(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2011년08월05일
(11) 등록번호 10-1054970
(24) 등록일자 2011년08월01일

(51) Int. Cl.
H04W 12/06 (2009.01) *H04L 9/14* (2006.01)
H04W 12/04 (2009.01) *H04L 9/32* (2006.01)
(21) 출원번호 10-2009-7008495
(22) 출원일자(국제출원일자) 2007년10월24일
심사청구일자 2009년05월20일
(85) 번역문제출일자 2009년04월24일
(65) 공개번호 10-2009-0075705
(43) 공개일자 2009년07월08일
(86) 국제출원번호 PCT/JP2007/070706
(87) 국제공개번호 WO 2008/050792
국제공개일자 2008년05월02일
(30) 우선권주장
JP-P-2006-293253 2006년10월27일 일본(JP)
(56) 선행기술조사문헌
US06189096 B1*
US06367009 B1*
WO2005125084 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
인터내셔널 비지네스 머신즈 코포레이션
미국 10504 뉴욕주 아몬크 뉴오차드 로드
(72) 발명자
오카모토 고스케
일본 가나가와켄 야마토시 시모츠루마 1623반치 14 일본 아이비엠 주식회사 야마토 지교쇼 내
미야모토 다카시
일본 가나가와켄 야마토시 시모츠루마 1623반치 14 일본 아이비엠 주식회사 야마토 지교쇼 내
(74) 대리인
제일특허법인, 장성구, 김원준

전체 청구항 수 : 총 10 항 심사관 : 장상배

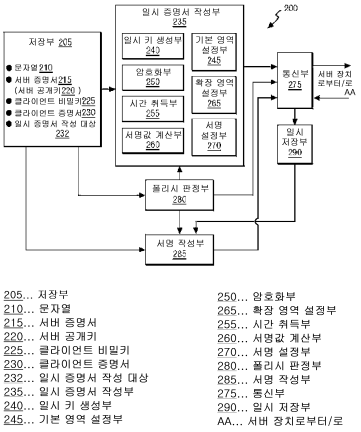
(54) 개인 정보를 포함하는 전자 증명서를 이용하여 통신 상대를 인증하기 위한 시스템, 장치, 방법, 및 컴퓨터 판독 가능한 기록 매체

(57) 요 약

[과제] 개인 정보를 포함하는 전자 인증서를 이용하여, 통신 상대를 인증하기 위한 기술을 제공.

[해결 수단] 클라이언트 장치는, 서버 장치로부터 전자 증명서의 요구를 수신하면, 저장부로부터 개인 정보를 포함하는 클라이언트 증명서 및 서버 장치의 서버 공개키를 판독하고, 서버 공개키를 이용하여 클라이언트 증명서를 암호화한다. 클라이언트 장치는 또한 전자 증명서의 기본 영역에 해당 전자 증명서가 일시 디지털 증명인 것을 나타내는 소정 사항을 설정하고, 또한 전자 증명서의 확장 영역에 암호화된 클라이언트 증명서를 설정함으로써, 일시 전자 증명서를 작성한다. 그리고 클라이언트 장치는 일시 전자 증명서를 서버 장치에 송신한다.

대 표 도



특허청구의 범위

청구항 1

개인 정보를 포함하는 전자 증명서를 이용하여 통신 상대를 인증하는 방법으로서,

클라이언트 장치에서,

서버 장치로부터 전자 증명서의 요구를 수신하는 단계와,

상기 요구의 수신에 응답하여, 개인 정보를 포함하는 클라이언트 증명서 및 상기 서버 장치의 서버 공개키를 상기 클라이언트 장치의 저장부로부터 판독하는 단계와,

상기 서버 공개키를 이용하여 상기 클라이언트 증명서를 암호화하는 단계와,

상기 서버 장치가 지원하는 포맷의 전자 증명서의 제 1 영역에 해당 전자 증명서가 일시 전자 증명서인 것을 나타내는 판정 정보를 설정하고, 또한 상기 전자 증명서의 제 2 영역에 암호화된 상기 클라이언트 증명서를 설정함으로써, 일시 전자 증명서를 작성하는 단계와,

상기 일시 전자 증명서를 서버 장치로 송신하는 단계를 포함하고,

상기 서버 장치에서,

전자 증명서를 수신하는 단계와,

수신한 상기 전자 증명서의 상기 제 1 영역으로부터 상기 판정 정보를 인출하는 단계와,

상기 판정 정보가, 수신한 상기 전자 증명서가 상기 일시 전자 증명서인 것을 나타내는지 여부를 판정하는 단계와,

수신한 상기 전자 증명서가 상기 일시 전자 증명서라고 판정한 경우, 상기 일시 전자 증명서의 상기 제 2 영역으로부터 암호화된 상기 클라이언트 증명서를 인출하는 단계와,

인출한 상기 클라이언트 증명서를 상기 서버 공개키에 대응하는 서버 비밀키를 이용하여 복호하는 단계와,

복호한 상기 클라이언트 증명서를 이용하여 상기 클라이언트 장치를 인증하는 단계를 포함하는

통신 상대를 인증하는 방법.

청구항 2

제 1 항에 있어서,

상기 서버 장치에서, 수신한 상기 전자 증명서가 상기 일시 전자 증명서가 아니라고 판정한 경우, 수신한 상기 전자 증명서를 이용하여 상기 클라이언트 장치를 인증하는 단계를 더 포함하는

통신 상대를 인증하는 방법.

청구항 3

제 1 항에 있어서,

상기 클라이언트 장치에서,

상기 제 2 영역에, 소정의 문자열과, 상기 소정의 문자열의 해시값을 상기 클라이언트 증명서에 포함된 클라이언트 공개키에 대응하는 클라이언트 비밀키를 이용하여 암호화한 서명값을 더 설정하는 단계를 더 포함하고,

상기 서버 장치에서,

수신한 상기 전자 증명서가 상기 일시 전자 증명서라고 판정한 경우에, 상기 일시 전자 증명서의 상기 제 2 영역에 포함된 상기 소정의 문자열로부터 구한 해시값과, 상기 일시 전자 증명서의 상기 제 2 영역에 기재된 상기 서명값을 상기 클라이언트 증명서로부터 인출한 상기 클라이언트 공개키를 이용하여 복호함으로써 획득한 값을 비교하는 것에 의해 통신 상대가 상기 클라이언트 증명서의 소유자 본인인 것을 확인하는 단계를 더 포함하는

통신 상대를 인증하는 방법.

청구항 4

제 1 항에 있어서,

상기 클라이언트 장치에서,

상기 클라이언트 장치 상의 현재 시각을 취득하는 단계와,

상기 제 2 영역에, 소정의 문자열, 상기 현재 시각을 나타내는 서명 시각, 및 상기 소정의 문자열 및 상기 서명 시각의 해시값을 상기 클라이언트 증명서에 포함되는 클라이언트 공개키에 대응하는 클라이언트 비밀키를 이용하여 암호화함으로써 획득한 서명값을 더 설정하는 단계를 더 포함하고,

상기 서버 장치에서,

수신한 상기 전자 증명서가 상기 일시 전자 증명서라고 판정한 경우에, 상기 일시 전자 증명서의 상기 제 2 영역에 기재된 상기 소정의 문자열 및 상기 서명 시각으로부터 획득되는 해시값과, 상기 일시 전자 증명서의 상기 제 2 영역에 기재된 상기 서명값을 상기 클라이언트 증명서로부터 인출한 상기 클라이언트 공개키를 이용하여 복호함으로써 획득되는 값을 비교하는 것에 의해, 통신 상대가 상기 클라이언트 증명서의 소유자 본인인 것을 확인하는 단계를 더 포함하는

통신 상대를 인증하는 방법.

청구항 5

클라이언트 장치에서 실행되는, 개인 정보를 포함하는 전자 증명서를 이용하여 통신 상대를 인증하기 위한 방법으로서,

서버 장치로부터 전자 증명서의 요구를 수신하는 단계와,

상기 요구의 수신에 응답하여, 개인 정보를 포함하는 클라이언트 증명서 및 상기 서버 장치의 서버 공개키를 저장부로부터 판독하는 단계와,

상기 서버 공개키를 이용하여 상기 클라이언트 증명서를 암호화하는 단계와,

상기 서버 장치가 지원하는 포맷의 전자 증명서의 제 1 영역에 상기 전자 증명서가 일시 전자 증명서인 것을 나타내는 판정 정보를 설정하고, 또한 상기 전자 증명서의 제 2 영역에 암호화된 상기 클라이언트 증명서를 설정함으로써, 일시 전자 증명서를 작성하는 단계와,

상기 일시 전자 증명서를 상기 서버 장치로 송신하는 단계를 포함하는

통신 상대 인증을 위한 방법.

청구항 6

서버 장치에서 실행되는, 개인 정보를 포함하는 전자 증명서를 이용하여 통신 상대를 인증하기 위한 방법으로서,

클라이언트 장치에 대하여 개인 정보를 포함하는 클라이언트 장치의 전자 증명서를 요구하는 단계와,

상기 클라이언트 장치로부터 상기 클라이언트 장치의 전자 증명서를 수신하는 단계와,

수신한 상기 전자 증명서의 제 1 영역으로부터 판정 정보를 인출하는 단계와,

상기 판정 정보가, 수신한 상기 전자 증명서가 개인 정보를 포함하는 일시 전자 증명서인 것을 나타내는지 여부를 판정하는 단계와,

수신한 상기 전자 증명서가 상기 일시 전자 증명서가 아니라고 판정된 경우, 수신한 상기 전자 증명서를 이용하여 상기 클라이언트 장치를 인증하는 단계와,

수신한 상기 전자 증명서가 상기 일시 전자 증명서라고 판정된 경우, 수신한 상기 전자 증명서의 제 2 영역으로부터 상기 서버 장치의 서버 공개키를 이용하여 암호화된 클라이언트 증명서를 인출하는 단계와,

암호화된 상기 클라이언트 증명서를 상기 서버 공개키에 대응하는 서버 비밀키를 이용하여 복호하는 단계와,

복호한 상기 클라이언트 증명서를 이용하여 상기 클라이언트 장치를 인증하는 단계를 포함하는

통신 상대 인증을 위한 방법.

청구항 7

개인 정보를 포함하는 전자 증명서를 이용하여 통신 상대를 인증하기 위한 시스템으로서,

클라이언트 장치와 서버 장치를 포함하되,

상기 클라이언트 장치는

상기 서버 장치로부터 전자 증명서의 요구를 수신하는 수신부와,

개인 정보를 포함하는 클라이언트 증명서 및 상기 서버 장치의 서버 공개키를 저장하는 저장부와,

상기 요구의 수신에 응답하여, 상기 저장부로부터 판독한 상기 서버 공개키를 이용하여 상기 클라이언트 증명서를 암호화하는 암호화부와,

상기 서버 장치가 지원하는 포맷의 전자 증명서의 제 1 영역에 상기 전자 증명서가 일시 전자 증명서인 것을 나타내는 판정 정보를 설정하고, 또한 상기 전자 증명서의 제 2 영역에 암호화된 상기 클라이언트 증명서를 설정하여, 일시 전자 증명서를 작성하는 작성부와,

상기 일시 전자 증명서를 서버 장치에 송신하는 송신부를 포함하며,

상기 서버 장치는

상기 서버 공개키에 대응하는 서버 비밀키를 저장하는 저장부와,

전자 증명서를 수신하는 수신부와,

수신한 상기 전자 증명서의 상기 제 1 영역으로부터 인출한 상기 판정 정보가, 수신한 상기 전자 증명서가 일시 전자 증명서인 것을 나타내는지 여부를 판정하는 판정부와,

상기 판정부가 일시 전자 증명서라고 판정하는 것에 응답하여, 수신한 상기 전자 증명서의 상기 제 2 영역으로부터 암호화된 상기 클라이언트 증명서를 인출하고, 상기 클라이언트 증명서를 상기 저장부로부터 판독한 서버 비밀키를 이용하여 복호하는 복호부와,

수신한 상기 전자 증명서가 일시 전자 증명서라고 상기 판정부가 판정한 경우, 상기 복호부에 의해 복호된 상기 클라이언트 증명서를 이용하여 클라이언트 장치를 인증하는 인증부를 포함하는

통신 상대를 인증하기 위한 시스템.

청구항 8

개인 정보를 포함하는 전자 증명서를 이용하여 통신 상대를 인증하기 위한 클라이언트 장치로서,

서버 장치로부터 전자 증명서의 요구를 수신하는 수신부와,

개인 정보를 포함하는 클라이언트 증명서 및 상기 서버 장치의 서버 공개키를 저장하는 저장부와,

상기 요구의 수신에 응답하여, 상기 저장부로부터 판독한 상기 서버 공개키를 이용하여 상기 클라이언트 증명서를 암호화하는 암호화부와,

상기 서버 장치가 지원하는 포맷의 전자 증명서의 제 1 영역에 상기 전자 증명서가 일시 전자 증명서인 것을 나타내는 판정 정보를 설정하고, 또한 상기 전자 증명서의 제 2 영역에 암호화된 상기 클라이언트 증명서를 설정함으로써, 일시 전자 증명서를 작성하는 작성부와,

상기 일시 전자 증명서를 서버 장치에 송신하는 송신부를 포함하는

통신 상대를 인증하기 위한 클라이언트 장치.

청구항 9

개인 정보를 포함하는 전자 증명서를 이용하여 통신 상대를 인증하기 위한 서버 장치로서,

서버 공개키에 대응하는 서버 비밀키를 저장하는 저장부와,

클라이언트 장치로부터 개인 정보를 포함하는 클라이언트 장치의 전자 증명서를 수신하는 수신부와,

수신한 상기 전자 증명서의 제 1 영역으로부터 인출한 판정 정보가, 수신한 상기 전자 증명서가 일시 전자 증명서인 것을 나타내는지 여부를 판정하는 판정부와,

상기 판정부가 일시 전자 증명서라고 판정하는 것에 응답하여, 수신한 상기 전자 증명서의 제 2 영역으로부터 암호화된 클라이언트 증명서를 인출하고, 상기 저장부로부터 판독한 서버 비밀키로 상기 클라이언트 증명서를 복호하는 복호부와,

수신한 상기 전자 증명서가 상기 일시 전자 증명서가 아니라고 상기 판정부가 판정할 경우, 수신한 상기 전자 증명서를 이용하여 상기 클라이언트를 인증하고, 일시 전자 증명서라고 상기 판정부가 판정할 경우, 상기 복호부에 의해 복호된 상기 클라이언트 증명서를 이용하여 상기 클라이언트 장치를 인증하는 인증부를 포함하는

통신 상대를 인증하기 위한 서버 장치.

청구항 10

제 1 항, 제 5 항 또는 제 6 항 중 어느 한 항에 따른 방법의 단계를 수행하기 위한 프로그램 코드 수단을 포함하는

컴퓨터 판독 가능한 기록 매체.

명 세 서

기 술 분 야

[0001] 본 발명은 전자 증명서를 사용한 통신 상대의 인증에 관한 것으로서, 특히 개인 정보를 포함하는 전자 증명서를 이용하여 통신 상대를 인증하는 기술에 관한 것이다.

배 경 기 술

[0002] 종래, 전자 상거래나 온 라인 뱅킹 등의 보안 통신이 요구되는 서버-클라이언트형 데이터 통신에서는, SSL(Secure Socket Layer) 및 그 후계 기술이며 RFC2246으로서 IETF(Intemet Engineering Task Force)에서 표준화된 TLS(Transport Layer Security)가 널리 이용되고 있다.

[0003] SSL/TLS의 핸드쉐이크 프로토콜에서는, 암호화 통신의 개시에 앞서, 서버-클라이언트 사이에서 암호화 통신을 시작하기 위해서 필요한 각종 파라미터의 협상이 행하여진다. 핸드쉐이크 프로토콜(Handshake Protocol)에서는, 최초로 상대의 인증이 행하여지고, 그 후 클라이언트와 서버의 양자가 공통으로 이용할 수 있는 압축/암호화 알고리즘으로부터 최적인 알고리즘의 이용이 결정된다. 핸드쉐이크 프로토콜에 의한 협상이 정상적으로 종료되면, 이후 서버-클라이언트 사이에서 암호화 통신이 개시된다.

[0004] 여기서, 핸드쉐이크 프로토콜에서의 상대 인증을, 서버 장치가 클라이언트 장치를 인증하는 경우를 예로 설명한다. 공개키 암호 방식을 이용하는 핸드쉐이크 프로토콜의 상대 인증에서는, 서버 장치로부터의 증명서 요구 메시지에 응답하여, 클라이언트 장치가, 자신의 전자 증명서를 클라이언트 증명서(Client Certicicate) 메시지의 본체에 포함시켜서 서버 장치에 송신한다. 전자 증명서를 수취한 서버 장치는, 그 정당성을, 보유하는 루트 인증국(C(A))의 키를 이용하여 확인한다. 전자 증명서에는 또한, 공개키 외에, 해당 공개키에 대응하는 비밀키의 소유자(전자 증명서의 발행 상대) 정보, 공개키의 유효 기한 등의 서지 정보가 기재된다. 그래서 서버 장치는, 그러한 서지 정보를 참조해서 클라이언트 장치가 적당한 통신 상대인 것을 확인한다.

[0005] 다음에 클라이언트 장치는, 핸드쉐이크 프로토콜의 개시 메시지인 클라이언트 헬로(Client Hello) 메시지로부터 클라이언트 키 교환(Client Key Exchange) 메시지까지의 통신 내용의 요약(digest)을 클라이언트 장치의 비밀키로 암호화해서 서명을 작성하고, 이것을 증명서 검증(Certificate Verify) 메시지의 본체에 포함시켜서 서버 장

치에 송신한다. 서버 장치는, 증명서 검증 메시지의 본체에 포함되는 정보를 클라이언트 장치의 전자 증명서에 기재되는 공개키로 복호함으로써, 현재의 통신 상대가 전자 증명서의 소유자 본인인 것을 확인한다(비특허 문헌 1 참조).

[0006] 이와 같이, SSL/TLS가 제공하는 상대 인증의 기능은 매우 엄밀한 것이며, 타인에 의한 가장이나 변경이 중대한 문제가 되는 전자 정부, 전자 자치체에 최적인 인증 방식이라고 할 수 있다. 그런데, 전자 정부·전자 자치체의 기반으로서, 최근 공적 개인 인증 서비스가 개시되었다(비특허 문헌 2 참조). 공적 개인 인증 서비스라는 것은, 행정 기관이 제공하는 전자 신청·신고 서비스를 이용할 때에 사용할 수 있는 전자 증명서를, 도도부현 지사가 발행하는 서비스다. 전자 증명서의 발행은, 전국 어디에 살고 있는 사람에 대해서도 저렴한 비용으로 행하여진다. 따라서, 공적 개인 인증 서비스에 의해 발행되는 전자 증명서를 SSL/TLS의 클라이언트 증명서로서 사용하는 것이 요구된다.

[0007] 비특허 문헌 1 : T.Dierks, E.Rescorla, "The Tansport Layel Security(TLS) Protocol", [online], 평성 16년 4월, RFC4346, [평성 18년 9월 22일 검색], 인터넷 <URL:http://www.ietf.org/rfc/rfc4346.txt>

[0008] 비특허 문헌 2 : "공적 개인 인증 서비스 포털 사이트", [online], 평성 16년 1월 29일(사이트 개설), 공적 개인 인증 서비스 도도부현 협의회, [평성 18년 9월 22일 검색], 인터넷 <URL:http://www.jpki.go.jp/index1.html>

발명의 상세한 설명

[0009] (발명의 개시)

[0010] (발명이 해결하고자 하는 과제)

[0011] 그러나, 공적 개인 인증 서비스에 의해 발행되는 전자 증명서에는, 주민 기본 대장에 기록된 성명, 주소, 생년월일, 성별이 공개키의 소유자 정보로서 기재되어 있다. 그 때문에, 이것을 SSL/TLS의 클라이언트 증명서로서 사용하면, 상술한 바와 같이 SSL/TLS에서는 암호화 통신의 개시에 앞서 상대 인증이 행하여지기 위해서, 성명, 주소라는 개인 정보가 암호화되지 않고 그대로 송신되어버린다. 또, 전자 증명서의 규격으로서는, ITU(International Telecommunication Union)가 권고한 X.509이 있다. X.509는 SSL/TLS에서도 채용되고 있어 표준 사양으로 되어 있지만, 이 규격에는 기재 정보를 안전하게 송신할 수 있는 기구는 포함되어 있지 않다.

[0012] 그래서, 본 발명은, 개인 정보를 포함하는 전자 증명서를 이용한 통신 상대의 인증에 있어서, 도청 등의 개인 정보로의 부정 액세스를 방지하는 통신 상대의 인증 방법, 장치, 시스템 및 프로그램을 제공하는 것을 목적으로 한다. 본 발명의 또 하나의 목적은, 개인 정보를 포함하는 전자 증명서를 이용한 안전한 통신 상대의 인증에 있어서, 종래의 통신 상대의 인증 방법과 호환성을 유지하는 것이다.

[0013] (과제를 해결하기 위한 수단)

[0014] 상기의 목적을 달성하는 본 발명은, 다음과 같은 개인 정보를 포함하는 전자 증명서를 이용하여 통신 상대를 인증하기 위한 방법에 의해 실현된다. 이 방법은, 클라이언트 장치가 서버 장치로부터 전자 증명서의 요구를 수신하는 것으로부터 개시된다. 요구의 수신에 응답하여, 클라이언트 장치는, 저장부로부터 개인 정보를 포함하는 클라이언트 증명서와 서버 장치의 서버 공개키를 판독하고, 서버 공개키를 이용하여 개인 정보를 포함하는 클라이언트 증명서를 암호화한다. 그리고 클라이언트 장치는 서버 장치가 지원하는 포맷의 전자 증명서의 제 1 영역에 해당 전자 증명서가 일시 전자 증명서인 것을 나타내는 판정 정보를 설정하고, 또한 제 2 영역에 암호화된 클라이언트 증명서를 설정함으로써, 일시 전자 증명서를 작성한다. 일시 전자 증명서를 작성할 수 있으면, 클라이언트 장치는 이것을 서버 장치에 송신한다.

[0015] 전자 증명서의 수신에 응답하여, 서버 장치는 수신한 전자 증명서의 제 1 영역으로부터 판정 정보를 인출한다. 그리고 서버 장치는, 판정 정보가 수신한 전자 증명서가 일시 전자 증명서인 것을 나타내는지 여부를 판정한다. 수신한 전자 증명서가 일시 전자 증명서가 아니라고 판정된 경우, 서버 장치는 수신한 전자 증명서를 이용하여 클라이언트 장치를 인증한다. 한편, 수신한 전자 증명서가 일시 전자 증명서라고 판정된 경우, 서버 장치는 일시 전자 증명서의 제 2 영역에 기재되는 클라이언트 증명서를 이용하여 클라이언트 장치를 인증한다. 후자의 경우, 서버 장치는 전처리로서, 제 2 영역로부터 암호화된 클라이언트 증명서를 인출하고, 이것을 서버 공개키

에 대응하는 서버 비밀키를 이용하여 복호한다.

[0016] 클라이언트 증명서에 포함되는 개인 정보는, 성명, 주소, 생년월일, 성별, 회사명, 메일 어드레스 등, 개인을 특정할 수 있는 임의의 정보다. 개인 정보를 포함하는 클라이언트 증명서는, 공적 개인 인증 서비스에 의해 발행된 클라이언트의 전자 증명서로서 좋다. 이 경우 전자 증명서에는, 해당 전자 증명서에 기재된 공개키에 대응하는 비밀키의 소유자 정보로서, 주민 기본 대장에 기재된 성명, 주소, 생년월일, 성별이 기재된다.

[0017] 서버 장치가 지원하는 전자 증명서의 포맷은 X.509로서 좋다. 바람직하게는, 제 1 영역은 X.509 증명서의 기본 영역이며, 제 2 영역은 X.509 증명서의 확장 영역이다. 이 대신에, 서버 장치가 지원하는 포맷의 전자 증명서의 제 1 영역은 X.509 증명서의 확장 영역이며, 전자 증명서가 일시 전자 증명서인 것을 나타내는 판정 정보로서, 증명서 폴리시를 이용해도 좋다. 또한, 클라이언트 장치에서 수신되는 전자 증명서의 요구는, SSL(Secure Socket Layer) 또는 TLS(Transport Layer Security)의 핸드쉐이크 프로토콜의 증명서 요구 메시지로서 좋다.

[0018] 또, 클라이언트 장치는, 전자 증명서의 제 2 영역에, 소정의 문자열과, 해당 문자열의 해시값을 클라이언트 증명서에 포함되는 클라이언트 공개키에 대응하는 클라이언트 비밀키를 이용하여 암호화한 서명값을 더 추가로 설정해도 좋다. 이 경우, 서버 장치는 수신한 전자 증명서가 일시 전자 증명서라고 판정하는 것을 조건으로 하여, 일시 전자 증명서의 제 2 영역에 기재되는 문자열의 해시값을 더 구한다. 또, 서버 장치는 일시 전자 증명서의 제 2 영역에 기재되는 서명값을 클라이언트 증명서에 기재되는 클라이언트 공개키를 이용하여 복호한다. 그리고 이들 2개의 값이 일치하는지 여부를 판정함으로써, 서버 장치는 통신 상대가 클라이언트 증명서의 소유자 본인인 것을 확인한다.

[0019] 이 대신에, 클라이언트 장치는, 전자 증명서의 제 2 영역에, 소정의 문자열과, 현재 시각을 나타내는 서명 시각과, 소정의 문자열과 서명 시각의 해시값을 클라이언트 증명서에 포함되는 클라이언트 공개키에 대응하는 클라이언트 비밀키를 이용하여 암호화한 서명값을 더 추가로 설정해도 좋다. 현재 시각은 서명시에 클라이언트 장치 상에서 취득된다. 이 경우, 서버 장치는 수신한 전자 증명서가 일시 전자 증명서라고 판정하는 것을 조건으로 하여, 일시 전자 증명서의 제 2 영역에 기재되는 소정의 문자열과 서명 시각의 해시값을 더 구한다. 또한, 서버 장치는 일시 전자 증명서의 제 2 영역에 기재되는 서명값을 클라이언트 증명서에 기재되는 클라이언트 공개키를 이용하여 복호한다. 그리고 이들 2개의 값이 일치하는지 여부를 판정함으로써, 서버 장치는 통신 상대가 클라이언트 증명서의 소유자 본인인 것을 확인한다.

[0020] 바람직하게는, 서버 장치는, 수신한 전자 증명서가 일시 전자 증명서인 것을 조건으로 하여, 서버 장치 상에서 현재 시각을 취득한다. 그리고 서버 장치는, 과거에 사용된 본인 확인 정보의 재이용을 금지하기 위해, 현재 시각과 일시 전자 증명서의 제 2 영역에 기재되는 서명 시각의 차이를 구하고, 구한 차이가 허용 범위 내인지 여부를 판단한다.

[0021] 이상, 클라이언트 장치 및 서버 장치를 포함하는 시스템에서의, 통신 상대를 인증하기 위한 방법으로서 본 발명을 설명했지만, 본 발명은, 통신 상대를 인증하기 위한 시스템 또는 해당 시스템에 상기 방법을 실행시키기 위한 프로그램으로서 파악할 수도 있다. 또 본 발명은, 클라이언트 장치 또는 서버 장치에서의, 통신 상대를 인증하기 위한 방법 또는 해당 각 방법을 클라이언트 장치 또는 서버 장치에 실행시키기 위한 프로그램으로서 파악할 수도 있다. 또한, 본 발명은, 통신 상대를 인증하기 위한 클라이언트 장치 또는 서버 장치로서 파악할 수도 있다.

[0022] (발명의 효과)

[0023] 본 발명에 의하면, 개인 정보를 포함하는 전자 증명서를 이용한 통신 상대의 인증에서, 도청 등의 개인 정보로의 부정 액세스를 방지할 수 있다. 더욱이 본 발명의 통신 상대의 인증 기술을 이용하면, 종래의 통신 상대 인증 방법과의 호환성도 유지할 수 있다.

실 시 예

[0024] 이하, 본 발명을 실시하기 위한 최선의 형태를 도면에 근거해서 상세하게 설명하지만, 이하의 실시예는 청구의 범위에 따른 발명을 한정하는 것은 아니고, 또한 실시예 내에 설명되어 있는 특징의 조합 모두가 발명의 해결 수단에 필수적이라고 한정하는 것은 아니다. 또, 실시예의 설명의 전체를 통해서 동일한 요소에는 동일 번호를

부여하고 있다.

[0025] 도 1은, 본 발명의 일 실시예에 따른 통신 상대를 인증하기 위한 시스템(100)의 구성의 일 예를 나타낸다. 본 실시예에 따른 통신 상대를 인증하기 위한 시스템(100)는, 서버 장치(400)에서의 전자 증명서의 요구에 응답해서 클라이언트 장치(200)가 자신의 개인 정보를 포함하는 전자 증명서를 송신할 경우에, 도청 등에 의한 개인 정보로의 부정 액세스를 방지하면서, 종래의 통신 상대의 인증 방법과의 호환성을 유지하는 것을 목적으로 한다. 또, 본 실시예에서는, 종래의 통신 상대의 인증 방법은 SSL/TLS의 핸드쉐이크 프로토콜을 따른다.

[0026] 통신 상대를 인증하기 위한 시스템(100)는, 서버 장치(400)와의 통신을 요구하는 클라이언트 장치(200)와, 통신 상대를 인증하기 위해서 전자 증명서를 요구하는 서버 장치(400)를 포함한다. 클라이언트 장치(200)와 서버 장치(400)는, 인터넷 등의 네트워크(300)를 거쳐서 접속된다. 또, 클라이언트 장치(200)는, 자신을 증명하는 전자 증명서로서 개인 정보를 포함하는 클라이언트의 전자 증명서를 미리 취득하고 있는 것으로 한다.

[0027] SSL/TLS를 이용한 통신에서는, 통신 상대의 인증은 핸드쉐이크 프로토콜을 따르는 수속의 초기에 행하여진다. 서버 장치(400)는 우선, 서버 증명서를 포함하는 서버 증명서(Server Certificate) 메시지를 클라이언트 장치(200)에 송신한다. 서버 증명서에는 공개키 암호 방식을 따르는 서버의 공개키가 포함된다. 그 때문에 클라이언트 장치(200)는 이 시점에서 서버 공개키를 취득한다. 다음에 서버 장치(400)는 클라이언트 장치(200)에 클라이언트 증명서 메시지를 송신하여, 클라이언트 장치(200)에 전자 증명서를 요구한다. 요구를 수신한 클라이언트 장치(200)는, 자신의 저장부로부터 개인 정보를 포함하는 클라이언트 증명서와 서버 장치(400)의 서버 공개키를 판독하고, 개인 정보로의 부정 액세스를 막기 위해서 서버 공개키로 클라이언트 증명서를 암호화한다.

[0028] 암호화된 클라이언트 증명서는 그대로는 서버 장치(400)에서 전자 증명서로서 인식되지 않는다. 그 때문에 클라이언트 장치(200)는, 서버 장치(400)가 지원하는 전자 증명서의 포맷을 따르는 일시 전자 증명서를 작성한다. SSL/TLS는 전자 증명서의 포맷으로서 X.509를 채용한다. X.509에는 복수의 버전이 있고, 현재 가장 잘 이용되고 있는 버전3에는, 발행자 정보나 공개키 등의 기본 사항이 기재되는 기본 영역 이외에, 독자의 정보를 기재할 수 있는 확장 영역이 새롭게 마련되어 있다. 그래서 클라이언트 장치(200)는, X.509 증명서의 기본 영역 또는 확장 영역에 해당 전자 증명서가 일시 전자 증명서인 것을 나타내는 판정 정보를 설정하고, 또 X.509 증명서의 확장 영역에 암호화된 클라이언트 증명서를 설정함으로써, 일시 전자 증명서를 작성한다. 그리고 클라이언트 장치(200)는 클라이언트 증명서 메시지에 일시 전자 증명서를 포함해서 서버 장치(400)에 송신한다.

[0029] 서버 장치(400)는, 클라이언트 장치로부터 일시 전자 증명서가 포함된 클라이언트 증명서 메시지를 수신하고, 일시 전자 증명서의 기본 영역 또는 확장 영역으로부터 판정 정보를 인출한다. 그리고 서버 장치(400)는 판정 정보가, 수신한 전자 증명서가 일시 전자 증명서인 것을 나타내는지 여부를 판정한다. 수신한 전자 증명서가 일시 전자 증명서가 아니라고 판정된 경우, 서버 장치(400)는 수신한 전자 증명서를 이용하여 클라이언트 장치를 인증한다. 한편, 수신한 전자 증명서가 일시 전자 증명서라고 판정된 경우, 서버 장치(400)는, 일시 전자 증명서의 확장 영역으로부터 암호화된 클라이언트 증명서를 인출하고, 이것을 서버 공개키에 대응하는 서버 비밀키로 복호한다. 그래서 서버 장치(400)는 복호한 클라이언트 증명서를 이용하여 클라이언트 장치를 인증한다.

[0030] 이상과 같이 클라이언트 장치(200)는, 서버 장치(400)가 지원하는 포맷의 전자 증명서 내에 자신을 증명하는 참된 전자 증명서를 설정하므로, 개인 정보를 포함하는 클라이언트 증명서를 암호화해서 송신하는 것이 가능해지고, 제삼자에 의한 개인 정보로의 부정 액세스가 방지된다. 또한, 서버 장치(400)는, 소정의 영역에 기재되는 판정 정보에 의해 수신한 전자 증명서가 일시 전자 증명서인지 여부를 판정하므로, 판정 결과에 따라 상대 인증에 이용되는 전자 증명서로 해야 할 대상을 바꾸는 것이 가능해지고, 종래의 통신 상대의 인증 방법과의 호환성이 유지된다.

[0031] 도 2는 본 발명의 일 실시예에 따른 클라이언트 장치(200)의 기능 구성의 일 예를 나타낸다. 클라이언트 장치(200)는, 저장부(205), 일시 증명서 작성부(235), 폴리시 판정부(280), 서명 작성부(285) 및 통신부(275)를 포함한다. 일시 증명서 작성부(235)는, 서버 장치(400)가 지원하는 전자 증명서의 포맷을 따르는 일시 증명서를 작성하는 기능을 갖고, 일시 키 작성부(240), 기본 영역 설정부(245), 암호화부(250), 시각 취득부(255), 서명값 계산부(260), 확장 영역 설정부(265), 및 서명 설정부(270)를 포함한다. 저장부(205)는, 미리 취득한 개인 정보를 포함하는 클라이언트 증명서(230), 해당 클라이언트 증명서(230)에 기재되는 공개키 암호 방식을 따르는 클라이언트 공개키에 대응하는 클라이언트 비밀키(225), 서버 장치에서 취득한 서버 증명서(215), 소정의 문자열(210), 및 일시 증명서 작성 대상 폴리시 일람(232)을 저장한다.

[0032] 여기서 도 3(a)을 참조하여, SSL/TLS에서 채용되는 X.509 버전3의 전자 증명서의 포맷을 설명한다. X.509 증명서는 크게 나누어서 기본 영역과 확장 영역의 2개 영역으로 구성된다. 기본 영역에는, X.509의 버전, 증명서의 시리얼 번호, 증명서의 서명에 사용되고 있는 해시·알고리즘 및 공개키 알고리즘(서명 방식), 증명서의 발행자인 발행자 정보, 해당 기본 영역에 설정되는 공개키의 유효 기한 및 이에 대응하는 비밀키의 소유자 정보를 포함하는 서지 정보와, 공개키 정보가 설정된다. 또 확장 영역에는, X.509 버전2로부터 추가된 인증국 고유 식별 정보 및 소유자 고유 식별 정보, 또한 X.509 버전3으로부터 추가된 확장형, 확장값 및 크리티컬 비트의 3개 세트의 집합이, 각각 임의로 설정가능하다. 또 확장형에는 X.509 버전3에서 정해진 표준의 확장형 외에, 독자의 새로운 확장형을 포함시키는 것이 가능하다.

[0033] X.509 증명서에는 또한, 기본 영역 및 확장 영역에 설정되는 정보를 해시 처리해서 얻을 수 있는 해시값을 인증국의 비밀키로 암호화한, 인증국의 서명이 첨부된다. 전자 증명서의 수신자는, 인증국의 루트 증명서를 이용하여 인증국의 서명을 검증함으로써 전자 증명서의 유효성을 확인할 수 있다. 즉, 기본 영역 및 확장 영역에 설정되는 정보를 해시 처리해서 얻을 수 있는 해시값과, 인증국의 루트 증명서에 기재되는 루트 공개키를 이용하여 복호한 인증국의 서명이 일치하는지 여부를 판정함으로써, 서명이 확실히 인증국에 의해 첨부된 것, 및 기본 영역 및 확장 영역에 기재되는 정보가 손상이나 변경되지 않은 것을 확인할 수 있다. 또, 루트 증명서라는 것은, 전자 증명서를 발행하는 인증국이, 그 정당성을 증명하기 위해서 스스로 서명해서 발행하는 전자 증명서다.

[0034] 저장부(205)에 저장되는 서버 증명서(220)는, 상술한 바와 같이 SSL/TLS를 이용한 통신의 인증 처리에서, 서버 장치(400)로부터 클라이언트 장치(200)에 송신된 것이다. 따라서 본 실시예에 따른 서버 증명서(220)는 X.509의 포맷을 따른다. 또한, 저장부(205)에 저장되는 개인 정보를 포함하는 클라이언트 증명서(230)는, 본 실시예에서는 공적 개인 인증 서비스에 의해 발행된 것으로 한다. 도 3(b)에, 공적 개인 인증 서비스에 의해 발행된 X.509의 포맷을 따르는 클라이언트 증명서의 일 예를 나타낸다. 클라이언트 증명서의 기본 영역에는, 도 3(a)를 참조해서 설명한 대로의 정보가 기재된다. 한편, 클라이언트 증명서(230)의 확장 영역에는, 독자적으로, 주민 기본 대장에 기재되는 성명, 생년월일, 성별, 주소가 기재된다. 마찬가지로 확장 영역에 기재되는 증명서 폴리시는, 증명서의 목적이나 이용 용도를 규정하는 것이다. 여기에서는, 해당 증명서가 공적 개인 인증 서비스에 의해 발행된 것을 나타내는 정보가 OID(Object Identifier) 형식으로 기재된다. OID라는 것은, 국제적으로 등록해 표준화 기관에 의해 승인된 특별히 형식화된 번호이며, ISO 표준에 등록된 특정한 객체나 객체류를 나타내는 것이다.

[0035] 또 클라이언트 증명서(230)에 첨부되는 서명값 B는 도도부현 지사에 의해 실시되는 서명이다.

[0036] 또, 공적 개인 인증 서비스에서는, 남에 의한 부정 사용을 막기 위해, 전자 증명서와 해당 전자 증명서가 증명하는 공개키에 대응하는 비밀키는 이용자의 IC 카드에 저장된다. 따라서, 도 2에서는 일시 증명서 작성에 필요한 정보는 전부 동일한 저장부(205)에 저장되는 것처럼 도시되어 있지만, 클라이언트 증명서(230) 및 클라이언트 비밀키(225)는 실제로는 IC 카드에 저장되고, IC 카드 리더 라이터에 의해 판독된다. 저장부(205)에 저장되는 소정의 문자열은, 미리 서버 장치(400)와의 사이에서 정해진 문자열이며, 서명으로서 이용하는데도 적절한 임의의 문자열이다. 또 저장부(205)에 저장되는 일시 증명서 작성 대상 폴리시 일람(232)은, 개인 정보를 포함하는 전자 증명서에 설정될 수 있는 증명서 폴리시의 일람이다. 본 실시예에 따른 일시 증명서 작성 대상 폴리시 일람(232)은, 공적 개인 인증 서비스에 의해 발행된 것을 나타내는 증명서 폴리시가 리스트된다.

[0037] 통신부(수신부)(275)는, 서버 장치(400)로부터 전자 증명서의 요구를 수신하고, 폴리시 판정부(280)에 메시지의 수신을 통지한다. 폴리시 판정부(280)는, 전자 증명서의 요구의 통지에 응답하여, 저장부(205)로부터 클라이언트 증명서(230)와 일시 증명서 작성 대상 폴리시 일람(232)을 판독한다. 그리고, 폴리시 판정부(280)는, 클라이언트 증명서(230)의 확장 영역에 기재되는 증명서 폴리시가, 일시 증명서 작성 대상 폴리시 일람(232)에 리스트되어 있는 증명서 폴리시인지 여부를 판정한다.

[0038] 클라이언트 증명서(230)의 증명서 폴리시가 일시 증명서 작성 대상 폴리시 일람(232)에 리스트되어 있을 경우, 폴리시 판정부(280)는 일시 증명서 작성부(235)에 일시 전자 증명서의 작성을 의뢰한다. 클라이언트 증명서(230)의 증명서 폴리시가 일시 증명서 작성 대상 폴리시 일람(232)에 리스트되어 있지 않을 경우, 즉 클라이언트 증명서(230)가 개인 정보를 포함하지 않을 경우에는, 폴리시 판정부(280)는, 저장부(205)로부터 판독한 클라이언트 증명서(230)를, 통신부(송신부)(275)를 거쳐서 그대로 서버 장치(400)에 송신한다. 또, 본 실시예에 따른 클라이언트 증명서(230)는 개인 정보를 포함하기 위해, 폴리시 판정부(280)는 일시 증명서 작성부(235)에 일시 전자 증명서의 작성을 의뢰한다.

[0039] 일시 증명서 작성부(235)는, 폴리시 판정부(280)로부터의 의뢰에 응답하여, 서버 장치(400)가 지원하는 전자 증명서의 포맷, 즉 본 실시예에서는 X.509에 따르는 일시 전자 증명서의 작성을 다음과 같이 시작한다. 일시 키 작성부(240)는, 일시 전자 증명서 작성에 사용하기 위해서, 공개키 암호 방식을 따르는 1 세트의 키, 즉 일시 공개키와 이에 대응하는 일시 비밀키를 생성한다. 기본 영역 설정부(245)는, 일시 전자 증명서의 기본 영역을 설정한다. 일례로서 기본 영역 설정부(245)는, 저장부(205)로부터 서버 증명서(215)에 기재되는 소유자 정보를 판독하고, 이것을 일시 전자 증명서의 발행자 정보의 필드에 복사한다. 이로써 일시 전자 증명서를 수신한 서버 장치(400)에 대하여, 해당 전자 증명서가 일시 전자 증명서인 것을 나타낼 수 있다.

[0040] 이 대신에, 전자 증명서가 일시 전자 증명서인 것을 나타내는 증명서 폴리시를 이용해도 좋다. 전자 증명서의 기본 영역의 발행자 정보의 필드나, 전자 증명서의 확장 영역의 증명서 폴리시의 필드는, 일반적으로 전자 증명서의 종별을 식별할 목적으로 사용되고 있는 필드다. 이 때문에 이들 필드를 전자 증명서가 일시 전자 증명서인 것을 나타내는 정보를 기재하기 위해서 이용했을 경우에는, 독자 정의의 필드를 이용하는 경우와 같이 , 전자 증명서의 내용이 제삼자에 대하여 의미가 불분명해지지는 않는다. 기본 영역 설정부(245)는 또한, 소유자 정보의 필드에 자신의 정보를 설정하고, 더욱이 공개키의 필드에 일시 키 작성부(240)가 생성한 일시 공개키를 설정한다. 기본 영역의 기타 필드에 대해서는, 각각 임의의 적절한 값이 설정된다.

[0041] 암호화부(250)는, 저장부(205)로부터 클라이언트 증명서(230) 및 서버 증명서(215)에 기재되는 서버 공개키(220)를 판독하고, 서버 공개키(220)를 이용하여 클라이언트 증명서(230)를 암호화한다. 시각 취득부(255)는 클라이언트 장치(200) 상의 현재 시각을 취득한다. 서명값 계산부(260)는, 저장부(205)로부터 문자열(210)을 판독하고, 시각 취득부(255)에 의해 취득된 현재 시각과 문자열을 서명 대상으로 삼아서 서명값을 계산한다. 즉 서명값 계산부(260)는, 현재 시각과 문자열(210)을 해시 함수를 이용하여 해시 처리하고, 얻어진 해시값을 저장부(205)에 저장되는 클라이언트 비밀키(225)를 이용하여 암호화한다.

[0042] 서명값 계산에 채용하는 해시 함수는, 미리 서버 장치(400)와의 사이에서 정해두어도 좋고, 또는 클라이언트 증명서(230)의 서명에 이용되고 있는 것과 같은 것으로 해도 좋다. 또 이용한 해시 함수 정보를 일시 전자 증명서의 확장 영역을 이용해서 서버 장치(400)에 통지해도 좋다. 또한, 서명값 계산부(260)는, 저장부(205)로부터 판독한 문자열(210)만을 서명 대상으로 삼아도 좋다.

[0043] 확장 영역 설정부(265)는 일시 전자 증명서의 확장 영역에, 암호화부(250)에 의해 암호화된 클라이언트 증명서(230)를 설정한다. 확장 영역 설정부(265)는 또한, 본인 확인 정보로서 일시 전자 증명서의 확장 영역에, 저장부(205)로부터 판독된 문자열(210), 시각 취득부(255)에 의해 취득된 현재 시각(이하, 「서명 시각」이라 함), 및 서명값 계산부(260)에 의해 계산된 서명값을 추가 설정해도 좋다. 또한, 서명 설정부(270)는 일시 전자 증명서에 서명을 실시한다. 즉 서명 설정부(270)는 기본 영역 및 확장 영역에 설정된 정보를 해시 처리하고, 얻어진 해시값을 서버 증명서(215)에 기재되는 서버 공개키(220)를 이용하여 암호화한 서명값을 일시 전자 증명서에 설정한다.

[0044] 도 3(c)에 일시 증명서 작성부(235)에 의해 작성된 일시 전자 증명서의 일 예를 나타낸다. 상술한 바와 같이, 본 실시예에 따른 일시 전자 증명서의 발행자 정보 필드에는, 해당 전자 증명서가 일시 디지털 증명인 것을 나타내는 판정 정보(본 실시예에서는 서버 장치(400) 정보)가 기재된다. 또한, 일시 전자 증명서의 확장 영역에는, 암호화 완료의 클라이언트 증명서(230)와 본인 확인 정보인 문자열(210), 서명 시각, 서명값 C가 기재된다. 더욱이, 일시 전자 증명서에는, 서버 장치(400)의 서버 공개키를 이용하여 계산된 서명값 B가 첨부된다. 통신부(송신부)(275)는, 일시 증명서 작성부(235)에 의해 작성된 일시 전자 증명서를 전자 증명서의 요구에 대한 응답으로서 서버 장치(400)로 송신한다.

[0045] 일시 저장부(290)는, SSL/TLS의 핸드쉐이크 프로토콜의 개시 메시지인 클라이언트 헬로 메시지로부터 클라이언트 키 교환 메시지까지의 통신 내용을 일시적으로 저장한다. 서명 작성부(285)는, 통신부(송신부)(275)로부터 송신되는 전자 증명서가 확실히 클라이언트 장치(200)에 의해 송신된 것을 서버 장치(400)가 확인할 때에 사용 가능한 서명을, 일시 저장부(290)가 저장하는 상기 정보를 사용해서 작성한다. 즉, 서명 작성부(285)는, 일시 저장부(290)로부터 상기 통신 내용을 판독해서 해시 처리하는 것에 의해 해시값을 구하고, 이것을 송신하는 전자 증명서에 기재되는 공개키에 대응하는 비밀키로 암호화하는 것에 의해 서명을 작성한다. 그리고 서명 작성부(285)는, 작성한 서명을, 전자 증명서와 함께 또는 그 송신 후에, 통신부(송신부)(275)를 거쳐서 서버 장치(400)에 송신한다.

[0046] 이상과 같이, 본 발명의 실시예에 따른 클라이언트 장치(200)에 의하면, 전자 증명서의 확장 영역을 이용해서 서버 장치(400)가 지원하는 포맷의 전자 증명서 내에 자신을 증명하는 참된 전자 증명서를 설정하므로, 개인 정

보를 포함하는 클라이언트 증명서를 암호화한 상태로 송신할 수 있어, 제삼자에 의한 개인 정보로의 부정 액세스를 방지할 수 있다.

[0047] 도 4는 본 발명의 일 실시예에 따른 서버 장치(400)의 기능 구성의 일 예를 나타낸다. 서버 장치(400)는, 통신부(405), 일시 저장부(410), 판정부(415), 복호부(420), 저장부(425), 및 인증부(430)를 포함한다. 저장부(425)는 서버 비밀키(430)와 신뢰 완료 증명서 일람(435)을 저장한다. 여기서 서버 비밀키(430)는, 클라이언트 장치(200)에 송신한 서버 증명서(215)에 기재되는 서버 공개키(220)에 대응하는 비밀키이다. 또한, 신뢰 완료 증명서 일람(435)은, 복수의 인증국의 루트 증명서의 일람이며, 루트 증명서의 정당성은 서버 장치(400)에서 이미 확인되어 있는 것으로 한다. 인증부(430)는, 통신 상대를 인증하는 기능을 갖고, 증명서 검증부(435)와 본인 확인부(440)를 포함한다. 본인 확인부(440)는 전자 증명서가 확실히 본인으로부터 송신된 것을 확인하는 기능을 갖고, 서명 검증부(445)와 시각 검증부(450)를 포함한다.

[0048] 통신부(405)는, 전자 증명서의 요구에 대한 응답으로서 클라이언트 장치(200)로부터 전자 증명서를 수신한다. 수신한 전자 증명서는 일시 저장부(410)에 저장된다. 판정부(415)는 일시 저장부(410)로부터 전자 증명서에 기재되는 판정 정보, 즉 본 실시예에서는 전자 증명서의 기본 영역에 기재되는 발행자 정보를 판독하고, 수신한 전자 증명서가 일시 전자 증명서인 것을 판정 정보가 나타내고 있는지 여부를 판정한다. 수신한 전자 증명서가 일시 전자 증명서인 것을 나타낼 경우, 즉 본 실시예에서는 발행자 정보가 서버 장치(400) 자신을 나타낼 경우, 판정부(415)는 판정 결과를 복호부(420)와 인증부(430)에 통지한다. 한편, 수신한 전자 증명서가 일시 전자 증명서인 것을 나타내지 않을 경우, 판정부(415)는 판정 결과를 인증부(430)에만 통지한다.

[0049] 복호부(420)는, 수신한 전자 증명서가 일시 전자 증명서라는 통지에 응답하여, 일시 저장부(410)로부터 수신한 전자 증명서의 확장 영역에 기재되는 암호화된 클라이언트 증명서(230)를 판독한다. 그리고 복호부(420)는, 판독한 클라이언트 증명서(230)를 저장부(425)에 저장되는 대응하는 서버 비밀키(430)를 이용하여 복호한다. 복호된 클라이언트 증명서(230)는 그 후 인증부(430)로 넘겨진다.

[0050] 인증부(430)는, 수신한 전자 증명서는 일시 전자 증명서가 아니라고 판정부(415)가 판정한 경우, 수신한 전자 증명서와 해당 전자 증명서와 함께 또는 그 후에 클라이언트 장치(200)로부터 송신되는 서명을 이용하여 클라이언트 장치(200)를 인증한다. 한편, 수신한 전자 증명서는 일시 전자 증명서라고 판정부(415)가 판정한 경우, 인증부(430)는 복호된 클라이언트 증명서(230)와 일시 전자 증명서의 확장 영역에 설정되는 서명을 이용하여 클라이언트 장치(200)를 인증한다. 인증부(430)에 의한 인증 처리는, 판정부(415)로부터의 판정 결과의 통지에 응답해서 개시되어, 증명서 검증부(435)와 본인 확인부(440)에 의한 처리가 행하여진다.

[0051] 전자 증명서의 검증 방법은 판정부(415)에 의한 판정 결과에 관계없이 기본적으로 같다. 그래서 이하에서는, 개인 정보를 포함하는 클라이언트 증명서(230)를 검증하는 경우를 예로, 증명서 검증부(435)에 의한 처리를 설명한다. 또, 개인 정보를 포함하는 클라이언트 증명서(230)를 검증 대상으로 하는 경우, 후술하는 본인 확인부(440)에 의한 처리의 성공을 조건으로 해도 좋다.

[0052] 증명서 검증부(435)는, 복호부(420)로부터 복호된 클라이언트 증명서(230)를 수취하여, 전자 증명서의 검증, 즉, 클라이언트 증명서(230)에 첨부된 서명의 검증과, 클라이언트 증명서(230)에 기재되는 서지 정보의 확인을 실행한다. 서명의 검증은 다음과 같이 해서 실행한다. 우선, 클라이언트 증명서(230)에 기재되는 발행자 정보를 참조하여, 저장부(425)에 저장되는 신뢰 완료 증명서 일람(435) 중에서 해당하는 인증국(본 실시예에서는, 도도부현 지사)의 루트 증명서를 검색한다. 다음에, 루트 증명서에 기재되는 루트 공개키를 이용하여 클라이언트 증명서(230)에 첨부된 서명을 복호한다. 그리고, 이것을 클라이언트 증명서(230)의 기본 영역 및 확장 영역에 기재되는 정보를 해시 처리해서 얻은 해시값과 비교해서 일치하는지 여부를 판정한다. 2개가 일치하면 검증은 성공이다. 또, 서명에 사용되는 알고리즘은, 클라이언트 증명서(230)에 기재되는 서명 방식에 의해 확인할 수 있다.

[0053] 다음에, 클라이언트 증명서(230)에 기재되는 서지 정보의 확인에는, 일례로서 클라이언트 증명서(230)의 유효기한 및 실효의 확인, 그리고 소유자 정보나 개인 정보를 참조한 통신 상대의 확인이 포함된다. 여기에서, 클라이언트 증명서의 실효를 확인하는 방법을 설명한다. 인증국이 전자 증명서의 실효를 이용자에게 통지하기 위해서는 2개 방법이 있고, 하나는 실효된 증명서의 리스트를 정기적으로 공개하는 증명서 CRL(Certificate Revocation List) 방법이며, 하나는 증명서의 실효 정보를 유지한 서버가, 클라이언트로부터의 증명서의 실효 정보의 문의에 대답하는 OCSP(Online Certificate Status Protocol) 방법이다. 공적 개인 인증 서비스에서는 전자의 방법이 채용되고 있고, 따라서 본 실시예에서는, 증명서 검증부(435)는 인증국에 CRL을 요구하고, 수신한 CRL에 클라이언트 증명서가 리스트되어 있는지 여부를 판정함으로써 실효를 확인한다. 또, 상술한 개인 정

보를 참조한 통신 상대의 확인은, 개인 정보를 포함하는 클라이언트 증명서(230)를 검증 대상으로 하는 경우로 한정된다.

[0054] 본인 확인부(440)는, 검증 대상의 전자 증명서가 확실히 클라이언트 증명서(230)의 소유자에 의해 송신된 것을 확인한다. 수신한 전자 증명서는 일시 전자 증명서라고 판정부(415)가 판정한 경우, 서명 검증부(445)는, 일시 저장부(410)로부터 일시 전자 증명서의 확장 영역에 기재되는 본인 확인 정보를 판독하여, 서명의 검증을 실행한다. 본인 확인 정보를 이용한 서명의 검증은 다음과 같이 해서 행하여진다. 우선 본인 확인 정보에 포함되는 문자열(210)과 서명 시각을 미리 클라이언트 장치(200)와의 사이에서 정해진 해시 함수를 이용하여 해시 처리해 해시값을 얻는다. 다음에 본인 확인 정보에 포함되는 서명값 C를, 복호된 클라이언트 증명서(230)에 기재되는 클라이언트 공개키를 이용하여 복호한다. 끝으로 복호된 서명값 C와 상기 해시값을 비교한다. 2개가 일치하면, 클라이언트 증명서(230)는 확실히 클라이언트 증명서(230)의 소유자에 의해 송신된 것이라고 할 수 있다.

[0055] 한편, 수신한 전자 증명서는 일시 전자 증명서가 아니라고 판정부(415)가 판정한 경우, 서명 검증부(445)는, 전자 증명서와 함께 또는 전자 증명서의 수신 후에, 클라이언트 장치(200)로부터 송신되는 서명에 대하여 검증 처리를 실행한다. 클라이언트 장치(200)의 기능 구성의 설명에서 상술한 바와 같이, SSL/TLS의 핸드쉐이크 프로토콜에서의 상대 인증에서는, 본인 확인 정보로서, 핸드쉐이크 프로토콜의 개시 메시지인 클라이언트 헬로 메시지로부터 클라이언트 키 교환 메시지까지의 통신 내용이 이용된다. 그리고, 그러한 통신 내용의 해시값을 전자 증명서에 기재되는 공개키에 대응하는 비밀키로 암호화하는 것에 의해 계산된 서명값이, 클라이언트 증명서 메시지의 뒤에 송신되는 증명서 검증 메시지의 본체에 포함되어 클라이언트 장치(200)로부터 송신된다.

[0056] 그래서, 수신한 전자 증명서가 그대로 검증 대상이 될 경우, 서명 검증부(445)는 다음과 같이 해서 서명 검증을 실행한다. 통신부(405)에서 클라이언트 장치(200)로부터 증명서 검증 메시지가 수신되면, 서명 검증부(445)는 일시 저장부(410)를 거쳐서 증명서 검증 메시지 본체에 포함되는 서명값을 판독한다. 그리고, 서명 검증부(445)는 서명값을 클라이언트 장치(200)로부터 수신한 전자 증명서에 기재되는 공개키로 복호한다. 또 일시 저장부(410)는, 클라이언트 헬로 메시지로부터 클라이언트 키 교환 메시지까지의 통신 내용을 일시적으로 저장한다. 그래서 서명 검증부(445)는 일시 저장부(410)로부터 이들 통신 내용을 판독해서 해시값을 구하고, 복호한 서명값과 비교한다. 2개가 일치하면, 수신한 전자 증명서는 확실히 해당 전자 증명서의 소유자에 의해 송신된 것이라고 할 수 있다.

[0057] 또, 본 실시예에서는 종래의 통신 상대의 인증 방법, 즉 SSL/TLS의 핸드쉐이크 프로토콜에서의 상대 인증과의 호환성을 유지하기 위해서, 일시 전자 증명서를 서버 장치(400)로 송신할 경우에도, 클라이언트 장치(200)는 증명서 검증 메시지를 작성해 서버 장치(400)로 송신하는 것으로 한다. 이 경우 사용되는 클라이언트의 비밀키는 일시 전자 증명서에 기재되는 일시 공개키에 대응하는 일시 비밀키이다. 단, 서버 장치(400)는 증명서 검증 메시지 본체에 포함되는 서명을 검증할 필요는 없다.

[0058] 본인 확인부(440)는 또한, 일시 전자 증명서의 확장 영역에 서명 시각이 기재될 경우, 일시 전자 증명서의 확장 영역에 기재되는 본인 확인 정보가 재이용된 것이 아닌 것을 확인해도 좋다. 이 경우, 시각 검증부(450)는 우선 서버 장치(400) 상의 현재 시각을 취득한다. 그리고, 현재 시각과 일시 전자 증명서의 확장 영역에 기재되는 서명 시각의 차이를 계산하고, 구한 차이가 허용 범위 내인지 여부를 판정한다. 허용 범위 내이면, 본인 확인 정보는 재이용된 것이 아니라고 할 수 있다. 이렇게 서명에 서명 시각을 포함시키는 것에 의해 본인 확인 정보의 재이용을 금지함으로써, 일시 전자 증명서를 도청해서 본인 확인 정보를 훔친 제삼자가 가짜의 일시 전자 증명서를 작성하는 것을 방지할 수 있다.

[0059] 이상과 같이 , 본 발명의 실시예에 따른 서버 장치(400)에 의하면, 클라이언트 장치(200)로부터 전자 증명서를 수신했을 경우에, 우선 전자 증명서의 소정의 영역에 기재되는 판정 정보를 이용하여, 수신한 전자 증명서가 일시 전자 증명서가 일시 전자 증명서인지 여부를 판정하므로, 판정 결과에 따라 상대 인증에 이용되는 전자 증명서로 해야 할 대상을 바꾸는 것이 가능해진다. 즉, 본 발명의 실시예에 따른 서버 장치(400)에 의하면, 암호화된 전자 증명서와 통상의 암호화되지 않고 있는 전자 증명서의 양쪽을 처리하는 것이 가능해져, 종래의 통신 상대의 인증 방법과의 호환성을 유지할 수 있다.

[0060] 다음에, 도 5의 흐름도를 참조하여, 본 실시예에 따른 클라이언트 장치(200)의 동작을 설명한다. 도 5(a)는 서버 장치(400)로부터의 전자 증명서의 요구에 응답해서 전자 증명서를 송신할 때까지의 클라이언트 장치(200)의 처리의 흐름을 나타낸다. 클라이언트 장치(200)는, 서버 장치(400)로부터 클라이언트 장치(200)를 인증하기 위한 전자 증명서의 요구를 수신하면(단계 500), 저장부(205)로부터 서버 장치(400)로 송신해야 할 클라이언트 증

명서(230)와 일시 증명서 작성 대상 폴리시 일람(232)을 판독한다(단계 503). 그리고 클라이언트 장치(200)는, 클라이언트 증명서(230)의 확장 영역으로부터 증명서 폴리시를 인출하여(단계 506), 인출한 증명서 폴리시가 일시 증명서 작성 대상 폴리시 일람(232)에 리스트되어 있는지 여부를 판단한다(단계 509).

[0061] 인출한 증명서 폴리시가 일시 증명서 작성 대상 폴리시 일람(232)에 리스트되어 있을 경우(단계 509: 예), 일시 전자 증명서를 작성하기 위한 사전 준비가 개시된다. 즉 클라이언트 장치(200)는 우선, 저장부(205)로부터 서버 증명서(215)를 판독하고(단계 512), 판독한 서버 증명서(215)로부터 소유자 정보와 서버 공개키를 인출한다(단계 515). 또한, 클라이언트 장치(200)는, 일시 전자 증명서에 사용하기 위한 공개키 방식을 따르는 1 세트의 키, 즉 일시 공개키와 일시 비밀키를 생성한다(단계 518).

[0062] 사전 준비가 끝나면, 클라이언트 장치(200)는 준비한 정보를 이용하여 서버 장치(400)가 지원하는 전자 증명서의 포맷을 따르는 일시 전자 증명서를 작성한다(단계 521). 일시 전자 증명서의 작성 방법에 대해서는 후술한다. 클라이언트 장치(200)는, 작성한 일시 전자 증명서를 서버 장치(400)에 송신하면(단계 524), 일시 전자 증명서에 기재되는 일시 공개키에 대응하는 일시 비밀키를 이용하여 서명을 작성하고, 이것을 서버 장치(400)로 송신한다(단계 527).

[0063] 한편, 단계 509에서 "아니오"인 경우, 즉 인출한 증명서 폴리시가 일시 증명서 작성 대상 폴리시 일람(232)에 리스트되어 있지 않고 클라이언트 증명서(230)에 개인 정보가 포함되어 있지 않을 경우, 클라이언트 장치(200)는, 저장부(205)로부터 판독한 클라이언트 증명서(230)를 그대로 서버 장치(400)로 송신한다(단계 530). 그리고, 클라이언트 장치(200)는, 클라이언트 증명서(230)에 기재되는 클라이언트 공개키에 대응하는 클라이언트 비밀키를 이용하여 서명을 작성하고, 이것을 서버 장치(400)에 송신한다(단계 536). 단계 527 또는 단계 533의 후처리는 종료된다.

[0064] 도 5(b)를 참조해서 일시 전자 증명서 작성의 처리의 흐름을 설명한다. 클라이언트 장치(200)는 우선, 도 5(a)의 단계 515 및 518에서 준비한 정보를 이용하여, 일시 전자 증명서의 기본 영역의 설정을 실행한다(단계 540). 즉, 발행자 정보의 필드에 서버 장치(400)를 나타내는 소유자 정보를 설정하고, 또 공개키 정보의 필드에 일시 공개키를 설정한다. 기타 필드에 대해서는, 각각 임의의 적절한 값을 설정한다. 다음에 클라이언트 장치(200)는, 도 5(a)의 단계 515에서 취득한 서버 공개키를 이용하여, 개인 정보를 포함하는 클라이언트 증명서를 암호화한다(단계 545). 또 클라이언트 장치(200)는, 클라이언트 증명서가 확실히 그 소유자에 의해 송신된 것을 나타내기 위해서 본인 확인 정보를 작성한다(단계 550). 본인 확인 정보의 작성 방법에 대해서는 후술한다. 그리고 클라이언트 장치(200)는, 암호화 완료의 클라이언트 증명서와 본인 확인 정보를 일시 전자 증명서의 확장 영역에 설정한다(단계 555). 끝으로 클라이언트 장치(200)는, 서버 공개키(220)를 이용하여 일시 전자 증명서에 서명을 실시한다(단계 560). 그리고 처리는 종료된다.

[0065] 도 5(c)를 참조하여, 본인 확인 정보의 작성 방법의 처리의 흐름을 설명한다. 클라이언트 장치(200)는, 저장부(205)로부터 미리 서버 장치(400)와의 사이에서 정해 둔 문자열을 판독한다(단계 570). 다음에 클라이언트 장치(200)는 클라이언트 장치(200) 상의 현재 시각을 취득한다(단계 575). 그리고 판독한 문자열과 현재 시각을 서명 대상으로 하여, 클라이언트 증명서(230)에 기재되는 클라이언트 공개키에 대응하는 클라이언트 비밀키를 이용하여 서명값을 계산한다(단계 580). 그리고 처리는 종료된다.

[0066] 다음에, 도 6의 흐름도를 참조하여, 본 실시예에 따른 서버 장치(400)의 동작을 설명한다. 도 6(a)는 서버 장치(400)에 의한 처리의 흐름의 개요를 나타낸다. 서버 장치(400)는, 통신 상대인 클라이언트 장치(200)를 인증하기 위해서, 클라이언트 장치(200)에 전자 증명서의 요구를 송신한다(단계 600). 클라이언트 장치(200)로부터 전자 증명서를 수신하면(단계 603), 서버 장치(400)는 이것을 검증한다(단계 606). 계속해서 서버 장치(400)는 클라이언트 장치(200)로부터 서명을 수신한다(단계 609). 서버 장치(400)는 서명을 검증하고, 수신한 전자 증명서가 확실히 해당 전자 증명서의 소유자로부터 송신된 것을 확인한다(단계 612). 그리고 처리는 종료된다.

[0067] 도 6(b)를 참조하여, 서버 장치(400)에 의한 전자 증명서의 검증 처리의 흐름을 설명한다. 우선 서버 장치(400)는, 수신한 전자 증명서의 기본 영역으로부터 발행자 정보를 인출하여(단계 615), 수신한 전자 증명서가 일시 전자 증명서인지 여부를 판정한다(단계 620). 일시 전자 증명서라고 판정된 경우(단계 620: 예), 서버 장치(400)는 일시 전자 증명서를 검증한다(단계 625). 일시 전자 증명서의 검증에 대해서는 후술한다. 단계 630에서 일시 전자 증명서의 검증이 성공했을 경우, 서버 장치(400)는 일시 전자 증명서 내에 포함되는 클라이언트 증명서(230)를 클라이언트 장치(200) 인증을 위한 검증 대상으로 인식한다(단계 635). 한편, 수신한 전자 증명서는 일시 전자 증명서가 아니라고 판정된 경우(단계 620 : 아니오), 서버 장치(400)는 수신한 전자 증명서 그

것을 클라이언트 장치(200) 인증을 위한 검증 대상으로 인식한다(단계 637).

[0068] 그래서 처리는 단계 635 또는 단계 637로부터 단계 640으로 진행하고, 서버 장치(400)는, 검증 대상의 증명서에 실시된 서명을 검증한다(단계 640). 단계 640에서 검증이 성공하면, 서버 장치(400)는 검증 대상의 증명서에 기재된 유효 기한으로부터 증명서가 아직 유효한 것을 검증한다(단계 645). 단계 645에서, 검증이 성공하면, 서버 장치(400)는 검증 대상의 증명서의 발행자와 통신하여, 증명서가 실효하지 않고 있는 것을 검증한다(단계 650). 단계 650에서 검증에 성공하면, 서버 장치(400)는, 검증 대상의 증명서에 기재된 소유자 정보를 참조하여, 클라이언트 장치(200)가 적당한 통신 상대인 것을 검증한다(단계 652). 단계 652에서의 검증의 성공은, 전자 증명서 검증의 성공을 의미한다. 또, 검증의 순서는 도 6(b)에 나타내는 순서로 제한되지 않는다.

[0069] 단계 630에서 일시 전자 증명서의 검증에 실패했을 경우, 또는 단계 640, 645, 650 및 652 중 어느 한 단계에서 검증에 실패했을 경우, 처리는 단계 660으로 진행되고, 검증이 실패한 것을 클라이언트 장치(200)로 통지한다. 검증의 실패를 알리기 위해서, SSL/TLS에서는 경보 프로토콜(Alert Protocol)을 이용한다. 예를 들면 증명서의 유효 기한이 중단된 경우, 증명서 만기(Certificate_expired) 메시지를 클라이언트 장치(200)에 송신한다. 또한, 증명서가 실효되어 있을 경우에는, 증명서 취소(CeTtificate_revoked) 메시지를 클라이언트 장치(200)에 송신한다.

[0070] 도 6(c)를 참조하여, 서버 장치(400)에 의한 일시 전자 증명서의 검증 처리의 흐름을 설명한다. 우선 서버 장치(400)는, 일시 전자 증명서의 확장 영역으로부터 암호화된 클라이언트 증명서(230)를 인출하여(단계 665), 저장부(425)로부터 판독한 서버 비밀키(430)를 이용하여 클라이언트 증명서(230)를 복호한다(단계 670). 다음에 서버 장치(400)는 일시 전자 증명서의 확장 영역으로부터, 본인 확인 정보로서 기재되어 있는 서명 대상, 즉 문자열과 서명 시각을 인출하여(단계 675), 소정의 해시 함수를 이용하여 서명 대상의 해시값을 구한다. 서버 장치(400)는 또한, 일시 전자 증명서의 확장 영역으로부터 본인 확인 정보로서 기재되어 있는 서명값을 인출한다(단계 680). 서버 장치(400)는, 복호한 클라이언트 증명서에 기재되어 있는 클라이언트 공개키를 이용하여 인출한 서명값을 복호하고, 이것을 해시값과 비교해서 서명을 검증한다(단계 685).

[0071] 단계 690에서 검증이 성공했을 경우, 즉 클라이언트 증명서(230)가 확실히 클라이언트 증명서(230)의 소유자로부터 송신되었다고 확인할 수 있을 경우, 서버 장치(400)는 또한 서버 장치(400) 상의 현재 시각을 취득한다(단계 695). 그리고 서버 장치(400)는, 취득한 현재 시각과 일시 전자 증명서의 확장 영역에 기재된 서명 시각의 차이를 계산한다(단계 700). 계산한 차이가 허용 범위 내일 경우(단계 705: 예), 즉, 일시 전자 증명서의 확장 영역에 기재된 본인 확인 정보가 재이용된 것이 아니라고 확인할 수 있는 경우, 서버 장치(400)는 검증 성공을 보존한다(단계 710). 단계 740에서 서명 검증이 실패했을 경우 또는 단계 705에서 계산한 차이가 허용 범위 내가 아닐 경우, 서버 장치(400)는 검증 실패를 보존한다(단계 715). 그리고 처리는 종료된다.

[0072] 도 7은 본 실시예에 따른 클라이언트 장치(200)의 하드웨어 구성의 일 예를 나타낸다.

[0073] 도 7은 또 서버 장치(400)의 하드웨어 구성의 일례이기도 하다. 이하에서는, 클라이언트 장치(200)의 하드웨어 구성으로서 도 7을 설명한다. 클라이언트 장치(200)는, 호스트 콘트롤러(715)에 의해 서로 접속되는 CPU(710) 및 RAM(730)을 포함하는 CPU 주변부와, 입출력 콘트롤러(735)에 의해 호스트 콘트롤러(715)에 접속되는 카드 버스 콘트롤러(740) 및 카드 버스 콘트롤러(740)에 접속되는 IC 카드 리더 라이터(745), 통신 인터페이스(770), 하드디스크 드라이브(750), 및 CD-ROM 드라이브(760)을 포함하는 입출력부와, 입출력 콘트롤러(735)에 접속되는 슈퍼 I/O 콘트롤러(780) 및 슈퍼 I/O 콘트롤러(780)에 접속된 플렉서블 디스크 드라이브(790), 플래시 롬(800), 및 키보드 마우스 콘트롤러(810)를 갖는 레거시 입출력부를 포함한다.

[0074] 호스트 콘트롤러(715)는, 높은 전송 레이트로 RAM(730)에 액세스하는 CPU(710)를 RAM(730)과 접속한다. CPU(710)는, 하드 디스크에 저장된 프로그램에 근거해서 동작하여, 각부의 제어를 실행한다. 본 발명의 실시예에 따른 통신 상대를 인증하기 위한 클라이언트 장치(200)용의 프로그램은, 하드 디스크에 저장되고, RAM(730)을 이용하여 CPU(710)에 의해 실행된다. 클라이언트 장치(200)용의 프로그램은, 클라이언트 장치(200)를, 저장부(205), 폴리시 판정부(280), 서명 작성부(285), 일시 저장부(290), 일시 증명 작성부(235), 즉, 일시 키 작성부(240), 기본 영역 설정부(245), 암호화부(250), 시각 취득부(255), 서명값 계산부(260), 확장 영역 설정부(265), 및 서명 설정부(270), 및 통신부(275)로서 기능시킨다. 그 구체적인 기능 및 동작은, 도 2 및 도 5를 이용하여 설명한 것과 동일하기 때문에 설명을 생략한다.

[0075] 한편, 본 발명의 실시예에 따른 서버 장치(400)용의 프로그램은, 서버 장치(400)를, 통신부(405), 일시 저장부(410), 판정부(415), 복호부(420), 저장부(425), 및 인증부(430), 즉, 증명서 검증부(435), 및 서명 검증부

(445) 및 시각 검증부(450)를 포함하는 본인 확인부(440)로서 기능시킨다. 그 구체적인 기능 및 동작은, 도 4 및 도 6을 이용하여 설명한 것과 동일하기 때문에 설명을 생략한다. 또, 본 발명의 실시예에 따른 클라이언트 장치(200)용 및 서버 장치(400)용의 프로그램은, 컴퓨터에 의해 판독 가능한 매체에 저장할 수 있다. 컴퓨터로 판독 가능한 매체라는 것은, 명령 실행 시스템, 장치 또는 기기에 사용되거나 혹은 이들에 관련되는 프로그램을 포함하고, 기억하고, 통신하고, 전파하고,혹은 반송할 수 있는 임의의 장치일 수 있다. 매체는, 전자적, 자기적, 광학적, 전자적, 적외선 또는 반도체 시스템(또는, 장치 또는 기기) 혹은 전파 매체일 수 있다. 컴퓨터 판독 가능한 매체의 예에는, 반도체 또는 솔리드 스테이트 기억 장치, 자기 테이프, 꺼낼 수 있는 컴퓨터 디스켓, 랜덤 액세스 메모리(RAM), 리드 온리 메모리(ROM), 리지드 자기 디스크 및 광 디스크가 포함된다. 현 시점에서의 광디스크의 예에는, 컴팩트 디스크 리드 온리 메모리(CD-ROM), 컴팩트 디스크 리드/라이터(CD-R/W) 및 DVD가 포함된다.

[0076] 입출력 콘트롤러(735)는, 비교적 고속의 입출력 장치인 카드 버스 콘트롤러(740) 및 카드 버스 콘트롤러(740)에 접속되는 IC 카드 리더 라이터(745), 통신 인터페이스(770), 하드디스크 드라이브(750), 및 CD-ROM 드라이브(760)를 호스트 콘트롤러(715)와 접속한다. 통신 인터페이스(770)는 네트워크를 거쳐서 서버 장치(400) 등의 외부 장치와 통신한다.

[0077] 또, 입출력 콘트롤러(735)에는, 플렉서블 디스크 드라이브(790)나 키보드 마우스 콘트롤러(810) 등의 비교적 저속의 입출력 장치와, 플래시 롬(800)이 접속된다. 플래시 롬(800)은, 클라이언트 장치(200)의 기동시에 CPU(710)가 실행하는 부팅 프로그램이나, 클라이언트 장치(200)의 하드웨어에 의존하는 프로그램 등을 저장한다. 플렉서블 디스크 드라이브(790)는, 플렉서블 디스크로부터 프로그램 또는 데이터를 판독하고, RAM(730)을 거쳐서 슈퍼 I/O 콘트롤러(735)에 제공한다. 슈퍼 I/O 콘트롤러(735)는, 플렉서블 디스크나, 예를 들면 패러럴 포트, 시리얼 포트, 키보드 포트, 마우스 포트 등을 거쳐서 각종 입출력 장치를 접속한다.

[0078] 이상, 실시예를 이용하여 본 발명을 설명했지만, 본 발명의 기술 범위는 상기 실시예에 기재된 범위로는 한정되지 않는다. 상기 실시예에, 각종 변경 또는 개량을 가할 수 있는 점이 당업자에게 명확하다. 따라서, 그러한 변경 또는 개량을 가한 형태도 당연히 본 발명의 기술적 범위에 포함된다.

도면의 간단한 설명

[0079] 도 1은 본 발명의 일 실시예에 따른 통신 상대를 인증하기 위한 시스템(100)의 구성의 일 예를 나타낸다.

[0080] 도 2는 본 발명의 일 실시예에 따른 클라이언트 장치(200)의 기능 구성의 일 예를 나타낸다.

[0081] 도 3(a)는 X.509 증명서의 포맷을 나타낸다. 도 3(b)는 본 발명의 실시예에 따른 개인 정보를 포함하는 클라이언트 증명서의 일 예를 나타낸다. 도 3(c)는 본 발명의 실시예에 따른 일시 전자 증명서의 일 예를 나타낸다.

[0082] 도 4는 본 발명의 일 실시예에 따른 서버 장치(400)의 기능 구성의 일 예를 나타낸다.

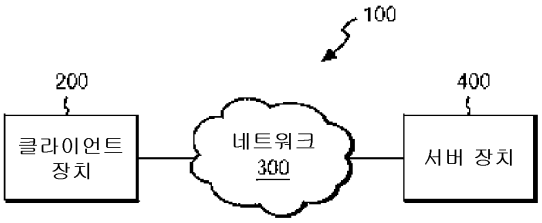
[0083] 도 5(a)는 본 발명의 실시예에 따른 클라이언트 장치(200)에서의, 서버 장치(400)에 의한 통신 상대를 인증하기 위한 처리 흐름의 일 예를 나타내는 흐름도를 나타낸다. 도 5(b)는 본 발명의 실시예에 따른 일시 전자 증명서 작성 처리의 흐름의 일 예를 나타내는 흐름도이다. 도 5(c)는 본 발명의 실시예에 따른 본인 확인 정보 작성 처리의 흐름의 일 예를 나타내는 흐름도이다.

[0084] 도 6(a)는 본 발명의 실시예에 따른 서버 장치(400)에서의 통신 상대 인증을 위한 처리의 흐름의 일 예를 나타내는 흐름도를 나타낸다. 도 6(b)는 본 발명의 실시예에 따른 전자 증명서 검증 처리의 흐름의 일 예를 나타내는 흐름도이다. 도 6(c)는 본 발명의 실시예에 따른 일시 전자 증명서 검증 처리의 흐름의 일 예를 나타내는 흐름도이다.

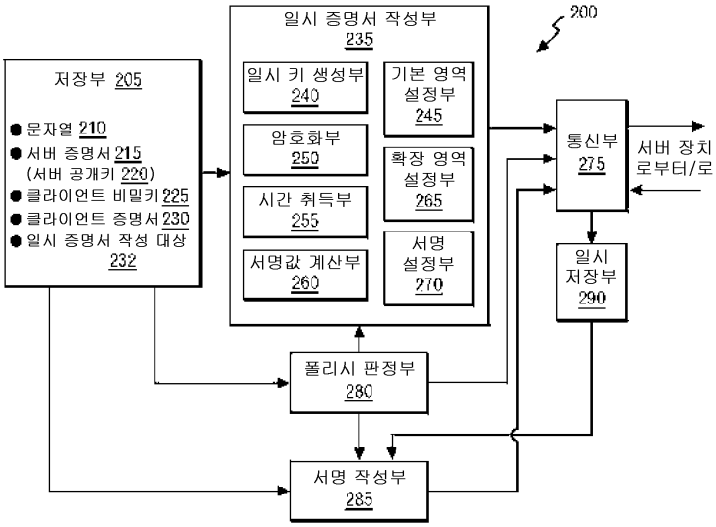
[0085] 도 7은 본 발명의 실시예에 따른 클라이언트 장치(200) 및 서버 장치(400)의 하드웨어 구성의 일 예를 나타낸다.

도면

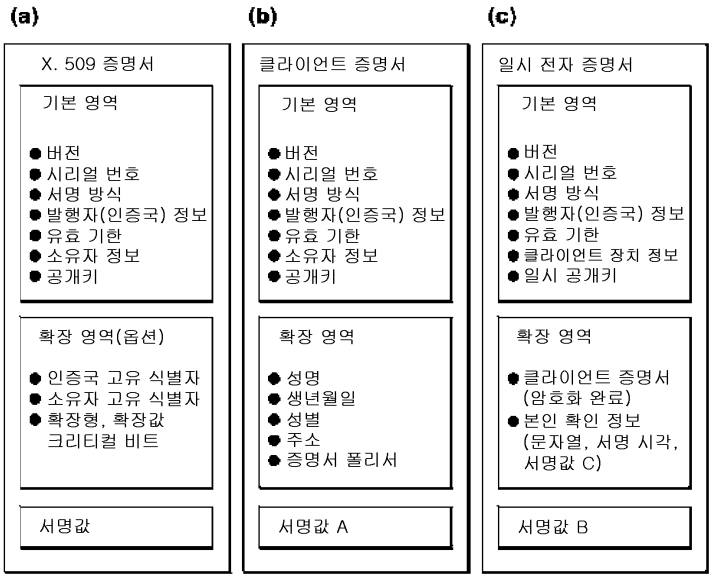
도면1



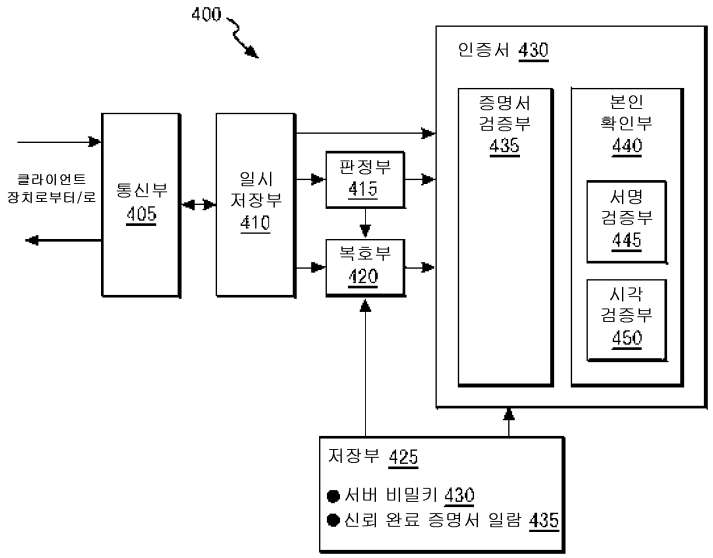
도면2



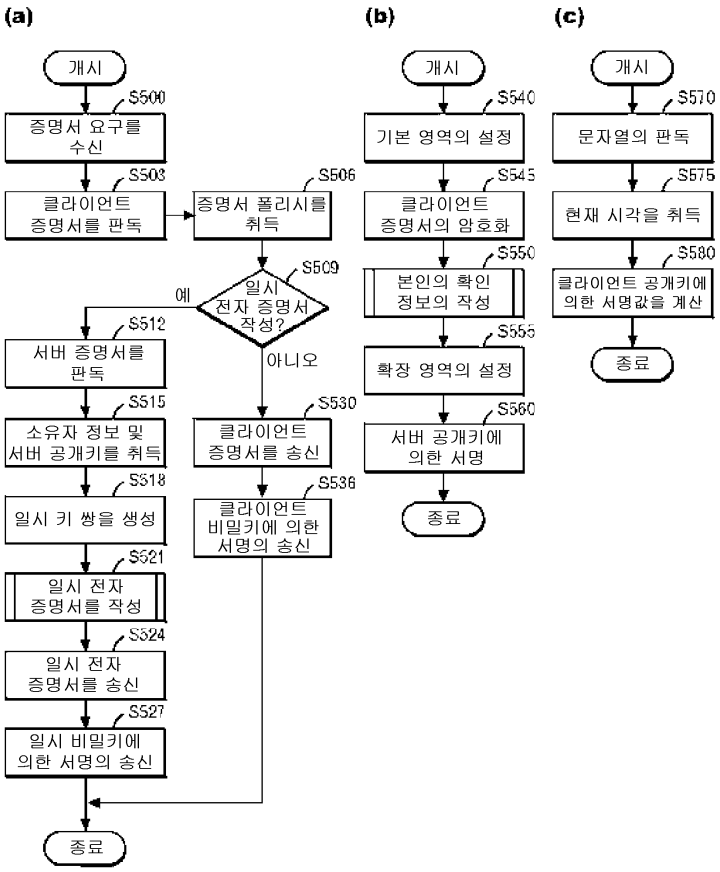
도면3



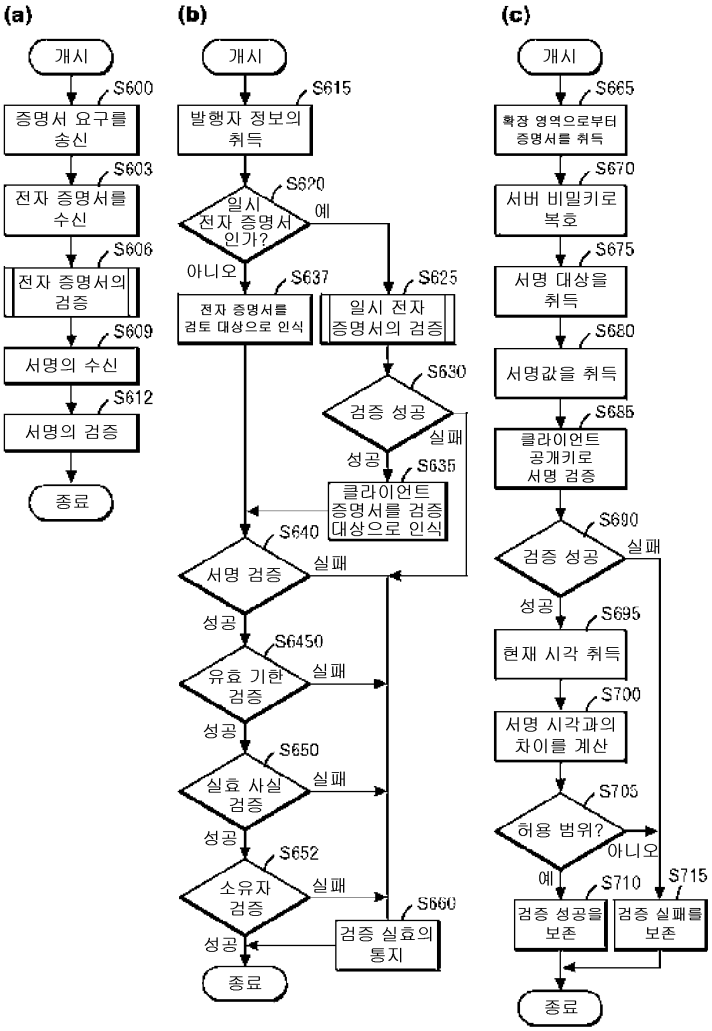
도면4


400
인증서 430
증명서 검증부 435
본인 확인부 440
서명 검증부 445
시각 검증부 450
클라이언트 장치로부터/로
통신부 405
일시 저장부 410
판정부 415
복호부 420
저장부 425
서버 비밀키 430
신뢰 완료 증명서 일람 435

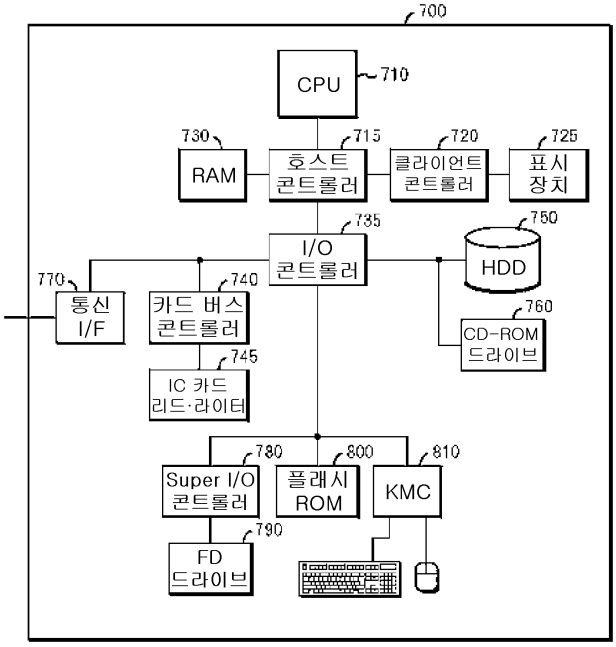
도면5


(a)
(b)
(c)
개시
S500
증명서 요구를 수신
S503
클라이언트 증명서를 판독
S506
증명서 폴리시를 취득
S509
일시 전자 증명서 작성?
예
아니오
S512
서버 증명서를 판독
S515
소유자 정보 및 서버 공개키를 취득
S518
일시 키 쌍을 생성
S521
일시 전자 증명서를 작성
S524
일시 전자 증명서를 송신
S527
일시 비밀키에 의한 서명의 송신
S530
클라이언트 증명서를 송신
S536
클라이언트 비밀키에 의한 서명의 송신
종료
S540
기본 영역의 설정
S545
클라이언트 증명서의 암호화
S550
본인의 확인 정보의 작성
S555
확장 영역의 설정
S560
서버 공개키에 의한 서명
종료
S570
문자열의 판독
S575
현재 시각을 취득
S580
클라이언트 공개키에 의한 서명값을 계산
종료

도면6


(a)
개시
S600
증명서 요구를 송신
S603
전자 증명서를 수신
S606
전자 증명서의 검증
S609
서명의 수신
S612
서명의 검증
종료
(b)
개시
S615
발행자 정보의 취득
S620
일시 전자 증명서인가?
예
아니오
S637
전자 증명서를 검토 대상으로 인식
S625
일시 전자 증명서의 검증
S630
검증 성공
실패
성공
S635
클라이언트 증명서를 검증 대상으로 인식
S640
서명 검증
실패
성공
S6450
유효 기한 검증
실패
성공
S650
실효 사실 검증
실패
성공
S652
소유자 검증
실패
S660
검증 실효의 통지
성공
종료
(c)
개시
S665
확장 영역으로부터 증명서를 취득
S670
서버 비밀키로 복호
S675
서명 대상을 취득
S680
서명값을 취득
S685
클라이언트 공개키로 서명 검증
S690
검증 성공
실패
성공
S695
현재 시각 취득
S700
서명 시각과의 차이를 계산
S705
허용 범위?
아니오
예
S710
검증 성공을 보존
S715
검증 실패를 보존
종료

도면7


700
CPU
710
730
RAM
715
호스트
콘트롤러
720
클라이언트
콘트롤러
725
표시
장치
735
I/O
콘트롤러
750
HDD
770
통신
I/F
740
카드 버스
콘트롤러
760
CD-ROM
드라이브
745
IC 카드
리드·라이터
780
Super I/O
콘트롤러
800
플래시
ROM
810
KMC
790
FD
드라이브