 또는 앞에서 말한 자의 하도급계약자, 판매자, 대행인, 공급자, 고용인, 이사는 계약 위반 (기초적 위약 포함), 불법행위 (과실 포함), 법령 또는 책임에 대한 다른 주장으로 인한 것을 막론하고 우발적, 특별적, 법적, 징벌적, 예시적, 간접적, 신뢰적, 또는 결과적 손해 (사업 손실, 사업기회의 손실, 자료 손실, 저축 손실 또는 기타 재산적 손실)에 대한 책임을 지지 않는다.

상기 제한은 본 계약서에 명시된 제한된 보상대책의 주된 목적이 실패하고 Entrust.net 또는 Entrust.net SSL 웹 서버인증기관 산하에서 운영되는 독립적 제3등록 기관 또는 재판매자, 공동판매자, 또는 앞에서 말한 자의 하도급계약자, 판매자, 대행인, 공급자, 고용인, 이사가 동 손해의 발생 가능성에 대하여 조언을 받았을지라도 적용된다.

어떤 관할 법원은 결과적 또는 우발적 피해에 대한 책임의 면제 또는 제한을 허용하지 않기 때문에 동 책임 한도가 어떤 신청자, 가입자, 신뢰당사자 또는 기타 개인, 실체, 조직에 적용되지 않을 수 있다. 동 실무 준칙의 진술, 보증, 조건에 대한 부인과 책임제한은 동 인증서, 실무준칙, 기타 가입계약서, 신뢰당사자계약서에 있어서 핵심적 부분을 구성한다. 모든 신청자, 가입자, 신뢰당사자 및 기타 개인, 실체, 조직은 상기 진술, 보증, 조건의 부인 및 책임 제한이 없이는 Entrust.net가 동 인증서를 가입자에게 발행하지 않고, 독립적 제3등록 기관, 재판매자, 공동판매자 또는 앞에서 말한 자의 하도급 계약자, 판매자, 대행인, 공급자, 고용인, 이사는 동 인증서와 관련하여 서비스를 제공하지 않으며, 또한 본 규정은 위험부담에 대한 합리적인 분배에 관하여 규정한 것임을 인정한다.

2.2.1.4 기타 제외

Entrust.net과 Entrust.net SSL 웹 서버인증기관 산하에서 운영되는 독립적 제3등록 기관 또는 재판매자, 공동판매자, 또는 앞에서 말한 자의 하도급계약자, 판매자, 대행인, 공급자, 고용인, 이사 어느 누구도 다음의 경우 신청자, 가입자, 신뢰당사자, 또는 기타 개인, 실체, 조직에 대하여 Entrust.net SSL 웹 서버인증서 또는 동 인증서와 관련하여 제공되는 서비스의 사용에 의해 또는 이와 관련하여 발생하는 손실, 비용, 경비, 책임, 손해, 청구 또는 합의금액에 관하여 책임이 없다:

- (i) Entrust.net SSL 웹 서버인증서가 가입자나 개인, 실체 또는 단체의 실수, 의사표시의 하자, 또는 기타 행위나 누락으로 인하여 발행된 경우;
- (ii) Entrust.net SSL 웹 서버인증서의 기간이 만료되었거나 취소된 경우;
- (iii) Entrust.net SSL 웹 서버인증서가 수정되었거나 달리 변경된 경우;
- (iv) 가입자가 Entrust.net SSL 웹 서버인증서의 정보가 변경되거나 동 인증서에 포함된 정보를 잘못되거나 부정확하게 만드는 상황이 발생하였음에도 불구하고 동 인증서의 사용을 중지하지 않은 경우;
- (v) 가입자가 Entrust.net SSL 웹 서버인증실무준칙 또는 가입계약서를 위반한 경우 또는 신뢰당사자가 동 실무 준칙 또는 신뢰당사자계약서를 위반한 경우;
- (vi) Entrust.net SSL 웹 서버인증서와 관련된 비밀키가 손상된 경우;
- (vii) Entrust.net SSL 웹 서버인증서가 Entrust.net SSL 웹 서버인증실무준칙에서 허용된 것 이외의 용도로 사용되거나 해당 법에 위반하여 사용된 경우.

어떠한 경우에도 Entrust.net 또는 Entrust.net SSL 웹 서버인증기관 산하에서 운영되는 독립적 제3등록 기관 또는 재판매자, 공동판매자, 또는 앞에서 말한 자의 하도급계약자, 판매자, 대행인, 공급자, 고용인, 이사는 인증서 발행 또는 발행 요청을 거부한 것으로 인하여 또는 이와 관련하여 발생하는 손실, 비용, 책임, 지출, 손해, 청구 또는 합의금액에 관하여 신청자, 가입자, 또는 기타 개인, 실체 또는 조직에게 책임을 지지 않는다. 어떠한 경우에도

Entrust.net 또는 Entrust.net SSL 웹 서버인증기관 산하에서 운영되는 독립적 제3등록 기관, 재판매자, 공동판매자 또는 앞에서 말한 자의 하도급 계약자, 판매자, 대행인, 공급자, 고용인 또는 이사는 인증서 발행 또는 발행요청 지연으로 인하여 또는 이와 관련하여 발생하는 손실, 비용, 책임, 지출, 손해, 청구 또는 화해 금액에 대하여 신청자, 가입자, 또는 기타 개인, 실체 또는 조직에게 책임을 지지 않는다.

어떠한 경우에도 Entrust.net 또는 Entrust.net SSL 웹 서버인증기관 산하에서 운영되는 독립적 제3등록 기관 또는 재판매자, 공동판매자, 또는 앞에서 말한 자의 하도급계약자, 판매자, 대행인, 공급자, 고용인, 이사는 Entrust.net SSL 서버인증서 또는 동 인증서에 포함된 정보가 어느 관할 구역의 개인, 실체 또는 조직의 특허권, 상표권, 영업비밀, 기타 지적재산권을 침해하고, 오용하고, 희석하고, 부당 경쟁을 하거나 달리 위반한 것에 관한 소송이나 분쟁으로 인하여 또는 이와 관련하여 발생하는 손실, 지출, 비용, 책임, 손해, 청구 또는 합의금액에 관하여 신청자, 가입자, 또는 기타 개인, 실체 또는 조직에게 책임을 지지 않는다.

2.2.1.5 위험한 활동

Entrust.net SSL 웹 서버인증서 및 동 인증서와 관련하여 Entrust.net이 제공하는 서비스는 위험한 활동 또는 핵시설, 항공비행, 통신시스템, 항공수송통제, 의료기구 또는 직접적인 생명보조 기구의 작동을 포함하는 실패 위험 없는 이행을 요구하는 목적으로 사용되거나 이에 관련하여 사용되도록 계획되고, 제조되거나 의도되지 않았다. Entrust.net과 Entrust.net SSL 웹 서버인증기관 산하에서 운영되는 독립적 제3등록 기관 또는 재판매자, 공동판매자, 또는 앞에서 말한 자의 하도급계약자, 판매자, 대행인, 공급자, 고용인, 이사는 특별히 명시적, 묵시적, 법적, 거래상 또는 달리 위와 같은 사용에 대한 모든 진술, 보증 및 조건을 부인한다.

2.2.2 등록기관의 책임

Entrust.net SSL 웹 서버인증기관에 대하여 2.2.1항에 적용되는 것과 동일한 책임규정이 Entrust.net SSL 웹 서버인증기관 산하에서 운영되는 독립적 제3등록 기관 또는 재판매자, 공동판매자, 또는 앞에서 말한 자의 하도급계약자, 판매자, 대행인, 공급자, 고용인, 이사에 적용된다.

2.3 재정책임

가입자와 신뢰당사자는 자신이 참여하고 Entrust.net SSL 웹 서버인증서 또는 동 인증서에 관련하여 제공된 서비스를 사용한 거래에 대하여 동 가입자, 신뢰당사자, 그리고 기타 개인, 실체 또는 조직에게 발생한 재정적 결과에 대한 책임을 진다. Entrust.net는 동 인증서 또는 동인증서에 관련하여 제공된 서비스를 사용하여 완성된 거래의 재정적 결과에 대하여 어떠한 진술이나 보증 또는 조건도 제공하지 않으며 Entrust.net 및 Entrust.net SSL 웹 서버인증

기관 산하에서 운영되는 독립적 제3등록 기관 또는 재판매자, 공동판매자, 또는 앞에서 말한 자의 하도급계약자, 판매자, 대행인, 공급자, 고용인, 이사는 동 인증서 또는 동 인증서에 관련되어 제공된 서비스에 대한 사용 또는 신뢰에 대하여 본 계약서에서 명백하게 규정하는 경우를 제외하고 책임을 지지 않는다.

2.3.1 신뢰당사자에 의한 면책

신뢰당사자는 자신이 Entrust.net SSL 웹 서버인증서 또는 동 인증서와 관련하여 제공된 서비스를 사용 또는 신뢰함으로써 발생하는 또는 이와 관련하여 발생하는 모든 책임, 손실, 비용, 지출, 손해, 청구 및 합의금액 (합리적인 변호사 비용, 소송비용 및 전문가 비용 포함)에 관하여 Entrust.net 및 Entrust.net SSL 웹 서버인증기관 산하에서 운영되는 독립적 제3등록 기관 또는 재판매자, 공동판매자, 또는 앞에서 말한 자의 하도급계약자, 판매자, 대행인, 공급자, 고용인, 이사 (집합적으로 "면책당사자")의 책임을 면책한다. 이는 (i) 동 인증서의 유효성을 신뢰당사자가 확인하지 못하는 경우, (ii) 기간이 만료되거나 취소된 인증서를 신뢰당사자가 신뢰하는 경우, (iii) 신뢰당사자가 인증서 실무준칙, 가입계약서, 신뢰당사자계 약서 및 해당법률이 허용하는 것 이외의 목적으로 인증서를 사용하는 경우, (iv) 신뢰당사자가 어떠한 상황에서 인증서를 신뢰하는 데에 있어 합당한 판단을 하지 못하는 경우 또는 (v) 동 인증서 또는 동 인증서에 관련하여 제공되는 정보에 대한 신뢰당사자의 신뢰가 어떤 관할 구역의 개인, 실체 또는 조직의 지적재산권 또는 기타 권리를 침해하고, 오용하고, 희석하고, 부당 경쟁을 하거나 달리 위반하였음에 관한 소송이나 주장을 포함한다. 상기에도 불구하고, 신뢰당사자는 면책당사자의 고의적인 부당행위로 인하여 또는 이와 관련하여 발생하는 책임, 손실, 비용, 지출, 손해, 청구 및 합의금액(합리적인 변호사 비용, 소송비용 및 전문가 비용 포함)에 관하여 면책당사자의 책임을 면책할 의무가 없다.

2.3.1.1 가입자에 의한 면책

가입자는 신뢰당사자가 Entrust.net SSL 웹 서버인증서 또는 동 인증서와 관련하여 제공된 서비스를 신뢰함으로써 발생하는 또는 이와 관련하여 발생하는 모든 책임, 손실, 비용, 지출, 손해, 청구 및 합의금액(합리적인 변호사 비용, 소송비용 및 전문가 비용 포함)에 관하여 Entrust.net 및 Entrust.net SSL 웹 서버인증기관 산하에서 운영되는 독립적 제3등록 기관 또는 재판매자, 공동판매자, 또는 앞에서 말한 자의 하도급계약자, 판매자, 대행인, 공급자, 고용인, 이사(집합적으로 "면책당사자")의 책임을 면책한다. 이는 (i) 동 인증서 사용 또는 신청에 있어서 가입자에 의한 실수, 의사표시의 하자 또는 생략의 경우, (ii) 동 인증서에 포함된 정보를 가입자가 변경한 경우, (iii) 인증서 실무준칙, 가입계약서, 신뢰당사자 계약서 및 해당법률이 허용하는 것 이외의 목적으로 인증서를 사용하는 경우, (iv) 가입자가 인증서의 공개 키에 상응하는 비밀키의 손실, 공개, 손상 또는 무허가 사용을 방지하기 위하여 필요한 주

의 조치를 취하지 않은 경우, (v) 동 인증서 또는 동 인증서에 관련하여 제공되는 정보에 대한 가입자의 사용이 어떤 관할 구역의 개인, 실체 또는 조직의 지적재산권 또는 기타 권리를 침해하고, 오용하고, 희석하고, 부당 경쟁을 하거나 달리 위반하였음에 대한 소송이나 주장을 포함한다. 상기에도 불구하고, 가입자는 면책당사자의 고의적인 부당행위로 인하여 또는 이와 관련하여 발생하는 책임, 손실, 비용, 지출, 손해, 청구 및 합의금액 (합리적인 변호사 비용, 소송비용 및 전문가 비용 포함)에 대하여 면책당사자의 책임을 면책할 의무가 없다.

2.3.2 신뢰관계

Entrust.net SSL 웹 서버 인증 실무준칙, 가입계약서, 신뢰당사자 계약서의 어떠한 사항도 Entrust.net, Entrust.net SSL 웹 서버인증기관 산하에서 운영되는 독립적 제3등록 기관 또는 재판매자, 공동판매자, 또는 앞에서 말한 자의 하도급계약자, 판매자, 대행인, 공급자, 고용인, 이사를 신청인, 가입자, 신뢰당사자 또는 기타 개인, 실체 또는 조직의 피신탁자, 동업자, 대리인, 수탁자 또는 법적 대리인으로 지명하거나 어떠한 목적으로든 Entrust.net, Entrust.net SSL 웹 서버인증기관 산하에서 운영되는 독립적 제3등록 기관 또는 재판매자, 공동판매자, 또는 앞에서 말한 자의 하도급계약자, 판매자, 대행인, 공급자, 고용인, 이사들과 가입자, 신뢰당사자 또는 기타 개인, 실체 또는 조직간에 신뢰관계를 형성한 것으로 간주되지 않는다. Entrust.net SSL 웹 서버 인증 실무준칙, 가입계약서, 신뢰당사자 계약서의 어떠한 사항도 가입자, 신뢰당사자 또는 기타 개인, 실체 또는 조직에게 Entrust.net, Entrust.net SSL 웹 서버인증기관 산하에서 운영되는 독립적 제3등록 기관 또는 재판매자, 공동판매자, 또는 앞에서 말한 자의 하도급계약자, 판매자, 대행인, 공급자, 고용인, 이사를 대리하여 행동하거나 법적으로 구속하고 이들에게 의무나 책임을 부과 또는 인정하거나 의사표시를 대리를 할 권리를 부여하지 않는다.

2.3.3 관리절차

규정 없음.

2.4 해석과 시행

2.4.1 준거법

국제사법을 제외한 캐나다 온타리오주 법률은 Entrust.net SSL 웹 서버 인증 실무준칙, 가입계약서, 신뢰당사자 계약서의 해설, 효력, 해석, 시행 및 이행에 적용된다. 국제물품판매계약에 대한 유엔의정서는 명시적으로 Entrust.net SSL 웹 서버 인증 실무준칙, 가입계약서, 신뢰당사자 계약서에 적용되지 아니한다. 대체적 분쟁해결절차에 따라 해결되지 못한,

Entrust.net SSL 웹 서버 인증 실무준칙, 가입계약서, 신뢰당사자 계약서 또는 Entrust.net SSL 웹 서버인증서나 동 인증서와 관련하여 제공된 서비스로 인하여 또는 이와 관련하여 발생하는 소송분쟁은 캐나다 온타리오 오타와에 위치한 지방 또는 연방법원의 관할에 귀속 되고 각 개인, 실체 또는 조직은 동 법원이 동 분쟁에 대한 직접적이고 전속적인 재판권을 가지고 있음에 동의한다. 어떠한 사안이 지방 또는 연방 법원에 소송제기되는 경우, 신청인, 가입자 및 신뢰당사자는 배심심리에 관한 권리를 포기한다.

2.4.1.1. 불가항력

Entrust.net, 및 Entrust.net SSL 웹 서버인증기관 산하에서 운영되는 독립적 제3등록 기관 또는 재판매자, 공동판매자, 또는 앞에서 말한 자의 하도급계약자, 판매자, 대행인, 공급자, 고용인, 이사 어느 누구도 자신의 합리적인 통제를 벗어난 원인으로 인하여 Entrust.net SSL 웹 서버 인증 실무준칙, 가입계약서 또는 신뢰당사자 계약서의 조건 이행지연 또는 이를 이행하지 못하거나 준수하지 못함으로써 또는 이와 관련하여 발생하는 손실, 비용, 지출, 책임, 손해, 청구 및 합의금액에 대하여 책임을 지지 않는다. 동 원인은 자연재해, 공공의 적, 폭동 및 반란, 전쟁, 사고, 화재, 파업 및 기타 노동 관련 문제 (Entrust.net이 동 요구를 수용해야 하는 위치에 있는지 여부에 관계 없이), 입출항금지, 사법적 조치, 상급 인정 기관에 의한 실패 또는 불이행, 수출허가 또는 승인, 필요한 인력, 재료, 에너지, 시설, 부품 또는 기계 획득의 실패 또는 불가능 및 민간 또는 군 기관의 조치 등을 포함한다.

2.4.1.2. 해석

Entrust.net SSL 웹 서버 인증 실무준칙에 "조항"이라고 언급되는 것은 본 실무준칙의 조항을 말한다. 동 실무준칙에서 사용되는 중성명사 및 그 변화형은 남성, 여성 명사를 포함한 것으로 간주되고 문맥에 맞게 단수로 사용되는 모든 용어는 복수를 포함하거나 복수로 사용되는 모든 용어는 단수를 포함하고 있는 것으로 간주된다. "본 계약의", "본 계약상", "본 계약에 의한" 및 기타 유사한 취지의 용어는 동 실무준칙에 포함된 일부분이 아닌 전체로서 동 실무준칙을 의미하며 때때로 개정되거나 보충된다. 본 계약에서 "~를 포함한"이란 용어의 의미는 제외한다는 의미가 아닌 "~를 포함하나 이에 제한되지 않는"의 의미이다.

2.4.2 일부무효, 존속, 통합, 통지

2.4.2.1 일부무효

가능한 한 본 계약서, Entrust.net SSL 웹 서버인증실무준칙, 가입계약서 및 기타 신뢰당사자 계약서의 각 규정은 해당 법규에 따라 유효하도록 해석된다. 만일 본 계약서, Entrust.net

SSL 웹 서버인증실무준칙, 가입계약서, 또는 기타 신뢰당사자 계약서의 규정 적용이 어떤 특정한 사실이나 상황에 따라 중재인이나 관할 법원에 의해 유효하지 않거나 집행될 수 없을 경우, (i) 다른 특정한 사실이나 상황에 적용되는 동 규정의 효력 및 집행 가능성과 본 계약서, Entrust.net SSL 웹 서버인증실무준칙, 가입계약서, 또는 신뢰당사자 계약서 기타 규정의 효력은 이에 따라 영향을 받거나 손상되지 않으며 (ii) 동 규정은 그 의도를 유효하게 하기 위해 최대한 가능한 범위에서 시행되고 그러한 규정을 유효하게 하고 집행을 가능하게 하기 위해 필요한 범위까지의 추가적 조치 없이 수정된다.

보다 확실히 하기위해, (I)책임 또는 손실의 제한, (II)진술, 보증, 조건 또는 책임의 부인, 또는 (III) 면책과 관련한 Entrust.net SSL 웹 서버인증실무준칙, 가입계약서, 또는 신뢰당사자 계약서 각 조항은 Entrust.net SSL 웹 서버인증실무준칙, 가입계약서, 또는 신뢰당사자 계약서의 기타 규정과는 명확히 별도로 간주되며 동 목적으로 해석되고 집행될 것을 명백히 이해하고 동의한다.

2.4.2.2 존속

“정의”의 제목을 가진 조항과 2.1.3.1, 2.1.4.1, 2.2, 2.3, 2.4, 2.8, 2.9, 3.1.5, 3.1.6, 4.6, 8.2항은 Entrust.net SSL 웹 서버인증실무준칙과 가입계약서, 또는 신뢰당사자계약서의 종결 또는 만료 이후에도 존속한다. Entrust.net SSL 웹 서버인증실무준칙, 가입계약서 및 신뢰당사자 계약서의 종료 이후에도 존속하는 모든 항에 대한 언급은 해당 항의 하부조항도 포함한다. 모든 지불의무는 Entrust.net SSL 웹 서버인증실무준칙, 가입계약서 및 신뢰당사자계약서의 종료 또는 만료 이후에도 존속한다.

2.4.2.3 통합

Entrust.net SSL 웹 서버 인증 실무준칙, 가입계약서 및 신뢰당사자 계약서는 Entrust.net, Entrust.net SSL 웹 서버인증기관 산하에서 운영되는 독립적 제3등록 기관 또는 재판매자, 공동판매자, 또는 앞에서 말한 자의 하도급계약자, 판매자, 대행인, 공급자, 고용인, 이사 및 관련 사항에 대한 신청자, 가입자, 신뢰당사자 또는 기타 개인, 실체 또는 조직의 모든 권리 및 의무를 규정하고 동 권리 및 의무는 구두이든 문서이든 이전의 계약, 의사교환 또는 어떤 행태의 양해각서에 따라 중대되거나 손상될 수 없다. Entrust.net, Entrust.net SSL 웹 서버인증기관 산하에서 운영되는 독립적 제3등록 기관 또는 재판매자, 공동판매자, 또는 앞에서 말한 자의 하도급계약자, 판매자, 대행인, 공급자, 고용인, 이사의 권리 및 의무는 구두로 개정되거나 포기될 수 없으며 Entrust.net의 적법하게 위임받은 대표자가 서명하거나 증명한 서면에 의해서만 개정될 수 있다.

2.4.2.4 조항의 대립

Entrust.net SSL 웹 서버 인증 실무준칙 조항과 Entrust.net 또는 Entrust.net SSL 웹 서버인증

기관 산하에서 운영되는 독립적 제3등록 기관과 Entrust.net SSL 웹 서버인증서 또는 동 인증서와 관련하여 제공되는 서비스에 대하여 가입자 또는 신뢰당사자간 명시적인 서면 계약간에 대립이 있는 경우, 동 명시적인 서면 계약이 우선한다. 동 인증서 조항과 가입자 계약 또는 신뢰당사자 계약의 조항간에 불일치가 발생하는 경우, Entrust.net SSL 웹 서버 인증 실무준칙의 조건이 적용된다.

2.4.2.5 포기

언제든지 Entrust.net이 Entrust.net SSL 웹 서버 인증 실무준칙, 가입계약서 또는 신뢰당사자 계약서의 조항을 이행하지 못하거나 가입자, 신뢰당사자 또는 기타 개인, 실체 또는 조직으로 하여금 동 계약의 조항을 이행하도록 요구하지 못하는 경우에도 이는 동 조항에 대한 현재 또는 미래의 포기로 해석되지 않으며, Entrust.net의 추후 동 조항의 이행 능력에 영향을 미치지 않는다. Entrust.net의 Entrust.net SSL 웹 서버 인증 실무준칙, 가입계약서 또는 신뢰당사자계약서의 조건 또는 요구에 대한 명시적 포기는 동 조항, 조건 또는 요구를 준수할 미래의 의무의 포기로 해석되지 않는다. Entrust.net SSL 웹 서버인증기관 산하에서 운영되는 독립적 등록기관 또는 재판매자 ("등록기관")가 언제든지 동 실무준칙, 가입계약서 또는 신뢰당사자 계약서를 이행하지 못하거나 동 준칙 및 계약서를 가입자, 신뢰당사자 또는 기타 개인, 실체 또는 조직이 이행하도록 요구하지 못하는 경우에도 이는 동 조항에 대한 현재 또는 미래의 포기로 해석되지 않으며, 동 등록기관의 차후 동 조항의 이행 능력에 영향을 미치지 않는다. 가입계약서 또는 신뢰당사자계약서의 조항, 조건 또는 요구에 대한 등록기관의 명시적 포기는 동 조항, 조건 또는 요구에 대한 미래의 준수 의무의 포기로 해석되지 않는다.

2.4.2.6 통지

Entrust.net SSL 웹 서버인증실무준칙, 가입계약서, 또는 신뢰당사자 계약서에 따른 가입자, 신청자, 또는 신뢰당사자에 의한 통지는 서면으로 하되 아래에 명시된 주소로 선불우편, 팩시밀리, 또는 익일배달 쿠리어로 보내져야 하며 (i) 팩시밀리나 익일 배달 쿠리어의 경우, 익일 영업일, 그리고 (ii) 선불 우편의 경우는 우편을 보낸 때부터 5일 후의 영업일에 효력이 있다. Entrust.net SSL 웹 서버인증실무준칙, 가입계약서, 또는 신뢰당사자 계약서에 따라 Entrust.net이 송부할 통지는 Entrust.net 파일에 있는 가입자의 최종주소, e-mail 주소 또는 팩시밀리 번호로 e-mail, 팩시밀리 또는 쿠리어로 한다. E-mail의 경우, 통지는 익일 영업일에 유효하며 선불우편, 팩시밀리 또는 익일 배달 쿠리어에 의한 통지의 경우, 동 통지는 사용된 통지 수단에 따라 (i) 또는 (ii)에 명시된 날을 기준으로 유효하다.

Entrust.net 통지 주소

Entrust.net Inc.

1000 Innovation Drive
Ottawa, Ontario
Canada K2K 3E7

Attention: Director Operations, Entrust.net
Fax: 1-877-839-3538

2.4.2.7 양도

Entrust.net SSL 웹 서버인증서와 Entrust.net SSL 웹 서버인증실무준칙, 가입 동의서, 또는 신뢰당사자 계약서에 따라 부여된 권리는 가입계약서 또는 신뢰당사자 계약서를 체결한 신청자, 가입자 또는 신뢰당사자에게 개별적으로 귀속되며, 자발적이건 비자발적이건, 법에 집행에 따르건, 또는 다른 방법으로 Entrust.net 또는 신청자, 가입자 또는 신뢰당사자가 계약을 체결한 Entrust.net SSL 웹 서버인증기관 하의 등록 기관의 사전 서면 동의 없이, 양도, 판매, 이전 또는 달리 처분될 수 없다. 동 서면 동의 없이 시도된 양도 또는 이전은 무효이며 자동적으로 Entrust.net SSL 웹 서버인증실무준칙, 가입 동의서, 또는 신뢰당사자 계약서에 따른 동 신청자, 가입자 또는 신뢰당사자의 권리를 종료한다. Entrust.net은 Entrust.net SSL 웹 서버인증실무준칙, 가입 동의서, 또는 신뢰당사자 계약서를 동 실무준칙 및 계약서에 따른 권리 및 의무와 함께 (i) 계열사, 또는 (ii) Entrust.net SSL 웹 서버인증실무준칙, 가입계약서, 또는 신뢰당사자 계약서와 관계된 Entrust.net 사업의 실질적 자산 또는 주식의 판매, 합병, 기타 양도의 일부로 양도, 판매, 이전 또는 달리 처분할 수 있다. 상기 제한에 따라 본 계약서는 구속력을 지니며, 경우에 따라서 Entrust.net, Entrust.net 인증기관 하에 운영하는 제3등록 기관, 신청자, 가입자 또는 신뢰당사자의 허가된 승계인과 양수인의 이익으로 유효하다.

2.4.3 분쟁 해결 절차

가입자, 신청자 또는 신뢰당사자와 Entrust.net 또는 Entrust.net 인증 기관 하에 운영되는 독립적 제3의 등록 기관 사이의 분쟁은 미국 중재 협회의 상업 조정 규칙에 따라 온타리오, 오타와에서 영어로 개최되는 조정으로 해결된다. 동 분쟁의 해결이 30일 내에 조정을 통해 해결되지 못할 경우, 동 분쟁은 구속력 있는 중재로 해결된다. 중재위원회는 중재 가능한 모든 문제에 대해 결정을 할 권리를 지닌다. 분쟁은 본 규정에 의해 수정된 미국 중재 협회의 규칙에 따라 중재단에 의해 최종적으로 해결된다. 동 중재는 온타리오, 오타와에서 개최되며, 중재는 미국 중재 협회가 기술위원 중에서 선임하고 전자상거래 분쟁에 대한 지식을 가진 1명의 중재위원 앞에서 영어로 진행된다. 동 중재 위원은 국제사법 규정에 상관 없이, 온타리오 지방 법을 적용하고 중재 심리의 종결일로부터 30일 이내에 그러나 동 분쟁사안이 중재에 제출된 날로부터 1년을 넘지 않는 기간 내에 서면결정을 내려야 한다. 중재위원의 결정은 구속력과 결정력을 지니며 관할 법원에 제시될 수 있다. 각 중재에서 승리한 당

사자는 실제로 발생한 적당한 변호사 비용을 포함하여 그러한 중재에 따른 비용의 전체 또는 일부에 대한 보상의 권리를 가진다. Entrust.net 인증실무준칙, 가입계약서, 또는 신뢰당사자 계약서의 어떠한 내용도 (i) Entrust.net SSL 웹 서버인증서의 무결성에 영향을 미치는 추정된 손상 또는 (ii) Entrust.net SSL 웹 서버인증실무준칙, 가입계약서 또는 신뢰당사자 계약서의 조건에 대한 추정된 위반에 관하여 2.4.3항 위반 및 중재위원의 권한박탈없이 Entrust.net 또는 Entrust.net 인증 기관에 의해 운영되는 제3등록 기관이 해당 관할법원에 일시적 또는 영구적 금지명령을 신청하는 것을 금지하지 않는다. 중재 또는 조치의 개시는 Entrust.net SSL 웹 서버인증실무준칙, 가입계약서 또는 신뢰당사자 계약서에 따른 신청자, 가입자 또는 신뢰당사자의 의무를 면제하지 않는다.

2.4.3.1 중재 및 소송 제기기간

Entrust.net SSL 웹 서버인증서 또는 Entrust.net SSL 웹 서버인증서와 관련하여 제공되는 서비스와 관계된 분쟁에 관한 모든 중재 또는 법적 조치는 (i) 분쟁의 대상인 Entrust.net SSL 웹 서버인증서의 만료일 또는 취소일 또는 (ii) 서비스 또는 분쟁의 대상인 Entrust.net SSL 웹 서버인증서와 관련된 서비스 제공일 중 이른 날짜이후 1년 이내에 실시된다. 만일, Entrust.net SSL 웹 서버인증서 또는 Entrust.net SSL 웹 서버인증서와 관련하여 제공되는 서비스와 관계된 분쟁에 관한 중재 또는 소송이 동 기간 내에 실시되지 않으면, 중재 또는 소송을 제기하려는 당사자는 동 중재 또는 소송을 제기하거나 진행하는 것이 금지된다.

2.5 비용

Entrust.net SSL 웹 서버인증서와 관련하여 Entrust.net에서 제공되는 서비스 비용은 Entrust.net 저장소에 규정되어 있다. 동 비용은 변경될 수 있으며, 그러한 변경은 Entrust.net 저장소에 공고되는 즉시 유효하다. Entrust.net SSL 웹 서버인증서와 관련하여 독립적 제3등록 기관, 재 판매자, 공동판매자가 제공하는 서비스에 대한 비용은 그러한 제3등록 기관, 재판매자, 공동판매자가 운영하는 웹 사이트에 게시된다. 동 비용은 변경될 수 있으며, 변경은 그 웹 사이트에 게시되는 즉시 유효하다.

2.5.1 인증서 발행과 갱신 비용

Entrust.net이 부과하는 비용에 대해서 Entrust.net 저장소를 참고하라. Entrust.net 인증 기관 하에 운영되는 등록기관, 재판매자, 공동판매자가 부과하는 비용에 대해서는 동 등록기관, 재판매자 및 공동판매자의 웹사이트를 참고하라.

2.5.2 인증서 접속 비용

Entrust.net이 부과하는 비용에 대해서 Entrust.net 저장소를 참고하라. Entrust.net 인증 기관 하에 운영되는 등록기관, 재판매자, 공동판매자가 부과하는 비용에 대해서는 동 등록기관, 재판매자, 공동판매자의 웹사이트를 참고하라.

2.5.3 취소 또는 상태 정보 접속 비용

Entrust.net이 부과하는 비용에 대해서 Entrust.net 저장소를 참고하라. Entrust.net 인증 기관 하에 운영되는 등록기관, 재판매자, 공동판매자가 부과하는 비용에 대해서는 동 등록기관, 재판매자, 공동판매자의 웹 사이트를 참고하라.

2.5.4 정책 정보와 같은 기타 서비스에 대한 비용

Entrust.net이 부과하는 비용에 대해서 Entrust.net 저장소를 참고하라. Entrust.net 인증 기관 하에 운영되는 등록기관, 재판매자, 공동판매자가 부과하는 비용에 대해서는 동 등록기관, 재판매자, 공동판매자의 웹 사이트를 참고하라.

2.5.5 환불정책

Entrust.net, Entrust.net 인증 기관 하에 운영되는 등록기관, 재판매자, 또는 공동판매자는 Entrust.net SSL 웹 서버인증서 또는 Entrust.net SSL 웹 서버인증서와 관련하여 제공되는 서비스에 대해 환불을 하지 않는다.

2.6 공표와 저장소

Entrust.net은 Entrust.net SSL 웹 서버인증서 및 Entrust.net SSL 웹 서버인증기관, Entrust.net 등록 기관, Entrust.net SSL 웹 서버인증기관 하에 운영되는 제3등록 기관의 운영과 관련된 모든 다양한 정보를 저장할 수 있도록 Entrust.net 저장소를 관리한다. Entrust.net SSL 웹 서버인증실무준칙과 다양한 관련 정보는 Entrust.net 저장소에 공표된다. Entrust.net SSL 웹 서버인증실무준칙은 신청하는대로 Entrust.net에서 인쇄본으로 받아 볼 수 있다.

2.6.1 인증기관 정보 공표

다음의 Entrust.net SSL 웹 서버인증서 정보는 Entrust.net 저장소에 공표된다.

- (i) Entrust.net SSL 웹 서버인증실무준칙
- (ii) Entrust.net SSL 웹 서버인증서 가입 및 신뢰 관련 정보와 계약서
- (iii) Entrust.net SSL 웹 서버인증기관이 수행하는 Entrust.net SSL 웹 서버인증서 취소.

Entrust.net 저장소의 Entrust.net SSL 웹 서버인증서와 인증서 취소목록에 사용되는 데이터 양식은 X.500 추천 시리즈(1997 판)에 정의된 관련 개요와 X.500 추천 시리즈에 정의된 몇몇 강화된 부분에 따른다.

2.6.2 공표 빈도

Entrust.net SSL 웹 서버인증실무준칙은 Entrust.net SSL 웹 서버인증실무준칙 8항에 규정된

방침에 따라 재발행되고 공표될 수 있다.

2.6.3 접속 관리

Entrust.net SSL 웹 서버인증실무준칙은 Entrust.net 저장소에 공표된다.

Entrust.net SSL 웹 서버인증실무준칙은 모든 신청자, 가입자, 신뢰당사자의 이용이 가능하나 Entrust.net 정책 기관에서만 수정할 수 있다.

2.6.4 저장소

Entrust.net SSL 웹 서버인증기관은 Entrust.net SSL 웹 서버인증서 관련 및 CRL 정보 접속 허용을 위해 Entrust.net 저장소를 유지 관리한다. Entrust.net 저장소의 정보는 웹 인터페이스를 통해 접속 가능하며 본 Entrust.net SSL 웹 서버인증실무준칙에 규정된 바와 같이 정기적으로 업데이트 된다. Entrust.net 저장소는 유일하게 승인된 Entrust.net SSL 웹 서버인증서의 CRL과 기타 정보에 대한 출처이다.

2.7 준수성 감사

Entrust.net SSL 웹 서버인증기관, Entrust.net이 운영하는 등록 기관 및 Entrust.net SSL 웹 서버인증기관 하에 운영되는 제3등록 기관은 Entrust.net SSL 웹 서버인증실무준칙에 서술된 규정 및 절차에의 준수성 여부를 감사 받는다.

2.7.1 준수성 감사 빈도

Entrust.net SSL 웹 서버인증기관, Entrust.net이 운영하는 등록 기관 및 Entrust.net SSL 웹 서버인증기관 하에 운영되는 독립적 제3등록 기관은 Entrust.net SSL 웹 서버인증실무준칙에 규정된 관행 및 절차의 준수 여부에 대해 1년에 1회 감사를 받는다. 만일 감사 보고서가 개선 조치를 권고한 경우, Entrust.net 또는 해당 제3등록기관은 그러한 감사 보고서 수령 후 30일 이내에 시정 조치를 취한다.

2.7.2 감사의 자격/신분

준수성 감사는 인증기관과 등록기관 평가에 자격이 있는 공인 회계 법인에 의해 수행된다. Deloitte & Touche LLP가 Entrust.net 인증기관과 Entrust.net이 운영하는 등록기관에 대한 감사기관으로 선정되었다.

2.7.3 피감사자와 감사와의 관계

Entrust.net 인증기관과 Entrust.net이 운영하는 등록기관, 또는 Entrust.net 인증기관 하에 운영되는 독립적인 제3등록 기관에 대한 준수성 감사 수행에 선정된 공인 회계 법인은 감사의 대상이 되는 당사자로부터 독립적이어야 한다.

2.7.4 감사 대상

준수성 감사는 Entrust.net 인증기관과 Entrust.net이 운영하는 등록기관, 또는 Entrust.net 인증기관 하에 운영되는 독립적인 제3등록 기관이 본 Entrust.net SSL 웹 서버인증실무준칙에 서술된 방침과 규정을 이행함에 있어 그 준수성을 테스트한다.

2.7.5 결함에 따른 시정조치

결함을 지적한 준수성 감사결과를 수령하는 즉시 감사대상인 Entrust.net 인증기관, Entrust.net이 운영하는 등록기관, 또는 Entrust.net 인증기관 하에 운영되는 독립적인 제3등록 기관은 그러한 결함을 시정하기 위해 신속하게 상업적으로 상당한 노력을 취한다.

2.7.6 결과 통보

모든 준수성 감사 결과는, Entrust.net 인증기관의 경우 Entrust.net 운영기관에, Entrust.net SSL 웹 서버 인증기관이 운영하는 등록기관의 경우 Entrust.net 운영기관에, Entrust.net SSL 웹 서버 인증기관 하에 운영되는 제3등록 기관의 경우 동 등록기관을 위한 운영기관에 각 통보된다.

2.8 기밀성

Entrust.net 또는 Entrust.net 인증기관 하에 운영되는 독립적 제3등록기관, 재판매자, 공동판매자는 본 Entrust.net SSL 웹 서버인증실무준칙과 가입계약서, 신뢰당사자 계약서 의한 경우를 제외하고, 신청자 또는 가입자 이름(또는 Entrust.net SSL 웹 서버인증서를 신청할 때 신청자나 가입자가 제공하는 기타 정보)을 공개 또는 판매하지 않는다. Entrust.net 또는 Entrust.net 인증기관 하에 운영되는 독립적 제3등록기관, 재판매자, 공동판매자는 Entrust.net SSL 웹 서버인증실무준칙과 가입계약서, 신뢰당사자계약서에 규정된 것 이외의 목적으로 동 정보가 사용되거나 유출되는 것을 방지하기 위해 상업적으로 합당한 정도의 주의를 기울인다. 상기에도 불구하고, 신청자와 가입자는 Entrust.net SSL 웹 서버인증서 신청과 함께 제공된 어떤 정보는 Entrust.net SSL 웹 서버인증서에 사용되며 Entrust.net과 Entrust.net 인증 기관 하에 운영되는 모든 독립적 제3등록 기관, 모든 재판매자 및 공동판매자는 동 정보를 공개적으로 사용할 권리가 있음을 인정한다.

2.8.1 기밀로 유지되어야 하는 정보의 형태

Entrust.net SSL 웹 서버인증서 신청, 사용 또는 신뢰와 관련하여 신청자, 가입자, 신뢰당사자가 제공하고 아래 2.8.2항에서 규정된 정보에 포함되지 않는 정보는 기밀 정보로 간주된다. Entrust.net과, Entrust.net 인증기관 산하의 독립적 제3등록기관은 Entrust.net SSL 웹 서버인증서 신청에 제공된 정보를 검증함에 있어 Entrust.net을 보조하거나 Entrust.net SSL 웹 서버인증기관 또는 Entrust.net이 운영하는 등록 기관의 운영에 있어 Entrust.net을 보조하는 하도급계약자나 대행사에게 동 정보를 공개할 수 있는 권한을 지닌다. 기밀 정보로 간주되

는 정보는 법적, 사법적 또는 행정적 절차 또는 기타 법에 의해 요구되는 경우가 아닌 이상 공개되지 않는다. Entrust. Net과, Entrust.net 인증 기관 하의 독립적 제3등록 기관은 법적, 사법적, 행정적 또는 기타 법이 요구하는 절차와 관련하여 도움을 주는 법률 및 재정 고문과 합병, 양수 또는 조직 개편과 관련하여 잠재적 양수자, 법률 고문, 회계사, 은행 및 금융 기관들과 그들의 고문에게 기밀 정보로 간주되는 정보를 공개할 수 있다.

2.8.2 기밀로 취급되지 않는 정보의 형태

Entrust.net SSL 웹 서버인증서 또는 인증서 취소목록에 포함된 정보는 기밀정보로 간주되지 않는다. Entrust.net SSL 웹 서버 인증실무준칙에 포함된 정보는 기밀정보로 간주되지 않는다. 상기에 대한 제한 없이, (i) Entrust. Net과, Entrust.net 인증기관 산하의 독립적 제3등록 기관, 재판매자, 공동판매자의 과실 없이 알려지고, (ii) 가입자 외의 출처로부터 기밀적 또는 물권적 제한없이 Entrust. Net과, Entrust.net 인증기관 하의 독립적 제3등록 기관, 재판매자, 공동판매자에게 정당하게 알려지거나, (iii) Entrust. Net과, Entrust.net SSL 웹 서버인증기관 하의 독립적 제3등록 기관, 재판매자, 공동판매자가 독자적으로 개발하거나, (iv) 가입자에게 공개 승인을 받은 정보는 기밀정보로 간주되지 않는다.

2.8.3 인증서 취소/사용 중지 정보의 공개

Entrust.net SSL 웹 서버인증서가 Entrust.net SSL 웹 서버인증기관에 의해 취소된 경우, 취소된 Entrust.net SSL 웹 서버인증서에 대한 일련번호는 인증서 취소목록에 포함된다.

2.8.4 법 집행 공무원에 공개

Entrust. Net과, Entrust.net 인증 기관 하의 독립적인 제3등록 기관, 재판매자, 공동판매자는 기밀정보로 간주되는 정보를 해당 법에 따라 법 집행 공무원에게 공개할 권리를 지닌다.

2.8.5 민사절차에 의한 공개

Entrust. Net과, Entrust.net 인증 기관 하의 독립적 제3등록 기관, 재판매자, 공동판매자는 기밀 정보와 관련된 증재, 소송, 또는 기타 법적, 사법적, 행정적 절차 기간 동안 기밀정보로 간주되는 동 정보를 공개할 수 있다. 위와 같은 공개는 Entrust. Net과, Entrust.net 인증기관 산하의 독립적 제3등록 기관, 재판매자, 공동판매자가 증재, 소송, 또는 기타 법적, 사법적, 행정적 목적으로 정당하게 요구되는 범위 내에서 동 정보의 사용과 공개를 제한하는 법원의 명령을 얻기 위해 상업적으로 합리적인 노력을 다하는 한 허용된다.

2.8.6 소유자 요청에 따른 공개

Entrust. Net과, Entrust.net 인증 기관 하의 독립적 제3등록 기관, 재판매자, 공동판매자는 신청자, 가입자 또는 신뢰당사자의 요청에 따라 당 신청자, 가입자 또는 신뢰당사자가 Entrust.net, 등록기관, 재판매자, 또는 공동판매자에게 제공한 정보를 공개할 수도 있다.

2.8.7 기타 정보공개 상황

규정 없음

2.9 지적재산권

Entrust.net는, 신청자 또는 가입자에 의하여 제공되고 Entrust.net SSL 웹 서버인증서에 포함되어 신청자 또는 가입자 소유인 정보를 제외하고, Entrust.net SSL 웹 서버인증서에 대한 모든 권리, 소유권 및 이익(지적 재산권 포함)을 소유한다. 모든 신청자와 가입자는, Entrust.net SSL 인증실무준칙, 가입계약서 및 신뢰당사자계약서에 규정된 목적을 위하여 알려져 있거나 추후 고안될지 여부를 불문하고 모든 통신수단과 방법을 통해 동 정보를 사용, 복사, 변경, 공개적으로 전시 및 유통할 수 있도록 Entrust.net과 Entrust.net 인증기관 하의 등록기관에게 비독점적, 세계적, 사용료가 납부된, 사용료 무료인 라이선스를 허용한다. Entrust.net과 Entrust.net 인증기관 하의 등록 기관은 2.4.2.7항에서 규정된 이전, 전도, 또는 양도에 따라 동 라이선스를 이전, 전도, 양도할 자격을 지닌다. Entrust.net은 가입자와 신뢰 당사자에게 Entrust.net SSL 웹 서버 인증실무준칙, 가입계약서 및 신뢰당사자 계약서대로 Entrust.net SSL 웹 서버인증서가 사용되는 한 Entrust.net SSL 웹 서버인증서를 사용, 복사 및 유통할 수 있는 비독점적, 비양도적 라이선스를 허용한다. 단, 그러한 Entrust.net SSL 웹 서버인증서는 완전하고 정확하게 복제되고, 명확한 Entrust.net의 서면 승인이 없이 공개된 데이터베이스, 저장실, 또는 디렉토리에 공개되지 않는다. 본 실무준칙에서 명확히 밝힌 것을 제외하고, 함축적, 에스토펠(과거의 언행과 모순되는 주장을 금하기 위한 영미법상의 원칙)적, 추측적, 또는 그와 비슷한 경우에 어떠한 권리도 인정되는 것으로 간주되지 않는다. 이용가능성에 관하여, Entrust.net은 독자적인 판단에 따라 가입자에게 발급된 Entrust.net SSL 웹서버 인증서와 함께 사용될 경우에만, 가입자에게 1개 이상의 교차 인증서 사본을 발급할 수 있다. Entrust.net은 교차 인증서와 관련한 (모든 지적소유권을 포함하여) 모든 권리, 자격 및 소유권을 가진다.

Entrust.net는 (i) Entrust.net SSL 웹 서버 인증실무준칙의 첫 번째 페이지 상의 저작권 통지가 동 실무준칙의 사본에 포함되고, (ii) 동 실무준칙이 완전하고 정확하게 복제되는 경우 Entrust.net SSL 웹 서버인증실무준칙을 복제하도록 허용한다. Entrust.net는 Entrust.net SSL 웹 서버인증서에 대한 모든 권리, 소유권 및 이익 (지적 재산권 포함)을 소유한다.

어떠한 경우에도 Entrust.net, Entrust.net SSL 웹 서버인증기관하에 운영되는 독립적 제3등록 기관, 재판매자, 공동판매자, 또는 앞에서 말한 자의 하도급 계약자, 판매자, 공급자, 고용인, 이사는 어떤 관할권의 개인, 실체 또는 조직의 특허권, 상표권, 저작권, 영업비밀, 또는 기타 지적재산권이나 다른 권리를 침해하고, 오용하고, 희석하고, 부당 경쟁을 하거나 달리 위반 하였음에 대한 소송이나 주장으로 인하여 또는 이와 관련하여 발생하는 손실, 비용, 책임,

지출, 손해, 청구 또는 합의금액에 대하여 신청자, 가입자 또는 신뢰당사자 또는 제3자에게 책임을 지지 않는다.

3. 신원확인 및 인증

3.1 초기 등록

Entrust.net SSL 웹 서버인증서를 받고자 하는 경우, 신청자는 (i) 안전하고 암호화된 키 쌍을 형성하고 (ii) Entrust.net SSL 웹 서버 인증실무준칙과 가입계약서의 모든 조건에 동의하고 (iii) Entrust.net이 운영하는 등록기관 또는 Entrust.net SSL 웹 서버인증기관하에 운영되는 독립적 제3등록기관("등록기관")이 요청하는 모든 정보를 실수, 의사표시의 하자, 또는 누락 없이 제공하여 Entrust.net SSL 웹 서버인증신청서를 제출하여야 한다. 신청자가 신청서를 제출하고 Entrust.net SSL 웹 서버인증실무준칙과 가입계약서의 조건을 승락하는대로, 등록기관이나 그 등록 기관이 지정한 제3 기관은 Entrust.net SSL 웹 서버인증신청서에 포함된 정보에 대한 제한적 검증을 실시한다. 만일 그러한 검증이 성공적인 경우, 등록기관은 스스로의 판단에 따라 Entrust.net SSL 웹 서버인증기관으로부터 신청자에 대한 Entrust.net SSL 웹서버인증서 발행을 요청한다. 만일 등록기관이 Entrust.net SSL 웹 서버인증서 발행 요청을 거절한다면, 등록 기관은 (i)거절 사유를 신청자에게 e-mail로 통지하기 위하여 상업적으로 합당한 노력을 다하고 (ii)즉시 Entrust.net SSL 웹 서버인증서 신청과 관련하여 지불된 비용을 반환한다. 신청서가 검증을 통과한 경우, 등록기관은 Entrust.net SSL 웹 서버인증기관에 인증서 발행을 요청하고, Entrust.net SSL 웹 서버인증서가 발행되면 그 사실을 신청자에게 e-mail로 통지한다. 신청자는 Entrust.net SSL 웹 서버인증서를 찾는데 사용되는 URL을 제공 받는다. 동 인증서 발급 이후 Entrust.net, Entrust.net SSL 웹 서버인증기관하에 운영되는 제3의 독립적 등록기관, 재판매자, 공동판매자, 또는 앞에서 말한 자의 하도급 계약자, 판매자, 공급자, 고용인, 이사 누구도 신청서에 제공된 정보에 대한 지속적인 감시, 조사 또는 검증을 이행할 의무가 없다.

3.1.1 명칭 유형

Entrust.net SSL 웹 서버인증서의 주체 이름은 X.500 고유명칭(DN)을 따른다. Entrust.net SSL 웹 서버인증기관은 아래에 규정된 단일명칭규정을 사용한다. 각 Entrust.net SSL 웹 서버인증서는 다음과 같은 정보를 포함한다.

- (i) "국가 명칭" (C)은 신청자가 위치하고 Entrust.net SSL 웹 서버인증서를 설치할 월드와이드 웹 서버가 위치한 국가이며 두자리의 ISO 3166 국가별 코드이다.
- (ii) "업체명" (O)은 법인, 조합, 또는 기타 실체의 경우 그 업체의 이름이다. 단독 소유인 경우, 업체명은 신청자의 이름이 될 수 있다.
- (iii) "업체 부서 명" (OU)는 선택적 영역이다. OU는 업체 내의 다른 그룹을 구분하기 위

해서 이용된다 (예를들면, 인사, 마케팅 및 개발 부서를 구별하기 위하여).

(iv) 공동 이름 (CN)은 신청자가 Entrust.net SSL 웹 서버인증서를 설치하고자 하는 월드와이드 웹 서버의 DNS에서 사용되는 완전히 확인된 호스트 이름 또는 경로이다.

3.1.2 의미있는 명칭의 필요

Entrust.net SSL 웹 서버인증서에서 사용될 공동 이름 (CN)의 가치는 신청자가 Entrust.net SSL 웹 서버인증서를 설치하고자 하는 월드와이드 웹 서버의 DNS에서 사용되는 완전히 확인된 호스트 이름 또는 경로이다.

3.1.3 다양한 명칭 형태의 해석 규칙

Entrust.net SSL 웹 서버인증서의 주체 명칭은 3.1.1항과 3.1.2항에 규정된 대로 해석된다.

3.1.4 명칭의 유일성

명칭은 Entrust.net 저장소에서 각 주체별로 명백하게 정의된다. 고유명칭의 속성은 개별 이름이 부여되는 각 월드와이드 웹 서버에 유일하여야 하며 이는 2개의 Entrust.net SSL 웹 서버인증서에 동일한 주체 명칭이 부여되는 것을 방지하기 위해 사용된다. 각 Entrust.net SSL 웹 서버인증서는 각각의 일련 번호를 발행 받는다.

3.1.5 명칭에 대한 분쟁의 해결 절차

Entrust.net SSL 웹 서버인증서의 주체 명칭은 선착순으로 발행된다. Entrust.net SSL 웹 서버인증서에 사용하기 위해 주체 명칭을 승인함에 있어 Entrust.net SSL 웹 서버인증기관 하에 운영되는 등록기관은 동 정보의 사용이 개인, 실제 또는 조직의 지적 재산권 또는 기타 권리를 침해하고, 오용하고, 희석하고 부당경쟁을 하거나 달리 위반하는 지에 대한 여부를 판단하지 않는다. Entrust.net 인증 기관과 Entrust.net 인증 기관 하에 운영되는 등록 기관은 인증서의 정보 사용과 관련하여 가입자와 제3 기관 사이의 분쟁에 대한 중재자의 역할을 하지 않으며 이에 대한 해결방안을 제시하지 않는다. Entrust.net SSL 웹 서버 인증실무준칙은 Entrust.net SSL 웹 서버인증서의 정보와 관련하여 가입자나 제3 기관에 절차적 또는 실제적 권리를 주지 않는다. Entrust.net 인증 기관과 Entrust.net 인증 기관 하에 운영되는 등록기관은 Entrust.net SSL 웹 서버인증서의 정보로 인해 발생하는 가입자들 사이 또는 가입자와 제3 자 사이의 분쟁과 관련하여, 혹은 가입자와 Entrust.net SSL 웹 서버인증기관 또는 Entrust.net SSL 웹 서버인증기관 하의 등록 기관 사이의 분쟁, 혹은 제3 자와 Entrust.net SSL 웹 서버인증기관 또는 Entrust.net SSL 웹 서버인증기관 하의 등록 기관사이의 분쟁과 관련하여 법적, 또는 형평법상의 구제방안(금지명령 포함)을 구하는 것이 금지 되지 않는다. Entrust.net 인증 기관과 Entrust.net 인증 기관 하에 운영되는 등록 기관은 관할법원 또는 중재인으로부터 Entrust.net SSL 웹 서버인증서 취소명령을 받는 대로 Entrust.net SSL 웹 서버인증서를 취소할 권리와 취소를 요청할 권리를 지닌다.

3.1.6 인지, 인증 및 상표권의 역할

Entrust.net SSL 웹 서버인증기관과 Entrust.net SSL 웹 서버인증기관 하에 운영되는 등록기관은 일정한 경우 제3의 청구인의 상표권을 침해할 가능성이 있는 정보를 포함하고 있는 Entrust.net SSL 웹 서버인증서와 관련하여 조치를 취할 수 있다. 위 청구인이 Entrust.net SSL 웹 서버인증기관과 Entrust.net SSL 웹 서버인증기관 하에 운영되는 등록기관에게 (i) 미국, 캐나다, 일본, 호주 또는 기타 유럽연합국가의 주된 상표등록기관이 동 등록이 현재 유효함을 증명하고 발행한 지 3개월을 초과하지 아니한 인증된 상표 등록증 사본, 및 (ii) 가입자의 Entrust.net SSL 웹 서버인증서에 포함된 정보가 청구인의 상표권 권리를 침해하고 있음을 진술하는 청구인의 분쟁대상인 Entrust.net SSL 웹 서버인증서 가입자에 대한 사전 서면통지서 사본, 및 (iii) 통지 방법 및 Entrust.net SSL 웹 서버인증서 가입자가 동 통지를 수령하였음을 믿는 근거를 표시하는 청구인의 진술을 제공하는 경우, Entrust.net SSL 웹 서버인증기관 또는 Entrust.net SSL 웹 서버인증기관 하에 운영되는 등록기관은 다음과 같은 조치를 취할 수 있다. Entrust.net SSL 웹 서버인증기관과 Entrust.net SSL 웹 서버인증기관 하에 운영되는 등록기관은 가입자의 Entrust.net SSL 웹 서버인증서의 발행일이 분쟁 청구인이 제공한 상표권 등록증의 등록일 보다 앞선 것인지 여부를 판단할 수 있다. 만일 가입자의 Entrust.net SSL 웹 서버인증서 발행일이 청구인의 상표권 등록증의 등록일 보다 앞선 경우, Entrust.net SSL 웹 서버인증기관이나 Entrust.net SSL 웹 서버인증기관 하에 운영되는 등록기관은 관할 법원이나 중재단의 공식적인 명령이 있지 않는 한 더 이상의 조치를 취하지 않는다. 만일 가입자의 Entrust.net SSL 웹 서버인증서 발행일이 청구인의 상표권 등록증의 등록일 이후인 경우, Entrust.net SSL 웹 서버인증기관이나 Entrust.net SSL 웹 서버인증기관 하에 운영되는 등록기관은 가입자에게 미국, 캐나다, 일본, 호주 또는 기타 유럽연합국가의 주된 상표등록기관으로부터 가입자의 해당 상표권 소유에 대한 증거를 제공하도록 요청한다. 만일 가입자가 청구인의 상표 등록 보다 앞서거나 동일한 날짜에 발행된 인증된 상표권 등록증을 제출하면, Entrust.net SSL 웹 서버인증기관이나 Entrust.net SSL 웹 서버인증기관 하에 운영되는 등록기관은 관할 법원이나 중재단의 공식적인 명령이 있지 않는 한, 더 이상의 조치를 취하지 않는다. 만일 동 가입자가 10영업일 이내에 회신을 하지 않거나 가입자가 제출한 상표권 등록증의 등록일이 청구인의 상표권 등록일 이후인 경우, Entrust.net SSL 웹 서버인증기관이나 Entrust.net SSL 웹 서버인증기관 하에 운영되는 등록기관은 분쟁의 대상이 되는 Entrust.net SSL 웹 서버인증서를 취소하거나 취소요청을 할 수 있다.

만일 가입자가 청구인에 대해 소송을 제기하거나, 청구인이 가입자에 대해 소송을 제기하는 경우, 동 소송이 발행된 Entrust.net SSL 웹 서버인증서의 정보와 관계되고 소송을 제기한 당사자가 Entrust.net SSL 웹 서버인증기관이나 Entrust.net SSL 웹 서버인증기관 하에 운영되는 등록기관에 검인된 소장 또는 진술서를 제출하면, Entrust.net SSL 웹 서버인증실무준

칙, 가입계약서 또는 신뢰당사자 계약서에 따라 Entrust.net SSL 웹 서버인증서 상태 변경이 요구되지 않는 한, Entrust.net SSL 웹 서버인증기관은 Entrust.net SSL 웹 서버인증서의 현재 상태를 유지하거나, Entrust.net SSL 웹 서버 인증기관 하에 운영되는 등록기관은, Entrust.net SSL 웹 서버인증기관에 Entrust.net SSL 웹 서버인증서의 유지를 요청한다. 소송 기간 동안, 관할 법원 및 중재인의 명령이나 Entrust.net SSL 웹 서버인증실무준칙, 가입계약서 또는 신뢰당사자 계약서에서 제시되거나 요구되지 않는 한, Entrust.net SSL 웹 서버인증기관은 분쟁상태에 있는 인증서를 취소하지 않으며, Entrust.net SSL 웹 서버인증기관 하에 운영되는 등록기관은 분쟁 상태에 있는 인증서 취소를 요청하지 않는다. 위에 명시된 소송의 경우, Entrust.net SSL 웹 서버인증기관과 Entrust.net SSL 웹 서버인증기관 하에 운영되는 등록기관은 분쟁의 대상인 Entrust.net SSL 웹 서버인증서와 관련하여 소송 당사자로 지명될 필요 없이 관할 법원의 지시를 따른다. Entrust.net SSL 웹 서버인증서와 관련하여 소송 당사자로 지명되는 경우 Entrust.net이나 Entrust.net SSL 웹 서버인증기관 하에 운영하는 제3의 등록기관은 동 소송에 응소하고 방어함에 있어 적절한 조치를 취할 권리가 있다. Entrust.net SSL 웹 서버인증서와 관련한 소송에 관계된 가입자 또는 신뢰당사자는 Entrust.net SSL 웹 서버 인증 실행 준칙, 가입계약서 및 신뢰당사자 계약서의 조건을 준수한다.

Entrust.net SSL 웹 서버인증기관 하에 운영되는 등록기관은 Entrust.net SSL 웹 서버인증기관에게 그러한 등록 기관의 요청에 따라 발행된 Entrust.net SSL 웹 서버인증서에 포함된 정보와 관련한 분쟁에 대해 통지를 한다.

3.1.7 비밀 키 소유 입증 방법

등록기관은 Entrust.net SSL 웹 서버인증신청서와 신청자가 제출한 CSR에 대한 서명을 확인함으로써 가역 비대칭 알고리즘 (RSA)을 사용하여 형성된 CSR의 소유 확인 시험을 수행한다.

3.1.8 단체의 신원확인

Entrust.net SSL 웹 서버인증기관 하에 운영되는 등록기관은 신청자나 가입자가 제출한 단체 신원에 대한 제한적인 검증을 수행한다. 동 기관은 신청서에 기재된 업체의 신원, 주소 및 도메인 이름이 제3자의 데이터베이스 및/또는 정부 자료와 일치하는지 결정한다. Entrust.net SSL 웹 서버인증신청서의 제한된 검증을 위한 정보와 출처는 신청자 또는 가입자의 관할 지역에 따라 다양할 수 있다. 정부 자료에 등록되지 않은 단체인 경우, Entrust.net SSL 웹 서버인증기관 하에 운영되는 등록기관은 그 업체의 존재여부를 확인하기 위해 상업적으로 합리적인 노력을 다한다. 동 노력은 은행 또는 기타 신용할 만한 사람이나 기관을 통한 조사를 포함한다. Entrust.net SSL 웹 서버인증기관 하에 운영되는 등록기관은 Entrust.net 정책 기관이 책정한 검증관행서를 준수한다.

Entrust.net 정책 기관은 단체 신원확인 검증절차를 향상시키기 위해 스스로의 판단에 따라 검증관행을 갱신할 수 있다. 동 검증관행서에 대한 갱신은 Entrust.net SSL 웹 서버 인증실무준칙을 개정하기 위한 표준절차에 따라 공포된다.

3.1.9 개인 신원확인

Entrust.net SSL 웹 서버인증기관 하에 운영되는 등록기관은 신청자나 가입자가 제출한 개인의 신원에 대한 제한적인 검증을 수행한다. 개인 신원의 정확성을 기하기 위해, 개인은 Entrust.net SSL 웹 서버인증기관 하에 운영되는 등록기관의 대리인 또는 신청자 관할 지역의 공증인 앞에 출석해야 한다. 개인은 3장의 사진 신분증을 제출해야 한다. 신원확인에 적합한 신분증의 유형은 신청자의 관할권에 따른다. Entrust.net 정책 기관은 개인 신원 검증 과정을 향상 시키기 위해 스스로의 판단에 따라 검증 관행을 개정할 수 있다. 동 검증관행에 대한 변경은 Entrust.net SSL 웹 서버인증실무준칙을 개정하기 위한 표준절차에 따라 공포된다.

3.2 일상적 키 재생성

각 Entrust.net SSL 웹 서버인증서는 인증서의 만료일을 포함한다. 만료일이 있는 이유는 인증서와 관련된 키 쌍의 누출을 최소화하기 위한 것이다. 이런 이유로 신규 Entrust.net SSL 웹 서버인증 신청서 처리과정 진행시, Entrust.net은 새로운 키 쌍을 형성하고 키 쌍 중 새로운 공개 키를 Entrust.net SSL 웹 서버인증신청서와 함께 제출하도록 요구된다. Entrust.net은 Entrust.net SSL 웹 서버인증서를 갱신하지 않는다. 그러므로 만일 가입자가 현재의 Entrust.net SSL 웹 서버인증서 만료일 후에도 Entrust.net SSL 웹 서버인증서를 지속적으로 사용하기를 원하면, 가입자는 반드시 새로운 Entrust.net SSL 웹 서버인증서를 구매하고 만료될 인증서와 대체해야 한다. 가입자가 새 Entrust.net SSL 웹 서버인증 신청서를 접수하려면 3.1항에 명시된대로 새로운 키 쌍의 생성 및 인증서의 초기 신청에 필요한 모든 정보의 제출을 포함하여 초기 신청 과정을 완료하여야 한다. 가입자의 Entrust.net SSL 웹 서버인증서 신청서를 처리한 등록 기관은 Entrust.net SSL 웹 서버인증서의 만료사실에 관하여 신청서에 명기된 기술 담당자에게 e-mail을 송부함으로써 가입자에게 이를 통지하기 위한 상업적으로 합당한 노력을 다한다. Entrust.net SSL 웹 서버인증서 만료 즉시, 가입자는 동 Entrust.net SSL 웹 서버인증서 사용을 중지하고, 동 인증서가 설치되었던 장치나 소프트웨어로부터 인증서를 삭제하여야 한다.

3.3 취소 후 키 재생성

Entrust.net SSL 웹 서버인증기관과 Entrust.net SSL 웹 서버인증기관 하의 등록 기관은 취소된 인증서를 갱신하지 않는다. 만일 가입자가 인증서 취소 후 Entrust.net SSL 웹 서버인증서를 사용하기를 원한다면, 가입자는 반드시 새로운 인증서를 신청하고 취소된 인증서와 교체하여야 한다. 다른 Entrust.net SSL 웹 서버인증서를 얻고자 한다면, 가입자는 3.1항에 명

시된대로 새로운 키 상의 생성 및 인증서의 첫 신청에 필요한 모든 정보의 제출을 포함하여 초기 신청과정을 완료하여야 한다. Entrust.net SSL 웹 서버인증서 취소 즉시, 가입자는 그러한 Entrust.net SSL 웹 서버인증서 사용을 중지하고, 동 인증서가 설치되었던 장치나 소프트웨어로부터 인증서를 삭제하여야 한다.

3.4 취소 요청

가입자는 언제든지 Entrust.net SSL 웹 서버인증서의 취소를 요청할 수 있다. 단, 가입자는 인증서 신청을 처리한 등록기관에 가입자 자신이 동 인증서가 발행된 개인, 조직 또는 실체임을 입증하여야 한다. 등록 기관은 가입자가 Entrust.net SSL 웹 서버인증신청서 제출 시 제출한 암호문이나 일부 정보를 요청하여 가입자의 Entrust.net SSL 웹 서버인증서 취소 요청을 인증한다. 동 정보 수령 및 확인 이후, 등록 기관은 취소 요청 확인 후 48시간 이내에 가입자의 Entrust.net SSL 웹 서버인증서 취소를 요청하고, Entrust.net SSL 웹 서버인증기관은 이에 따라 Entrust.net 저장소에 있는 CRL에 취소된 인증서의 일련 번호를 공고한다. Entrust.net SSL 웹 서버 인증기관 하의 등록기관은 인증서 신청서에 명기된 기술 책임자 및 보안 책임자에게 e-mail을 보내어 가입자의 Entrust.net SSL 웹 서버인증서가 취소되었음을 통지하기 위해 상업적으로 합당한 노력을 다한다.

4. 운영 조건

4.1 인증 신청서

Entrust.net SSL 웹 서버인증서를 획득하기 위해서 신청자는 반드시 Entrust.net SSL 웹 서버인증실무준칙의 3.1항에 명시된 절차를 따라야만 한다. Entrust.net이 운영하는 등록 기관이나 Entrust.net SSL 웹 서버인증기관하에 운영되는 독립적 제3등록 기관은 신청자의 신원에 대한 제한적인 검증을 수행하기위해 3.1.8항과 3.1.9항에 명시된 절차를 따른다.

4.2 인증서 발행

신청자가 제출한 신청서의 정보에 대해 제한된 검증을 수행한 후, Entrust.net SSL 웹 서버인증기관 하에 운영되는 등록 기관은 Entrust.net SSL 웹 서버인증기관에 Entrust.net SSL 웹 서버인증서 발행을 요청할 수 있다. 이러한 요청에 따라 Entrust.net SSL 웹 서버인증기관은 Entrust.net SSL 웹 서버인증실무준칙 7항에 명시된 인증서 프로파일에 따라 Entrust.net SSL 웹 서버인증서를 생성하고 디지털 방식으로 서명한다.

4.3 인증서 승락

Entrust.net SSL 웹 서버인증서가 형성되고 저장소에 저장되면, 인증서 발행을 요구한 등록 기관은 가입자에게 인증서가 발행되었고 사용이 가능하다는 e-mail 통지를 하기 위해 상업적으로 합당한 노력을 한다. 이러한 e-mail은 가입자가 Entrust.net SSL 웹 서버인증서를 수

령할 때 사용할 URL을 포함한다.

4.4 인증서 정지 및 취소

Entrust.net SSL 웹 서버인증기관은 Entrust.net SSL 웹 서버 인증기관 하에 운영되는 등록 기관으로부터 인증서의 유효한 취소 요청을 받은 후 인증서를 취소한다. 동 등록 기관은 가입자로부터 유효한 Entrust.net SSL 웹 서버인증서 취소 요청을 받은 후 Entrust.net SSL 웹 서버인증기관에 인증서 취소 요청을 할 권리가 있고 취소 요청을 할 수 있다. 만일 등록 기관이 가입자가 Entrust.net SSL 웹 서버인증서 사용을 중단해야 하는 사유의 발생을 인식한 경우, 등록기관은 Entrust.net SSL 웹 서버인증기관에 해당 가입자의 인증서 취소 요청을 할 권리가 있고 취소 요청을 한다. Entrust.net SSL 웹 서버 인증기관은 Entrust.net SSL 웹 서버 인증서의 정지를 허가하지 않는다.

4.4.1 취소 상황

만일 Entrust.net SSL 웹 서버인증기관 또는 등록 기관이 다음의 어떤 사항이 발생했다는 사실을 인지하거나 그에 대한 합당한 근거를 인식한 경우, Entrust.net SSL 웹 서버인증기관은 가입자의 Entrust.net SSL 웹 서버인증서를 취소할 권리가 있고 취소할 수 있으며 등록 기관은 Entrust.net SSL 웹 서버인증서 취소를 요청할 권리가 있고 요청해야 한다:

- (i) Entrust.net SSL 웹 서버인증기관의 비밀 키 또는 상위의 인증 기관의 비밀 키의 손상;
- (ii) 가입자의 Entrust.net SSL 웹 서버인증실무준칙 또는 가입계약서의 조건 위반;
- (iii) 가입자에게 발행된 Entrust.net SSL 웹 서버인증서에 포함된 정보의 변경;
- (iv) Entrust.net SSL 웹 서버인증서 비용 또는 서비스 비용에 대한 미지급;
- (v) Entrust.net SSL 웹 서버인증서가 Entrust.net SSL 웹 서버인증실무준칙 또는 가입계약서의 요구사항에 따라 발행되지 않았다는 결정, 또는;
- (vi) Entrust.net SSL 웹 서버인증서 또는 Entrust.net SSL 웹 서버인증기관의 무결성, 보안성 또는 신뢰성에 영향을 미칠 수 있다고 합당하게 예상되는 기타 이유.

가입자는 가입자의 비밀 키 손상을 의심 또는 인식한 경우, Entrust.net SSL 웹 서버인증서에 포함된 정보의 변화에 대한 변경을 의심하게 되거나 또는 인식한 경우, 또는 Entrust.net SSL 웹 서버인증서에 포함된 정보를 부정확, 불완전, 또는 잘못되게 만드는 상황의 변화를 의심하게 되거나 또는 인식한 경우, Entrust.net SSL 웹 서버인증서의 취소를 요청한다. 그러한 취소 요청은 가입자의 인증서 신청을 처리한 등록기관에 신청한다. 만일 가입자의 Entrust.net SSL 웹 서버인증서가 어떠한 이유로든 취소된 경우, 그 Entrust.net SSL 웹 서버인증서를 처리한 등록 기관은 Entrust.net SSL 웹 서버인증신청서에 기재된 기술 담당자 및 보안 책임자에게 e-mail을 보내어 가입자에게 통지할 수 있도록 상업적으로 합당한 노력을

다한다. Entrust.net SSL 웹 서버인증서의 취소는 본 Entrust.net SSL 웹 서버인증실무준칙, 가입계약서, 또는 신뢰당사자 계약서에 따른 가입자의 계약 의무에 영향을 주지 않는다.

4.4.2 인증서 취소 요청을 할 수 있는 자

가입자는 언제나 어떠한 이유로든 Entrust.net SSL 웹 서버인증서 취소를 요청할 수 있다. 가입자는 Entrust.net SSL 웹 서버인증서 취소를 요청한 경우, 앞의 3.4항에 명시되었듯이 그 인증서 신청서를 처리한 등록기관에 자신을 입증하여야 한다. 3.4항과 4.4.3항에 명시되었듯이 가입자가 자신을 적절히 입증하지 않는 한 Entrust.net SSL 웹 서버인증기관이 인증서를 취소하거나 Entrust.net SSL 웹 서버인증기관 하에 운영되는 등록기관이 인증서 취소를 요청하도록 요구되지 않는다. 언제나 4.4.1항에 명시된 이유로 Entrust.net SSL 웹 서버인증기관은 인증서를 취소할 권한이 있고 취소하며, Entrust.net SSL 웹 서버인증기관 하에 운영되는 등록기관은 인증서 취소를 요청할 권한이 있으며 요청한다.

4.4.3 인증서 취소 요청 절차

Entrust.net SSL 웹 서버인증기관 하에 운영되는 등록기관은 (i) Entrust.net SSL 웹 서버인증신청서와 함께 가입자가 제출한 일부 정보, (ii) Entrust.net SSL 웹 서버인증신청서와 함께 가입자가 제출한 암호문 또는 가입자 측의 담당자 확인으로 가입자의 Entrust.net SSL 웹 서버인증서 취소 요청을 확인한다. 그러한 정보 수령 및 확인이 이루어지면, 등록 기관은 인증서를 발행한 Entrust.net SSL 웹 서버인증기관에 인증서 취소 요청서를 보낸다. 그러한 취소 요청서를 받은 Entrust.net SSL 웹 서버인증기관은 취소 요청서를 받은 후 48시간 이내에 취소된 Entrust.net SSL 웹 서버인증서의 일련 번호를 Entrust.net 저장실의 CRL에 공고한다. 어떠한 이유로든 가입자의 Entrust.net SSL 웹 서버인증서가 취소되면, 등록 기관은 Entrust.net SSL 웹 서버인증신청서에 기재되었던 기술담당 및 보안 책임자에게 e-mail 통지를 하여 가입자에게 통지할 수 있도록 상업적으로 합리적인 노력을 한다.

4.4.4 취소 요청 유예기간

비밀키의 손상 또는 손상이 의심되는 경우 가입자는 손상 또는 손상이 의심되는 사실을 발견한 즉시, 해당 Entrust.net SSL 웹 서버인증서 취소를 요청한다. 기타 요인에 의한 취소요청은 가능한 한 빨리 하도록 한다.

4.4.5 중지 상황

Entrust.net 웹 서버인증기관은 Entrust.net SSL 웹 서버인증서를 중지하지 않는다.

4.4.6 중지를 요청할 수 있는 사람

Entrust.net 웹 서버인증기관은 Entrust.net SSL 웹 서버인증서를 중지하지 않는다.

4.4.7 중지 요청 절차

Entrust.net 웹 서버인증기관은 Entrust.net SSL 웹 서버인증서를 중지하지 않는다.

4.4.8 중지기간의 한계

Entrust.net 웹 서버인증기관은 Entrust.net SSL 웹 서버인증서를 중지하지 않는다.

4.4.9 CRL 발행 빈도

Entrust.net SSL 웹 서버인증기관은 최소한 24시간마다 1번씩 CRL을 발행하기 위해서 상업적으로 타당한 노력을 기울인다. CRL은 대략 자정에 일반적으로 발행된다. 심각한 손상의 발견 등 어떤 상황에 있어서, CRL은 동 시간 사이에도 발행될 수 있다.

4.4.10 CRL 확인 요구

신뢰당사자는 자신이 신뢰하기를 원하는 Entrust.net. SSL 웹 서버인증서의 취소 여부를 확인해야 한다. 신뢰당사자는 자신이 신뢰하기를 원하는 Entrust.net. SSL 웹 서버인증서의 취소 여부를 결정하기 위해서 적합한 저장소에서 유지되는 인증서 취소목록을 확인한다. 어떠한 경우에도 Entrust.net, Entrust.net SSL 웹 서버인증기관 하에 운영되는 독립적 제3등록기관, 재판매자, 공동판매자, 또는 앞에서 말한 자의 하도급계약자, 판매자, 대행인, 공급자, 고용인, 이사는 Entrust.net SSL 웹 서버인증서의 취소나 만료에 대해서 신뢰당사자가 확인하지 못하거나 취소되거나 만료된 인증서를 신뢰당사자가 신뢰함으로써 발생하는 어떠한 손해에 대해서도 책임을 지지 않는다.

4.4.11 온라인 취소/상태 확인 유용성

Entrust.net 저장소에 있는 CRL은 일련 번호로 검색할 수 있다.

4.4.12 온라인 취소 확인 요구

4.4.10항 참조

4.4.13 유효한 취소 공고의 다른 형식

다른 방식이 규정되지 않는다.

4.4.14 취소 공고의 다른 형식 대한 확인 요구

규정 없음.

4.4.15 키 손상에 대한 특별 요구사항

가입자의 Entrust.net SSL 웹 서버인증서에 포함된 공개 키에 대응하는 비밀키가 손상되었음을 가입자가 의심하거나 알게되면, 가입자는 4.4.3항에 규정되어 있는 절차에 따라 가입자의

Entrust.net SSL 웹 서버인증서 신청을 처리한 등록기관에게 의심되거나 실질적인 손상에 관해 통보한다. 가입자는 그런 Entrust.net SSL 웹 서버인증서 사용을 즉각 중단하고 Entrust.net SSL 웹 서버인증서가 설치되어 있던 장치 그리고 (또는) 소프트웨어로부터 Entrust.net SSL 웹 서버인증서를 제거한다. 가입자는 동 손상 또는 손상이 의심되는 상황을 조사하고 위 상황에 의해 영향을 받았을 수 있는 신뢰당사자에게 통보할 책임이 있다.

4.5 보안 감사 절차

Entrust.net SSL 웹 서버인증기관 내의 중요한 보안 사안은 자동적으로 시간 검인되고 감사 기록파일에 감사기록으로 기록된다. 감사기록파일은 정기적으로 처리된다 (방침 위반 또는 기타 중요 사안에 대한 검토). 감사기록의 수정을 방지하기 위하여 확인 코드가 감사기록 파일과 함께 사용된다. 감사기록파일은 정기적으로 보관된다. 최근의 감사기록파일을 포함한 모든 파일은 백업 매체로 옮겨져서 안전한 기록 시설에 보관된다.

4.6 기록 보관

Entrust.net SSL 웹 서버인증기관의 감사기록파일 및 데이터 베이스는 보관된다. Entrust.net SSL 웹 서버 인증기관의 데이터 베이스는 최소한 3년 동안 보관된다. 감사기록 파일은 최소한 1년간 보관된다. Entrust.net SSL 웹 서버인증기관의 데이터 베이스는 Entrust 소프트웨어 마스터 키에 의해서 암호화되고 보호된다. 보관 매체는 Entrust.net 가 위임한 직원만이 접근할 수 있는 제한된 접근 시설 내 저장장치에 의해서 보호된다. 보관 파일은 생성되면서 백업이 된다. 원본은 Entrust.net SSL 웹 서버인증기관 시스템과 함께 저장되고 사이트상에 저장된다. 백업 파일은 안전하고 지리적으로 분리된 위치에 저장된다.

4.7 키 변환

관련 키 쌍의 노출을 최소화 하기 위해서 일정 기간 후에 만료하는 Entrust.net SSL 웹 서버인증서가 가입자에게 발행된다. 이러한 이유로 만료되는 Entrust.net SSL 웹 서버인증서를 대체하기 위해 각 Entrust.net SSL 웹 서버인증 신청서와 함께 새로운 키 쌍이 생성되어 새로운 공개키가 제출되어야 한다. Entrust.net SSL 웹 서버인증서 갱신을 위한 과정은 3.02항에 규정되어 있다.

4.8 손상과 재해 복구

Entrust.net SSL 웹 서버인증기관은 시스템 정지 발생시 적절한 서비스 복구를 제공하기 위한 재해 복구 계획을 가진다.

Entrust.net는 Entrust.net SSL 웹 서버인증기관의 무결성을 유지하기 위해서 엄격한 보안 통제를 요구한다. Entrust.net의 입장에서 Entrust.net SSL 웹 서버 인증기관에 의해 사용되는 비밀키의 손상은 거의 발생하지 않을 것으로 보지만 Entrust.net는 동 손상 발생시 적용될 정책과 절차를 보유하고 있다. 모든 가입자는 적어도 동 손상에 대해 가능한한 신속하게 통

보 받고 정보가 Entrust.net 저장소에 게재될 것이다.

4.9 CA 종료

Entrust.net SSL 웹 서버인증기관이 운영을 종료하는 경우, 동 기관이 발행한 모든 Entrust.net SSL 웹 서버인증서는 취소된다.

5. 물리적, 절차적, 인적 보안 통제

5.1 물리적 통제

Entrust/Authority 소프트웨어는 Entrust.net SSL 웹 서버인증기관의 소프트웨어 구성요소로 사용된다. Entrust.net SSL 웹 서버인증기관을 위한 하드웨어와 소프트웨어는 산업적 기준에 부합되거나 능가하는 물리적 보안 및 접근 통제 절차를 구비한 보안 설비 내에 위치된다. Entrust/Authority 소프트웨어가 있는 공간은 2인 지대로 지정되고 한 사람이 단독으로 동 공간에 있는 것을 방지하기 위해 통제된다. 경보 시스템이 보안직원에게 Entrust.net SSL 웹 서버 인증기관의 접근에 관한 규칙 위반사실을 통보하기 위해 사용된다.

5.2 절차적 통제

Entrust.net SSL 웹 서버 인증기관은 Entrust.net SSL 웹 서버인증기관 소프트웨어의 민감한 작동을 위해서 여러 신뢰성 있는 역할을 가지고 있다. Entrust.net SSL 웹 인증기관 내에 사용된 Entrust/Authority 소프트웨어에 접근하기 위해서 운영 직원은 신원 조사를 받는다. 행정 인원의 추가 또는 인증 기관 정책 변경에 관련된 Entrust.net SSL 웹 서버 인증기관 운영은 1인 이상의 운영인원이 요구된다.

5.3 인적 통제

Entrust.net SSL 웹 서버인증기관을 위한 운영 직원은 Entrust.net SSL 웹 서버인증기관에 대한 그들의 운영 책임과 충돌되는 다른 책임을 부여 받지 않는다. Entrust.net SSL 웹 서버인증기관을 위한 운영 직원에게 부여된 특권은 그들에게 할당된 의무를 수행하기 위해서 요구되는 최소한으로 제한된다.

6. 기술적 보안 통제

6.1 키 쌍 생성과 설치

6.1.1 키 쌍 생성

Entrust.net SSL 웹 서버인증기관을 위한 서명 키 쌍은 Entrust/Master 통제 신청서의 초기 개설시에 생성되고, Entrust.net SSL 웹 서버인증기관을 위한 마스터 키에 의해서 보호된다.

하드웨어 키 생성은 최소한 FIPS 140-1 level 3에 따라 사용된다.

6.1.2 실체에 대한 비밀키 전달

적용 안됨

6.1.3 인증서 발행인에 대한 공개키 전달

Entrust.net SSL 웹 서버인증서내에 포함되어 있는 공개키는 Entrust.net SSL 웹 서버인증서 신청 진행의 일부분으로서 인증서 서명 요구서(CSR)에 있는 Entrust.net SSL 웹 서버 기관에게 전달된다.

6.1.4. 사용자에게 CA 공개키 전달

Entrust.net SSL 웹 서버인증 기관에 대한 공개키 인증서는 GTE Corporation (“GTE”) 인증기관에 의해 교차 인증된다. GTE 인증기관을 위해 자체 서명된 공개키 인증서는 공통 월드와이드 웹 서버 브라우저와 웹 서버 소프트웨어에 소프트웨어 제조 업체에 의해 사전 설치된다.

6.1.5 키 사이즈

SSL 서버 키 사이즈는 가입자의 월드와이드 웹 서버 소프트웨어에 의해서 결정된다.

6.1.6 공개키 매개변수 생성

가입자의 월드와이드 웹 서버 소프트웨어 서버는 어떠한 공개키 매개변수가 사용될 지를 통제한다.

6.1.7 매개변수 품질 확인

공개키 매개변수의 품질은 매개변수를 생성하는 가입자의 월드와이드 웹 서버 소프트웨어에 의해서 결정된다. Entrust.net, Entrust.net SSL 웹 서버인증기관 하에 운영되는 독립적 제3등록기관, 재판매자, 공동판매자, 또는 앞에서 말한 자의 하도급계약자, 판매자, 대행인, 공급자, 고용인, 이사는 누구도 Entrust.net SSL 웹 서버인증서에 포함된 공개키의 품질에 대해서 어떠한 진술, 보증, 또는 조건을 제시하지 않는다

6.1.8 하드웨어/소프트웨어 키 생성

Entrust.net SSL 웹 서버인증서와 관련된 가입자의 키 쌍을 생성하는 방법은 오직 가입자의 통제하에 있으며 Entrust.net, Entrust.net SSL 웹 서버인증기관 하에 운영되는 독립적 제3등록기관, 재판매자, 공동판매자, 또는 앞에서 말한 자의 하도급계약자, 판매자, 대행인, 공급자, 고용인, 이사는 누구도 가입자의 키 쌍 생성을 위한 책임과 의무를 갖지 않는다.

6.1.9 키 사용 목적

Entrust.net SSL 웹 서버인증기관에 의해 발행된 Entrust.net SSL 웹 서버인증서는 Entrust.net SSL 웹 서버인증서가 사용될 수 있는 용도를 제한하는 키사용과 확장키 사용 인증서 확장을 포함한다. 가입자와 신뢰당사자는 Entrust.net SSL 웹 서버인증서 업무 준칙과 해당 법률을 준수하여 Entrust.net SSL 웹 서버인증서를 사용해야 한다.

6.2 비밀 키 보호

Entrust.net SSL 웹 서버인증기관은 Entrust.net SSL 웹 서버인증기관의 비밀키를 보호하기 위해서 FIPS 140-1 레벨 3로 인증된 하드웨어와의 연계하여 Entrust/Authority 소프트웨어를 사용한다. 가입자는 가입자의 Entrust.net SSL 웹 서버인증서내에 있는 공개키와 연관된 비밀키를 보호할 책임을 진다. Entrust.net는 Entrust.net SSL 웹 서버인증기관의 비밀키를 보관 (escrow)하지 않는다.

6.3 키 쌍 관리의 다른 측면

규정 없음

6.4 활성화 데이터

규정 없음

6.5 컴퓨터 보안 통제

Entrust.net SSL 웹 서버인증기관이 운영되는 워크스테이션은 이 Entrust.net SSL 웹 서버 실무 준칙 5.1항에 규정된 것처럼 물리적으로 안전하다. Entrust.net SSL 웹 서버인증기관이 운영되는 워크스테이션의 운영 시스템은 사용자 신원 및 검증을 집행한다. Entrust/Authority 소프트웨어 데이터 베이스와 감사기록파일에 대한 접근은 Entrust.net SSL 웹 서버인증실무준칙 내에 규정된 바에 따라 제한된다. Entrust.net SSL 웹 서버인증기관에게 접근하도록 하는 권한을 부여 받은 모든 운영 인원은 동 기관을 위해 사용되는 Entrust/Authority 소프트웨어를 포함하고 있는 물리적인 공간에 대해 접근을 하기 위해 PIN과 함께 하드웨어 토큰을 사용하도록 요구된다.

6.6 인증서 유효기간 기술적 통제

Entrust.net SSL 웹 서버인증실무준칙에 규정된 보안 환경의 효과와 타당성은 매년 검토된다. 시스템 보안을 유지하기 위한 목적으로 키의 길이를 증가시키거나 운영상 절차의 수정이 필요한 지의 여부를 결정하기 위해서 위험 및 위협에 대한 평가가 수시로 수행될 것이다.

6.7 네트워크 보안 통제

Entrust/Authority 소프트웨어 인터페이스를 통한 Entrust/Authority 소프트웨어에 대한 원격

접근은 안전 교환 프로토콜과 Entrust/Session 소프트웨어의 보안 기능을 사용함으로써 보호된다.

6.8 암호화 모듈 공학적 통제

Entrust/Authority 소프트웨어 암호화 모듈은 FIPS 140-1 레벨1 요구에 적합하도록 설계된다. 선택적 하드웨어 토큰은 보다 높은 수준의 FIPS 확인에 일치할 키 쌍을 생성하는데 사용된다. 그러나 그것은 적어도 레벨 1과 일치해야만 한다.

7. 인증서와 CRL 프로파일

7.1 인증서 프로파일

Entrust.net SSL 웹 서버인증기관에 의해 발행된 Entrust.net SSL 웹 서버인증서에 대한 프로파일은 SSL(보안 소켓 레이어) 프로토콜 사양에 일치한다.

7.2 CRL 프로파일

다음의 X.509 버전 2 CRL 포맷이 Entrust.net SSL 웹 서버인증기관에 의해 사용된다.

버전 : v2로 설정

서명 : CRL을 사인하기 위해 사용되는 알고리즘의 확인자

발행자 : CRL을 발행하는 인증기관의 완전한 DN (고유 명칭)

이번 개정 : CRL 발행 시간

다음 개정 : 다음 CRL 개정의 예정 시간

취소된 인증서 : 취소된 인증서 정보 목록

8. 내역 관리

8.1 연락 정보

Director Operations, Entrust.net Inc.

Entrust.net Inc

1000 Innovation Drive

Ottawa, Ontario

Canada K2K 3E7

전화 : (613) 270-3157

이메일 : entrust.OA@entrust.net

8.2 내역 변경 절차

Entrust.net는 수시로 Entrust.net SSL 웹 서버인증실무준칙과 그 조건들을 스스로의 판단에 따라 수정할 수 있다. Entrust.net 판단에 따라 신청자, 가입자 그리고 신뢰당사자에 대해 영향을 주지 않거나 거의 주지 않을 것으로 보이는 Entrust.net SSL 웹 서버인증실무준칙에 대한 수정은 Entrust.net SSL 웹 서버인증실무준칙의 버전 번호를 변경하지 않고 신청자, 가입자 그리고 신뢰당사자에 대한 통지 없이 이루어질 수 있다. 동 변경은 Entrust.net 저장소에 공표하는 즉시 유효하다.

Entrust.net 판단으로 신청자, 가입자 그리고 신뢰당사자에게 중대한 영향을 줄 수 있는 Entrust.net SSL 웹 서버인증실무준칙에 대한 수정은 Entrust.net 저장소에 공표되며 Entrust.net가 위와 같이 수정된 Entrust.net SSL 웹 서버인증실무준칙을 유효일 전에 취소하지 않는 한 Entrust.net 저장소에 공표된 지 15일 후 효력을 갖는다. Entrust.net가 Entrust.net SSL 웹 서버인증실무준칙에 대한 중요한 수정을 하는 경우 Entrust.net SSL 웹 서버인증실무준칙의 버전 번호가 그에 상응하게 변경될 것이다. 만약 가입자가 개정된 버전의 Entrust.net SSL 웹 서버인증실무준칙이 유효화 되기 이전에 가입자의 Entrust.net SSL 웹 서버인증서를 사용중지하거나 제거하거나 또는 취소 요청을 하지 않는다면, 동 가입자는 개정된 버전의 Entrust.net SSL 웹 서버인증실무준칙의 조건에 동의한 것으로 간주되며 동 개정된 버전의 Entrust.net SSL 웹 서버 인증 준칙 규약의 조건에 구속된다.

8.3 발행과 통지 정책

Entrust.net SSL 웹 서버인증실무준칙에 대한 주요 변경 이전에 추후 변경에 대한 통지는 Entrust.net 저장소에 게재된다.

8.4 CPS 승인 절차

Entrust.net SSL 웹 서버인증실무준칙과 추후의 변경은 Entrust.net 정책 기관에 의해서 승인된다.

9. 약자

CA	인증 기관
CPS	인증 실무 준칙
CRL	인증서 취소 목록
CSR	인증서 서명 요청서
DN	고유명칭
DNS	도메인 이름 서버
DSA	전자 서명 알고리즘
HTTP	하이퍼텍스트 전달 프로토콜

IETF	인터넷 공학 업무팀
ITU-T	국제 통신 연합-통신 표준화 부문
MAC	메시지 확인 코드
OA	운영 기관
OID	객체 식별자
PA	정책 기관
PIN	개인 식별 번호
PKI	공개키 기반 구조
RA	등록기관
RDN	상대적 고유명칭
RFC	설명문 요구
SEP	보안 교환 프로토콜
SSL	보안 소켓 레이어
URL	Universal Resource Locator

10.정의

제휴업체: Entrust 그리고 Entrust가 직/간접적으로 통제하는 법인이나 다른 실체를 의미한다. 본문에서, 한 당사자가 이사회 또는 기타 통제 기구에서 50% 또는 그 이상의 의결권을 직, 간접적으로 소유하거나 통제한다면 동인은 그 법인 또는 다른 실체를 “통제한다.”

신청자 : Entrust.net SSL 웹 서버인증서를 신청하였으나 아직까지 Entrust.net SSL 웹 서버인증서를 받지 못한 개인, 실체 또는 기관, 또는 Entrust.net SSL 웹 서버인증서나 인증서들을 갖고 있으면서 갱신 신청 혹은 추가 신청한 개인, 실체, 또는 기관을 의미한다.

영업일 : 토요일, 일요일, 온타리오주 오타와시의 법정 또는 시의 공휴일을 제외한 날을 의미한다.

인증서 : 최소한 (a) 인증서를 발행하는 인증기관을 밝히고, (b) 주체를 명시하거나 달리 밝히며, (c) 키 쌍의 공개키를 포함하며, (d) 운영기간을 밝히며, (e) 일련 번호를 포함하고 있는 인증기관에 의해서 전자적으로 서명된 전자문서를 의미한다.

인증서 취소 목록 : 인증 기관이 전자적으로 서명한 취소된 인증서의 일련 번호를 가진 시간 검인이 된 목록을 의미한다.

인증 기관 : (1) 주체의 공개키 및 주체 확인을 위한 기타 정보를 포함하고 있는 인증서를

만들고 전자적으로 서명하며 (2) 인증서에서 확인된 주체와의 통신을 촉진시키기 위해 인증서를 이용가능하게 하고 (3) 취소되어 더 이상 사용하지 않거나 신뢰되지 않는 인증서에 대한 정보를 포함하는 인증서 취소목록을 만들고 전자적으로 서명하는 실체나 기관을 의미한다.

인증 실무 준칙 : 인증기관이 인증서에 대한 발행, 관리, 취소, 갱신, 접근을 가능하게 하는데 사용하는 관행서와 인증기관이 그러한 서비스를 이용하게 만들기 위한 조건을 의미한다.

공동판매자 : Entrust.net나 Entrust.net SSL 웹 서버인증기관이 운영하는 등록 기관에 의해 Entrust.net SSL 웹 서버인증서의 보급을 촉진시킬 권한을 부여받은 사람, 실체, 또는 기관을 의미한다.

손상 : 민감한 정보나 데이터에 대해 의심되거나 실질적인 상실, 누출, 또는 통제의 상실을 의미한다.

CPS : 인증 실무 준칙 참조

CRL : 인증서 폐기 목록 참조

Cross Certification(s) : 교차인증서는 (i)Entrust.net 인증기관이 발행하거나, Entrust.net 인증기관을 위한 공개/비밀 키쌍의 공개키를 포함하고; (ii)GTE Corporation("GTE") 또는 그의 계승회사에서 운영하는 인증기관의 디지털 서명을 포함하며; (iii)GTE 공개키 인증서를 사용하여 가입자의 SSL 인증서 공개키의 확인을 가능하게 하고; (iv)만료일이 2006년 2월 23일이나 그 이전으로 되어 있는 인증서를 의미한다.

Entrust.net : Entrust.net Inc.를 의미한다.

Entrust.net 운영 기관 : Entrust.net SSL 웹 서버인증기관의 운영에 책임이 있고 Entrust.net의 대리인으로 또는 이를 대표해서 일하는 인원을 의미한다.

Entrust.net 정책 기관 : Entrust.net SSL 웹 서버 인증기관의 운영을 관리하는 정책과 절차를 결정하는 책임이 있고 Entrust.net의 대리인으로 또는 이를 대표해서 일하는 인원을 의미한다.

Entrust.net 저장소 : Entrust.net SSL 웹 서버인증기관이 발행한 Entrust.net SSL 웹 서버인증서 형태, 동 인증서와 관련하여 Entrust.net가 제공하는 서비스, Entrust.net가 동 인증서 및

동 인증서에 관련한 서비스에 대하여 부과하는 비용, 인증서 취소 목록, Entrust.net SSL 웹 서버인증서 실무준칙 및 Entrust.net SSL 웹 서버인증서의 사용을 지배하는 기타 정보나 계약을 포함하여 동 인증서와 관련하여 Entrust.net가 제공하는 동 인증서 및 서비스에 대한 정보를 포함하고 있는 데이터베이스 및 웹사이트의 집합을 의미한다.

Entrust.net SSL 웹 서버인증기관 : Entrust.net SSL 웹 서버인증서 발행, 관리, 취소, 갱신, 접근 부여의 목적으로 Entrust.net에 의해 또는 이를 대리하여 운영되는 인증 기관을 의미한다.

Entrust.net SSL 웹 서버인증실무준칙 : 본 문서를 의미한다.

Entrust.net SSL 웹 서버 CPS : Entrust.net SSL 웹 서버인증실무준칙 참조

Entrust.net SSL 웹 서버인증서 : 월드와이드 웹 서버에 사용되기 위해 Entrust.net SSL 웹 서버인증기관에 의해 발행된 SSL 인증서를 의미한다.

Entrust.net SSL 웹 서버인증신청서 : Entrust.net SSL 웹 서버인증서 발행 신청시 Entrust.net SSL 웹 서버인증기관하에 운영되는 등록기관에 의해 요청된 그리고 신청자에 의해 제출된 형식과 신청 정보를 의미한다.

FIPS : 연방 정보 처리 기준을 의미한다. 이는 하드웨어, 소프트웨어, 데이터, 통신가동을 위한 특별 이행 요구, 준칙, 포맷, 통신 프로토콜 그리고 다른 요구들을 규정한 미국 연방 기준이다.

IETF : 인터넷 공학 업무팀을 의미한다. 인터넷 공학 업무팀은 인터넷 구조 발전과 효과적인 인터넷의 작동과 관련된 네트워크 디자이너, 운영자, 판매자, 연구자의 국제적 공동체이다.

키 쌍 : 두개의 수학적으로 관련된 암호화된 키이며 다음과 같은 특성을 갖고 있다. (i) 한쪽의 키는 메시지를 암호화하기 위해 사용되며 그 메시지는 다른 쪽 키를 사용해야만 해독 될 수 있고, (ii) 한쪽 키를 알고 있다고 하더라도 다른 쪽 키를 발견하기는 계산적으로 불가능하다.

Object Identifier (객체 식별자) : 객체 식별자 등록을 위해 국제적으로 인정되는 절차에 따라 등록된 특별히 포맷된 숫자의 순서를 의미한다.

OID : 객체 식별자 참조

운영기간 : 인증서와 관련하여 유효기간을 의미한다. 운영기간은 전형적으로 인증서가 발행되는 날짜(또는 인증서에 규정된 것과 같은 이후의 날짜)부터 시작되고 인증서에 언급된 것과 같은 날짜와 시간에, 인증서가 취소될 경우 그 이전에 각 종료한다.

PKIX : X.509 버전 3 인증서에 기반한 PKI 구성요소를 위한 기술 내역을 개발하는 IETF 운영 그룹을 의미한다.

비밀키 : 암호화된 메시지를 판독하기 위해 사용되는 키 쌍 중 한 키를 의미한다. 이 키는 기밀로 유지되어야 한다.

공개키 : 메시지를 암호화하기 위해 사용되는 키 쌍 중 한 키를 의미한다. 공개키는 키 쌍 중에서 비밀키를 갖고 있는 사람에게 암호화된 메시지를 보내고자 하는 자가 자유롭게 사용할 수 있다. 공개키는 보통 인증기관에 의해서 발행된 인증서 내에 공개적으로 사용되도록 만들어져 있으며 종종 저장장소나 데이터베이스에 접근하여 얻어진다. 공개키는 상응하는 비밀키를 갖고 있는 사람에 의해서만 판독될 수 있는 메시지를 암호화하기 위해서 사용된다.

RA : 등록 기관 참조

등록기관 : 다음의 두가지 기능을 수행하는 존재를 의미한다. (1) 인증서내에 명명될 주체로부터의 정보 수령 및 (2) 주체가 제공하는 정보에 관하여 제3자 데이터베이스의 정보를 통한 제한된 검증 수행. 주체가 제공한 정보가 동 제3 자 데이터 베이스 내에 있는 정보와 상응하는 경우, 등록기관은 등록기관에 의해 검증된 정보를 포함하는 인증서를 인증기관이 생성하고, 전자적 서명을 하고, 발행하도록 요청하는 요청서를 보낸다.

신뢰당사자 : 가입자의 공개키를 획득하고 신원을 확인하기 위해 Entrust.net SSL 웹 서버인증서 또는 Entrust.net SSL 웹 서버인증기관하의 저장 장소 내에 제공된 기타 정보를 사용하거나 신뢰하는 개인, 단체, 또는 기관을 의미한다.

신뢰당사자 계약서 : Entrust.net SSL 웹 서버인증서와 관련하여 특정한 정보와 서비스의 제공과 사용에 관한 신뢰당사자와 Entrust.net 또는 신뢰당사자와 독립된 제3 인증 기관 또는 Entrust.net, SSL 웹 서버인증기관하의 재판매자 간의 계약을 의미한다.

저장소 : 인증기관이 발행한 인증서에 관한 정보가 포함되어 있는 데이터 베이스와 웹사이트의 집합을 의미한다. 그것은 인증기관이 발행한 인증서와 서비스의 형태, 인증기관이 발행한 인증서와 서비스의 비용, 인증서 취소 목록, 인증기관의 준칙과 절차의 서술 및 인증

기관이 발행한 인증서의 사용을 지배하기 위한 다른 정보나 계약등을 포함한다.

재판매자 : Entrust.net 또는 Entrust.net SSL 웹 서버인증기관하에서 운영되고 있는 등록기관으로부터 Entrust.net SSL 웹 서버인증서 사용권한에 대한 허가권을 부여받은 사람, 단체, 또는 기관을 의미한다.

취소 : 인증서와 관련하여 인증서의 운영기간을 앞서서 특정 시간으로부터 장래에 대하여 그 효력을 종료시키는 것을 의미한다.

주체 : 인증서에 포함되어 있는 공개키를 소유한 사람, 단체, 또는 기관을 의미한다.

가입자 : Entrust.net SSL 웹 서버인증서를 신청하여 발행받았던 사람, 단체, 또는 기관을 의미한다.

가입자 계약 : Entrust.net SSL 웹 서버인증서의 발행, 관리, 접근 제공 및 기타 Entrust.net SSL 웹 서버인증서와 관련된 다른 서비스의 제공과 관련, 가입자와 Entrust.net 또는 가입자와 독립된 제3의 등록기관 또는 Entrust.net SSL 웹 서버인증기관의 재판매자 사이의 계약을 의미한다.