(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2014 년 11 월 20 일 (20.11.2014)

WIPO | PCT

(10) 국제공개번호
WO 2014/185594 A1

(51) 국제특허분류:
H04L 9/32 (2006.01)

(21) 국제출원번호: PCT/KR2013/007834

(22) 국제출원일: 2013 년 8 월 30 일 (30.08.2013)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2013-0055633 2013 년 5 월 16 일 (16.05.2013) KR

(71) 출원인: **삼성에스디에스 주식회사 (SAMSUNG SDS CO., LTD.)** [KR/KR]; 135-918 서울시 강남구 역삼 2 동 707-19 일옥빌딩, Seoul (KR).

(72) 발명자: **김선득 (KIM, Sundeuk)**; 138-222 서울시 송파구 잠실 2 동 잠실엘스아파트 118-2304, Seoul (KR). **오현택 (OH, Hyun Taek)**; 152-773 서울시 구로구 신도림동 동아 3 차아파트 306-501, Seoul (KR).

(74) 대리인: **노준태 (NOH, Jun Tae)** 등; 137-953 서울시 서초구 서초중앙로 53 6 층 (서초동, 대림빌딩), 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, IS, JP, KE, KG, KN, KP, KZ, LA, LC, LK, LR, LS, LT, 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.

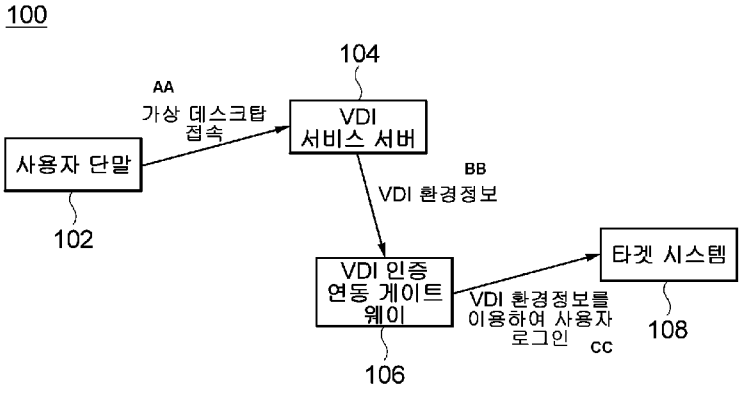
(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, 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: SINGLE SIGN-ON SYSTEM AND METHOD IN VDI ENVIRONMENT

(54) 발명의 명칭 : VDI 환경에서의 싱글 사인온 시스템 및 방법



102 ... User terminal
104 ... VDI service server
106 ... VDI authentication-interworking gateway
108 ... Target system
AA ... Connection to virtual desktop
BB ... VDI environment information
CC ... User log-in using VDI environment information

(57) Abstract: Disclosed are a single sign-on system and method in a virtual desktop infrastructure (VDI) environment. The single-sign-on system in a VDI environment, according to one embodiment of the present invention, comprises: a VDI service server for providing a virtual desktop environment to a user terminal according to a request from the user terminal; and a VDI authentication-interworking gateway for receiving VDI environment information on the user terminal from the VDI service server and performing user authentication of a target system in the virtual desktop environment by using the received VDI environment information.

(57) 요약서:

[다음 쪽 계속]

WO 2014/185594 A1

VDI 환경에서의 싱글 사인온 시스템 및 방법이 개시된다. 본 발명의 일 실시예에 따른 VDI 환경에서의 싱글 사인온 시스템은, 사용자 단말의 요청에 따라 상기 사용자 단말에 가상 데스크탑 환경을 제공하는 VDI 서비스 서버, 및 상기 VDI 서비스 서버로부터 상기 사용자 단말의 VDI 환경정보를 수신하고, 수신된 상기 VDI 환경정보를 이용하여 상기 가상 데스크탑 환경 내에서의 타겟 시스템에 대한 사용자 인증을 대행하는 VDI 인증 연동 게이트웨이를 포함한다.

명세서

발명의 명칭: VDI 환경에서의 싱글 사인온 시스템 및 방법

기술분야

[1] 본 발명은 VDI(Virtual Desktop Infrastructure) 환경에서 싱글 사인온(SSO; Single-Sign-On) 서비스를 제공하기 위한 기술과 관련된다.

[2]

배경기술

[3] VDI(Virtual Desktop Infrastructure)란 네트워크로 연결된 서버 상에 가상 데스크탑 환경을 구축하여 놓고, 사용자는 키보드, 마우스 등의 입력 수단 및 디스플레이 등의 필수 장치들로만 구성된 씬 클라이언트(Thin Client) 또는 제로 클라이언트(Zero Client)를 통해 상기 서버에 접속하여 가상 데스크탑 내에서 작업을 수행하는 형태의 컴퓨팅 기술을 의미한다. VDI는 사용자가 물리적 장소에 관계 없이 동일한 데스크탑 환경을 이용할 수 있으며, 보안 등에도 장점이 있어 기업 등의 업무 환경을 중심으로 그 사용이 점차 증가하고 있다.

[4] 한편, 싱글 사인 온(SSO; Single-Sign-On) 기술이란 한 번의 로그인 과정만으로 복수 개의 서비스에 자동으로 접속할 수 있도록 하는 기술을 의미한다. 예를 들어, 업무를 위하여 A, B, 및 C의 3개의 시스템에 각각 접속하여야 한다고 가정하자. 이 경우, 만약 SSO가 적용되지 않을 경우에는 3개의 시스템에 각각 아이디/패스워드를 입력하여야 하지만, SSO가 적용될 경우에는 어느 하나의 시스템에 대한 로그인만으로도 나머지 시스템에 대한 접속이 자동으로 완료되게 된다.

[5] 만약, 사용자가 자신이 현재 사용중인 클라이언트를 이용하여 VDI 시스템 내의 가상 데스크탑에 접속하고, 접속된 가상 데스크탑 내에서 타겟 시스템(예를 들어, 사내 업무용 시스템)에 로그인한다고 가정하자. 이 경우, 사용자는 먼저 자신의 클라이언트를 이용하여 VDI 서비스 시스템에 로그인하여 가상 데스크탑에 접속하고, 접속된 가상 데스크탑 내에서 타겟 시스템에 재차 로그인하게 된다. 즉, 가상 데스크탑을 통해 타겟 시스템에 접속하기 위해서 사용자는 VDI 서비스 시스템 로그인 및 타겟 시스템 로그인을 포함하는 2단계의 과정을 거쳐야 하는 불편함이 있게 된다.

[6] 이와 같은 불편을 해소하기 위해서 VDI 서비스 시스템 로그인 및 타겟 시스템 로그인을 SSO를 통하여 통합하는 방안을 고려해 볼 수 있다. 그러나, VDI 서비스 시스템의 로그인은 사용자가 사용중인 로컬 단말(로컬 데스크탑)에서 수행되는 것이고, 타겟 시스템 로그인은 VDI 서비스 시스템 내의 가상 데스크탑 내에서 수행되는 것이며, 보안 등의 이유로 로컬 단말(로컬 데스크탑)과 가상 데스크탑 간에는 키보드입력, 화면전송을 제외한 모든 정보 교환이 차단되기 때문에, 기존의 VDI 서비스 시스템에서는 VDI 서비스 시스템 로그인 및 타겟 시스템

로그인 간의 SSO 기능을 제공하는 것이 불가능하였다.

[7]

발명의 상세한 설명

기술적 과제

[8] 본 발명의 실시예들은 사용자의 로컬 단말(로컬 데스크탑)에서 VDI 환경에서의 가상 데스크탑 접속 및 가상 데스크탑 내에서의 타겟 시스템 접속을 통합하여 한 번의 로그인 과정만으로 가능하도록 하는 수단을 제공하기 위한 것이다.

[9]

과제 해결 수단

[10] 본 발명의 일 실시예에 따른 VDI 환경에서의 싱글 사인온 시스템은, 사용자 단말의 요청에 따라 상기 사용자 단말에 가상 데스크탑 환경을 제공하는 VDI 서비스 서버, 및 상기 VDI 서비스 서버로부터 상기 사용자 단말의 VDI 환경정보를 수신하고, 수신된 상기 VDI 환경정보를 이용하여 상기 가상 데스크탑 환경 내에서의 타겟 시스템에 대한 사용자 인증을 대행하는 VDI 인증 연동 게이트웨이를 포함한다.

[11] 상기 VDI 환경정보는, 상기 사용자 단말의 VDI 계정 정보, 상기 사용자 단말의 로컬 IP 주소, 가상 데스크탑 IP 주소, 상기 가상 데스크탑의 호스트네임, 상기 가상 데스크탑이 속한 도메인 그룹, 또는 상기 사용자 단말의 하드웨어 정보 중 하나 이상을 포함할 수 있다.

[12] 상기 VDI 인증 연동 게이트웨이는, 수신된 상기 VDI 환경정보를 이용하여 사용자 인증 정보를 생성하고, 생성된 상기 인증 정보를 암호화하여 상기 타겟 시스템으로 송신할 수 있다.

[13] 상기 VDI 인증 연동 게이트웨이는, 상기 타겟 시스템이 싱글 사인온 대상인지의 여부를 판단하고, 상기 판단 결과 싱글 사인온 대상인 경우 상기 사용자 인증 정보를 생성할 수 있다.

[14] 암호화된 상기 인증 정보는, 상기 인증 정보의 생성 시각을 포함할 수 있다.

[15] 상기 VDI 인증 연동 게이트웨이는, 상기 인증 정보의 생성 시각을 이용하여 생성된 상기 인증 정보를 1차 암호화하고, 기 설정된 암호화 키를 이용하여 1차 암호화된 상기 인증 정보 및 상기 생성 시각을 포함하는 문자열을 2차 암호화하여 상기 타겟 시스템으로 송신할 수 있다.

[16] 상기 타겟 시스템은, 기 설정된 복호화 키를 이용하여 상기 VDI 인증 연동 게이트웨이로부터 수신된 문자열을 복호화하여 상기 1차 암호화된 인증 정보 및 상기 생성 시각을 추출하고, 추출된 상기 생성 시각을 이용하여 상기 1차 암호화된 인증 정보로부터 상기 사용자 인증 정보를 획득하며, 획득된 상기 사용자 인증 정보 및 상기 VDI 서비스 서버로부터 획득되는 VDI 환경정보를 이용하여 상기 가상 데스크탑 환경 내에서의 상기 사용자 단말에 대한 인증을

수행할 수 있다.

[17] 상기 타겟 시스템은, 획득된 상기 생성 시각과 현재 시각과의 차이가 기 설정된 범위를 초과하는 경우, 상기 인증에 실패한 것으로 판단할 수 있다.

[18] 상기 타겟 시스템은, 획득된 상기 사용자 인증 정보가 상기 VDI 서비스 서버로부터 획득되는 VDI 환경정보와 상이할 경우, 상기 인증에 실패한 것으로 판단할 수 있다.

[19] 한편, 본 발명의 일 실시예에 따른 VDI 환경에서의 싱글 사인온 방법은, VDI 서비스 서버에서, 사용자 단말의 요청에 따라 상기 사용자 단말에 가상 데스크탑 환경을 제공하는 단계, 및 VDI 인증 연동 게이트웨이에서, 상기 VDI 서비스 서버로부터 상기 사용자 단말의 VDI 환경정보를 수신하고, 수신된 상기 VDI 환경정보를 이용하여 상기 가상 데스크탑 환경 내에서의 타겟 시스템에 대한 사용자 인증을 대행하는 단계를 포함한다.

[20] 상기 VDI 환경정보는, 상기 사용자 단말의 VDI 계정 정보, 상기 사용자 단말의 로컬 IP 주소, 가상 데스크탑 IP 주소, 상기 가상 데스크탑의 호스트네임, 상기 가상 데스크탑이 속한 도메인 그룹, 또는 상기 사용자 단말의 하드웨어 정보 중 하나 이상을 포함할 수 있다.

[21] 상기 사용자 인증을 대행하는 단계는, 수신된 상기 VDI 환경정보를 이용하여 사용자 인증 정보를 생성하고, 생성된 상기 인증 정보를 암호화하여 상기 타겟 시스템으로 송신하도록 구성될 수 있다.

[22] 상기 사용자 인증을 대행하는 단계는, 상기 타겟 시스템이 싱글 사인온 대상인지의 여부를 판단하는 단계를 더 포함하며, 상기 VDI 인증 연동 게이트웨이는, 상기 판단 결과 상기 타겟 시스템이 싱글 사인온 대상인 경우 상기 사용자 인증 정보를 생성할 수 있다.

[23] 암호화된 상기 인증 정보는, 상기 인증 정보의 생성 시각을 포함할 수 있다.

[24] 상기 사용자 인증을 대행하는 단계는, 상기 인증 정보의 생성 시각을 이용하여 생성된 상기 인증 정보를 1차 암호화하는 단계, 및 기 설정된 암호화 키를 이용하여 1차 암호화된 인증 정보 및 상기 생성 시각을 2차 암호화하여 상기 타겟 시스템으로 송신하는 단계를 더 포함할 수 있다.

[25] 상기 타겟 시스템은, 기 설정된 복호화 키를 이용하여 상기 VDI 인증 연동 게이트웨이로부터 수신된 문자열을 복호화하여 상기 1차 암호화된 인증 정보 및 상기 생성 시각을 추출하고, 추출된 상기 생성 시각을 이용하여 상기 1차 암호화된 인증 정보로부터 상기 사용자 인증 정보를 획득하며, 획득된 상기 사용자 인증 정보 및 상기 VDI 서비스 서버로부터 획득되는 VDI 환경정보를 이용하여 상기 가상 데스크탑 환경 내에서의 상기 사용자 단말에 대한 인증을 수행할 수 있다.

[26] 상기 타겟 시스템은, 획득된 사용자 인증 정보와 상기 VDI 서비스 서버로부터 획득되는 VDI 환경정보가 상이할 경우, 상기 인증에 실패한 것으로 판단할 수 있다.

[27] 상기 타겟 시스템은, 획득된 상기 생성 시각과 현재 시각과의 차이가 기 설정된 범위를 초과하는 경우, 상기 인증에 실패한 것으로 판단할 수 있다.

[28]

발명의 효과

[29] 본 발명의 실시예들에 따를 경우, 로컬 단말(로컬 데스크탑)에서 VDI 환경에서의 가상 데스크탑 접속 및 가상 데스크탑 내에서의 타겟 시스템 접속을 통합함으로써, 사용자가 한 번의 로그인 과정만으로 VDI 가상 데스크탑 접속 및 타겟 시스템 접속을 완료할 수 있게 되는 바, VDI 환경에서 사용자의 편의성을 증대시킬 수 있다.

[30]

도면의 간단한 설명

[31] 도 1은 본 발명의 일 실시예에 따른 VDI 환경에서의 싱글 사인온 시스템(100)을 설명하기 위한 블록도이다.

[32] 도 2는 본 발명의 일 실시예에 따른 VDI 서비스 서버(104)의 상세 구성을 나타낸 블록도이다.

[33] 도 3은 본 발명의 일 실시예에 따른 VDI 환경에서의 싱글 사인온 방법(300)을 설명하기 위한 흐름도이다.

[34]

발명의 실시를 위한 형태

[35] 이하, 도면을 참조하여 본 발명의 구체적인 실시형태를 설명하기로 한다. 그러나 이는 예시에 불과하며 본 발명은 이에 제한되지 않는다.

[36] 본 발명을 설명함에 있어서, 본 발명과 관련된 공지기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략하기로 한다. 그리고, 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

[37] 본 발명의 기술적 사상은 청구범위에 의해 결정되며, 이하의 실시예는 본 발명의 기술적 사상을 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 효율적으로 설명하기 위한 일 수단일 뿐이다.

[38]

[39] 도 1은 본 발명의 일 실시예에 따른 VDI 환경에서의 싱글 사인온 시스템(100)을 설명하기 위한 블록도이다. 도시된 바와 같이, 본 발명의 일 실시예에 따른 VDI 환경에서의 싱글 사인온 시스템(100)은 사용자 단말(102), VDI 서비스 서버(104), VDI 인증 연동 게이트웨이(106) 및 타겟 시스템(108)을 포함한다.

[40] 사용자 단말(102)은 후술할 VDI 서비스 서버(104)에 접속하여 가상 데스크탑 서비스를 제공받는 사용자 기기이다. 사용자 단말(102)은 데이터의 입출력을

위한 적절한 입력 수단, 출력 수단 및 VDI 서비스 서버(104)로의 접속을 위한 네트워크 접속 수단을 포함하는 모든 종류의 디바이스를 포함할 수 있다. 예를 들어, 사용자 단말(102)은 데스크탑 컴퓨터, 노트북 컴퓨터 등의 개인용 컴퓨터, 또는 이동통신 단말, 스마트폰, 태블릿 등의 휴대용 기기를 포함할 수 있다.

[41] 사용자 단말(102)은 가상 데스크탑을 제공받기 위하여 VDI 서비스 서버(104)에 접속 및 인증을 수행할 수 있다. 이때, 상기 인증은 예를 들어 사용자가 입력한 아이디 및 패스워드를 이용하여 수행될 수 있으나, 본 발명은 특정한 인증 방식에 한정되는 것은 아니다.

[42] VDI 서비스 서버(104)는 사용자 단말(102)의 요청에 따라 사용자 단말(102)에 가상 데스크탑 환경을 제공한다. 또한, VDI 서비스 서버(104)는 후술할 VDI 인증 연동 게이트웨이(106)의 요청에 따라 사용자 단말(102)의 VDI 환경정보를 VDI 인증 연동 게이트웨이(106)로 제공한다. 구체적인 VDI 서비스 서버(104)의 상세 구성에 대해서는 도 2에서 상세히 설명하기로 한다.

[43] VDI 인증 연동 게이트웨이(106)는 VDI 서비스 서버(104)로부터 사용자 단말(102)의 VDI 환경정보를 수신하고, 수신된 상기 VDI 환경정보를 이용하여 상기 사용자 단말(102)이 접속한 가상 데스크탑 환경 내에서의 타겟 시스템(108)에 대한 사용자 인증을 대행한다.

[44] 타겟 시스템(108)은 가상 데스크탑에 접속한 사용자 단말(102)이 상기 가상 데스크탑 내에서 접속을 수행하기 위한 시스템이다. 본 발명의 실시예에서 타겟 시스템(108)의 종류는 특별히 제한되지 않으며, 예를 들어 기업 또는 특정 단체의 사내 인트라넷 시스템 또는 웹 포탈 등이 본 발명에서의 타겟 시스템(108)이 될 수 있다.

[45] 본 발명의 실시예에서 타겟 시스템(108)은 VDI 인증 연동 게이트웨이(106)로부터 사용자 단말(102)의 인증 요청을 수신하고, 수신된 인증 요청에 포함된 정보를 타겟 시스템(108)에서 VDI 서비스 서버(104)로 조회한 VDI 환경정보와 비교하여 사용자 단말(102)이 접속한 가상 데스크탑 환경에서의 사용자 접속을 허용 또는 차단하도록 구성된다. VDI 인증 연동 게이트웨이(106) 및 타겟 시스템(108) 간의 구체적인 인증 과정에 대해서는 후술하기로 한다.

[46]

[47] 도 2는 본 발명의 일 실시예에 따른 VDI 서비스 서버(104)의 상세 구성을 나타낸 블록도이다. 다만, 도시된 VDI 서비스 서버(104)의 구성은 단지 예시적인 것으로서, 후술할 실시예는 본 발명의 이해를 돕기 위하여 본 발명의 실시예들에 따른 VDI 서비스 서버(104)의 가능한 여러 실시예 중 하나를 기재한 것에 불과함을 유의한다. 즉, 본 발명에 따른 VDI 환경에서의 싱글 사인온 시스템(100)에서 VDI 인증 연동 게이트웨이(106)는 VDI 서비스 서버의 종류와 관계 없이 어떠한 형태의 VDI 서비스 서버와도 연계하여 타겟 시스템(108) 로그인을 수행할 수 있도록 구성된다. 따라서 본 발명의 권리범위를 해석함에 있어 VDI 서비스 서버(104)는 도 2에 예시된 것 이외에 이용 가능한 모든 종류의

VDI 서비스 제공 시스템을 포함하는 것으로 해석되어야 한다.

[48] 도시된 바와 같이, 본 발명의 일 실시예에 따른 VDI 서비스 서버(104)는 VDI 웹 포탈 서버(200), 데이터베이스(202), VDI 관리서버(204), 데이터 스토어 서버(206) 및 VDI 호스트 서버(208)를 포함하는 일련의 서버군으로 구성된다.

[49] VDI 웹 포탈 서버(200)는 VDI 서비스를 제공받고자 하는 사용자 단말(102)이 가장 먼저 접속하게 되는 서버이다. VDI 웹 포탈 서버(200)는 사용자 단말(102)의 접속 및 인증을 위한 적절한 인터페이스를 구비할 수 있으며, 예를 들어 상기 인터페이스는 웹 페이지 형태로 구성될 수 있다.

[50] 가상 데스크탑을 이용하기 위하여, 사용자 단말(102)은 VDI 웹 포탈 서버(200)에 접속하여 사용자 단말(102)의 인증에 필요한 정보를 입력할 수 있다. 이때 상기 인증에 필요한 정보는, 예를 들어 사용자 단말(102)을 이용하는 사용자의 아이디/패스워드일 수 있다. VDI 웹 포탈 서버(200)은 입력된 정보를 데이터베이스(202)에 저장된 정보와 비교하여 사용자 단말(102)의 접속을 허용 또는 차단한다. 상기 데이터베이스는, 예를 들어 액티브 디렉토리(Active Directory), 래디우스(Radius), 오라클 데이터베이스(Oracle DB) 등 인증을 수행하고 인증정보를 저장 및 관리할 수 있는 하드웨어 장비로 구성될 수 있다.

[51] 데이터베이스(202)는 사용자 단말(102)의 인증에 필요한 정보가 저장되는 공간이다. 전술한 바와 같이, VDI 웹 포탈 서버(200)는 사용자 단말(102)로부터 인증 요청이 수신되는 경우, 수신된 정보를 데이터베이스(202)에 저장된 정보와 비교하여 사용자 단말(102)을 인증하게 된다.

[52] 또한, 데이터베이스(202)는 각 사용자 단말(102)의 VDI 환경정보를 저장 및 관리한다. 이때 상기 VDI 환경정보는, 사용자 단말(102)의 VDI 계정 정보, 사용자 단말(102)의 로컬 IP 주소, 가상 데스크탑 IP 주소, 가상 데스크탑의 호스트네임(hostname), 가상 데스크탑이 속한 도메인 그룹, 또는 사용자 단말(102)의 하드웨어 정보 중 하나 이상을 포함하여 구성될 수 있다. 상기 정보 중 사용자 단말(102)의 로컬 IP 주소 및 사용자 단말(102)의 하드웨어 정보는 사용자 단말(102)의 인증 과정에서 사용자 단말(102)로부터 획득될 수 있다. 또한, 상기 하드웨어 정보는 사용자 단말(102)의 중앙처리장치 또는 메모리 사양, 또는 사용자 단말(102)을 구성하는 각 구성들의 일련번호 등 사용자 단말(102)을 하드웨어적으로 식별할 수 있는 모든 종류의 정보가 포함될 수 있다.

[53] VDI 관리서버(204)는 VDI 웹 포탈 서버(200)로부터 인증이 완료된 사용자 단말(102)의 가상 데스크탑 생성 요청을 수신하고, 이에 따라 데이터베이스(202)에 저장된 사용자 단말(102)의 VDI 환경정보를 VDI 호스트 서버(208)로 제공한다. 또한, VDI 관리서버(204)는 사용자 단말(102)의 가상 데스크탑 이미지를 생성하고, 생성된 가상 데스크탑 이미지를 VDI 호스트 서버(208)로 제공한다. 이를 위하여, VDI 관리서버(204)는 VDI 환경정보의 관리 및 제공을 위한 DDC(Desktop Delivery Controller), VM(Virtual Machine) Manager 및 가상 데스크탑 이미지 생성을 위한 PVS(Provisioning Server) 등을 포함할 수

있다.

[54] 데이터 스토어 서버(206)는 사용자 단말(102)이 가상 데스크탑 내에서 사용하는 파일 등의 사용자 데이터를 저장 및 관리한다. 데이터 스토어 서버(206)는 VDI 호스트 서버(208)의 요청에 따라 상기 사용자 데이터를 VDI 호스트 서버(208)에 제공한다.

[55] VDI 호스트 서버(208)는 VDI 관리서버(204)로부터 수신한 사용자 단말(102)의 VDI 환경정보 및 가상 데스크탑 이미지, 및 데이터 스토어 서버(206)로부터 수신한 사용자 데이터를 이용하여 가상 데스크탑을 생성하고, 생성된 가상 데스크탑을 사용자 단말(102)에 제공한다. 즉, 최초 VDI 웹 포탈 서버(200)에 접속하여 인증을 수행한 사용자 단말(102)은 이후 VDI 호스트 서버(208)에 접속하여 가상 데스크탑을 이용하게 된다.

[56]

[57] 도 3은 본 발명의 일 실시예에 따른 VDI 환경에서의 싱글 사인온 방법(300)을 설명하기 위한 흐름도이다.

[58] 사용자 단말(102)은 가상 데스크탑에 접속하여 작업을 수행하기 위하여, 먼저 VDI 웹 포탈 서버(200)에 VDI 접속 요청을 송신한다(302). 전술한 바와 같이, 상기 접속 요청에는 사용자 인증에 필요한 정보(예를 들어, 아이디/패스워드)를 포함할 수 있다.

[59] 상기 VDI 접속 요청을 수신한 VDI 웹 포탈 서버(200)는 수신된 접속 요청에 포함된 정보를 데이터베이스(202)에 저장된 정보와 비교하여 사용자 인증을 수행한다(304). 인증이 완료되면 VDI 웹 포탈 서버(200)는 VDI 관리서버(204)로 가상 데스크탑 생성 요청을 송신한다(306).

[60] 이후, VDI 관리 서버(204)는 데이터베이스(202)로 해당 사용자 단말(102) VDI 환경정보를 조회하여 이를 획득한다(308). 전술한 바와 같이, 상기 VDI 환경정보는, 사용자 단말(102)의 VDI 계정 정보, 사용자 단말(102)의 로컬 IP 주소, 가상 데스크탑 IP 주소, 가상 데스크탑의 호스트네임(hostname), 가상 데스크탑이 속한 도메인 그룹, 또는 사용자 단말(102)의 하드웨어 정보 중 하나 이상을 포함하여 구성될 수 있다. VDI 환경정보가 획득되면, VDI 관리 서버(204)는 상기 VDI 환경정보를 VDI 호스트 서버(208)로 송신한다(310). 또한, VDI 관리서버(204)는 사용자 단말(102)의 가상 데스크탑 이미지를 생성하고 이를 VDI 호스트 서버(208)로 송신한다(312).

[61] 한편, 데이터 스토어 서버(206)는 VDI 호스트 서버(208)로 사용자 단말(102)의 사용자 데이터를 전송한다(314). 도시된 실시예에서는 전술한 310, 312 및 314 단계가 시계열적으로 순차적으로 수행되는 것으로 도시되었으나, 이는 단지 예시적인 것으로서, 각 단계들은 동시에 수행될 수도 있고 순서를 바꾸어 수행될 수도 있음은 본 기술분야의 당업자에게 있어 자명한 사항이다.

[62] VDI 호스트 서버(208)는 상기 310 단계에서 수신한 사용자 단말(102)의 VDI 환경정보, 상기 312 단계에서 수신한 가상 데스크탑 이미지, 및 상기 314

단계에서 수신한 사용자 데이터를 이용하여 가상 데스크탑을 생성하고, 생성된 가상 데스크탑을 사용자 단말(102)에 제공한다(316). 그러면 사용자 단말(102)은 생성된 가상 데스크탑에 대한 접속을 수행한다(318).

[63] 상술한 과정을 거쳐 사용자 단말(102)이 가상 데스크탑 접속한 이후, 가상 데스크탑 안에서 타겟 시스템(108) 접속을 시도하면, VDI 인증 연동 게이트웨이(106)는 VDI 서비스 서버(104)로부터 사용자 단말(102)의 VDI 환경정보를 수신하고, 수신된 상기 VDI 환경정보를 이용하여 상기 가상 데스크탑 환경 내에서의 타겟 시스템(108)에 대한 사용자 인증을 대행하게 된다. 상기 과정을 좀 더 상세히 설명하면 다음과 같다.

[64] 먼저, VDI 호스트 서버(208)는 사용자 단말(102)의 가상 데스크탑 접속 완료 후 VDI 인증 연동 게이트웨이(106)로 타겟 시스템 접속 요청을 송신한다(320). 일 실시예에서, VDI 호스트 서버(208)는 가상 데스크탑에 접속한 사용자 단말(102)의 요청에 의하여 상기 타겟 시스템 접속 요청을 송신할 수도 있다. 또한 다른 실시예에서 VDI 호스트 서버(208)는 사용자 단말(102)의 가상 데스크탑 접속이 완료된 이후 기 설정된 타겟 시스템(108)에 대한 접속 요청을 자동으로 VDI 인증 연동 게이트웨이(106)로 전송할 수도 있다.

[65] 상기 접속 요청을 수신한 VDI 인증 연동 게이트웨이(106)는 먼저 요청된 접속 요청에 포함된 타겟 시스템(108)이 싱글-사인-온(SSO) 대상인지의 여부를 조회한다(322). 상기 조회 과정은, 예를 들어 VDI 인증 연동 게이트웨이(106) 또는 별도의 데이터베이스 등에 저장된 SSO 대상 서버 리스트를 참조함으로써 수행될 수 있다. 만약 상기 조회 결과 요청된 타겟 시스템(108)이 SSO 대상이 아닌 경우, VDI 인증 연동 게이트웨이(106)는 VDI 호스트 서버(208)로 타겟 시스템(108) 접속 불가를 통지한다.

[66] 이와 달리, 만약 상기 조회 결과 요청된 타겟 시스템(108)이 SSO 대상인 경우, VDI 인증 연동 게이트웨이(106)는 VDI 관리서버(204)를 통하여 사용자 단말(102)의 VDI 환경정보를 취득한다(324). 이때 VDI 인증 연동 게이트웨이(106)는 생성된 상기 가상 데스크탑의 IP를 이용하여 상기 가상 데스크탑 IP에 해당하는 VDI 환경정보를 VDI 관리서버(204)로부터 수신하도록 구성될 수 있다. 이후 VDI 인증 연동 게이트웨이(106)는 취득된 상기 VDI 환경정보를 이용하여 사용자 단말(102)의 인증을 위한 인증 정보를 생성한 뒤(326), 생성된 인증 정보를 타겟 시스템(108)으로 송신한다(328). 이때 VDI 인증 연동 게이트웨이(106)은 상기 인증 정보를 암호화하여 타겟 시스템(108)으로 송신할 수 있으며, 상기 암호화 시에는 생성된 인증 정보에 인증 정보의 생성 시각을 부가하여 암호화를 수행할 수 있다. 또한, VDI 인증 연동 게이트웨이(106)는 상기 암호화된 인증 정보의 안전한 전송을 위하여 HTTPS(TCP443, SSL) 방식으로 상기 암호화된 인증 정보를 타겟 시스템(108)으로 송신할 수 있으며, 타겟 시스템(108)의 종류에 따라 GET 방식, POST 방식, 쿠키 온 메모리(Cookie on Memory) 방식 등 다양한 종류의 메시지

전송 방식을 이용할 수 있다.

[67] 상기 암호화된 인증 정보의 생성 과정을 좀 더 상세히 설명하면 다음과 같다. 먼저, VDI 인증 연동 게이트웨이(106)는 수신된 사용자 단말(102)의 VDI 환경정보 중 적어도 일부를 이용하여 사용자 단말(102)의 인증을 위한 인증 정보를 생성한다. 즉, 상기 인증 정보는 사용자 단말(102)의 VDI 환경정보 중 사용자 단말(102)을 식별할 수 있는 정보 또는 하나 이상의 정보의 조합을 통하여 상기 인증 정보를 생성할 수 있다. 예를 들어, VDI 인증 연동 게이트웨이(106)는 사용자 단말(102)의 계정 정보(ID) 및 가상 데스크탑 IP 주소를 결합하여 상기 인증 정보를 결합할 수 있다.

[68] 인증 정보가 생성되면, 다음으로 VDI 인증 연동 게이트웨이(106)는 상기 인증 정보를 인증 정보의 생성 시각 정보를 암호화 키(KEY)로 하여 1차 암호화하고, 암호화된 문자열 및 상기 생성 시각을 기 설정된 암호화 키를 이용하여 2차 암호화한다. 이를 정리하면 다음과 같다.

[69]

[70] 1차 암호화: [ID, 가상 데스크탑 IP] + key(생성 시각)

[71] 2차 암호화: [1차 암호문, 생성 시각] + key(암호화 키)

[72]

[73] 상기 암호화 키 및 후술할 복호화 키는 VDI 인증 연동 게이트웨이(106) 및 타겟 시스템(108) 사이에서 사전에 설정된 값을 이용할 수 있다. 또한 본 발명의 실시예에서 암호화 및 복호화 알고리즘은 특별히 한정되지 않으며, 기존의 다양한 암복호화 방법 중 적절한 알고리즘을 이용할 수 있다.

[74] 상기와 같이 2차 암호화가 완료되면, VDI 인증 연동 게이트웨이(106)는 상기 2차 암호문을 보안 채널 등을 통하여 타겟 시스템(108)으로 전송한다.

[75] 타겟 시스템(108)은 VDI 인증 연동 게이트웨이(106)로부터 암호화된 인증 정보를 수신하고, 이를 이용하여 가상 데스크탑에 내에서의 사용자 단말(102) 인증을 수행한다(330, 332).

[76] 전술한 에에서, 타겟 시스템(108)이 VDI 인증 연동 게이트웨이(106)로부터 2차 암호문을 수신하는 경우, 타겟 시스템(108)은 먼저 기 설정된 복호화 키를 이용하여 수신된 2차 암호문을 복호화한다. 상기 1차 복호화가 완료되면 이로부터 1차 암호문 및 인증 정보의 생성 시각 정보가 추출된다.

[77] 타겟 시스템(108)은 추출된 상기 생성 시각과 현재 시각(복호화 당시의 시각)과의 차이를 계산하고, 계산된 차이가 기 설정된 범위를 초과하는 경우 사용자 단말(102)의 인증에 실패한 것으로 판단할 수 있다. 예를 들어, 타겟 시스템(108)은 상기 생성 시각이 다음의 범위를 벗어나는 경우 사용자 단말(102)의 인증에 실패한 것으로 판단할 수 있다.

[78]

[79] -3초 < 현재 시간 < +3초

[80]

[81] 상기와 같이 송신단에서의 인증 정보의 생성 시각과 수신단에서의 복호화 시각간의 범위를 설정함으로써 외부의 해킹 등의 가능성을 최소화할 수 있다. 상기 시간 범위는 VDI 인증 연동 게이트웨이(106) 및 타겟 시스템(108)의 성능, 네트워크 상태, 시각 동기화 여부 등의 다양한 환경을 고려하여 적절하게 설정될 수 있다.

[82] 만약 상기 계산 결과 생성 시각과 현재 시각과의 차이가 기 설정된 범위 내인 경우, 다음으로 타겟 시스템(108)은 상기 생성 시각을 키로 하여 상기 1차 암호문을 2차 복호화한다. 상기 2차 복호화의 결과로 타겟 시스템(108)은 원 인증 정보(상기 예에서는 ID 및 가상 데스크탑 IP 주소)를 얻을 수 있다. 이후 타겟 시스템(108)은 획득된 상기 인증 정보에 대응되는 VDI 환경정보를 VDI 관리서버(204)로부터 취득하고(330), 상기 인증 정보를 상기 330 단계에서 수신한 상기 VDI 환경정보와 비교하여 사용자 단말(102)을 인증하게 된다(332). 즉, 타겟 시스템(108)은 수신된 상기 인증 정보가 VDI 관리서버(204)에 저장된 정보와 동일할 경우 사용자 단말(102)의 인증에 성공한 것으로 판단하고, 동일하지 않은 경우에는 인증에 실패한 것으로 판단한다.

[83] 이와 같이, 본 발명의 실시예들에 따를 경우 사용자 단말(102)의 VDI 서비스 서버(104) 접속 후, VDI 서비스 서버(104)와 연동된 VDI 인증 연동 게이트웨이(106)가 사용자 단말(102)을 대신하여 타겟 시스템(108)의 인증을 수행함으로써, 사용자는 VDI 서비스 서버(104)에 로그인하는 것 만으로 가상 데스크탑 접속 및 타겟 시스템(108) 로그인을 동시에 수행할 수 있는 장점이 있다.

[84]

[85] 한편, 본 발명의 실시예는 본 명세서에서 기술한 방법들을 컴퓨터상에서 수행하기 위한 프로그램을 포함하는 컴퓨터 판독 가능 기록매체를 포함할 수 있다. 상기 컴퓨터 판독 가능 기록매체는 프로그램 명령, 로컬 데이터 파일, 로컬 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체는 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 분야에서 통상의 지식을 가진 자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD와 같은 광 기록 매체, 플롭티컬 디스크와 같은 자기-광 매체, 및 롬, 램, 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함할 수 있다.

[86] 이상에서 대표적인 실시예를 통하여 본 발명에 대하여 상세하게 설명하였으나, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자는 상술한 실시예에 대하여 본 발명의 범주에서 벗어나지 않는 한도 내에서 다양한 변형이 가능함을

이해할 것이다.

[87] 그러므로 본 발명의 권리범위는 설명된 실시예에 국한되어 정해져서는 안 되며, 후술하는 특허청구범위뿐만 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다.

청구범위

[청구항 1] 사용자 단말의 요청에 따라 상기 사용자 단말에 가상 데스크탑 환경을 제공하는 VDI 서비스 서버; 및
상기 VDI 서비스 서버로부터 상기 사용자 단말의 VDI 환경정보를 수신하고, 수신된 상기 VDI 환경정보를 이용하여 상기 가상 데스크탑 환경 내에서의 타겟 시스템에 대한 사용자 인증을 대행하는 VDI 인증 연동 게이트웨이를 포함하는 VDI 환경에서의 싱글 사인온 시스템.

[청구항 2] 청구항 1에 있어서,
상기 VDI 환경정보는, 상기 사용자 단말의 VDI 계정 정보, 상기 사용자 단말의 로컬 IP 주소, 가상 데스크탑 IP 주소, 상기 가상 데스크탑의 호스트네임, 상기 가상 데스크탑이 속한 도메인 그룹, 또는 상기 사용자 단말의 하드웨어 정보 중 하나 이상을 포함하는, VDI 환경에서의 싱글 사인온 시스템.

[청구항 3] 청구항 1에 있어서,
상기 VDI 인증 연동 게이트웨이는, 수신된 상기 VDI 환경정보를 이용하여 사용자 인증 정보를 생성하고, 생성된 상기 인증 정보를 암호화하여 상기 타겟 시스템으로 송신하는, VDI 환경에서의 싱글 사인온 시스템.

[청구항 4] 청구항 3에 있어서,
상기 VDI 인증 연동 게이트웨이는, 상기 타겟 시스템이 싱글 사인온 대상인지의 여부를 판단하고, 상기 판단 결과 싱글 사인온 대상인 경우 상기 사용자 인증 정보를 생성하는, VDI 환경에서의 싱글 사인온 시스템.

[청구항 5] 청구항 4에 있어서,
암호화된 상기 인증 정보는, 상기 인증 정보의 생성 시각을 포함하는, VDI 환경에서의 싱글 사인온 시스템.

[청구항 6] 청구항 5에 있어서,
상기 VDI 인증 연동 게이트웨이는, 상기 인증 정보의 생성 시각을 이용하여 생성된 상기 인증 정보를 1차 암호화하고,
기 설정된 암호화 키를 이용하여 1차 암호화된 상기 인증 정보 및 상기 생성 시각을 포함하는 문자열을 2차 암호화하여 상기 타겟 시스템으로 송신하는, VDI 환경에서의 싱글 사인온 시스템.

[청구항 7] 청구항 6에 있어서,
상기 타겟 시스템은, 기 설정된 복호화 키를 이용하여 상기 VDI 인증 연동 게이트웨이로부터 수신된 문자열을 복호화하여 상기 1차 암호화된 인증 정보 및 상기 생성 시각을 추출하고,

추출된 상기 생성 시각을 이용하여 상기 1차 암호화된 인증 정보로부터 상기 사용자 인증 정보를 획득하며,
획득된 상기 사용자 인증 정보 및 상기 VDI 서비스 서버로부터 획득되는 VDI 환경정보를 이용하여 상기 가상 데스크탑 환경 내에서의 상기 사용자 단말에 대한 인증을 수행하는, VDI 환경에서의 싱글 사인온 시스템.

[청구항 8] 청구항 7에 있어서,
상기 타겟 시스템은, 획득된 상기 생성 시각과 현재 시각과의 차이가 기 설정된 범위를 초과하는 경우, 상기 인증에 실패한 것으로 판단하는, VDI 환경에서의 싱글 사인온 시스템.

[청구항 9] 청구항 7에 있어서,
상기 타겟 시스템은, 획득된 상기 사용자 인증 정보가 상기 VDI 서비스 서버로부터 획득되는 VDI 환경정보와 상이할 경우, 상기 인증에 실패한 것으로 판단하는, VDI 환경에서의 싱글 사인온 시스템.

[청구항 10] VDI 서비스 서버에서, 사용자 단말의 요청에 따라 상기 사용자 단말에 가상 데스크탑 환경을 제공하는 단계; 및
VDI 인증 연동 게이트웨이에서, 상기 VDI 서비스 서버로부터 상기 사용자 단말의 VDI 환경정보를 수신하고, 수신된 상기 VDI 환경정보를 이용하여 상기 가상 데스크탑 환경 내에서의 타겟 시스템에 대한 사용자 인증을 대행하는 단계를 포함하는 VDI 환경에서의 싱글 사인온 방법.

[청구항 11] 청구항 10에 있어서,
상기 VDI 환경정보는, 상기 사용자 단말의 VDI 계정 정보, 상기 사용자 단말의 로컬 IP 주소, 가상 데스크탑 IP 주소, 상기 가상 데스크탑의 호스트네임, 상기 가상 데스크탑이 속한 도메인 그룹, 또는 상기 사용자 단말의 하드웨어 정보 중 하나 이상을 포함하는, VDI 환경에서의 싱글 사인온 방법.

[청구항 12] 청구항 10에 있어서,
상기 사용자 인증을 대행하는 단계는, 수신된 상기 VDI 환경정보를 이용하여 사용자 인증 정보를 생성하고, 생성된 상기 인증 정보를 암호화하여 상기 타겟 시스템으로 송신하도록 구성되는, VDI 환경에서의 싱글 사인온 방법.

[청구항 13] 청구항 12에 있어서,
상기 사용자 인증을 대행하는 단계는, 상기 타겟 시스템이 싱글 사인온 대상인지의 여부를 판단하는 단계를 더 포함하며,
상기 VDI 인증 연동 게이트웨이는, 상기 판단 결과 상기 타겟 시스템이 싱글 사인온 대상인 경우 상기 사용자 인증 정보를

생성하는, VDI 환경에서의 싱글 사인온 방법.

[청구항 14] 청구항 12에 있어서,
암호화된 상기 인증 정보는, 상기 인증 정보의 생성 시각을 포함하는, VDI 환경에서의 싱글 사인온 방법.

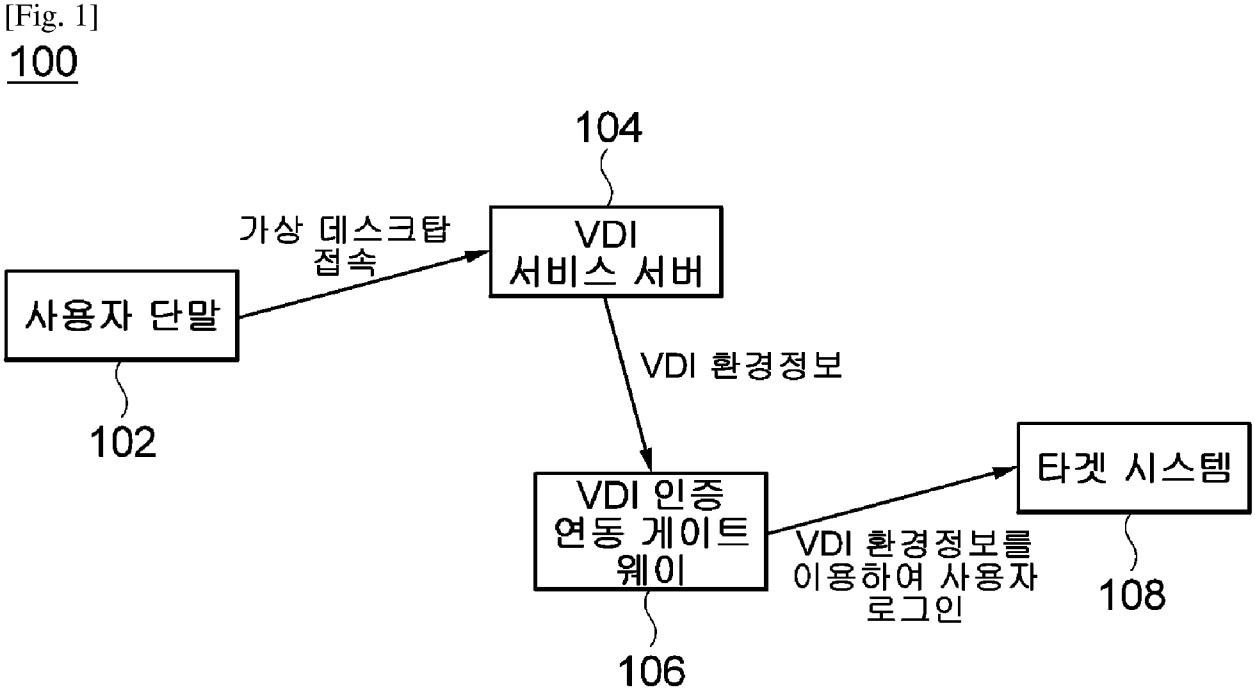
[청구항 15] 청구항 14에 있어서,
상기 사용자 인증을 대행하는 단계는,
상기 인증 정보의 생성 시각을 이용하여 생성된 상기 인증 정보를 1차 암호화하는 단계; 및
기 설정된 암호화 키를 이용하여 1차 암호화된 인증 정보 및 상기 생성 시각을 2차 암호화하여 상기 타겟 시스템으로 송신하는 단계를 더 포함하는, VDI 환경에서의 싱글 사인온 방법.

[청구항 16] 청구항 15에 있어서,
상기 타겟 시스템은, 기 설정된 복호화 키를 이용하여 상기 VDI 인증 연동 게이트웨이로부터 수신된 문자열을 복호화하여 상기 1차 암호화된 인증 정보 및 상기 생성 시각을 추출하고,
추출된 상기 생성 시각을 이용하여 상기 1차 암호화된 인증 정보로부터 상기 사용자 인증 정보를 획득하며,
획득된 상기 사용자 인증 정보 및 상기 VDI 서비스 서버로부터 획득되는 VDI 환경정보를 이용하여 상기 가상 데스크탑 환경 내에서의 상기 사용자 단말에 대한 인증을 수행하는, VDI 환경에서의 싱글 사인온 방법.

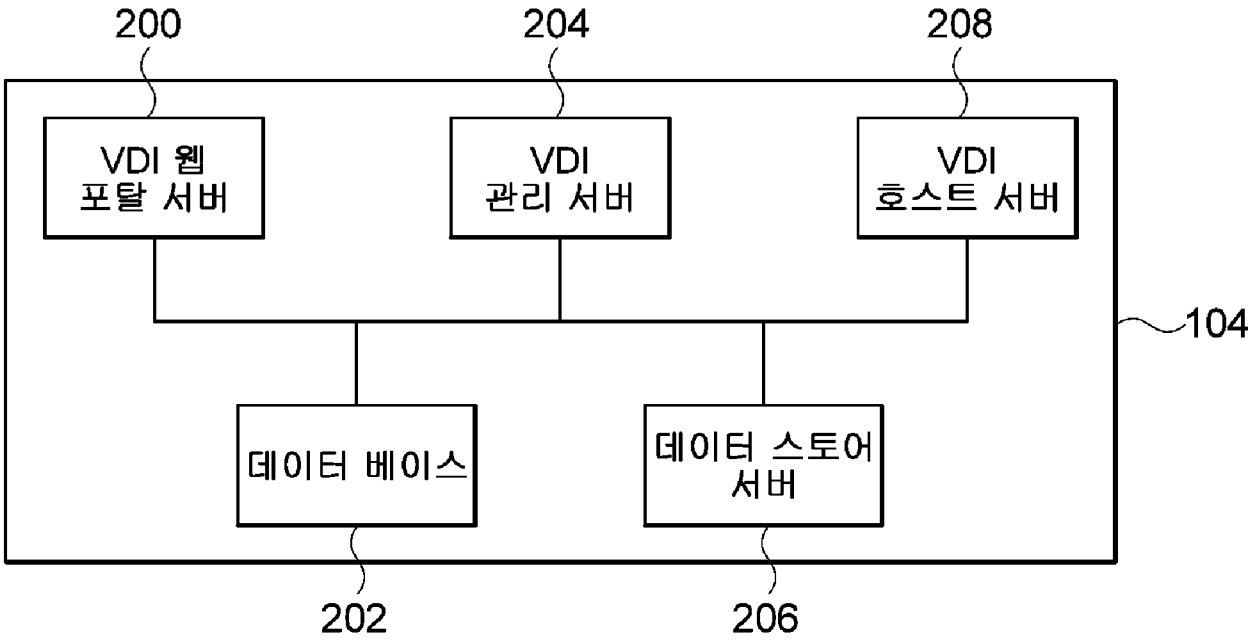
[청구항 17] 청구항 16에 있어서,
상기 타겟 시스템은, 획득된 상기 생성 시각과 현재 시각과의 차이가 기 설정된 범위를 초과하는 경우, 상기 인증에 실패한 것으로 판단하는, VDI 환경에서의 싱글 사인온 방법.

[청구항 18] 청구항 16에 있어서,
상기 타겟 시스템은, 획득된 상기 사용자 인증 정보가 상기 VDI 서비스 서버로부터 획득되는 VDI 환경정보와 상이할 경우, 상기 인증에 실패한 것으로 판단하는, VDI 환경에서의 싱글 사인온 방법.

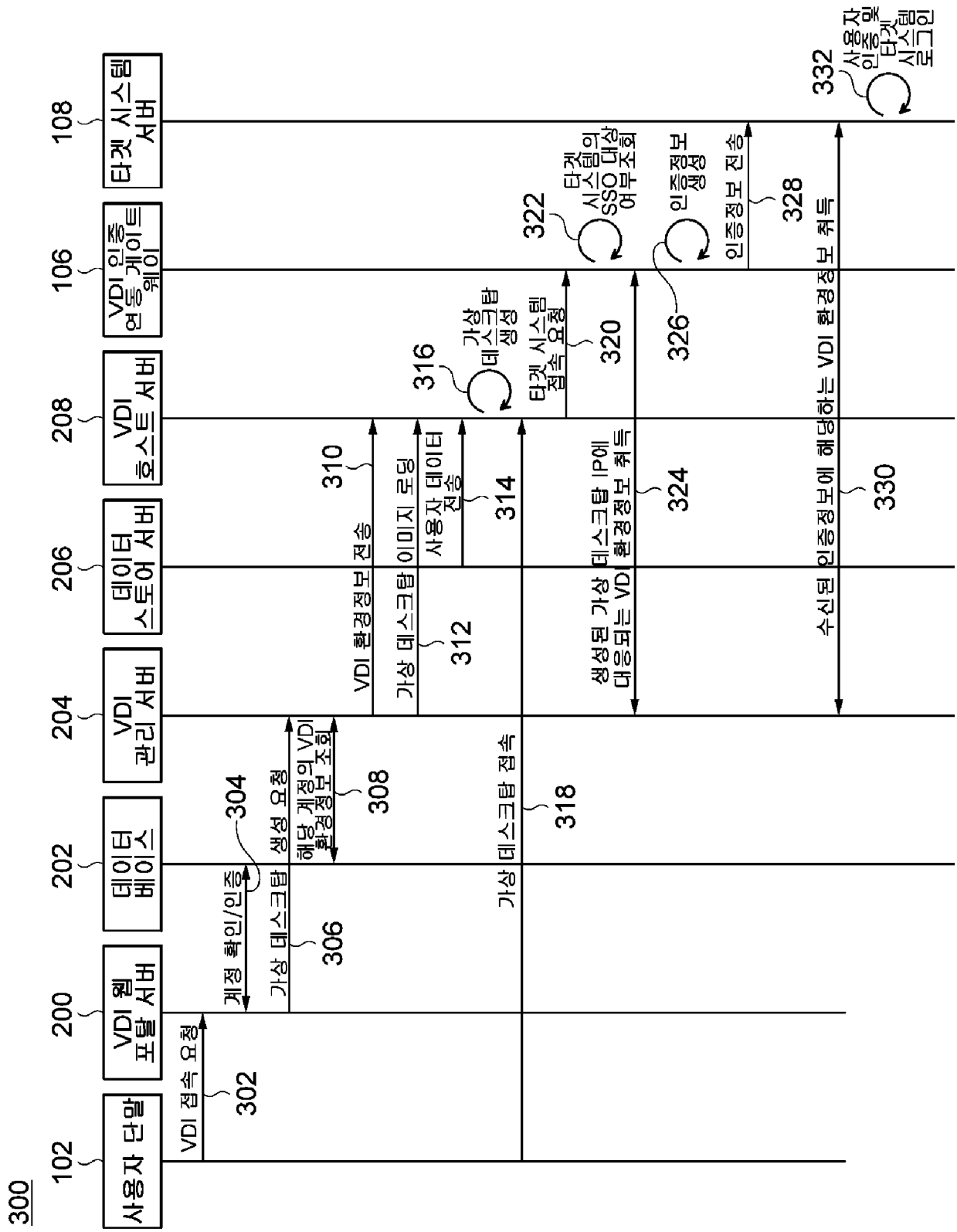
[Fig. 1]


100
104
가상 데스크탑 접속
VDI 서비스 서버
사용자 단말
VDI 환경정보
102
VDI 인증 연동 게이트웨이
타겟 시스템
VDI 환경정보를 이용하여 사용자 로그인
108
106

[Fig. 2]


200
204
208
VDI 웹 포탈 서버
VDI 관리 서버
VDI 호스트 서버
104
데이터 베이스
데이터 스토어 서버
202
206

[Fig. 3]


300
102 사용자 단말
200 VDI 웹 포탈 서버
202 데이터베이스
204 VDI 관리 서버
206 데이터 스토어 서버
208 VDI 호스트 서버
106 VDI 인증 연동 게이트웨이
108 타겟 시스템 서버
VDI 접속 요청
302
계정 확인/인증
304
가상 데스크탑 생성 요청
306
해당 계정의 VDI 환경정보 조회
308
VDI 환경정보 전송
310
가상 데스크탑 이미지 로딩
312
사용자 데이터 전송
314
316 가상 데스크탑 생성
타겟 시스템 접속 요청
320
가상 데스크탑 접속
318
322 타겟 시스템 SSO 대상 여부 조회
326 인증정보 생성
인증정보 전송
328
생성된 가상 데스크탑 IP에 대응되는 VDI 환경정보 취득
324
수신된 인증정보에 해당하는 VDI 환경정보 취득
330
332 사용자 인증 및 타겟 시스템 로그인

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2013/007834

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; G06F 15/16; G06F 21/20; G06F 17/30; G06F 7/04

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: Virtual Desktop Infrastructure, cloud, single-sign, integrated authorization, time

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2011-0107409 A1 (WILKINSON, Anthony et al.) 05 May 2011 See paragraphs [0014]-[0015], [0020]-[0022], [0024]-[0027], [0031], [0033]; claim 15; and figures 1, 3.	1-4,10-13
Y		5-9,14-18
Y	KR 10-2008-0095830 A (CDNETWORKS) 29 October 2008 See paragraphs [0019], [0031], [0033], [0048] and claim 1.	5-9,14-18
A	US 2012-0084570 A1 (KUZIN, Sergey A. et al.) 05 April 2012 See paragraphs [0063]-[0065], [0078]-[0081]; claim 1; and figures 7, 9.	1-18
A	KR 10-2012-0087644 A (HANNAM UNIVERSITY INSTITUTE FOR INDUSTRY-ACADEMIA COOPERATION) 07 August 2012 See paragraphs [0020]-[0029]; claim 1; and figures 1, 2.	1-18
A	US 8255984 B1 (GHOSTINE, Peter E. et al.) 28 August 2012 See column 7, line 24 - column 8, line 50 and figures 3, 4.	1-18

☐ 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
28 JANUARY 2014 (28.01.2014)	**28 JANUARY 2014 (28.01.2014)**

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/KR2013/007834

Patent document cited in search report	Publication date	Patent family member	Publication date
US 2011-0107409 A1	05/05/2011	AU 2010-315255 A1	26/04/2012
		EP 2489150 A2	22/08/2012
		JP 2013-510351 A	21/03/2013
		WO 2011-056906 A2	12/05/2011
		WO 2011-056906 A3	18/08/2011
KR 10-2008-0095830 A	29/10/2008	KR 10-0906645 B1	07/07/2009
US 2012-0084570 A1	05/04/2012	CN 102404314 A	04/04/2012
		US 8505083 B2	06/08/2013
KR 10-2012-0087644 A	07/08/2012	NONE	
US 8255984 B1	28/08/2012	NONE	

국 제 조 사 보 고 서

국제출원번호
PCT/KR2013/007834

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04L 9/32(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

H04L 9/32; G06F 15/16; G06F 21/20; G06F 17/30; G06F 7/04

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: VDI, 클라우드, 싱글사인, 통합인증, 시간

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
X	US 2011-0107409 A1 (ANTHONY WILKINSON et al.) 2011.05.05 단락 [0014]-[0015], [0020]-[0022], [0024]-[0027], [0031], [0033]; 청구항 15; 및 도면 1, 3 참조.	1-4,10-13
Y		5-9,14-18
Y	KR 10-2008-0095830 A ((주) 씨디네트웍스) 2008.10.29 단락 [0019], [0031], [0033], [0048] 및 청구항 1 참조.	5-9,14-18
A	US 2012-0084570 A1 (SERGEY A. KUZIN et al.) 2012.04.05 단락 [0063]-[0065], [0078]-[0081]; 청구항 1; 및 도면 7, 9 참조.	1-18
A	KR 10-2012-0087644 A (한남대학교 산학협력단) 2012.08.07 단락 [0020]-[0029]; 청구항 1; 및 도면 1, 2 참조.	1-18
A	US 8255984 B1 (PETER E. GHOSTINE et al.) 2012.08.28 컬럼 7, 라인 24 - 컬럼 8, 라인 50 및 도면 3, 4 참조.	1-18

☐ 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
2014년 01월 28일 (28.01.2014)	2014년 01월 28일 (28.01.2014)

ISA/KR의 명칭 및 우편주소
대한민국 특허청
(302-701) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)
팩스 번호 +82-42-472-7140

심사관
김도원
전화번호 +82-42-481-5560

국제조사보고서
대응특허에 관한 정보

국제출원번호
PCT/KR2013/007834

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
US 2011-0107409 A1	2011/05/05	AU 2010-315255 A1	2012/04/26
		EP 2489150 A2	2012/08/22
		JP 2013-510351 A	2013/03/21
		WO 2011-056906 A2	2011/05/12
		WO 2011-056906 A3	2011/08/18
KR 10-2008-0095830 A	2008/10/29	KR 10-0906645 B1	2009/07/07
US 2012-0084570 A1	2012/04/05	CN 102404314 A	2012/04/04
		US 8505083 B2	2013/08/06
KR 10-2012-0087644 A	2012/08/07	없음	
US 8255984 B1	2012/08/28	없음	