(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2016 년 2 월 4 일 (04.02.2016)

WIPO | PCT

(10) 국제공개번호
WO 2016/018005 A1

(51) 국제특허분류:
H04L 9/32 (2006.01)

(21) 국제출원번호: PCT/KR2015/007739

(22) 국제출원일: 2015 년 7 월 24 일 (24.07.2015)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2014-0097601 2014 년 7 월 30 일 (30.07.2014) KR

(71) 출원인: **한국전력공사 (KOREA ELECTRIC POWER CORPORATION)** [KR/KR]; 520-350 전라남도 나주시 전력로 55, Jeollanam-do (KR).

(72) 발명자: **전경석 (JEON, Kyung Seok)**; 463-832 경기도 성남시 분당구 서현로 478 번길 14-3, Gyeonggi-do (KR). **김충효 (KIM, Chung Hyo)**; 305-727 대전시 유성구 전민로 71, 109 동 902 호, Daejeon (KR). **임용훈 (LIM, Yong Hun)**; 305-727 대전시 유성구 전민로 71, 106 동 1303 호, Daejeon (KR). **주성호 (JU, Seong Ho)**; 305-727 대전시 유성구 전민로 71, 107 동 1502 호, Daejeon (KR). **김종관 (KIM, Jong Kwan)**; 472-954 경기도 남양주시 늘을 3 로 7, 1108 동 1404 호, Gyeonggi-do (KR). **성창환 (SUNG, Chang Hwan)**; 472-951 경기도 남양주시 별내 5 로 81, 3106 동 1902 호, Gyeonggi-do (KR).

(74) 대리인: **특허법인 아주양헌 (AJU KIM CHANG & LEE)**; 137-860 서울시 서초구 사임당로 174, 강남미래타워 12-13 층, Seoul (KR).

(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

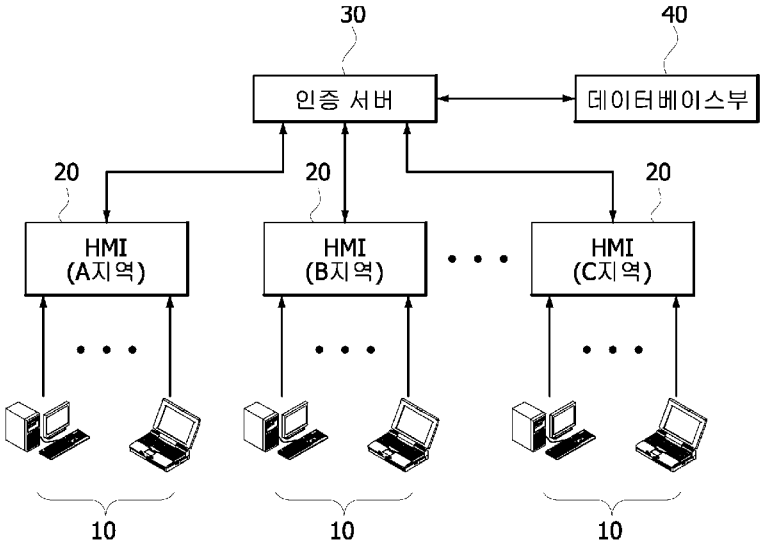
(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

공개:

— 국제조사보고서와 함께 (조약 제 21 조(3))

(54) **Title**: DISTRICT-BASED USER AUTHENTICATION DEVICE AND METHOD

(54) **발명의 명칭** : 지역 기반 사용자 인증 장치 및 방법



20 ... HMI (district)
30 ... Authentication server
40 ... Database unit

(57) **Abstract**: The present invention comprises the steps of: receiving a certificate for a control system from a user terminal and generating source information of an authentication request by a human-machine interface (HMI); generating an authentication request message using the certificate and the source information of an authentication request and transferring the authentication request message to an authentication server by the HMI; separating the certificate and the source information of the authentication request from the authentication request message and transferring identification information of the certificate to a database unit by the authentication server; transferring configured district information matched to the identification information to the authentication server by the database unit; and comparing the source information of the authentication request and the configured district information and determining whether they are the same, generating an authentication result on the basis of a result of the determination, and transferring the authentication result to the HMI, by the authentication server.

(57) 요약서:

[다음 쪽 계속]

WO 2016/018005 A1

본 발명은 HMI(Human-Machine Interface)가 사용자 단말로부터 제어시스템에 대한 인증서를 전달받아 인증요청 발생지 정보를 생성하는 단계, HMI 가 인증서와 인증요청 발생지 정보를 이용하여 인증요청 메세지를 생성하고, 인증요청 메세지를 인증서버로 전달하는 단계, 인증서버가 인증요청 메세지에서 인증서와 인증요청 발생지 정보를 분리하고, 인증서의 식별정보를 데이터베이스부로 전달하는 단계, 데이터베이스부가 식별정보에 매칭된 설정지역 정보를 상기 인증서버로 전달하는 단계 및 인증서버가 인증요청 발생지 정보와 설정지역 정보를 비교하여 동일 여부를 판정하고 판정 결과에 따라 인증결과를 생성하여 HMI 로 전달하는 단계를 포함하는 것을 특징으로 한다.

명세서

발명의 명칭: 지역 기반 사용자 인증 장치 및 방법

기술분야

[1] 본 발명은 지역 기반 사용자 인증 장치 및 방법에 관한 것으로서, 보다 상세하게는 에 사용자로부터 제어시스템에 대한 인증을 요청받는 경우, 사용자가 인증을 요청한 인증요청 발생지 정보와 해당 사용자에게 기 설정된 설정지역 정보가 동일하면 해당 사용자에게 제어 시스템에 대한 접근권한을 부여하는 지역 기반 사용자 인증 장치 및 방법에 대한 관한 것이다.

[2]

배경기술

[3] 전력 제어시스템(전력 SCADA(Supervisory Control and Data Acquisition))은 국가 주요 정보통신 기반시설로 지정되어 운영되고 있으며, 비인가자가 위·변조 공격으로 제어시스템을 장악하는 위험을 방지하고자 사용자 인증절차를 수립할 것을 권고하고 있다.

[4] 사용자는 HMI(Human-Machine Interface)을 통하여 전력설비의 감시·제어를 수행할 수 있는데, HMI는 사용자가 제시한 인증서를 인증서버에 전달하여 검증받은 후, 사용자의 전력설비 접근 여부를 결정한다.

[5] 전력시스템 내 사용자는 급전분소에서 주요 제어명령을 전송할 수 있다. 제어명령 수행 전에 본인의 인증서를 급전분소의 HMI에 전달하고, HMI는 해당 인증서를 급전소를 거쳐 전력 SCADA에 있는 인증서버에 검증요청을 하며, 그 검증결과를 수신한다. 인증서가 정상적으로 발행되었고 아직 유효기간이 남았다면, HMI는 사용자의 접근을 허용한다.

[6] 그러나, 사용자가 인사이동 등으로 인하여 다른 급전분소에 근무하게 된 후, 자신의 인증서로 현재의 급전분소의 HMI를 통해 전력설비에 접근시도를 하였을 경우, 상기한 바와 같은 과정을 거쳐 인증이 가능하다. 이 과정에서 사용자의 인증서가 정상적으로 발행된 것이고 유효기간이 남았다면, HMI는 접근을 허용한다.

[7] 그러나, 상기한 인증체계는 사용자의 위치와 상관없이 인증서의 유효성 검증만 통과되면 어떠한 급전분소에서도 인증받을 수 있도록 하고 있다. 만약 사용자가 인사이동없이 다른 급전분소의 HMI에 접근시도를 하더라도 인증서버가 이를 승인하게 된다.

[8] 즉, 사용자는 본인의 현재 근무지 이외의 다른 급전분소에서도 전력설비를 사용할 수 있다. 따라서, 종래의 인증서 인증체계는 사용자의 악의적 고의 또는 부주의로 인한 인증서 분실 등에 의해 전력설비의 제어권한이 광범위하게 노출되는 문제점이 있었다.

[9] 본 발명의 배경기술은 대한민국 공개특허공보 제2012-0136954호(2012.12.20)에

개시되어 있다.

[10]

발명의 상세한 설명

기술적 과제

[11] 본 발명은 전술한 문제점을 해결하기 위해 창안된 것으로서, 본 발명의 목적은 사용자로부터 제어시스템에 대한 인증을 요청받는 경우 사용자가 인증을 요청한 인증요청 발생지 정보와 해당 사용자에게 기 설정된 설정지역 정보가 동일하면 해당 사용자에게 제어 시스템에 대한 접근권한을 승인하는 지역 기반 사용자 인증 장치 및 방법을 제공하는 것이다.

[12] 본 발명의 다른 목적은 동일한 사용자라 하더라도 기 설정된 설정지역 이외의 지역에서는 해당 제어시스템에 대한 접근권한을 제한하여 제어시스템에 대한 무분별한 접근을 제한하고, 제어시스템에 대한 보안성을 더욱 향상시키는 지역 기반 사용자 인증 장치 및 방법을 제공하는 것이다.

[13]

과제 해결 수단

[14] 본 발명의 일 측면에 따른 지역 기반 사용자 인증 장치는 사용자 단말로부터 사용자의 인증서를 전달받아 인증요청 발생지 정보를 생성하고 상기 인증서와 상기 인증요청 발생지 정보를 이용하여 인증요청 메세지를 생성하는 HMI(Human-Machine Interface); 상기 인증서의 식별정보와 매칭된 설정지역 정보를 저장하는 데이터베이스부; 및 상기 인증요청 메세지에서 상기 인증서와 상기 인증요청 발생지 정보를 분리하고, 상기 인증서의 식별정보를 상기 데이터베이스부로 전달하여 상기 데이터베이스부로부터 상기 설정지역 정보를 전달받은 후, 상기 인증요청 발생지 정보와 상기 설정지역 정보를 비교하여 동일 여부를 판정하고 판정 결과에 따라 인증결과를 생성하여 상기 HMI로 전달하는 단계를 포함하는 것을 특징으로 한다.

[15] 본 발명에서, 상기 인증서버는 상기 인증요청 발생지 정보와 상기 설정지역 정보가 동일하면 인증승인 메세지를 생성하고, 상기 인증요청 발생지 정보와 상기 설정지역 정보가 상이하면 인증거부 메세지를 생성하는 것을 특징으로 한다.

[16] 본 발명에서, 상기 인증요청 발생지 정보는 상기 HMI의 설치 위치에 근거하여 생성되는 것을 특징으로 한다.

[17] 본 발명에서, 상기 인증요청 발생지 정보는 인증서 교환 프로토콜을 통해 전송되고, CMP(Certificate Management Protocol) 또는 OCSP(Online Certificate Status Protocol) 중 어느 하나인 것을 특징으로 한다.

[18] 본 발명에서, 상기 인증요청 발생지 정보와 상기 설정지역 정보의 계층구조는 동일한 것을 특징으로 한다.

[19] 본 발명에서, 상기 인증서버는 상기 인증서의 전자서명을 검증하여 상기

인증결과를 생성한 후 상기 HMI로 전달하는 것을 특징으로 한다.

[20] 본 발명에서, 상기 인증서버는 상기 인증서의 전자서명에 대한 검증이 성공함과 더불어 상기 인증요청 발생지 정보와 상기 설정지역 정보가 동일한 것으로 판정되면 인증승인 메세지를 생성하고, 상기 인증서의 전자서명에 대한 검증이 실패하거나 상기 인증요청 발생지 정보와 상기 설정지역 정보가 상이한 것으로 판정되면 인증거부 메세지를 생성하는 것을 특징으로 한다.

[21] 본 발명의 일 측면에 따른 지역 기반 사용자 인증 방법은 HMI(Human-Machine Interface)가 사용자 단말로부터 사용자의 인증서를 전달받아 인증요청 발생지 정보를 생성하는 단계; 상기 HMI가 상기 인증서와 상기 인증요청 발생지 정보를 이용하여 인증요청 메세지를 생성하고, 상기 인증요청 메세지를 인증서버로 전달하는 단계; 상기 인증서버가 상기 인증요청 메세지에서 상기 인증서와 상기 인증요청 발생지 정보를 분리하고, 상기 인증서의 식별정보를 상기 데이터베이스부로 전달하는 단계; 상기 데이터베이스부가 상기 식별정보에 매칭된 설정지역 정보를 상기 인증서버로 전달하는 단계; 및 상기 인증서버가 상기 인증요청 발생지 정보와 상기 설정지역 정보를 비교하여 동일 여부를 판정하고 판정 결과에 따라 인증결과를 생성하여 상기 HMI로 전달하는 단계를 포함하는 것을 특징으로 한다.

[22] 본 발명은 상기 인증결과를 생성하여 상기 HMI로 전달하는 단계에서, 상기 인증서버가 상기 인증요청 발생지 정보와 상기 설정지역 정보가 동일하면 인증승인 메세지를 생성하고, 상기 인증요청 발생지 정보와 상기 설정지역 정보가 상이하면 인증거부 메세지를 생성하는 것을 특징으로 특징으로 한다.

[23] 본 발명에서, 상기 인증요청 발생지 정보는 상기 HMI의 설치 위치에 근거하여 생성되는 것을 특징으로 한다.

[24] 본 발명에서, 상기 인증요청 발생지 정보는 인증서 교환 프로토콜을 통해 전송되고, CMP(Certificate Management Protocol) 또는 OCSP(Online Certificate Status Protocol) 중 어느 하나인 것을 특징으로 한다.

[25] 본 발명에서, 상기 인증요청 발생지 정보와 상기 설정지역 정보의 계층구조는 동일한 것을 특징으로 한다.

[26] 본 발명은 상기 인증서버가 상기 인증서의 전자서명을 검증하여 상기 인증결과를 생성한 후 상기 HMI로 전달하는 단계를 더 포함하는 것을 특징으로 한다.

[27] 본 발명은 상기 인증결과를 생성하여 상기 HMI로 전달하는 단계에서, 상기 인증서버가 상기 인증서의 전자서명에 대한 검증이 성공함과 더불어 상기 인증요청 발생지 정보와 상기 설정지역 정보가 동일한 것으로 판정되면 인증승인 메세지를 생성하고, 상기 인증서의 전자서명에 대한 검증이 실패하거나 상기 인증요청 발생지 정보와 상기 설정지역 정보가 상이한 것으로 판정되면 인증거부 메세지를 생성하는 것을 특징으로 한다.

[28]

발명의 효과

[29] 본 발명은 사용자로부터 제어시스템에 대한 인증을 요청받는 경우 사용자가 인증을 요청한 인증요청 발생지 정보와 해당 사용자에게 기 설정된 설정 지역이 동일하면 해당 사용자에게 제어 시스템에 대한 접근권한을 승인한다.

[30] 본 발명은 동일한 사용자라하더라도 기 설정된 설정지역 이외의 지역에서는 해당 제어시스템에 대한 접근권한을 제한하여 제어시스템에 대한 무분별한 접근을 제한할 수 있고, 제어시스템에 대한 보안성을 더욱 향상시킨다.

[31]

도면의 간단한 설명

[32] 도 1 은 본 발명의 일 실시예에 따른 지역 기반 사용자 인증 장치의 블럭 구성도이다.

[33] 도 2 는 본 발명의 일 실시예에 따른 HMI의 블럭 구성도이다.

[34] 도 3 은 본 발명의 일 실시예에 따른 인증요청 메세지의 일 예를 나타낸 도면이다.

[35] 도 4 는 본 발명의 일 실시예에 따른 인증서버의 블럭 구성도이다.

[36] 도 5 는 본 발명의 일 실시예에 따른 데이터베이스부의 블럭 구성도이다.

[37] 도 6 은 본 발명의 일 실시예에 따른 지역 기반 사용자 인증 방법을 도시한 순서도이다.

[38]

발명의 실시를 위한 최선의 형태

[39] 이하에서는 본 발명의 일 실시예에 따른 지역 기반 사용자 인증 장치 및 방법을 첨부된 도면들을 참조하여 상세하게 설명한다. 이러한 과정에서 도면에 도시된 선들의 두께나 구성요소의 크기 등은 설명의 명료성과 편의상 과장되게 도시되어 있을 수 있다. 또한 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로써, 이는 이용자, 운용자의 의도 또는 관례에 따라 달라질 수 있다. 그러므로 이러한 용어들에 대한 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야할 것이다.

[40]

발명의 실시를 위한 형태

[41] 도 1 은 본 발명의 일 실시예에 따른 지역 기반 사용자 인증 장치의 블럭 구성도이고, 도 2 는 본 발명의 일 실시예에 따른 HMI의 블럭 구성도이며, 도 3 은 본 발명의 일 실시예에 따른 인증요청 메세지의 일 예를 나타낸 도면이며, 도 4 는 본 발명의 일 실시예에 따른 인증서버의 블럭 구성도이며, 도 5 는 본 발명의 일 실시예에 따른 데이터베이스부의 블럭 구성도이다.

[42] 도 1 을 참조하면, 본 발명의 일 실시예에 따른 지역 기반 사용자 인증 장치는 사용자 단말(10), HMI(Human-Machine Interface)(20), 인증서버(30) 및 데이터베이스부(40)를 포함한다.

[43] 사용자 단말(10)은 통신망(미도시)을 통해 HMI(20)와 접속하여 각종 정보를 송수신하는 것으로서, 사용자의 인증서를 HMI(20)로 전달하여 제어시스템(미도시)에 대한 접근을 요청하고 인증서버(30)에서의 인증결과를 HMI(20)로부터 전달받아 출력한다. 사용자 단말(10)로는 통상의 업무용 PC(Personal Computer), 노트북 컴퓨터, 테블릿 PC, 스마트폰, PDA(Personal Digital Assistant) 등이 포함될 수 있으며, 이외에도 사용자의 인증서를 HMI(20)에 입력하여 제어시스템에 대한 접근을 요청하고 그 인증결과를 수신하며 이를 토대로 각종 업무를 수행 및 작업할 수 있는 다양한 단말이 모두 포함될 수 있다.

[44] 참고로, 제어시스템은 인증체계를 구비하여 비인가자에 대한 접속을 제한하는 중요 시설 시스템으로서, 국가 주요 정보통신 기반시설인 전력 제어시스템, 예를 들어 전력 SCADA(Supervisory Control and Data Acquisition)가 포함될 수 있다. 이에 본 실시예에서는 상기한 전력 제어시스템을 예시로 설명한다.

[45] HMI(20)는 사용자가 제어시스템에 대한 감시 및 제어를 수행할 수 있도록 하는 것으로서, 사용자 단말(10)로부터 사용자의 인증서를 전달받고, 인증서와 인증요청 발생지 정보를 이용하여 인증요청 메세지를 생성한 후, 인증서버(30)로 전달한다. 이후, HMI(20)는 인증서버(30)로부터 인증결과를 전달받아 사용자 단말(10)로 전달하고, 인증결과에 따라 제어시스템에 대한 사용자의 접근을 제한하거나 사용자에게 접근권한을 부여한다. 여기서, HMI(20)는 도 1 의 A지역, B지역 및 C지역과 같이 각 지역별로 각기 마련될 수 있다.

[46] 도 2 를 참조하면, HMI(20)는 인증요청 발생지 생성부(21), 인증 요청부(22) 및 인증결과 처리부(23)를 포함한다.

[47] 인증요청 발생지 생성부(21)는 사용자 단말(10)로부터 인증서가 전달되면 인증요청 발생지 정보를 생성한다. 인증요청 발생지 생성부(21)는 인증요청 발생지 정보를 현재 HMI(20)가 설치된 지역을 근거로 생성한다. HMI(20)가 설치된 지역은 사전에 설정된다.

[48] 인증 요청부(22)는 인증서와 인증요청 발생지 생성부(21)에서 생성된 인증요청 발생지 정보를 이용하여 인증요청 메세지를 생성하고, 생성된 인증요청 메세지를 인증서버(30)로 전달한다.

[49] 이 경우 인증 요청부(22)는 생성된 인증요청 메세지를 인증서 교환 프로토콜, 예를 들어 CMP(Certificate Management Protocol) 또는 OCSP(Online Certificate Status Protocol) 중 어느 하나로 전송한다. 일 예로, 제어시스템이 전력 제어시스템일 경우에는 CRL(Certificate Revocation List)의 갱신주기로 인해 보안상 취약점이 발생될 수 있으므로, 인증 요청부(22)는 상기한 CMP와 OCSP 중 OCSP를 통해 인증을 수행할 수 있다.

[50] 도 3 을 참조하면, OCSP의 인증요청 메세지(OCSP Request)의 구조에 있어서, requestorName은 선택적 필드(Optical field)이다. 이에, 인증요청 발생지 정보를 계층구조로 표현한 후, 이를 인증요청 메시지의 requestorName에 부가하여 전송한다.

[51] 예를 들어, 사용자가 전력 제어시스템을 운영하는 관리자이고, 해당 전력 제어시스템을 제어하기 위한 조직이 지역조직, 세부지역조직으로 세분화될 경우, 인증요청 발생지는 '지역조직/세부지역조직/감시제어담당부서/담당업무' 또는 '남서울지역본부/강남전력지사/변전팀/급전분소' 등으로 생성될 수 있다.

[52] 더욱이, 인증 요청부(22)는 상기한 인증요청 발생지 정보의 계층구조를 후술한 설정지역 정보의 계층구조와 동일하게 생성함으로써, 인증서버(30)가 인증요청 발생지 정보와 설정지역 정보를 정확하게 비교할 수 있도록 한다.

[53] 여기서, 설정지역 정보는 사용자별로 각기 설정된 지역정보로서 인증서의 식별정보에 매칭되며, 상기한 HMI(20)의 현재 위치에 따라 다양하게 설정될 수 있다. 도 1 을 참조하면 인증요청 발생지 정보와 설정지역 정보는 HMI(20)가 현재 설치된 A지역, B지역, C지역 중 어느 하나가 될 수 있다. 이 경우 설정지역 정보는 인증서의 식별정보에 매칭되고, 해당 HMI(20)의 현재 위치를 토대로 생성된 인증요청 발생지 정보와 해당 인증서의 식별정보에 매칭된 설정지역 정보가 동일한지 여부를 토대로 해당 사용자의 제어시스템에 대한 접근이 허용되므로, 각 사용자의 제어시스템에 대한 접근을 현재 위치에 따라 제한할 수 있게 된다.

[54] 일 예로, 사용자가 설정지역으로 A지역 HMI(20)를 토대로 설정된 경우, 나머지 B지역 HMI(20) 및 C지역 HMI(20)에서의 제어시스템에 대한 접근은 제한된다.

[55] 인증결과 처리부(23)는 인증서버(30)의 인증결과를 처리하는 것으로서, 인증서버(30)로부터 인증결과를 전달받으면 이 인증결과를 사용자 단말(10)로 전달하고 인증결과를 토대로 해당 사용자의 제어시스템에 대한 접근을 제한하거나 사용자에게 제어시스템에 대한 접근권한을 부여한다.

[56] 인증서버(30)는 HMI(20)로부터 전달받은 인증요청 메세지를 인증서와 인증요청 발생지 정보로 분리하고, 인증서의 식별정보를 데이터베이스부(40)에 전달한다. 이후, 데이터베이스부(40)로부터 식별정보에 매칭된 설정지역 정보를 전달받으면, 인증서버(30)는 인증요청 발생지 정보와 설정지역 정보를 비교하여 동일 여부를 판정하고, 그 판정 결과에 따라 인증결과를 생성하여 HMI(20)로 전달한다.

[57] 도 4 를 참조하면, 인증서버(30)는 인증요청 메세지 처리부(31), 전자서명 검증부(32), 식별정보 추출부(33), 비교부(34) 및 인증결과 생성부(35)를 포함한다.

[58] 인증요청 메세지 처리부(31)는 HMI(20)의 인증 요청부(22)로부터 인증요청 메세지를 전달받으면 이 인증요청 메세지를 인증서와 인증요청 발생지 정보로 분리한다. 이후 인증요청 메세지 처리부(31)는 인증서를 전자서명 검증부(32)와 식별정보 추출부(33)로 각각 전달하고 인증요청 발생지 정보를 비교부(34)로 전달한다.

[59] 전자서명 검증부(32)는 인증요청 메세지 처리부(31)에 의해 분리된 인증서의 전자서명을 검증하고, 그 검증결과를 인증결과 생성부(35)로 전달한다.

[60] 식별정보 추출부(33)는 인증요청 메세지 처리부(31)에 의해 분리된 인증서의 식별정보를 추출한 후, 추출된 식별정보를 데이터베이스부(40)로 전달하고 데이터베이스부(40)에 해당 식별정보에 매칭된 설정지역 정보를 요청한다.

[61] 여기서, 식별정보로는 사용자의 개인정보가 채용될 수 있으며, 이 개인정보에는 사용자의 주민등록번호 또는 조직내 개인번호(사번) 등이 포함될 수 있다.

[62] 비교부(34)는 인증요청 메세지 처리부(31)로부터 전달받은 인증요청 발생지 정보와 데이터베이스부(40)로부터 전달받은 설정지역 정보를 비교하여 동일 여부를 판단하고 그 판정 결과를 인증결과 생성부(35)로 전달한다.

[63] 인증결과 생성부(35)는 전자서명 검증부(32)의 검증결과와 비교부(34)의 판정결과를 토대로 인증결과를 생성하여 HMI(20)로 전달한다.

[64] 즉, 인증결과 생성부(35)는 인증서의 전자서명에 대한 검증이 성공함과 더불어 인증요청 발생지 정보와 설정지역 정보가 동일하면 인증승인 메세지를 생성한다. 반면에, 인증결과 생성부(35)는 인증서의 전자서명에 대한 검증이 실패하거나 인증요청 발생지 정보와 설정지역 정보가 상이한 것으로 판정되면 인증거부 메세지를 생성한다.

[65] 데이터베이스부(40)는 인증서버(30)로부터 식별정보를 전달받으면, 이 식별정보에 매칭된 설정지역 정보를 추출하여 인증서버(30)로 전달한다. 이러한 데이터베이스부(40)는 식별정보에 매칭된 설정지역 정보를 저장하는 저장부(41), 및 저장부(41)에서 식별정보에 매칭된 설정지역 정보를 추출하여 인증서버(30)로 전달하는 설정지역 추출부(42)를 포함한다.

[66] 이하, 본 발명의 일 실시예에 따른 지역 기반 사용자 인증 방법을 도 5 를 참조하여 상세하게 설명한다.

[67] 도 5 는 본 발명의 일 실시예에 따른 지역 기반 사용자 인증 방법을 도시한 순서도이다.

[68] 도 5 를 참조하면, 사용자 단말(10)이 통신망(미도시)을 통해 사용자의 인증서를 HMI(20)로 전달하여 제어시스템(미도시)에 대한 접근을 요청한다.

[69] HMI(20)의 인증요청 발생지 생성부(21)는 사용자 단말(10)로부터 제어시스템에 대한 인증서를 전달받고(S10), HMI(20)가 설치된 지역을 근거로 인증요청 발생지 정보를 생성한다(S20). 이 경우, 인증요청 발생지 생성부(21)는 상기한 인증요청 발생지 정보의 계층구조를 후술한 설정지역 정보의 계층구조와 동일하게 생성한다.

[70] 이후 HMI(20)의 인증 요청부(22)는 인증요청 발생지 생성부(21)에서 생성된 인증요청 발생지 정보와 인증서를 이용하여 인증요청 메세지를 생성한다(S30). 인증 요청부(22)는 인증요청 메시지를 인증서 교환 프로토콜, 예를 들어 CMP 또는 OCSP 중 어느 하나로 전송한다. 인증 요청부(22)는 선택적 필드인 requestorName에 인증요청 발생지 정보를 부가한다.

[71] 이후, HMI(20)는 인증요청 메세지를 인증서버(30)로 전달한다(S40).

[72] 인증서버(30)의 인증요청 메세지 처리부(31)는 HMI(20)로부터 인증요청 메세지를 전달받으면 이 인증요청 메세지를 인증서와 인증요청 발생지 정보로 분리(S50)하고, 인증서를 전자서명 검증부(32)와 식별정보 추출부(33)로 각각 전달하고 인증요청 발생지 정보를 비교부(34)로 전달한다.

[73] 이에, 인증서버(30)의 식별정보 추출부(33)는 인증요청 메세지 처리부(31)로부터 전달받은 인증서의 식별정보를 추출(S60)한 후, 추출된 식별정보를 데이터베이스부(40)로 전달(S70)하여 데이터베이스부(40)에 해당 식별정보에 매칭된 설정지역 정보를 요청한다.

[74] 설정지역 정보를 요청받은 데이터베이스부(40)의 설정지역 추출부(42)는 저장부(41)에서 식별정보에 매칭된 설정지역 정보를 추출(S80)하고, 추출된 설정지역 정보를 인증서버(30)로 전달한다(S90).

[75] 한편, 인증서버(30)의 전자서명 검증부(32)는 인증요청 메세지 처리부(31)로부터 전달받은 인증서의 전자서명을 검증한다(S100). 전자서명 검증부(32)는 인증서의 전자서명 검증에 성공하는지를 체크하고(S110), 전자서명 검증에 실패하면 그 검증결과를 인증결과 생성부(35)로 전달한다.

[76] 이에 따라, 인증서버(30)의 인증결과 생성부(35)는 인증거부 메세지를 생성하고(S130), 생성된 인증거부 메세지를 HMI(20)로 전달한다(S140).

[77] 인증거부 메세지를 전달받은 HMI(20)의 인증결과 처리부(23)는 사용자 단말(10)로 인증거부 메세지를 전달하고 해당 사용자의 제어시스템에 대한 접근을 제한한다(S150).

[78] 한편, 상술한 바와 같이 상기한 단계(S110)에서 인증서의 전자서명 검증이 성공한 것으로 체크되면, 인증서버(30)의 비교부(34)가 인증요청 메세지 처리부(31)로부터 전달받은 인증요청 발생지 정보와 데이터베이스부(40)로부터 전달받은 설정지역 정보를 비교하여 동일 여부를 판정(S120)하고, 그 판정 결과를 인증결과 생성부(35)로 전달한다.

[79] 이 경우, 인증서버(30)의 인증결과 생성부(35)는 인증서의 전자서명에 대한 검증이 성공함과 더불어 인증요청 발생지 정보와 설정지역 정보가 동일한 것으로 판정되면 인증승인 메세지를 생성하고(S130), 생성된 인증승인 메세지를 HMI(20)로 전달한다(S140). 이 경우, HMI(20)의 인증결과 처리부(23)는 인증승인 메세지를 사용자 단말(10)로 전달하고 사용자의 제어시스템에 대한 접근권한을 부여한다(S150).

[80] 반면에, 인증서버(30)의 인증결과 생성부(35)는 인증서의 전자서명에 대한 검증이 성공하더라도 인증요청 발생지 정보와 설정지역 정보가 상이한 것으로 판정되면 인증거부 메세지를 생성하고(S130), 생성된 인증거부 메세지를 HMI(20)로 전달한다(S140). 이 경우, HMI(20)의 인증결과 처리부(23)는 인증거부 메세지를 사용자 단말(10)로 전달하고 사용자의 제어시스템에 대한 접근을 제한한다(S150).

[81] 이와 같은 본 실시예는 사용자로부터 제어시스템에 대한 인증을 요청받는 경우

사용자가 인증을 요청한 인증요청 발생지 정보와 해당 사용자에게 기 설정된 설정 지역이 동일하면 해당 사용자에게 제어 시스템에 대한 접근권한을 승인한다.

[82] 또한 본 실시예는 동일한 사용자라하더라도 기 설정된 지역 이외의 지역에서는 해당 제어시스템에 대한 접근권한을 제한하여 제어시스템에 대한 무분별한 접근을 제한할 수 있고, 제어시스템에 대한 보안성을 더욱 향상시킬 수 있다.

[83] 본 발명은 도면에 도시된 실시예를 참고로 하여 설명되었으나, 이는 예시적인 것에 불과하며 당해 기술이 속하는 기술분야에서 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호범위는 아래의 특허청구범위에 의하여 정해져야할 것이다.

[84]

청구범위

[청구항 1] 사용자 단말로부터 사용자의 인증서를 전달받아 인증요청 발생지 정보를 생성하고 상기 인증서와 상기 인증요청 발생지 정보를 이용하여 인증요청 메세지를 생성하는 HMI(Human-Machine Interface);
상기 인증서의 식별정보와 매칭된 설정지역 정보를 저장하는 데이터베이스부; 및
상기 인증요청 메세지에서 상기 인증서와 상기 인증요청 발생지 정보를 분리하고, 상기 인증서의 식별정보를 상기 데이터베이스부로 전달하여 상기 데이터베이스부로부터 상기 설정지역 정보를 전달받은 후, 상기 인증요청 발생지 정보와 상기 설정지역 정보를 비교하여 동일 여부를 판정하고 판정 결과에 따라 인증결과를 생성하여 상기 HMI로 전달하는 단계를 포함하는 지역 기반 사용자 인증 장치.

[청구항 2] 제 1 항에 있어서,
상기 인증서버는 상기 인증요청 발생지 정보와 상기 설정지역 정보가 동일하면 인증승인 메세지를 생성하고, 상기 인증요청 발생지 정보와 상기 설정지역 정보가 상이하면 인증거부 메세지를 생성하는 것을 특징으로 하는 지역 기반 사용자 인증 장치.

[청구항 3] 제 1 항에 있어서, 상기 인증요청 발생지 정보는 상기 HMI의 설치 위치에 근거하여 생성되는 것을 특징으로 하는 지역 기반 사용자 인증 장치.

[청구항 4] 제 1 항에 있어서, 상기 인증요청 발생지 정보는 인증서 교환 프로토콜을 통해 전송되고, CMP(Certificate Management Protocol) 또는 OCSP(Online Certificate Status Protocol) 중 어느 하나인 것을 특징으로 하는 지역 기반 사용자 인증 장치.

[청구항 5] 제 1 항에 있어서, 상기 인증요청 발생지 정보와 상기 설정지역 정보의 계층구조는 동일한 것을 특징으로 하는 지역 기반 사용자 인증 장치.

[청구항 6] 제 1 항에 있어서, 상기 인증서버는 상기 인증서의 전자서명을 검증하여 상기 인증결과를 생성한 후 상기 HMI로 전달하는 것을 특징으로 하는 지역 기반 사용자 인증 장치.

[청구항 7] 제 6 항에 있어서, 상기 인증서버는
상기 인증서의 전자서명에 대한 검증이 성공함과 더불어 상기 인증요청 발생지 정보와 상기 설정지역 정보가 동일한 것으로 판정되면 인증승인 메세지를 생성하고, 상기 인증서의 전자서명에 대한 검증이 실패하거나 상기 인증요청 발생지 정보와 상기 설정지역 정보가 상이한 것으로 판정되면 인증거부 메세지를 생성하는 것을 특징으로 하는 지역 기반 사용자 인증 장치.

[청구항 8] HMI(Human-Machine Interface)가 사용자 단말로부터 사용자의 인증서를 전달받아 인증요청 발생지 정보를 생성하는 단계;

상기 HMI가 상기 인증서와 상기 인증요청 발생지 정보를 이용하여 인증요청 메세지를 생성하고, 상기 인증요청 메세지를 인증서버로 전달하는 단계;
상기 인증서버가 상기 인증요청 메세지에서 상기 인증서와 상기 인증요청 발생지 정보를 분리하고, 상기 인증서의 식별정보를 상기 데이터베이스부로 전달하는 단계;
상기 데이터베이스부가 상기 식별정보에 매칭된 설정지역 정보를 상기 인증서버로 전달하는 단계; 및
상기 인증서버가 상기 인증요청 발생지 정보와 상기 설정지역 정보를 비교하여 동일 여부를 판정하고 판정 결과에 따라 인증결과를 생성하여 상기 HMI로 전달하는 단계를 포함하는 지역 기반 사용자 인증 방법.

[청구항 9] 제 8 항에 있어서, 상기 인증결과를 생성하여 상기 HMI로 전달하는 단계에서,
상기 인증서버는 상기 인증요청 발생지 정보와 상기 설정지역 정보가 동일하면 인증승인 메세지를 생성하고, 상기 인증요청 발생지 정보와 상기 설정지역 정보가 상이하면 인증거부 메세지를 생성하는 것을 특징으로 하는 지역 기반 사용자 인증 방법.

[청구항 10] 제 8 항에 있어서, 상기 인증요청 발생지 정보는 상기 HMI의 설치 위치에 근거하여 생성되는 것을 특징으로 하는 지역 기반 사용자 인증 방법.

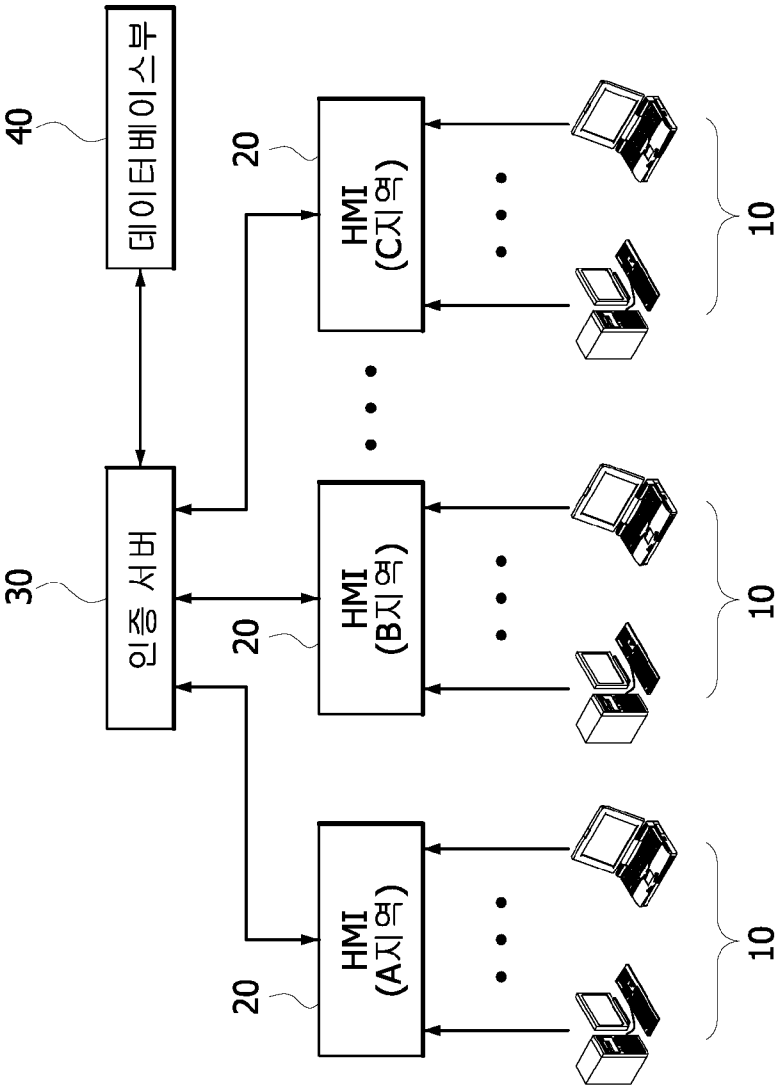
[청구항 11] 제 8 항에 있어서, 상기 인증요청 발생지 정보는 인증서 교환 프로토콜을 통해 전송되고, CMP(Certificate Management Protocol) 또는 OCSP(Online Certificate Status Protocol) 중 어느 하나인 것을 특징으로 하는 지역 기반 사용자 인증 방법.

[청구항 12] 제 8 항에 있어서, 상기 인증요청 발생지 정보와 상기 설정지역 정보의 계층구조는 동일한 것을 특징으로 하는 지역 기반 사용자 인증 방법.

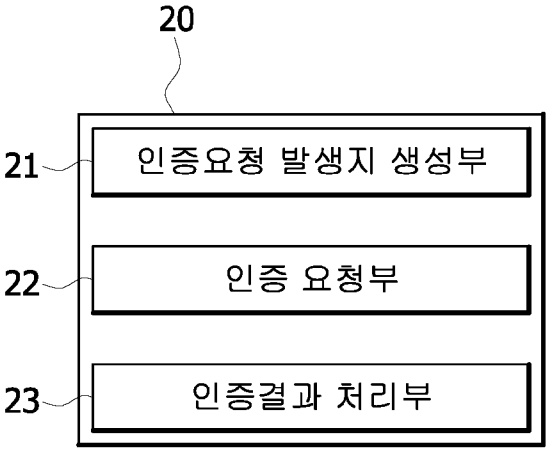
[청구항 13] 제 8 항에 있어서, 상기 인증서버가 상기 인증서의 전자서명을 검증하여 상기 인증결과를 생성한 후 상기 HMI로 전달하는 단계를 더 포함하는 것을 특징으로 하는 지역 기반 사용자 인증 방법.

[청구항 14] 제 13 항에 있어서, 상기 인증결과를 생성하여 상기 HMI로 전달하는 단계에서,
상기 인증서버는 상기 인증서의 전자서명에 대한 검증이 성공함과 더불어 상기 인증요청 발생지 정보와 상기 설정지역 정보가 동일한 것으로 판정되면 인증승인 메세지를 생성하고, 상기 인증서의 전자서명에 대한 검증이 실패하거나 상기 인증요청 발생지 정보와 상기 설정지역 정보가 상이한 것으로 판정되면 인증거부 메세지를 생성하는 것을 특징으로 하는 지역 기반 사용자 인증 방법.

[도1]


40
데이터베이스부
30
인증 서버
20
HMI (C지역)
20
HMI (B지역)
20
HMI (A지역)
10
10
10

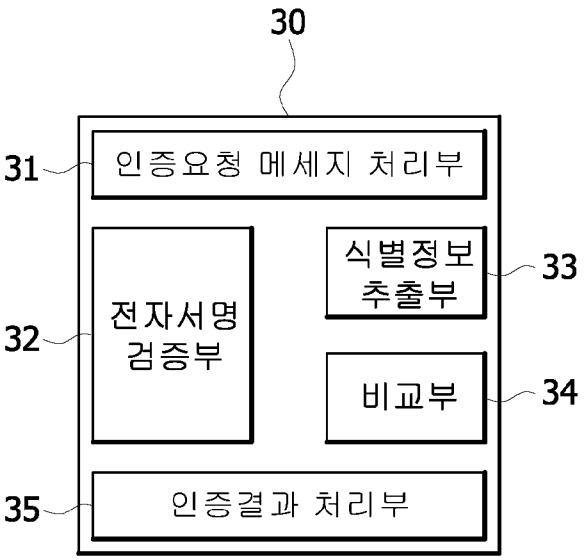
[도2]


20
21
인증요청 발생지 생성부
22
인증 요청부
23
인증결과 처리부

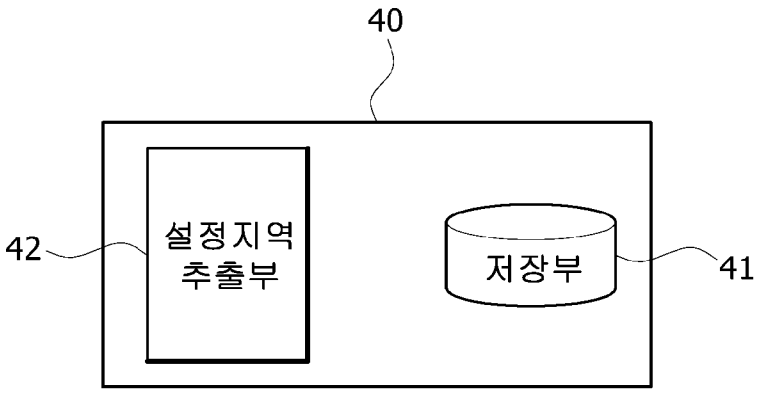
[도3]

```
OCSPRequest      ::=     SEQUENCE {
    tbsRequest                  TBSRequest,
    optionalSignature   [0]     EXPLICIT Signature OPTIONAL }

TBSRequest       ::=     SEQUENCE {
    version             [0]     EXPLICIT Version DEFAULT v1,
    requestorName       [1]     EXPLICIT GeneralName OPTIONAL,
    requestList                 SEQUENCE OF Request,
    requestExtensions   [2]     EXPLICIT Extensions OPTIONAL }

Signature        ::=     SEQUENCE {
    signatureAlgorithm      AlgorithmIdentifier,
    signature               BIT STRING,
    certs               [0] EXPLICIT SEQUENCE OF Certificate
OPTIONAL}
... 이하생략
```

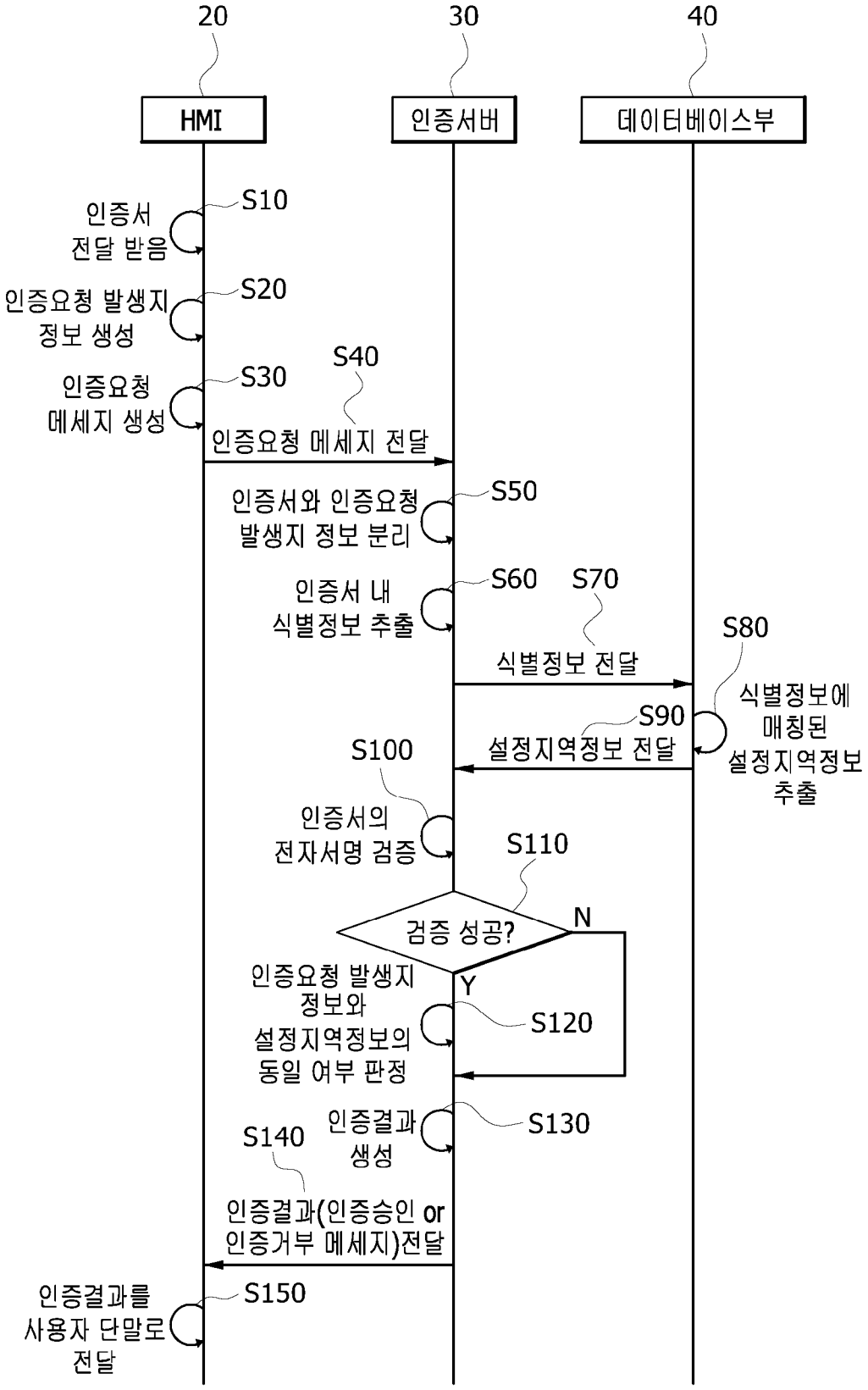
[도4]



[도5]



[도6]


20
30
40
HMI
인증서버
데이터베이스부
S10
인증서 전달 받음
S20
인증요청 발생지 정보 생성
S30
인증요청 메세지 생성
S40
인증요청 메세지 전달
S50
인증서와 인증요청 발생지 정보 분리
S60
인증서 내 식별정보 추출
S70
식별정보 전달
S80
식별정보에 매칭된 설정지역정보 추출
S90
설정지역정보 전달
S100
인증서의 전자서명 검증
S110
검증 성공?
N
Y
인증요청 발생지 정보와 설정지역정보의 동일 여부 판정
S120
인증결과 생성
S130
S140
인증결과(인증승인 or 인증거부 메세지)전달
S150
인증결과를 사용자 단말로 전달

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2015/007739

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L 9/32; H04L 9/08; H04L 9/14; H04M 1/00; G06Q 40/02; H04Q 9/00; G06Q 20/30

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean Utility models and applications for Utility models: IPC as above
Japanese Utility models and applications for Utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: certification, certification, position, region.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	KR 10-2011-0029040 A (KOREA FINANCIAL TELECOMMUNICATIONS) 22 March 2011 See paragraphs [0400], [0581], figure 5 and claim 1.	1-14
A	KR 10-2011-0113070 A (THE INDUSTRY & ACADEMIC COOPERATION IN CHUNGNAM NATIONAL UNIVERSITY (IAC)) 14 October 2011 See paragraphs [0035], [0057], [0058].	1-14
A	JP 2014-003481 A (AZBIL CORP.) 09 January 2014 See abstract, claims 1-4.	1-14

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 AUGUST 2015 (18.08.2015)	**19 AUGUST 2015 (19.08.2015)**
Name and mailing address of the ISA/KR Korean Intellectual Property Office Government Complex-Daejeon, 189 Seonsa-ro, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2015/007739

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2011-0029040 A	22/03/2011	NONE	
KR 10-2011-0113070 A	14/10/2011	JP 2011-223544 A US 2011-0249816 A1	04/11/2011 13/10/2011
JP 2014-003481 A	09/01/2014	NONE	

국 제 조 사 보 고 서

국제출원번호
PCT/KR2015/007739

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04L 9/32(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

H04L 9/32; H04L 9/08; H04L 9/14; H04M 1/00; G06Q 40/02; H04Q 9/00; G06Q 20/30

조사된 기술분야에 속하는 최소문헌 이외의 문헌

한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC
일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))

eKOMPASS(특허청 내부 검색시스템) & 키워드: 인증서, 인증, 위치, 지역.

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
X	KR 10-2011-0029040 A (사단법인 금융결제원) 2011.03.22 단락 [400],[581], 도면 5 및 청구항 1 참조.	1-14
A	KR 10-2011-0113070 A (충남대학교산학협력단) 2011.10.14 단락 [35],[57],[58] 참조.	1-14
A	JP 2014-003481 A (AZBIL CORP.) 2014.01.09 요약, 청구항 1-4 참조.	1-14

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

"A" 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

"E" 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

"L" 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

"O" 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

"T" 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

"X" 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

"Y" 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2015년 08월 18일 (18.08.2015)	2015년 08월 19일 (19.08.2015)

ISA/KR의 명칭 및 우편주소
대한민국 특허청
(35208) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)
팩스 번호 +82-42-472-7140

심사관
양종필
전화번호 +82-42-481-8595

국 제 조 사 보 고 서
대응특허에 관한 정보

국제출원번호
PCT/KR2015/007739

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2011-0029040 A	2011/03/22	없음	
KR 10-2011-0113070 A	2011/10/14	JP 2011-223544 A US 2011-0249816 A1	2011/11/04 2011/10/13
JP 2014-003481 A	2014/01/09	없음	