

- [0023] 상기 제1씨드층 및 상기 제2씨드층의 금속 입자를 촉매로 하여 상기 제3비정질층에서 결정질 박막이 생성되도록 열처리하는 결정화 단계;를 포함한 점에 특징이 있다.
- [0024] 상기 제1금속산화막 형성단계, 상기 제2금속산화막 형성단계, 상기 제1씨드층 형성단계, 상기 제2씨드층 형성단계에서의 열처리 온도는 50℃ 내지 1000℃이며,
- [0025] 상기 결정화 단계에서의 열처리 온도는 200℃ 내지 1000℃인 것이 바람직하다.
- [0026] 상기 제1금속층과 상기 제2금속층의 두께의 합은 10Å 내지 2000Å이며,
- [0027] 상기 제1금속산화막 및 상기 제2금속산화막의 두께는 각각 1Å 내지 300Å이며,
- [0028] 상기 제1금속층과 상기 제1비정질층의 두께의 비율은 1:0.5 내지 1:20이며,
- [0029] 상기 제2금속층과 상기 제2비정질층의 두께의 비율은 1:0.5 내지 1:20이며,
- [0030] 상기 제1비정질층 및 상기 제2비정질층의 두께는 각각 5Å 내지 3000Å 인 것이 바람직하다.
- [0031] 상기 제1금속층 또는 상기 제2금속층을 형성하는 금속은 니켈(Ni), 구리(Cu), 팔라듐(Pd), 코발트(Co), 알루미늄(Al), 은(Ag), 금(Au), 백금(Pt), 이리듐(Ir), 망간(Mn), 철(Fe), 크롬(Cr), 티타늄(Ti) 중 어느 하나인 것이 바람직하다.
- [0032] 상기 제1비정질층, 상기 제2비정질층, 상기 제3비정질층을 형성하는 재료는 실리콘, 실리콘게르마늄, 탄화실리콘, 게르마늄 중 어느 하나인 것이 바람직하다.
- [0033] 상기 제1비정질층 형성단계 후에 상기 제1금속층, 상기 제1금속산화막, 상기 제1비정질층 중 적어도 일부를 식각 방법으로 제거하거나,
- [0034] 상기 제2비정질층 형성단계 후에 상기 제2금속층, 상기 제2금속산화막, 상기 제2비정질층 중 적어도 일부를 식각 방법으로 제거하는 패터닝 단계를 포함할 수 있다.

발명의 효과

- [0035] 본 발명에 따른 다결정 박막의 제조방법은, 제3비정질층에 확산되어 그 제3비정질 실리콘층에서 실리콘 결정화 과정에서 제1씨드층과 제2씨드층이 결정화 온도를 낮추고 결정화된 박막의 결정립이 큰 효과가 있다. 따라서, 본 발명에 따른 다결정 박막의 제조방법은 종래의 제조방법에 비하여 생산성이 높은 장점이 있다.

도면의 간단한 설명

- [0036] 도 1은 금속유도결정화법에 의한 종래의 다결정 실리콘 박막의 제조방법을 설명하기 위한 도면이다.
- 도 2는 발명의 일 실시 예에 따른 제조공정을 보여주는 도면이다.
- 도 3은 도 2에 도시된 제1비정질층 형성단계 후의 단면을 보여주는 도면이다.
- 도 4는 도 2에 도시된 제1씨드층 형성단계 후의 단면을 보여주는 도면이다.
- 도 5는 도 2에 도시된 제2비정질층 형성단계 후의 단면을 보여주는 도면이다.
- 도 6은 도 2에 도시된 제2씨드층 형성단계 후의 단면을 보여주는 도면이다.
- 도 7은 도 2에 도시된 제3비정질층 형성단계 후의 단면을 보여주는 도면이다.
- 도 8은 도 2에 도시된 결정화 단계 후의 단면을 보여주는 도면이다.
- 도 9는 도 2에 도시된 결정화 단계 후의 결정질 박막의 표면을 광학 현미경으로 본 사진이다.
- 도 10은 도 9에 도시된 다결정 박막의 파수를 분석한 그래프이다.
- 도 11은 본 발명에 의해 제조된 다결정 실리콘 박막의 그래인 크기를 종래방법에 의해 제조된 다결정 실리콘 박막의 그래인 크기와 비교한 실험결과이다.

발명을 실시하기 위한 구체적인 내용

- [0037] 이하, 본 발명에 따른 일 실시 예를 첨부된 도면을 참조하여 상세히 설명한다.

- [0038] 도 2는 발명의 일 실시 예에 따른 제조공정을 보여주는 도면이다. 도 3은 도 2에 도시된 제1비정질층 형성단계 후의 단면을 보여주는 도면이다. 도 4는 도 2에 도시된 제1씨드층 형성단계 후의 단면을 보여주는 도면이다. 도 5는 도 2에 도시된 제2비정질층 형성단계 후의 단면을 보여주는 도면이다. 도 6은 도 2에 도시된 제2씨드층 형성단계 후의 단면을 보여주는 도면이다. 도 7은 도 2에 도시된 제3비정질층 형성단계 후의 단면을 보여주는 도면이다. 도 8은 도 2에 도시된 결정화 단계 후의 단면을 보여주는 도면이다.
- [0039] 도 2 내지 도 8을 참조하면, 본 발명의 일 실시 예에 따른 저온 다결정 박막의 제조방법(이하, "제조방법"이라 함)은 절연층 형성단계(S1)와, 제1금속층 형성단계(S2)와, 제1금속산화막 형성단계(S3)와, 제1비정질층 형성단계(S4)와, 제1씨드층 형성단계(S5)와, 제2금속층 형성단계(S6)와, 제2금속산화막 형성단계(S7)와, 제2비정질층 형성단계(S8)와, 제2씨드층 형성단계(S9)와, 제3비정질층 형성단계(S10)와, 결정화 단계(S11)를 포함한다.
- [0040] 상기 절연층 형성단계(S1)에서는 예컨대 유리와 같은 소재로 이루어진 기판(10) 상에 절연층(20)을 형성한다. 상기 절연층(20)은 스퍼터링(sputtering) 또는 플라즈마 화학증착(PECVD)과 같은 알려진 방법에 의해 수행될 수 있다. 상기 절연층(20)은 예컨대 산화물(SiO_2 , Al_2O_3 , MgO 등), 질화물(SiN , AlN , Si_3N_4 등), 플루오르 화합물(CaF_2 , MgF_2 , LaF_3 , LiF 등) 중 어느 하나로 이루어질 수 있다. 상기 절연층(20)은 절연 기능을 하기 위해 마련된 것이다. 또한, 절연층(20)은 후술하는 제1씨드층 형성단계(S5), 제2씨드층 형성단계(S9), 결정화 단계(S11)에서 상기 기판(10)으로부터 후술하는 제1비정질층(40) 또는 제2비정질층(60) 또는 제3비정질층(70)에 불순물이 확산 되어 제1비정질층(40), 제2비정질층(60), 제3비정질층(70)이 불순물에 오염되는 것을 방지하기 위해 마련된 것이다. 상기 절연층 형성단계(S1)에서의 열처리 온도는 50°C 내지 1000°C 인 것이 바람직하다. 상기 절연층 형성단계(S1)에서의 열처리 온도가 50°C 미만인 경우에는 절연층(20)을 형성하는 산화물, 질화물, 플루오르 화합물이 제대로 형성되지 않은 문제점이 있다. 한편, 상기 절연층 형성단계(S1)에서의 열처리 온도가 1000°C 를 초과하는 경우에는 유리로 된 기판(10)이 열 충격에 의해 파손될 수 있는 문제점이 있다.
- [0041] 상기 제1금속층 형성단계(S2)에서는 상기 절연층(20) 상에 예컨대 니켈(Ni), 구리(Cu), 팔라듐(Pd), 코발트(Co), 알루미늄(Al), 은(Ag), 금(Au), 백금(Pt), 이리듐(Ir), 망간(Mn), 철(Fe), 크롬(Cr), 티타늄(Ti)과 같은 제1금속층(30)을 형성시킨다. 상기 제1금속층(30)은 스퍼터링(sputtering) 또는 플라즈마 화학증착(PECVD)과 같은 알려진 방법에 의해 수행될 수 있다. 상기 제1금속층(30)의 두께는 후술하는 제1비정질층(40)의 두께와 상대적인 관계에서 결정하는 것이 바람직하다. 상기 제1금속층(30)의 두께는 $10\text{\AA}$ 내지 $300\text{\AA}$ 인 것이 바람직하다. 상기 제1금속층(30)의 두께가 $10\text{\AA}$ 미만인 경우에는 너무 얇은 두께로 인해 공정 재현성 문제와 넓은 면적에 증착시 상기 제1금속층(30)의 균일성(uniformity)이 나빠지는 문제점이 있다. 한편, 상기 제1금속층(30)의 두께가 $300\text{\AA}$ 를 초과하는 경우에는 많은 금속이 침투하여 금속 오염문제가 유발되어 결정화된 실리콘층을 포함하는 디바이스(device)의 특성을 저하시키는 문제점이 있다.
- [0042] 상기 제1금속산화막 형성단계(S3)에서는 상기 제1금속층 형성단계(S2)를 거친 제1금속층(30)을 열처리하여 그 제1금속층(30)의 표면에 제1금속산화막(35)을 형성하거나, 상기 제1금속층(30) 위에 금속산화막을 증착하여 제1금속산화막(35)을 형성할 수 있다. 상기 제1금속산화막(35)의 두께는 $1\text{\AA}$ 내지 $300\text{\AA}$ 인 것이 바람직하다. 상기 제1금속산화막(35)의 두께가 $1\text{\AA}$ 미만인 경우에는 상기 제1금속산화막(35)이 너무 얇아 제 기능을 수행하지 못하는 문제점이 있다. 한편, 상기 제1금속산화막(35)의 두께가 $300\text{\AA}$ 를 초과하는 경우에는 상기 제1금속층(30)으로부터 촉매 금속이 침투하기 어려워지는 문제점과 공정의 수행시간이 지나치게 길어져 비경제적인 문제점이 있다. 상기 제1금속산화막 형성단계(S3)에서의 열처리에 의해 제1금속산화막(35)을 형성하는 경우에 열처리 온도는 50°C 내지 1000°C 인 것이 바람직하다. 상기 제1금속산화막 형성단계(S3)에서의 열처리 온도가 50°C 미만인 경우에는 금속산화막(35)이 형성되지 않는 문제점이 있다. 한편, 상기 제1금속산화막 형성단계(S3)에서의 열처리 온도가 1000°C 를 초과하는 경우에는 유리로 이루어진 기판이 열 충격에 의해 파손되거나 손상되는 문제점이 발생할 수 있다.
- [0043] 상기 제1비정질층 형성단계(S4)에서는 상기 제1금속산화막(35) 위에 비정질층을 적층하여 제1비정질층(40)을 형성한다. 상기 제1비정질층(40)은 플라즈마 화학증착법과 같이 알려진 수단을 이용하여 상기 제1금속산화막(35) 위에 적층 함으로써 형성한다. 상기 제1비정질층(40)의 두께는 $5\text{\AA}$ 내지 $3000\text{\AA}$ 인 것이 바람직하다. 상기 제1비정질층(40)의 두께가 $5\text{\AA}$ 미만인 경우에는 상기 제1비정질층(40)의 두께가 너무 얇아서 공정 재현성이 나빠지는 문제점과 넓은 면적에 증착시 상기 제1비정질층(40)의 균일성(uniformity)이 나빠지는 문제점이 있다. 한편, 상기 제1비정질층(40)의 두께가 $3000\text{\AA}$ 를 초과하는 경우에는 상기 제1금속층(30)의 금속 원소와 결합하여 상기 제1비정질층(40)이 후술하는 제1씨드층(45)을 형성하는데 필요하지 않은 화학결합이 생성되는 문제점이 있다. 또한, 상기 제1금속층(30)의 두께와 상기 제1비정질층(40)의 두께의 비는 $1:0.5$ 내지 $1:20$ 인 것이 바람직하다. 상

기 제1금속층(30)의 두께와 상기 제1비정질층(40)의 두께의 비가 그 범위를 벗어나는 경우에는 전술한 바와 같이 제1비정질층(45)을 형성하는데 필요하지 않은 화합물이 생성되는 문제점이 있다. 즉 금속 유도전환에 필요한 제1비정질층(45)의 조성이나 조성의 화학결합이 형성되어 유도 결정화에 방해가 되는 것이다. 상기 제1비정질층(40)을 형성하는 재료는 실리콘(Si), 질화실리콘(Si₃N₄), 산화실리콘(SiO₂), 게르마늄(Ge) 중 어느 하나일 수 있다. 상기 제1비정질층 형성단계(S4) 후에는 페터닝 단계를 포함할 수 있다. 상기 페터닝 단계에서 는 상기 제1금속층(30), 상기 제1금속산화막(35), 상기 제1비정질층(40)의 전부 또는 어느 한 층의 일부만을 식 각 방법으로 제거한다. 상기 페터닝 단계는 필요에 따라 생략될 수 있다.

[0044] 상기 제1비정질층 형성단계(S5)에서는 상기 제1금속층(30)으로부터 촉매 금속 원자가 상기 제1비정질층(40)으로 이동하여 화학물을 형성하도록 열처리한다. 상기 제1비정질층 형성단계(S5)에서 형성된 제1비정질층(45)은 상기 제1금속층(30)과, 상기 제1금속산화막(35)과, 상기 제1비정질층(40)의 임자가 원에너지에 의해 이동하여 화학결합 된으로써 생성된다. 즉, 상기 제1금속층(30)으로부터 에전대 나켈(Ni)과 같은 촉매 금속 원자가 상기 제1비정질 층(40)으로 이동하여 상기 제1금속산화막(35)으로부터 이동된 산소(O)와 결합하여 에전대 NiSiGeO와 같은 화합 물을 형성한다. 상기 제1비정질층 형성단계(S5)에서 열처리는 고온 공정(furnace), 금속 열처리(RTA), 자외선(UV) 가열법 등에 의해 이루어질 수 있다. 상기 제1비정질층 형성단계(S5)에서 형성된 제1비정질층(45)은 후술하는 결정화 단계(S11)에서 제3비정질층(70)을 결정화하는 데 역할을 한다. 상기 제1비정질층 형성단계(S5)에서 의 열처리 온도는 50℃ 내지 1000℃인 것이 바람직하다. 상기 제1비정질층 형성단계(S5)의 열처리 온도가 50℃ 미만인 경우에는 제1비정질층(45)이 잘 형성되지 않는 문제점이 있다. 상기 제1비정질층 형성단계(S5)의 열처리 온도가 1000℃를 초과하는 경우에는 유리(glass)로 된 상기 기판(10)이 열 충격에 의해 변형 또는 파손되는 문제점 이 있다.

[0045] 상기 제2금속층 형성단계(S6)에서는 상기 제1비정질층(45) 위에 에전대 나켈(Ni), 구리(Cu), 할라늄(Pb), 코발트(Co), 알루미늄(Al), 은(Ag), 금(Au), 백금(Pt), 이리듐(Ir), 망간(Mn), 철(Fe), 크롬(Cr), 티타늄(Ti)과 같은 제2금속층(50)을 형성시킨다. 상기 제2금속층(50)은 스퍼터링(sputtering) 또는 플라즈마 화학증착(PECVD)과 같은 알려진 방법에 의해 수행될 수 있다. 상기 제2금속층(50)의 두께는 후술하는 제2비정질층(60)의 두께와 상대 적인 관계에서 결정하는 것이 바람직하다. 상기 제2금속층(50)의 두께는 10Å 내지 300Å인 것이 바람직하다. 상기 제2금속층(50)의 두께가 10Å 미만인 경우에는 너무 얇은 두께로 인해 공정 제원상 문제와 적은 면적에 증착시 상기 제1금속층(30)과 상기 제2금속층(50)의 두께의 합은 10Å 내지 2000Å 인 것이 바람직하다. 상기 제1금속 층(30)과 상기 제2금속층(50)의 두께의 합이 10Å 미만인 경우에는 너무 얇은 두께로 인해 공정 제원상 문제와 적은 면적에 증착시 상기 제1금속층(30) 또는 상기 제2금속층(50)의 균일성(uniformity)이 나빠지는 문제가 있다. 한편, 상기 제1금속층(30)과 상기 제2금속층(50)의 두께가 2000Å를 초과하는 경우에는 많은 금속이 침투 하여 금속 오염문제가 유발되어 결정화된 실리콘층을 포함하는 나비스(devicc)의 특성을 저하시키는 문제점이 있다.

[0046] 상기 제2금속산화막 형성단계(S7)에서는 상기 제2금속층(50)을 가진 제2금속층(50)을 열처리하여 그 제2금속층(50)의 표면에 제2금속산화막(55)을 형성하거나, 상기 제2금속층(50) 위에 금속산화막을 증착하여 제2금속산화막(55)을 형성할 수 있다. 상기 제2금속산화막(55)의 두께는 1Å 내지 300Å인 것이 바람직하다. 상기 제2금속산화막(55)의 두께가 1Å 미만인 경우에는 상기 제2금속산화막(55)이 너무 얇아 제 기층을 수형하지 못 하는 문제점이 있다. 한편, 상기 제2금속산화막(55)의 두께가 300Å를 초과하는 경우에는 상기 제2금속층(50)으로부터 촉매 금속이 침투하기 어려워지는 문제점과 공정의 수행시간이 지나치게 길어져 비경제적인 문제점이 있 다. 상기 제2금속산화막 형성단계(S7)에서의 열처리에 의해 제2금속산화막(55)을 형성하는 경우에 열처리 온도는 50℃ 내지 1000℃인 것이 바람직하다. 상기 제2금속산화막 형성단계(S7)에서의 열처리 온도가 50℃ 미만인 경우에는 제2금속산화막(55)이 형성되지 않는 문제점이 있다. 한편, 상기 제2금속산화막 형성단계(S7)에서의 열 처리 온도가 1000℃를 초과하는 경우에는 유리로 이루어진 기판이 열 충격에 의해 파손되거나 손상되는 문제점 이 발생될 수 있다.

[0047] 상기 제2비정질층 형성단계(S8)에서는 상기 제2금속산화막(55) 위에 비정질층을 적층하여 제2비정질층(60)을 형 성한다. 상기 제2비정질층(60)은 플라즈마 화학증착법과 같이 알려진 수단을 이용하여 상기 제2금속산화막(55) 위에 적층함으로써 형성한다. 상기 제2비정질층(60)의 두께는 5Å 내지 3000Å인 것이 바람직하다. 상기 제2비 정질층(60)의 두께가 5Å 미만인 경우에는 상기 제2비정질층(60)의 두께가 너무 얇아서 공정 제원상이 나빠지는

문제점과 넓은 면적에 증착시 상기 제2비정질층(60)의 균일성(uniformity)이 나빠지는 문제점이 있다. 한편, 상기 제2비정질층(60)의 두께가 3000Å를 초과하는 경우에는 상기 제2금속층(50)의 금속 원소와 결합하여 상기 제2비정질층(60)이 후술하는 제2씨드층(65)을 형성하는데 필요하지 않은 화학결합이 생성되는 문제점이 있다. 또한, 상기 제2금속층(50)의 두께와 상기 제2비정질층(60)의 두께의 비는 1:0.5 내지 1:20인 것이 바람직하다. 상기 제2금속층(50)의 두께와 상기 제2비정질층(60)의 두께의 비가 그 범위를 벗어나는 경우에는 전술한 바와 같이 제2씨드층(65)을 형성하는데 필요하지 않은 화학 결합이 생성되는 문제점이 있다. 즉 금속 유도결합에 필요한 제2씨드층(65)의 조성이 아닌 다른 조성의 화학결합이 형성되어 유도 결정화에 방해가 되는 것이다. 상기 제2비정질층(60)을 형성하는 재료는 실리콘(Si), 실리콘게르마늄(SiGe), 탄화실리콘(SiC), 게르마늄(Ge) 중 어느 하나일 수 있다. 상기 제2비정질층 형성단계(S8) 후에는 패터닝 단계를 포함할 수 있다. 상기 제2비정질층(60)의 재료는 상기 제1비정질층(40)의 재료와 동일하게 할 수도 있으며 서로 다르게 할 수도 있다.

[0049] 상기 패터닝 단계에서는 상기 제2금속층(50), 상기 제2금속산화막(55), 상기 제2비정질층(60)의 전부 또는 어느 한 층의 일부분을 식각 방법으로 제거한다. 상기 패터닝 단계는 필요에 따라 생략될 수 있다.

[0050] 상기 제2씨드층 형성단계(S9)에서는 상기 제2금속층(50)으로부터 촉매 금속 원자가 상기 제2비정질층(60)으로 이동하여 화합물을 형성하도록 열처리한다. 상기 제2씨드층 형성단계(S9)에서 형성된 제2씨드층(65)은 상기 제2금속층(50)과, 상기 제2금속산화막(55)과, 상기 제2비정질층(60)의 입자가 열에너지에 의해 이동하여 화학결합됨으로써 생성된다. 즉, 상기 제2금속층(50)으로부터 예컨대 니켈(Ni)과 같은 촉매 금속 원자가 상기 제2비정질층(60)으로 이동하여 상기 제2금속산화막(55)으로부터 이동된 산소(O)와 결합하여 예컨대 NiSiGeO와 같은 화합물을 형성한다. 상기 제2씨드층 형성단계(S9)에서 행해지는 열처리는 고온 공정(furnace), 금속 열처리(RTA), 자외선(UV) 가열법 등에 의해 이루어질 수 있다. 상기 제2씨드층 형성단계(S9)에서 형성된 제2씨드층(65)은 후술하는 결정화 단계(S11)에서 제3비정질층(70)을 결정화하는 핵 역할을 한다. 상기 제2씨드층 형성단계(S9)에서의 열처리 온도는 50℃ 내지 1000℃인 것이 바람직하다. 상기 제2씨드층 형성단계(S9)의 열처리 온도가 50℃ 미만인 경우에는 제2씨드층(65)이 잘 형성되지 않는 문제점이 있다. 상기 제2씨드층 형성단계(S9)의 열처리 온도가 1000℃를 초과하는 경우에는 유리(glass)로 된 상기 기판(10)이 열 충격에 의해 변형 또는 파손되는 문제점이 있다.

[0051] 상기 제3비정질층 형성단계(S10)에서는 상기 제2씨드층(65) 위에 결정화 하고자 하는 제3비정질층(70)을 적층하여 제3비정질층(70)을 형성한다. 상기 제3비정질층(70)을 형성하는 방법은 상기 제1비정질층(40)을 형성하는 방법을 채용할 수 있다. 상기 제3비정질층(70)을 형성하는 재료는 실리콘(Si), 실리콘게르마늄(SiGe), 탄화실리콘(SiC), 게르마늄(Ge) 중 어느 하나일 수 있다. 상기 제3비정질층(70)을 구성하는 재료와 상기 제1비정질층(40) 및 상기 제2비정질층(60)을 구성하는 재료는 동일할 수도 있으며 서로 다를 수도 있다.

[0052] 상기 결정화 단계(S11)에서는 상기 제1씨드층(45) 및 상기 제2씨드층(65)의 금속 입자를 촉매로 하여 상기 제3비정질층(70)에서 결정질 박막(80)이 생성되도록 열처리한다. 상기 결정화 단계(S11)에서의 열처리 온도는 200℃ 내지 1000℃인 것이 바람직하다. 본 실시 예에서, 상기 결정화 단계(S11)에서의 열처리는 RTA(Rapid Thermal Annealing) 장비를 사용하여 630℃에서 수행하였다. 상기 결정화 단계(S11)의 열처리 온도가 200℃ 미만인 경우에는 결정화하기에 온도가 낮아 결정화가 잘 되지 않은 문제점이 있다. 상기 결정화 단계(S11)의 열처리 온도가 1000℃를 초과하는 경우에는 유리(glass)로 된 상기 기판(10)이 열 충격에 의해 변형 또는 파손되는 문제가 발생할 수 있다.

[0053] 도 9는 도 2에 도시된 결정화 단계 후의 결정질 박막의 표면을 광학 현미경으로 본 사진이다. 도 10은 도 9에 도시된 다결정 박막의 파수를 분석한 그래프이다. 도 11은 본 발명에 의해 제조된 다결정 실리콘 박막의 그래인 크기를 종래방법에 의해 제조된 다결정 실리콘 박막의 그래인 크기와 비교한 실험결과이다.

[0054] 도 10에서 가로축은 파수(cm^{-1})를 나타내며 진동수에 대응하는 값이다. 파수(wave number)란 원자·분자·핵 분광학에서 빛의 진동수를 빛의 속도로 나누어서 단위 거리에 있는 파동의 수를 나타내는 진동수의 단위이다. 즉, 어떤 파의 진동수는 그리스 문자 ν (뉴)로 나타내는데 이는 광속 c 를 파장 λ 로 나눈 값과 같다. 즉 $\nu = c/\lambda$ 이다. 스펙트럼의 가시광선 영역에서 전형적인 스펙트럼 선은 $5.8 \times 10^{-5} \text{cm}$ 의 파장이며 $5.17 \times 10^{14} \text{Hz}$ 의 진동수에 해당한다. 그런데 이와 같은 진동수가 너무 큰 값을 갖기 때문에 이 숫자를 광속으로 나누어서 크기를 작게 하는 것이 편리하다. 진동수를 광속으로 나누면 ν/c 인데 이는 위 식에서 $1/\lambda$ 이다. 파장을 m단위로 제면 $1/\lambda$ 는 1m 내에서 발견되는 파의 수를 나타낸다. 파수는 대개 $1/\text{m}$, 즉 m^{-1} 와 $1/\text{cm}$, 즉 cm^{-1} 의 단위로 측정한다. 도 10에서 세로축은 단위 시간당 측정되는 파수의 합으로서 강도(intensity, CPS, Count Per Second)에 해당하는 값이다.

[0055] 도 10을 참조하면 520cm^{-1} 에서 최대 강도가 나타나고 있으므로 결정질 실리콘이 잘 형성된 것을 알 수 있다. 도 9는 본 발명에 따라 제조된 다결정 실리콘 박막의 표면의 1000배의 광학 현미경으로 본 사진이다. 도 11은 본 발명에 따라 제조된 다결정 실리콘의 그레인 크기와 관련하여 도 1에 도시된 종래의 방법으로 제조된 다결정 실리콘 그레인의 크기를 비교한 실험자료를 인용하였다. 도 11에 도시된 자료는 일반적으로 태양전지용으로 사용되는 다결정 실리콘 박막의 그레인 크기를 평가할 때 기판 상에 형성된 다결정 실리콘 박막의 임의의 영역을 $10\text{cm} \times 10\text{cm}$ 로 설정하고 그 영역에 존재하는 그레인의 크기가 $30\mu\text{m}$ 이상의 크기의 비율을 측정한 결과이다. 도 11을 참조하면 종래의 방법에 의해 제조된 다결정 실리콘 박막은 0% 비율이 측정된 반면에 본 발명에 따라 제조된 다결정 실리콘 박막은 90%의 비율이 측정되었다. 이와 같이 본 발명에 따른 제조방법은 종래의 방법에 비하여 결정화된 실리콘의 품질이 현저하게 우수한 것을 알 수 있다.

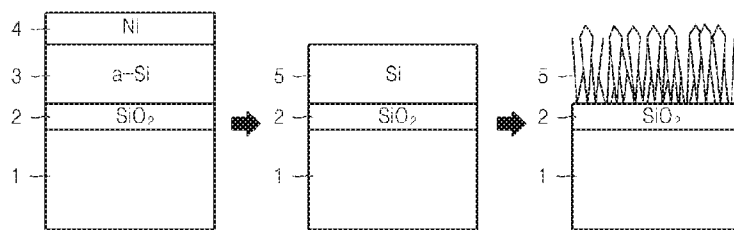
[0056] 이상, 바람직한 실시 예를 들어 본 발명에 대해 설명하였으나, 본 발명이 그러한 예에 의해 한정되는 것은 아니며, 본 발명의 기술적 사상을 벗어나지 않는 범주 내에서 다양한 형태의 실시 예가 구체화될 수 있을 것이다.

부호의 설명

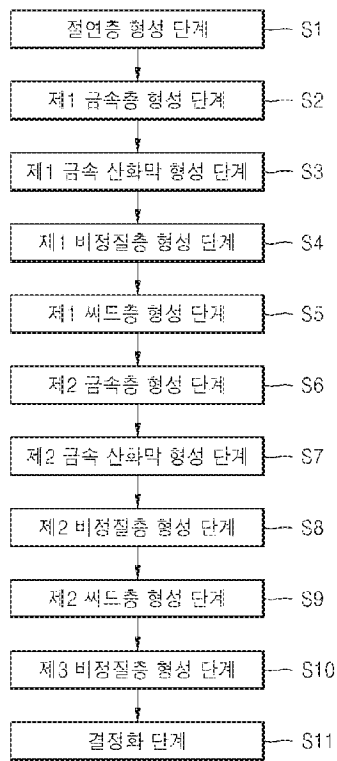
[0057] 10...기판	20...절연층
30...제1금속층	35...제1금속산화막
40...제1비정질층	45...제1씨드층
50...제2금속층	55...제2금속산화막
60...제2비정질층	65...제2씨드층
70...제3비정질층	80...결정질 박막
S1...절연층 형성단계	S2...제1금속층 형성단계
S3...제1금속산화막 형성단계	S4...제1비정질층 형성단계
S5...제1씨드층 형성단계	S6...제2금속층 형성단계
S7...제2금속산화막 형성단계	S8...제2비정질층 형성단계
S9...제2씨드층 형성단계	S10...제3비정질층 형성단계
S11...결정화 단계	

도면

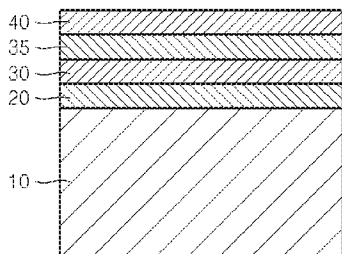
도면1



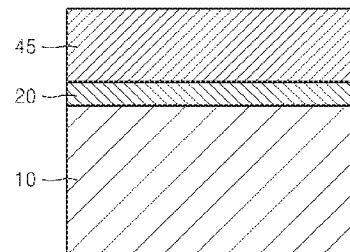
도면2



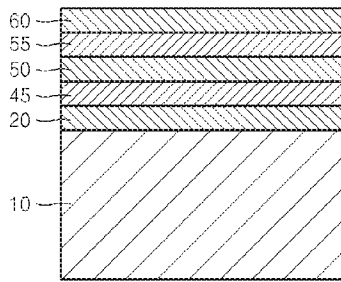
도면3



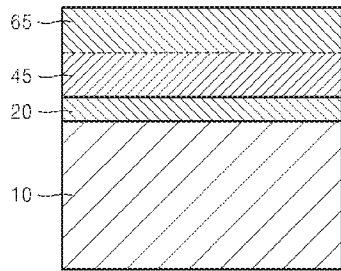
도면4



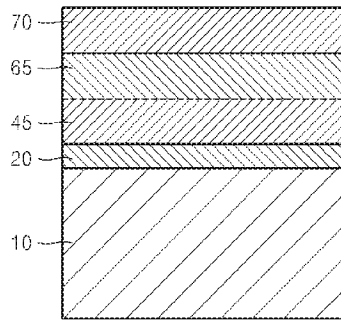
도면5



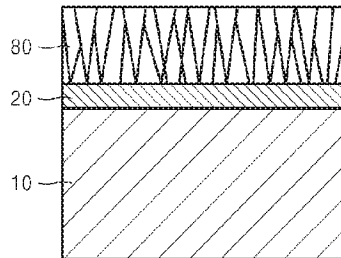
도면6



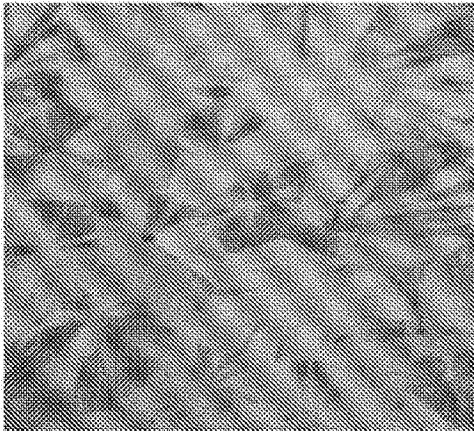
도면7



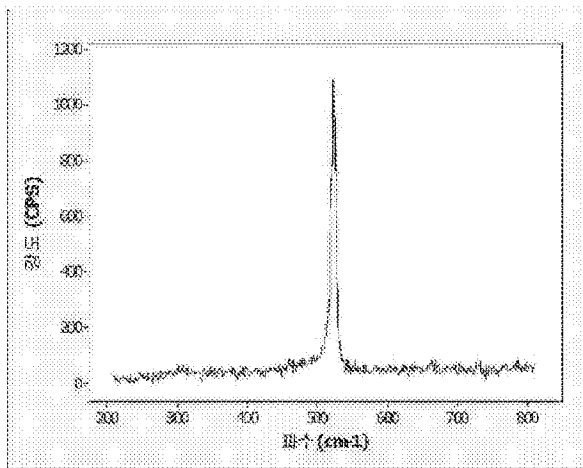
도면8



도면9



도면10



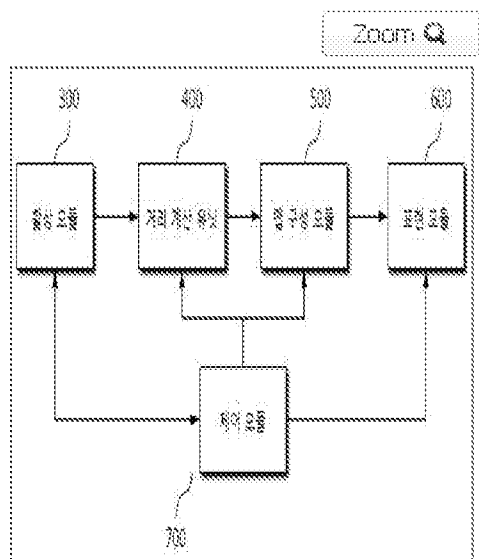
도면11

비교 항목	종래	본 발명
결정화 시간 (상대 비교)	100	90
합격율 (Grain 30 μ m 이상 크기의 비중(10x 10cm 기판 기준))	0%	90%

찰상장치를 이용하여 객체의 위치와 거리를 측정하고 이를 표현하는 장치

Using Imaging Device To Measure Position And Distance of the Objects, and Device expressing the same

(51) Int. CL.	G01C 11/36(2006.01) G01C 3/24(2006.01) B60R 21/00(2006.01) B60W 30/08(2006.01)
(52) CPC	
(21) Application No.(Date)	1020110130002 (2011.12.07)
(71) Applicant	Yoon, Tae-eun
(11) Registration No.(Date)	
(65) Unex. Pub. No.(Date)	1020130063593 (2013.06.17)
(11) Publication No.(Date)	
(86) Int'l Application No.(Date)	
(87) Int'l Unex. Pub. No.(Date)	
(30) Priority info. (Country / No. / Date)	
Legal Status	Unexamined
Examination Status	
Trial Info	
Kind/Right of Org. Application	New Application /
Right of Org. Application No.(Date)	
Related Application No.	
Request for an examination(Date)	N
Number of examination claims	4



KIPA (Korea Patent Abstract) PURPOSE: A device for expressing a distance to an object by measuring the same with a photographing device is provided to grasp positions of ambient objects by using the tactile sensation of a user.

CONSTITUTION: A device for expressing a distance to an object by measuring the same with a photographing device comprises a photographing module(300), a distance calculation unit(400), a map constituting module(500), and an expressing module(600). The photographing module photographs external images with one or more photographing devices. The distance calculation unit extracts objects of the images by receiving the images photographed by the photographing module and calculates distances to the objects and positions thereof. The map constituting module constitutes a map by digitalizing the calculated positions of the objects into coordinates and modulates the coordinates registered in the map. The expressing module expresses the coordinates registered in the map by moving an external lattice upwardly and downwardly.

COPYRIGHT KIPO 2013



(19) 대한민국특허청(KR)

(12) 공개특허공보(A)

(11) 공개번호 10-2013-0063593

(43) 공개일자 2013년06월17일

(51) 국제특허분류(Int. Cl.)

G01C 11/36 (2006.01) B60W 30/08 (2006.01)

G01C 3/24 (2006.01) B60R 21/00 (2006.01)

(21) 출원번호 10-2011-0130002

(22) 출원일자 2011년12월07일

심사청구일자 없음

(71) 출원인

윤태은

충청남도 천안시 서북구 월봉7길 77 (쌍용동, 청솔아파트)

(72) 발명자

윤태은

충청남도 천안시 서북구 월봉7길 77 (쌍용동, 청솔아파트)

윤균재

대전광역시 대덕구 비래동로32번길 22 (비래동)

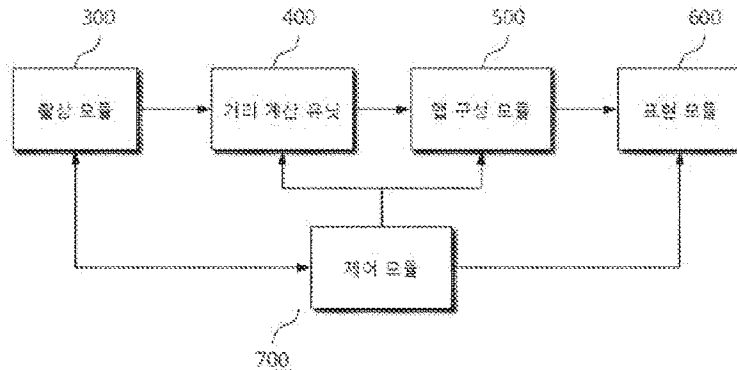
전체 청구항 수 : 총 4 항

(54) 발명의 명칭 활상장치를 이용하여 객체의 위치와 거리를 측정하고 이를 표현하는 장치

(57) 요약

본 발명은 활상장치를 이용한 객체의 위치와 거리 측정 및 표현 장치에 관한 것으로, 외부 영상을 촬영하는 활상 모듈; 활상 모듈로부터 얻어진 이미지들로부터 위치 및 거리 정보를 계산하는 거리 계산 유닛, 계산된 각 객체들의 위치를 물리적으로 표현하는 표현 모듈을 포함한다.

도 1



이러한 물체의 위치 및 거리 정보는 일례로 지능형 자동차 시스템에서 전방 또는 후방의 충돌방지 기능 등에 적용될 수 있으며, 기술 개발의 발달에 따라 현재는 전방 또는 후방의 물체 감지에 의한 정각적 감지 정보뿐만 아니라 카메라를 이용한 시각적 감지 정보까지 제공될 수 있도록 함으로써, 운전자가 더 용이하게 물체의 거리 및 위치 정보를 알 수 있도록 하고 있다.

[0003]

주행 조건을 제시할 수 있는 다양한 기술이 개발, 보급되고 있다. 위치와 거리 정보를 감지하거나 주차 중 후방에 위치한 물체의 위치와 거리 정보를 감지하여 운전자에게 최적의 있는 기술이 다양한 산업 분야에 적용되고 있으며, 특히 차량에 적용됨에 있어 주행 중 전방에 위치한 물체의 최근에 이르러, 영면 상에 위치한 전방의 물체를 인식하고 인식된 물체의 거리 정보와 위치 정보를 파악할 수

[0002]

배경 기술

거리를 측정하여 표현하는 장치에 관한 것이다. 의 위치와 거리를 측정하여 표현하는 장치에 관한 것으로, 환상장치를 통해 주변에 존재하는 객체들의 위치와 본 발명은 주변 주변 객체들의 위치를 표현하는 장치에 관한 것으로, 환상장치를 통해 주변에 존재하는 객체들

[0001]

기술 분야

발명 배경

상기 객체의 오르내림 조건을 통해 표현하는 것을 특징으로 하는 표현 모듈. 상기 표현 모듈은 맵 구성 모듈로부터 수신한 3차원 좌표 데이터에 따라 상기 기기의 특정 객체를 선택하고,

제 1항에 있어서,

청구항 4

방향이 변경되었다는 것이 판단되면, 상기 3차원의 좌표 데이터를 변경된 각도에 맞춰 수정하는 것을 특징으로 하는 맵 구성 모듈. 상기 맵 구성 모듈은 구성 웹에 대한 좌표를 3차원의 좌표 데이터 형태로 유식하고, 제 1항에 있어서,

청구항 3

상기 거리 계산 유닛은 환상 모듈로부터 수신한 영상에서 객체들을 구분하고, 상기 객체의 거리, 방향, 높이 정보를 계산하는 것을 특징으로 하는 거리 계산 유닛.

청구항 2

를 포함하는 환상장치를 이용하여 객체의 위치와 거리를 측정하고 이를 표현하는 장치. 상기 웹에 등록된 좌표들을 기기 외부의 객체의 오르내림 조건을 통해 표현하는 표현 모듈; 모듈;

계산된 물체들의 위치를 좌표화하여 웹을 구성하고, 방향 전환 시 웹에 등록된 좌표들을 수정하는 맵 구성 유닛을 계산하는 기지 계산 유닛; 및

상기 환상 모듈로부터 촬영된 영상을 전송받아 영상 내의 객체들을 추출하고, 추출된 상기 객체들의 거리 및 위치를 계산하는 기지 계산 유닛; 및

하나 이상의 환상장치를 통해 외부 영상을 촬영하는 환상 모듈;

청구항 1

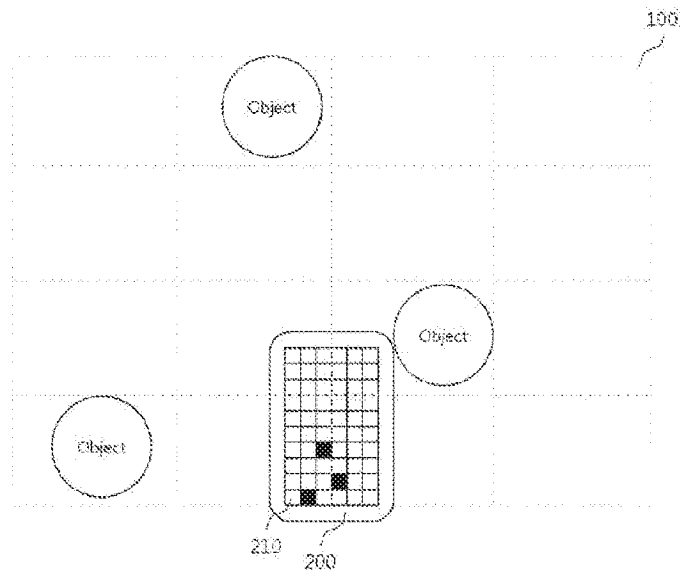
특허청구의 범위

- [0004] 이와 같은 정각적 또는 시각적 각기 정보를 구현하기 위한 종래의 방식은 조음파 또는 레이저를 통해 적방 또는 후방 물체의 대략적인 위치를 검지하여 검지된 정보를 주제어부에 송신하고, 송신된 정보를 운전자가 정각적 정보에 의해 취득할 수 있도록 하고 있다.
- [0005] 그러나, 이 경우에는 물체의 거리 및 위치 정보를 파악함에 있어서 전방 또는 후방으로 고정되어 있고, 감지 정보를 정각적 정보 또는 시각적 정보로만 제공하고 있다.
- 발명의 내용
- 해결하려는 문제
- [0006] 따라서, 본 발명의 목적은 주변 객체들의 위치를 측각을 이용하여 인지할 수 있도록 표현하는 장치를 제공함에 있다.
- 문제의 해결 수단
- [0007] 목적을 달성하기 위한 본 발명은 외부 영상을 촬영하는 촬상 모듈, 촬상 모듈로부터 얻어진 이미지들로부터 위치 및 거리 정보를 계산하는 거리 계산 유닛, 계산된 각 객체들의 위치를 물리적으로 표현하는 표현 모듈을 포함하는 것을 특징으로 하는 표현 장치의 구성을 개시한다.
- 발명의 효과
- [0008] 이상에서 살펴본 바와 같이 본 발명에 따른 촬상장치를 이용하여 객체의 위치와 거리 측정하고 이를 표현하는 장치에 따르면, 본 발명은 장치 사용자가 측각을 이용하여 주변 객체들의 위치를 파악할 수 있도록 한다.
- 도면의 간단한 설명
- [0009] 도 1은 본 발명의 실시 예에 따른 촬상장치를 이용하여 객체의 위치와 거리를 측정하고 이를 표현하는 장치의 구성을 개략적으로 나타낸 도면.
- 도 2는 본 발명의 실시 예에 따른 표현장치의 구성을 상세히 나타낸 도면.
- 발명을 실시하기 위한 구체적인 내용
- [0010] 이하, 실시 예를 설명함에 있어서 본 발명이 속하는 기술분야에 익히 알려져 있고 본 발명과 직접적으로 관련이 없는 기술 내용에 대해서는 설명을 생략한다. 또한, 실질적으로 동일한 구성과 기능을 가진 구성 요소들에 대해서는 상세한 설명을 생략하도록 한다.
- [0011] 마찬가지로, 일부 구성요소는 과장되거나 생략되거나 또는 개략적으로 도시되었으며, 각 구성요소의 크기는 실제 크기를 전적으로 반영하는 것이 아니다. 따라서 본 발명은 첨부한 도면에 그려진 상대적인 크기나 간격에 의해 제한되어지지 않는다.
- [0012] 본 발명은 촬상장치를 이용하여 객체의 위치와 거리를 측정하고 이를 표현하는 것에 의해, 장치 사용자가 측각을 이용하여 주변 객체들의 위치를 파악할 수 있도록 한다.
- [0013] 이하 본 발명의 실시 예에 따른 촬상장치를 이용하여 객체의 위치와 거리를 측정하고 이를 표현하는 장치의 각 구성들과 역할 및 기능에 대하여 도면을 참조하여 상세히 설명하기로 한다.
- [0014] 도 1은 본 발명의 실시 예에 따른 촬상장치를 이용하여 객체의 위치와 거리를 측정하고 이를 표현하는 장치의 구성을 개략적으로 나타낸 도면이다.
- [0015] 도 1을 참조하면, 본 발명의 촬상장치를 이용하여 객체의 위치와 거리를 측정하고 이를 표현하는 장치는 주변 객체들의 거리와 위치를 특정 단위(100)로 나누어 파악하여 표현장치(200) 내의 객체들(210)에 표시할 수 있다.
- [0016] 도 2는 본 발명의 실시 예에 따른 표현장치의 구성을 상세히 나타낸 도면이다.

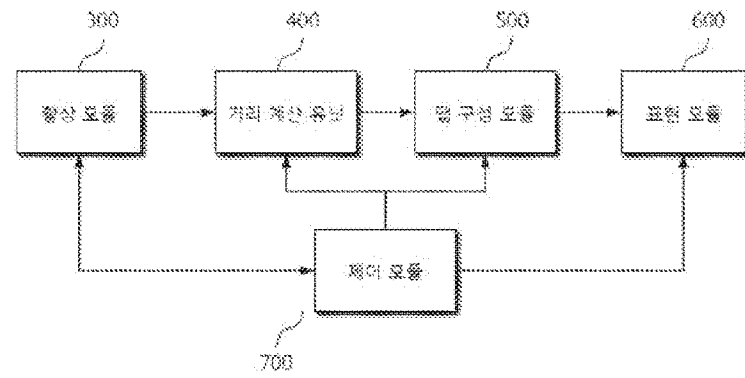
[0017]	도 2를 참조하면, 본 발명의 표현장치(200)는 외부 영상을 촬영하는 촬상모듈(300)로부터 촬영된 영상을 기반으로 거리 계산 유닛(400)에서 영상 내의 객체들을 분류하여 해당 객체의 거리와 위치를 구분한다. 거리 계산 유닛(400)은 상기 거리와 위치 정보를 맵 구성 모듈(500)로 전송하고, 맵 구성 모듈(500)은 상기 위치 정보를 3차원의 좌표 데이터 형태로 유지한다. 맵 구성 모듈(500)은 상기 좌표 데이터를 표현장치(200)의 방향 변경에 따라 수정하여 유지하며, 데이터 변경 시 표현 모듈(600)로 상기 데이터를 전송한다. 표현 모듈(600)은 수신한 상기 데이터에 따라 표현장치(200)의 해당 좌표의 격자(210)의 오르내림 조절을 통하여 표현한다.
[0018]	촬상모듈(300)은 표현장치(200)의 외부에 적어도 하나 이상의 고정 또는 이동형 촬상장치를 포함할 수 있다. 이러한 촬상장치를 이용하여 일정 단위 시간 당 외부의 영상을 촬영하여 거리 계산 유닛(400)으로 해당 이미지를 전송할 수 있다.
[0019]	거리 계산 유닛(400)은 스테레오 비전(stereo vision)의 깊이 맵(depth map) 정보를 이용하는 방법 또는, 하나의 영상은 이용하여 원근법(perspective)을 통해 거리를 계산할 수 있다. 상기 방법은 통하여 계산한 거리 및 위치 정보를 맵 구성 모듈(500)으로 전달할 수 있다.
[0020]	맵 구성 모듈(500)은 위치 정보를 전후방을 나타내는 x축, 좌우를 나타내는 y축, 높낮이를 나타내는 z축을 포함하는 3차원 데이터로 유지한다. 또한 표현장치(200)의 위치 이동에 따라 이미 측정된 데이터들을 이동한 정도에 따라 수정할 수 있다. 상기 데이터는 사용자 설정이나 설계자 의도에 따라 일정 시간 단위 또는 변화가 발생한 경우에 표현 모듈(600)로 전달할 수 있다.
[0021]	표현 모듈(600)은 표현장치(200) 내에 단위 좌표를 나타내는 단위 거리 표현 격자(210)를 조절할 수 있다. 단위 거리 표현 격자(210)의 표현 단위는 사용자 혹은 설계자의 의도에 따라 일정한 단위 거리로 고정되거나 조절할 수 있다. 맵 구성 모듈(500)로부터 수신한 데이터의 z축, x축 정보에 따라 해당 데이터가 어떤 단위 거리 표현 격자(210)에 포함되는지를 판단하고 y축 정보에 따라 해당 격자를 오르내림 조절을 할 수 있다.
[0022]	100 : 거리 인지 단위 200 : 거리 표현 장치 210 : 단위 거리 표현 격자 300 : 촬상 모듈 400 : 거리 계산 유닛 500 : 맵 구성 모듈 600 : 표현 모듈 700 : 제어 모듈

도면

도면1



도면2



(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
14 February 2008 (14.02.2008)

PCT

(10) International Publication Number
WO 2008/018744 A1

(51) International Patent Classification:
G06F 17/00 (2006.01)

(74) Agent: **CHOI, Tae Chang**; 3rd Floor, Hantap Tower Building, 735-10, Yeoksam-Dong, Gangnam-Gu, Seoul 135-923, (KR).

(21) International Application Number:
PCT/KR2007/003802

(22) International Filing Date: 8 August 2007 (08.08.2007)

(25) Filing Language: Korean

(26) Publication Language: English

(30) Priority Data:
10-2006-0075526 10 August 2006 (10.08.2006) KR

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, 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, KM, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(71) Applicant (for all designated States except US): **KOREA INSTITUTE FOR ELECTRONIC COMMERCE** [KR/KR]; 6F Textile Center, 944-31, Daeche-Dong, Kangnam-Gu, Seoul 135-713 (KR).

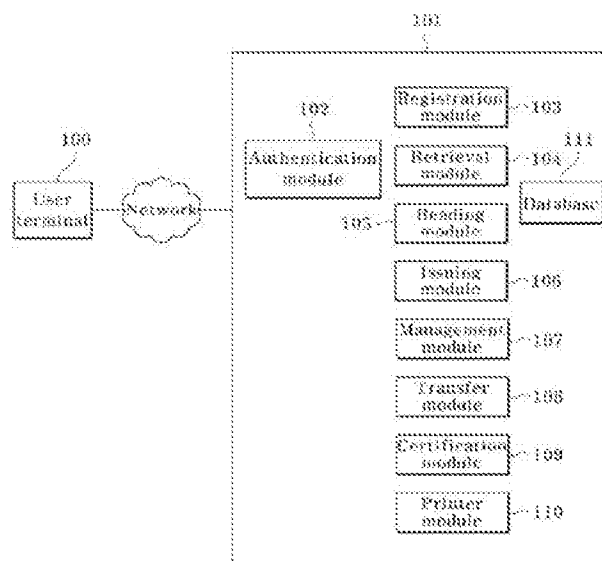
(72) Inventor; and

(75) Inventor/Applicant (for US only): **KANG, Hyun Ku** [KR/KR]; 528-1503, Jugong APT., Jamsil-Dong 27, Songpa-Gu, Seoul 138-220 (KR).

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TI, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SYSTEM OF ELECTRONIC DOCUMENT REPOSITORY WHICH GUARANTEES AUTHENTICITY OF THE ELECTRONIC DOCUMENT AND ISSUES CERTIFICATES AND METHOD OF REGISTERING, READING, ISSUING, TRANSFERRING, A CERTIFICATE ISSUING PERFORMED IN THE SYSTEM



(57) Abstract: Provided are an electronic document repository system which guarantees authenticity of electronic document and issues certificates and methods of registering, reading, issuing, and transferring electronic documents in the system, and a method of issuing certificates in the system. The electronic document repository system includes an authentication module, a registration module, a reading module, an issuing module, and a certification module.

WO 2008/018744 A1

**Published:**

- with international search report
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

Description

SYSTEM OF ELECTRONIC DOCUMENT REPOSITORY WHICH GUARANTEES AUTHENTICITY OF THE ELECTRONIC DOCUMENT AND ISSUES CERTIFICATES AND METHOD OF REGISTERING, READING, ISSUING, TRANSFERRING, A CERTIFICATE ISSUING PERFORMED IN THE SYSTEM

Technical Field

- [1] The present invention relates to an electronic document repository system for storing electronic documents in a licensed repository and issuing the electronic documents when the electronic documents are needed to be used for business. More particularly, the present invention relates to an electronic document repository system capable of maintaining authenticity of electronic documents stored in the repository system and issuing a certificate of original documents, methods for registering, reading, issuing, and transferring electronic documents in the system, and a method for issuing a certificate in the system.

[2]

Background Art

- [3] Widespread use of Information Technology (IT) has led to a great change in business enterprise processes. Commercial transactions, such as purchases and sales, as well as business processes are performed in an electronic manner. This has resulted in business flow innovations, changes in methods and content of transactions, and changes in enterprise activities including communication with customers.
- [4] This change had been led by a shift from use of paper documents to use of electronic documents. By producing numerous documents in an electronic form or by producing numerous documents in a paper form and then converting the same to electronic form for use in business through, for example, electronic payment systems, electronic document management systems, electronic document exchange systems, and the like, process innovations with an aim of becoming 'paperless' are realized.
- [5] Current uses of documents include three types: use of paper documents, use of electronic documents, and use of both paper and electronic documents.
- [6] First, paper documents are produced and distributed in a paper form and are ordinarily used by most people. The use of paper documents allows for easy verification of forgeries and falsifications but is costly in terms of retrieval, distribution and storage of the documents.

- [7] Recently, electronic documents have been widely used, distributed and stored by electronic payment systems, document management systems, and the like, of businesses. The use of the electronic documents can reduce retrieval and storage cost and can realize rapid business processing, but such electronic documents can be easily forged, falsified and copied. In addition, the use of the electronic documents is affected by storage medium types.
- [8] The use of both paper documents and electronic documents may be found, for example, when contracts are written at a bank, with a paper document produced and scanned to obtain an electronic document. This use is intended to solve shortcomings of the use of paper documents or electronic documents solely, but increases storage cost due to dual storage.
- [9] Accordingly, there is a need for a scheme capable of solving the aforementioned problems and allowing for efficient use of electronic documents. In particular, there is a need for an electronic document repository system capable of guaranteeing authenticity of electronic documents stored therein through reinforced security, and guaranteeing reliable distribution of the electronic documents between enterprises or individuals by issuing an authenticity certificate.

[10]

Disclosure of Invention

Technical Problem

- [11] It is an object of the present invention to provide an electronic document repository system which guarantees authenticity of electronic documents and issues certificates and methods of registering, reading, issuing, and transferring the electronic documents in the system, and a method of issuing certificates in the system.

[12]

Technical Solution

- [13] According to a first aspect of the present invention, there is provided an electronic document repository system connected to a user terminal over a network for guaranteeing authenticity of an electronic document and issuing an authenticity certificate, the system comprising: an authentication module for performing user authentication through a login process and controlling a system access right depending on a user when the user connects to the electronic document repository system; a registration module for checking an electronic document information package sent by the user, producing metadata, appending authentication information to the electronic document information package, and registering the resultant electronic document in a database; a reading module for producing a reading information package according to a user's reading right, performing security processing on the reading information

- package, and transmitting the resultant reading information package to the user upon receipt of a request from the user to read the electronic document; an issuing module for producing an issuing information package according to a user's issue right, performing security processing on the issuing information package, and transmitting the resultant issuing information package to the user upon receipt of a request from the user to issue the electronic document; and a certification module for issuing a certificate of the electronic document to the user or verifying the issued certificate.
- [14] Preferably, in the authentication module, the user authentication uses a licensed certificate, and the control of the system access right uses an Access Control List (ACL). In the registration module, the electronic document sent by the user may be first produced in an electronic form or produced in an image form obtained by scanning a paper document.
- [15] Preferably, in the reading module, the electronic document is read in such a manner that the user terminal receives the reading information package and outputs content of the electronic document on a screen of the user terminal, and the content of the electronic document is prevented from being modified, copied, stored, and screen-captured when read so that authenticity of the electronic document is guaranteed.
- [16] Preferably, the issuing module produces the issuing information package with metadata, the electronic document, a time stamp, and an electronic signature.
- [17] Preferably, when issuing the certificate, the certification module generates a unique identifier of the certificate and a security value for guaranteeing integrity of the electronic document, the certificate including a name of an issue requester (a name of a corporation), an identification number of the issue requester, such as a National Identification number, a Social Security number, etc. (a corporate registration number of a corporation), a serial number of the certificate, an issue request date and an issue date of the certificate, a validity period of the certificate, use of the certificate, and repository identification information. In the certification module, the certificate verification may include verification of information for and a format of the issued certificate, verification of authenticity based on a verification route described in the certificate, verification of a certificate issue list of the repository system, and verification of integrity of the certificate based on an electronic signature, a time stamp value, and a hash value described in the certificate.
- [18] Preferably, the system further comprises a retrieval module for retrieving the registered electronic document from the database when the user desires to search for the electronic document. Preferably, the system further comprises a management module for discarding stored electronic documents or storing the same for a long period, and transferring the electronic documents to another storage medium or platform in the electronic document repository system. Preferably, the system further

comprises a transfer module for checking a user's transfer right, transferring the registered electronic document to a receiving repository system, and discarding the electronic document stored in the database upon receipt of a request from the user to transfer the registered electronic document. Preferably, the system further comprises a printer module for controlling printing of the electronic document upon receipt of a request from the user to print electronic documents or various certificates, wherein the printer module checks a type of a printer connected to the user terminal and permits printing only if the printer is secure.

[19] According to a second aspect of the present invention, there is provided a method of registering an electronic document in the electronic document repository system, the method comprising the steps of: (a) producing, by a user terminal, an electronic document information package containing the electronic document, metadata, and authentication information according to a predetermined information package standard; (b) transmitting, by the user terminal, the electronic document information package to the electronic document repository system, and requesting to register the electronic document; (c) receiving, by the registration module, the electronic document information package and performing quality inspection on the electronic document information package; (d) producing, by the registration module, additional metadata, appending authentication information to the electronic document information package, and storing the electronic document in the database; and (e) notifying, by the registration module, the user terminal that the registration has been completed.

[20] Preferably, the quality inspection in step (c) includes checking for viruses, checking for errors, and verifying the metadata information of the electronic document described by the user.

[21] Preferably, the certification module issues the registration certificate to the user upon receipt of a request for the registration certificate from the user.

[22] According to a third aspect of the present invention, there is provided a method of reading an electronic document in the electronic document repository system, the method comprising the steps of: (a) requesting, by a user terminal, to read the electronic document; (b) checking, by a reading module, a user's reading right; (c) producing, by the reading module, a reading information package according to the user's reading conditions; (d) performing, by the reading module, security processing on the reading information package to guarantee authenticity of the electronic document; (e) performing security processing on the reading information package for transmission and reception, and transmitting the resultant reading information package to the user terminal; and (f) reading, by the user terminal, the electronic document by way of content of the electronic document output on a screen of the user terminal.

[23] Preferably, step (c) comprises the steps of: initializing the reading information

package; inserting metadata of the electronic document to be read into the reading information package; and converting the electronic document to be read that is stored in the electronic document repository system according to a user's request conditions, and inserting the converted electronic document into the reading information package.

[24] According to a fourth aspect of the present invention, there is provided a method of issuing an electronic document in the electronic document repository system, the method comprising the steps of: requesting, by a user terminal, to issue the electronic document; checking, by an issuing module, a user's issue right; producing, by the issuing module, an issuing information package; producing, by the certification module, a certificate to certify that the issuing information package is an original document; and performing security processing on the issuing information package and the certificate of the original document for transmission and reception, and transmitting the same to the user terminal.

[25] Preferably, metadata, the electronic document, a time stamp, and an electronic signature are inserted into the issuing information package.

[26] According to a fifth aspect of the present invention, there is provided a method of transferring an electronic document in the electronic document repository system, the method comprising the steps of: (a) requesting, by a user terminal, a specific receiving repository system to transfer the electronic document; (b) checking, by a transfer module, a user's right; (c) inquiring, by the transfer module, of the receiving repository system as to whether transfer of the electronic document is possible; (d) sending, by the receiving repository system, a response to the inquiry to the transfer module; (e) when the transfer is possible, transferring the electronic document from the transfer electronic document repository system to the receiving electronic document repository system; and (f) checking, by the transfer module, the transfer and recording a transfer history.

[27] Preferably, step (e) comprises the steps of: performing, by the transfer module of the transfer electronic document repository system, security processing for transmission and reception and transmitting the electronic document; receiving, by the receiving electronic document repository system, the electronic document and performing quality inspection on the electronic document; and registering, by the receiving electronic document repository system, the electronic document.

[28] According to a sixth aspect of the present invention, there is provided a method of issuing a certificate of an electronic document in the electronic document repository system, the method comprising the steps of: (a) requesting, by a user terminal, to issue a certificate; (b) verifying, by a certification module, a certificate issue request; (c) when the certificate issue request can be accepted, producing the certificate by the certification module; (d) performing, by the certification module, security processing for

transmission and reception and transmitting the certificate to the user terminal; and (e) modifying, by the certification module, a certificate issue list and recording a certificate issue history.

[29] Preferably, the certificate includes a registration certificate for registering an electronic document, a certificate of an original document used for issuing an electronic document, a discard certificate for discarding an electronic document, an authenticity certificate required for storing an electronic document for a long period, and a transfer certificate for transferring an electronic document.

[30] Preferably, step (c) includes producing the certificate by initializing a certificate format, inserting certificate related information into the certificate format, and performing security processing.

[31]

Advantageous Effects

[32] As described above, according to the present invention, security of the electronic document repository system is reinforced to assure authenticity of the electronic document stored in the system. When a user requests to issue a certificate, the system issues an electronic document and a certificate of an original document, thereby guaranteeing reliability and integrity of the electronic document. Thus, the user can use the electronic document comfortably.

[33]

Brief Description of the Drawings

[34] FIG. 1 is a block diagram illustrating an electronic document repository system according to an exemplary embodiment of the present invention;

[35] FIG. 2a is a class diagram of an electronic document information package transmitted by a user, and FIG. 2b is a class diagram of an electronic document information package stored in an electronic document repository system;

[36] FIG. 3 illustrates a metadata structure of a reading information package;

[37] FIG. 4 is a flowchart illustrating a method of registering an electronic document according to an exemplary embodiment of the present invention;

[38] FIG. 5 is a flowchart illustrating a method of reading an electronic document according to an exemplary embodiment of the present invention;

[39] FIG. 6 is a flowchart illustrating a method of issuing an electronic document according to an exemplary embodiment of the present invention;

[40] FIG. 7 is a flowchart illustrating a method of transferring an electronic document according to an exemplary embodiment of the present invention; and

[41] FIG. 8 is a flowchart illustrating a method of issuing a certificate of an electronic document according to an exemplary embodiment of the present invention.

[42]

Mode for the Invention

[43]

Hereinafter, exemplary embodiments of the present invention will be described in detail. However, the present invention is not limited to the exemplary embodiments disclosed below, but can be implemented in various types. Therefore, the present exemplary embodiments are provided for complete disclosure of the present invention and to fully inform the scope of the present invention to those ordinarily skilled in the art.

[44]

FIG. 1 is a block diagram illustrating an electronic document repository system according to an exemplary embodiment of the present invention.

[45]

Referring to FIG. 1, an electronic document repository system 101 is connected to a user terminal 100 over a network, and includes an authentication module 102, a registration module 103, a retrieval module 104, a reading module 105, an issuing module 106, a management module 107, a transfer module 108, a certification module 109, a printer module 110, and a database 111.

[46]

First, the authentication module 102 performs user authentication through a login process when the user connects to the electronic document repository system 101. If the login fails, the authentication module 102 notifies the user of an error. If the login is successful, the authentication module 102 approves user access with a differentiated system access right. In other words, the authentication module 102 controls access to the registration module 103, the reading module 105, the issuing module 106, the management module 107, the transfer module 108, and the certification module 109 according to the user's system access right.

[47]

The user authentication may be performed by using a licensed certificate. When the electronic document repository system receives a request for login from the user, the authentication module 102 requests an external certified authentication authority to check the validity of a user's certificate. The certified authentication authority checks the validity of the user's certificate and sends an authentication result to the electronic document repository system. Alternatively, the authentication module of the electronic document repository system may have a function of verifying the certificate.

[48]

Preferably, the authentication module 102 manages users access rights by using an Access Control List (ACL). The ACL is a table set to inform an operating system of the electronic document repository system of users rights to access specific system objects, such as directories or files.

[49]

The registration module 103 registers an electronic document information package produced by the user in the database 111 of the electronic document repository system 101. The electronic document may be first produced in an electronic form by the user.

Alternatively, the electronic document may be produced in an image form obtained by scanning a paper document.

[50] When the user sends the electronic document to the electronic document repository system, the electronic document repository system checks the electronic document information package, produces metadata, appends authentication information such as an electronic signature to the electronic document information package, and stores the resultant electronic document in a storage medium, which guarantees authenticity of electronic documents.

[51] FIG. 2a is a class diagram of the electronic document information package transmitted by a user, and FIG. 2b is a class diagram of the electronic document information package stored in an electronic document repository system. The electronic document information package and associated metadata are stored in the database of the electronic document repository system. In particular, the storage medium must be compliance equipment with a Write Only Read Many (WORM) function. Also, once a storage period is set, the storage medium should not allow for deletion, forgery, and falsification of data during the period.

[52] When the user wants an electronic document registered in the electronic document repository system, the retrieval module 104 retrieves the electronic document from the database. The electronic document may be retrieved by using metadata information of the electronic document, and a classification system.

[53] Upon receipt of a request from the user to read the electronic document, the reading module 105 controls and manages reading of the electronic document according to a user's reading right. The electronic document is read in a manner of outputting content of the electronic document on a screen of the user terminal 100 connecting to the electronic document repository system 101. In this case, it is necessary to prevent the content of the electronic document from being modified, copied, stored, and screen-captured so that authenticity of the electronic document is guaranteed. Accordingly, the reading module 105 produces a reading information package according to the user's reading conditions, with the reading information package processed for reading security by Digital Rights Management (DRM), watermarking, and the like. The reading module 105 also performs security processing for transmission and reception when sending the reading information package to the user. FIG. 3 illustrates a structure of the metadata of the reading information package.

[54] The issuing module 106 serves to control and manage issuing of the electronic document according to a user's issue right upon receipt of a request from the user to issue the electronic document. The issuing module 106 also serves to prevent and verify forgeries and falsifications of the electronic document content upon issuing the electronic document. The electronic document is issued in a manner of transmitting an

issuing information package to the user. An electronic document having a publication format, such as metadata, Portable Document Format (PDF), or an image file, and authentication information such as an electronic signature are inserted into the issuing information package.

- [55] The issuing module 106 inserts a time stamp and an electronic signature to produce the issuing information package, and performs security processing for transmission and reception to transmit the issuing information package to the user. Preferably, the time stamp may conform to a KS X ISO/IEC 18014 "time-stamping" standard, and the electronic signature may be produced by using a hash algorithm such as SHA-1 and SHA-256 or an encryption algorithm such as PKC#7. In addition, the security processing for transmission and reception is intended to transmit and receive a message according to a standardized procedure and method and by using HyperText Transfer Protocol (HTTP), Simple Object Access Protocol (SOAP), File Transfer Protocol (FTP), and the like. The security processing for transmission and reception may include confidentiality and integrity processing for transmitted and received messages, such as a Virtual Private Network (VPN), and transmission security processing for a network path, such as a Secure Sockets Layer (SSL).
- [56] The management module 107 performs processing for discarding electronic documents stored in the electronic document repository system or storing the same for a long period. The management module 107 also transfers the electronic documents to another storage medium or platform in the electronic document repository system.
- [57] The process of discarding the electronic documents includes completely discarding the electronic documents in the database not to be restored and recording a discard history when the user requests to discard the electronic documents. If a storage period has been set for the electronic document, the management module 107 notifies the user of this fact when the storage period has time remaining, and discards the electronic document when the storage period has expired. Upon receipt of a request from the user for long-term storage of the electronic document, the management module records metadata information needed for long-term storage. The management module may transfer the electronic document information package to a secondary storage device and record a long-term storage history, if necessary.
- [58] Upon receipt of a request from the user to transfer an electronic document, the transfer module 108 checks a user's transfer right, transfers the electronic document to a receiving repository system, and discards the electronic documents from the transfer repository system. The electronic document is transferred by standard protocol and a messaging manner, and it is desirable to keep platform and language independence between the repository systems.
- [59] The certification module 109 issues a certificate to the user or verifies the issued

- certificate. Examples of the certificate include a registration certificate for registering an electronic document, a certificate of an original document used for issuing an electronic document, a discard certificate for discarding an electronic document, an authenticity certificate required for moving an electronic document to a storage medium or a platform, a transfer certificate for transferring an electronic document, etc.
- [60] When issuing the certificate, the certification module 109 generates a unique identifier of the certificate and a security value for guaranteeing integrity of the electronic document, and appends an electronic signature proving an issue authority and a certificate issue time. Preferably, the certificate includes a name of an issue requester (a name of a corporation), an identification number of the issue requester, such as a National Identification number, a Social Security number, etc. (a corporate registration number of a corporation), a serial number of the certificate, an issue request date and an issue date of the certificate, a validity period of the certificate, use of the certificate, and repository identification information.
- [61] The certificate verification includes verification of information for and a format of the issued certificate, verification of authenticity based on a verification route described in the certificate, verification of a certificate issue list of the repository system, and verification of integrity of the certificate based on an electronic signature, a time stamp value, a hash value and the like described in the certificate.
- [62] The printer module 110 controls printing of the electronic document when a user having a print right requests to print the electronic document while reading the electronic document, and controls printing of the electronic document and various certificates when the user prints the issued electronic document and the certificates. The printer module 110 must check a type of a printer connected to the user terminal and permits printing only when the printer is secure. The printer module 110 performs security processing such as 2D bar code processing when the electronic document is printed by the user terminal.
- [63] Methods by which the user registers an electronic document, a method by which the user reads the electronic document, a method for issuing the electronic document to the user, a method for transferring the electronic document, and a method for issuing a certificate of the electronic document will now be described with reference to FIGS. 4 to 8.
- [64] FIG. 4 is a flowchart illustrating a method of registering an electronic document according to an exemplary embodiment of the present invention.
- [65] Referring to FIG. 4, a user produces an electronic document (S400) first. It will be easily appreciated that the electronic document may be first produced in an electronic form, or may be produced in an image form obtained by scanning a paper document.
- [66] To register the produced electronic document in the electronic document repository

system, the user then produces an electronic document information package containing an electronic document, metadata, and authentication information, such as an electronic signature, according to a predetermined information package standard defined in the electronic document repository system (S401).

[67] The user then transmits the electronic document information package to the electronic document repository system over a network by using the user terminal, and requests the registration module 103 of the electronic document repository system to register the electronic document (S402). Of course, the user needs to connect to the electronic document repository system and pass a login process in order to make a request for registration of the electronic document.

[68] The registration module 103 then receives the information package and performs quality inspection on the information package (S403). The quality inspection includes checking for viruses and errors, and verifying metadata information of the electronic document described by the user. When the information package does not pass the quality inspection, the registration module 103 may notify the user of this fact and request supplementation for passing the quality inspection.

[69] The registration module 103 then produces additional metadata, appends authentication information associated with the electronic document, and stores the electronic document in the database (S404). The authentication information may be a time stamp, an electronic signature, etc. A class diagram of the electronic document information package with the additional metadata is shown in FIG. 2b.

[70] A determination is then made as to whether the user requests the registration certificate (S405). If the user requests the registration certificate, the certification module 109 issues the registration certificate to the user (S406).

[71] Finally, the registration module 103 notifies the user that the registration has been completed (S407).

[72] FIG. 5 is a flowchart illustrating a method of reading an electronic document according to an exemplary embodiment of the present invention.

[73] First, the user connects to the electronic document repository system and requests to read an electronic document (S500). In this case, the user may designate reading conditions for the electronic document.

[74] The reading module 105 of the electronic document repository system then checks a user's reading right (S501). If the user has no right to read the electronic document, the reading module notifies the user of an error (S503).

[75] The reading module 105 then produces a reading information package according to the user's reading conditions (S504). The reading information package is produced by initializing a reading information package, inserting metadata into the reading information package, converting an original electronic document stored in the electronic

document repository system according to a user's request conditions, and inserting the converted electronic document into the reading information package.

[76] The reading module 105 then performs reading security processing, such as Digital Rights Management (DRM), watermarking, and the like on the reading information package (S505). That is, it is necessary to prevent the content of the electronic document from being modified, copied, stored, and screen-captured when the user reads the electronic document, so that authenticity of the electronic document is guaranteed.

[77] The reading module 105 then performs security processing on the reading information package for transmission and reception, and transmits the resultant information package to the user (S506).

[78] The user then reads the electronic document by way of content of the electronic document output on a screen of the user terminal 100 (S507).

[79] FIG. 6 is a flowchart illustrating a method of issuing an electronic document according to an exemplary embodiment of the present invention.

[80] Referring to FIG. 6, the user connects to the electronic document repository system and requests the electronic document repository system to issue the electronic document (S600). In this case, the user may designate an electronic document issuing conditions.

[81] The issuing module 106 of the electronic document repository system then checks a user's right (S601). If the user has no right to receive the electronic document, the issuing module 106 notifies the user of an error (S603) and the process stops.

[82] The issuing module 106 then produces an issuing information package (S604). An electronic document having a publication format, such as metadata, PDF, or an image file, and authentication information such as an electronic signature are inserted into the issuing information package. A time stamp and an electronic signature are also inserted into the issuing information package to prevent forgery and falsification of content of the electronic document.

[83] The certification module 109 then produces a certificate to certify that the issuing information package is an original document (S605). After issuing the certificate of the original document, the certification module 109 may record an issue history to the issue list.

[84] The certification module 109 then performs security processing on the issuing information package for transmission and reception and the certificate of the original document and transmits the same to the user (S606).

[85] FIG. 7 is a flowchart illustrating a method of transferring an electronic document according to an exemplary embodiment of the present invention.

[86] First, the user requests the electronic document repository system to transfer the

electronic document to a specific receiving repository system (S700). It is common for the user to request to transfer the electronic document, however, the electronic document repository system storing the electronic document may itself determine to transfer the electronic document.

- [87] The transfer module 108 of the electronic document repository system then checks a user's right (S701). If the user has no right to transfer the electronic document, the transfer module 108 notifies the user of an error (S703) and the process ends.
- [88] The transfer module 108 then inquires of the receiving repository system as to whether transfer of the electronic document is possible (S704). The receiving repository system sends a response to the inquiry to the transfer module 108 (S705). If the transfer is not possible, the receiving repository system notifies the transfer module 108 of an error (S707).
- [89] If the transfer is possible, the transfer module 108 transfers the electronic document from the transfer electronic document repository system to the receiving electronic document repository system (S708). Specifically, the transfer module 108 of the transfer electronic document repository system performs security processing for transmission and reception to transmit the electronic document information package together with related information, such as a certificate and history information. Accordingly, the receiving electronic document repository system performs a receiving process on the electronic document. That is, the receiving electronic document repository system receives the electronic document information package and the related information, performs quality inspection for suitability, and then registers the electronic document information package.
- [90] The transfer module of the transfer electronic document repository system then checks the transfer and records a transfer history (S709). If the user desires a transfer certificate, the certification module 109 produces the transfer certificate, issues it to the user, and records a certificate issue history. The certification module of the receiving electronic document repository system issues a registration certificate to the user.
- [91] FIG. 8 is a flowchart illustrating a method of issuing a certificate of an electronic document according to an exemplary embodiment of the present invention.
- [92] First, the user requests the certification module 109 of the electronic document repository system to issue a certificate (S800). Examples of the certificate include a registration certificate for registering an electronic document, a certificate of an original document used for issuing an electronic document, a discard certificate for discarding an electronic document, an authenticity certificate required for moving an electronic document to a storage medium or a platform, a transfer certificate for transferring an electronic document, etc.
- [93] Upon receipt of the request for the certificate, the certification module 109 verifies

the request (S801). If the registration certificate is requested, the certification module 109 issues the registration certificate only if the user has a right to register the electronic document. If the certificate issue request cannot be accepted, the certification module 109 notifies the user of an error (S803).

[94] If the certificate issue request is accepted, the certification module 109 produces a certificate (S804). The certificate may be produced by initializing a certificate format, inserting certificate related information into the certificate format, and performing security processing. Preferably, the certificate includes a name of an issue requester (a name of a corporation), an identification number of the issue requester, such as a National Identification number, a Social Security number, etc. (a corporate registration number of a corporation), a serial number of the certificate, an issue request date and an issue date of the certificate, a validity period of the certificate, use of the certificate, and repository identification information.

[95] The certification module 109 then performs security processing for transmission and reception and transmits a certificate to the user (S805). Finally, the certification module 109 modifies the certificate issue list and records the certificate issue history (S806).

[96] While the invention has been shown and described with reference to certain exemplary embodiments thereof, it will be understood by those skilled in the art that various changes in form and details may be made therein without departing from the spirit and scope of the invention as defined by the appended claims.

[97]

Claims

- [1] An electronic document repository system connected to a user terminal over a network for guaranteeing authenticity of an electronic document and issuing an authenticity certificate, the system comprising:
an authentication module for performing user authentication through a login process and controlling a system access right depending on a user when the user connects to the electronic document repository system;
a registration module for checking an electronic document information package sent by the user, producing metadata, appending authentication information to the electronic document information package, and registering the resultant electronic document in a database;
a reading module for producing a reading information package according to a user's reading right, performing security processing on the reading information package, and transmitting the resultant reading information package to the user upon receipt of a request from the user to read the electronic document;
an issuing module for producing an issuing information package according to a user's issue right, performing security processing on the issuing information package, and transmitting the resultant issuing information package to the user upon receipt of a request from the user to issue the electronic document; and
a certification module for issuing a certificate of the electronic document to the user or verifying the issued certificate.
- [2] The system of claim 1, wherein in the authentication module, the user authentication uses a licensed certificate, and the control of the system access right uses an Access Control List (ACL).
- [3] The system of claim 1, wherein in the registration module, the electronic document sent by the user is first produced in an electronic form or in an image form obtained by scanning a paper document.
- [4] The system of claim 1, further comprising a retrieval module for retrieving the registered electronic document from the database when the user desires to search for the electronic document.
- [5] The system of claim 1, wherein in the reading module, the electronic document is read in such a manner that the user terminal receives the reading information package and outputs content of the electronic document on a screen of the user terminal, and the content of the electronic document is prevented from being modified, copied, stored, and screen-captured when read so that authenticity of the electronic document is guaranteed.
- [6] The system of claim 1, wherein the issuing module produces the issuing in-

- formation package with metadata, the electronic document, a time stamp, and an electronic signature.
- [7] The system of claim 1, further comprising a management module for discarding stored electronic documents or storing the same for a long period, and transferring the electronic documents to another storage medium or platform in the electronic document repository system.
- [8] The system of claim 1, further comprising a transfer module for checking a user's transfer right, transferring the registered electronic document to a receiving repository system, and discarding the electronic document stored in the database upon receipt of a request from the user to transfer the registered electronic document.
- [9] The system of claim 1, wherein when issuing the certificate, the certification module generates a unique identifier of the certificate and a security value for guaranteeing integrity of the electronic document, the certificate including a name of an issue requester (a name of a corporation), an identification number of the issue requester (a corporate registration number of a corporation), a serial number of the certificate, an issue request date and an issue date of the certificate, a validity period of the certificate, use of the certificate, and repository identification information.
- [10] The system of claim 1, wherein in the certification module, the certificate verification includes verification of information and a format of the issued certificate, verification of authenticity based on a verification route described in the certificate, verification of a certificate issue list of the repository system, and verification of integrity of the certificate based on an electronic signature, a time stamp value, and a hash value described in the certificate.
- [11] The system of claim 1, further comprising a printer module for controlling printing of the electronic document upon receipt of a request from the user to print electronic documents or various certificates, wherein the printer module checks a type of a printer connected to the user terminal and permits printing only if the printer is secure.
- [12] A method of registering an electronic document in the electronic document repository system according to claim 1, the method comprising the steps of:
(a) producing, by a user terminal, an electronic document information package containing the electronic document, metadata, and authentication information according to a predetermined information package standard;
(b) transmitting, by the user terminal, the electronic document information package to the electronic document repository system, and requesting to register the electronic document;

- (c) receiving, by the registration module, the electronic document information package and performing quality inspection on the electronic document information package;
 - (d) producing, by the registration module, additional metadata, appending authentication information to the electronic document information package, and storing the electronic document in the database; and
 - (e) notifying, by the registration module, the user terminal that the registration has been completed.
- [13] The method of claim 12, wherein the quality inspection in step (c) includes checking for viruses, checking for errors, and verifying the metadata information of the electronic document described by the user.
- [14] The method of claim 12, wherein the certification module issues the registration certificate to the user upon receipt of a request for the registration certificate from the user.
- [15] A method of reading an electronic document in the electronic document repository system according to claim 1, the method comprising the steps of:
- (a) requesting, by a user terminal, to read the electronic document;
 - (b) checking, by a reading module, a user's reading right;
 - (c) producing, by the reading module, a reading information package according to the user's reading conditions;
 - (d) performing, by the reading module, security processing on the reading information package to guarantee authenticity of the electronic document;
 - (e) performing security processing on the reading information package for transmission and reception, and transmitting the resultant reading information package to the user terminal; and
 - (f) reading, by the user terminal, the electronic document by way of content of the electronic document output on a screen of the user terminal.
- [16] The method of claim 15, wherein step (c) comprises the steps of:
- initializing the reading information package;
 - inserting metadata of the electronic document to be read into the reading information package; and
 - converting the electronic document to be read that is stored in the electronic document repository system according to a user's request conditions, and inserting the converted electronic document into the reading information package.
- [17] A method of issuing an electronic document in the electronic document repository system according to claim 1, the method comprising the steps of:
- requesting, by a user terminal, to issue the electronic document;

checking, by an issuing module, a user's issue right;
 producing, by the issuing module, an issuing information package;
 producing, by the certification module, a certificate to certify that the issuing information package is an original document; and
 performing security processing on the issuing information package and the certificate of the original document for transmission and reception, and transmitting the same to the user terminal.

- [18] The method of claim 17, wherein metadata, the electronic document, a time stamp, and an electronic signature are inserted into the issuing information package.
- [19] A method of transferring an electronic document in the electronic document repository system according to claim 1, the method comprising the steps of:
 (a) requesting, by a user terminal, a specific receiving repository system to transfer the electronic document;
 (b) checking, by a transfer module, a user's right;
 (c) inquiring, by the transfer module, of the receiving repository system as to whether transfer of the electronic document is possible;
 (d) sending, by the receiving repository system, a response to the inquiry to the transfer module;
 (e) when the transfer is possible, transferring the electronic document from the transfer electronic document repository system to the receiving electronic document repository system; and
 (f) checking, by the transfer module, the transfer and recording a transfer history.
- [20] The method of claim 19, wherein step (e) comprises the steps of:
 performing, by the transfer module of the transfer electronic document repository system, security processing for transmission and reception and transmitting the electronic document;
 receiving, by the receiving electronic document repository system, the electronic document and performing quality inspection on the electronic document; and
 registering, by the receiving electronic document repository system, the electronic document.
- [21] A method of issuing a certificate of an electronic document in the electronic document repository system according to claim 1, the method comprising the steps of:
 (a) requesting, by a user terminal, to issue a certificate;
 (b) verifying, by a certification module, a certificate issue request;
 (c) when the certificate issue request can be accepted, producing the certificate by the certification module;

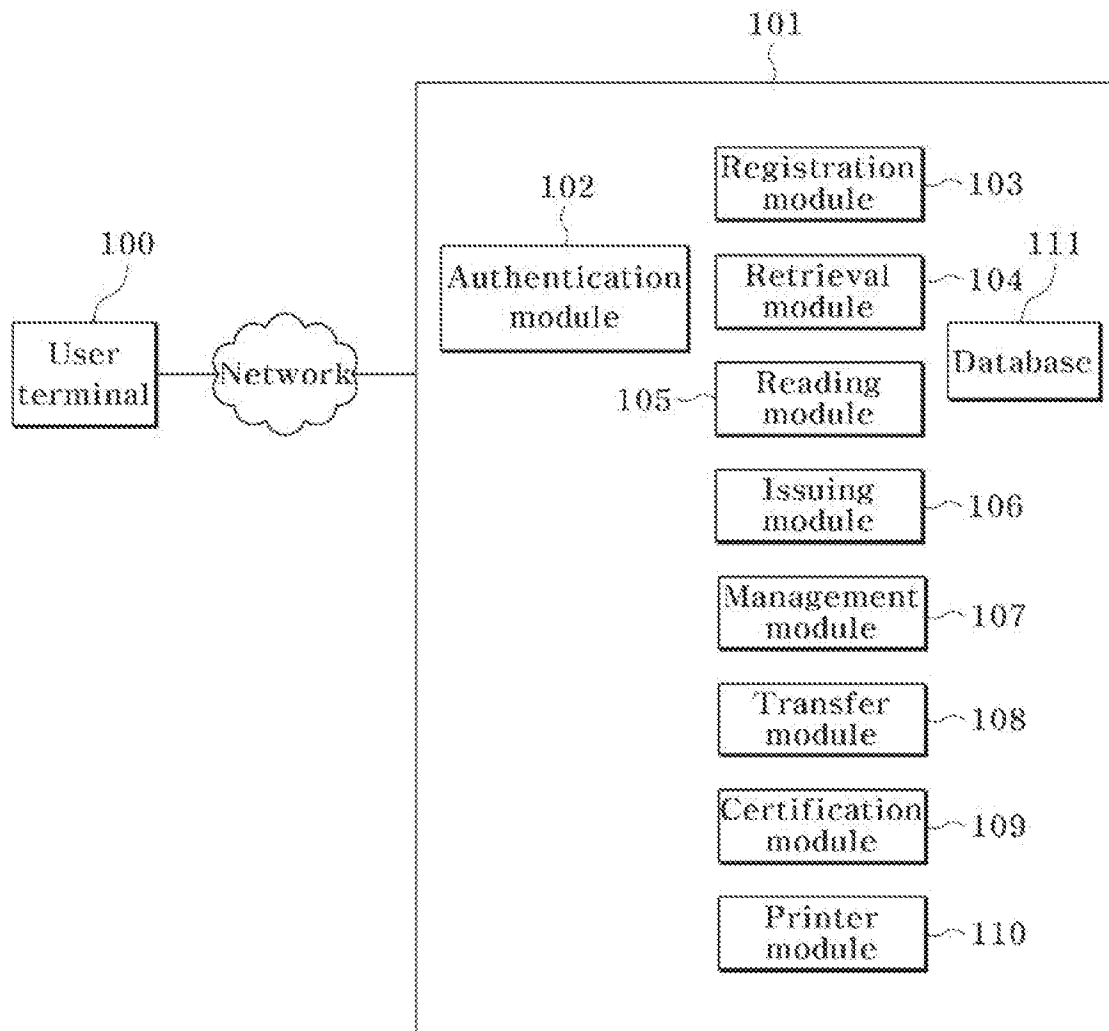
(d) performing, by the certification module, security processing for transmission and reception and transmitting the certificate to the user terminal; and

(e) modifying, by the certification module, a certificate issue list and recording a certificate issue history.

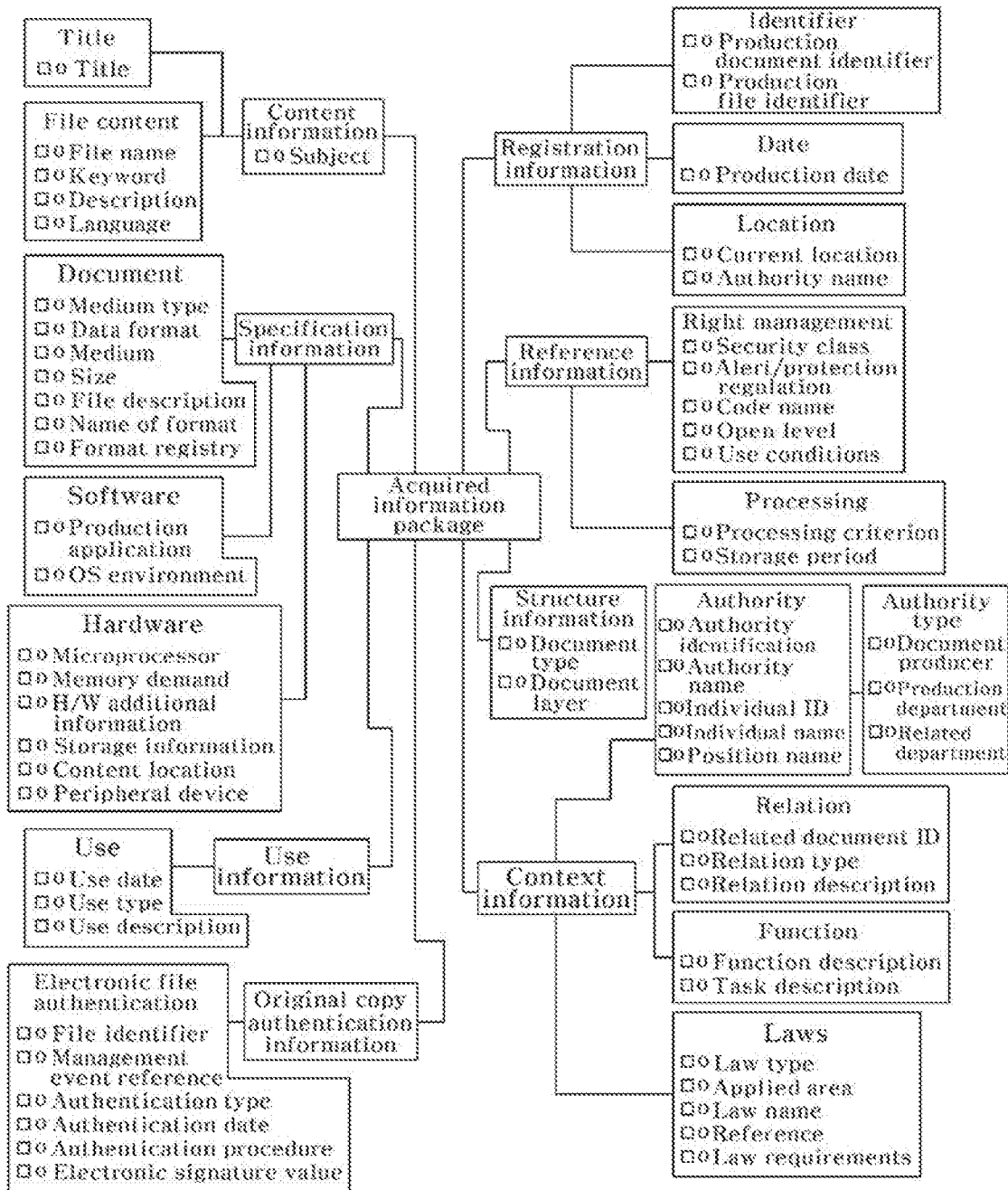
[22] The method of claim 21, wherein the certificate includes a registration certificate for registering an electronic document, a certificate of an original document used for issuing an electronic document, a discard certificate for discarding an electronic document, an authenticity certificate required for storing an electronic document for a long period, and a transfer certificate for transferring an electronic document.

[23] The method of claim 21, wherein step (c) includes producing the certificate by initializing a certificate format, inserting certificate related information into the certificate format, and performing security processing.

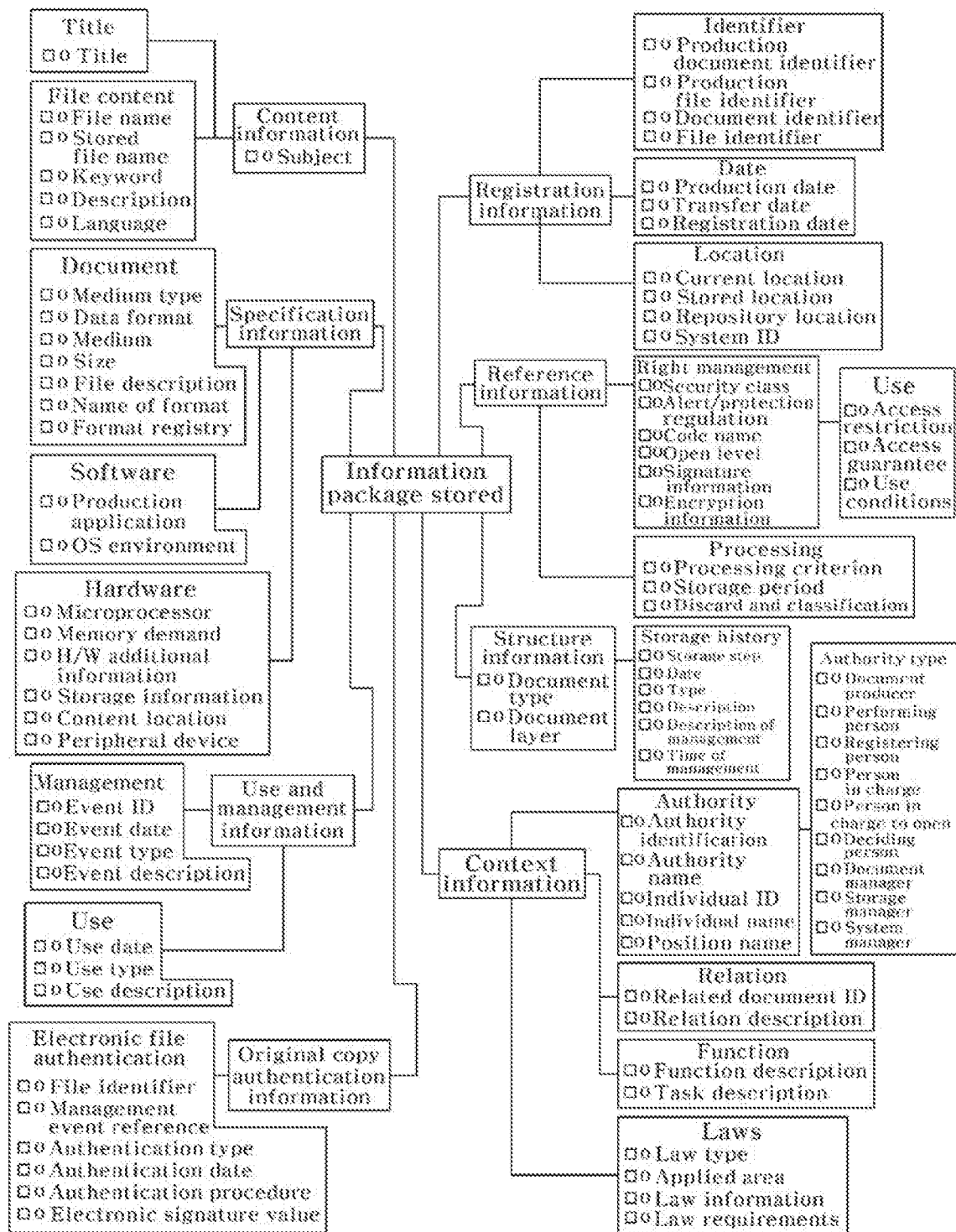
[Fig. 1]



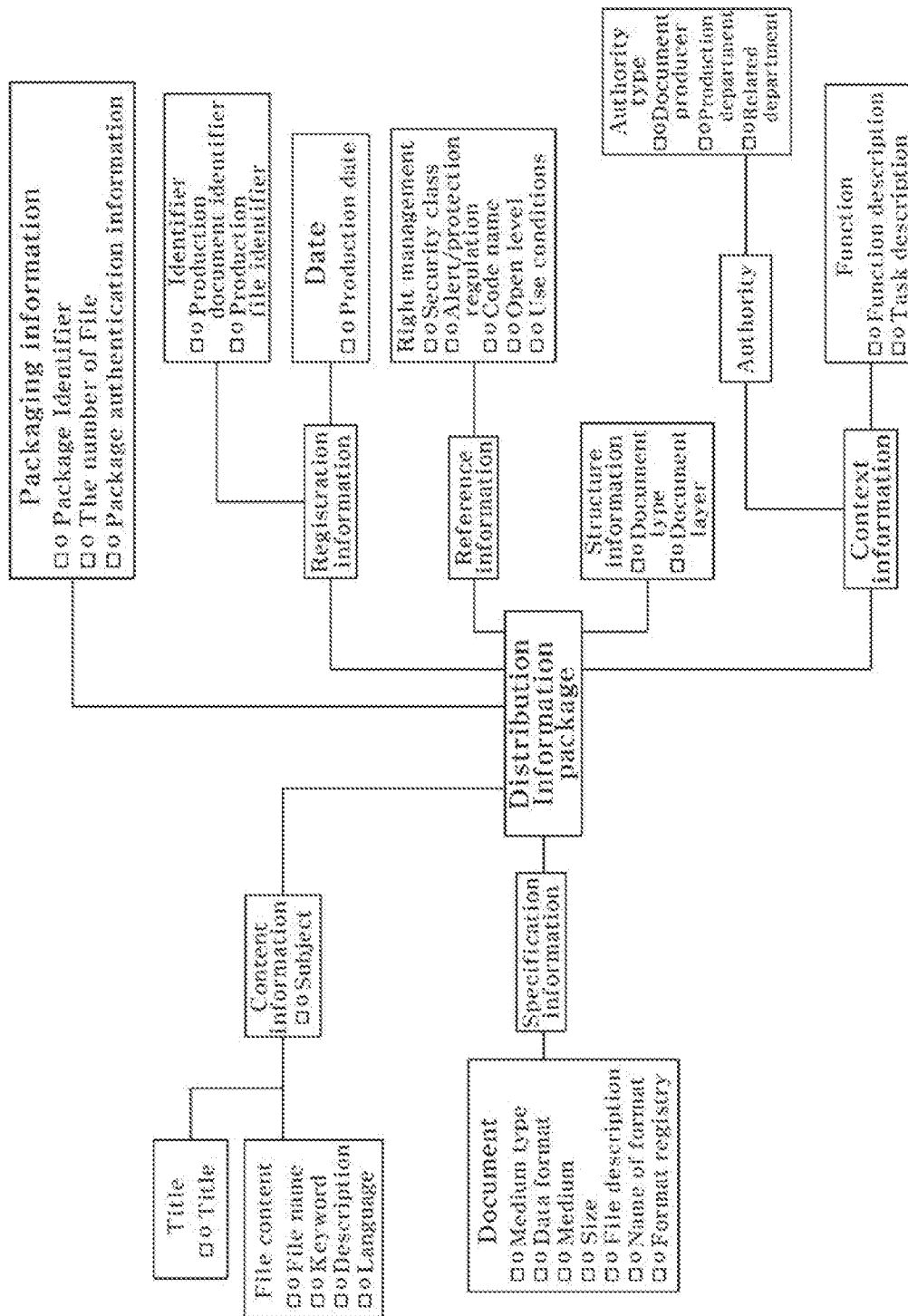
[Fig. 2]



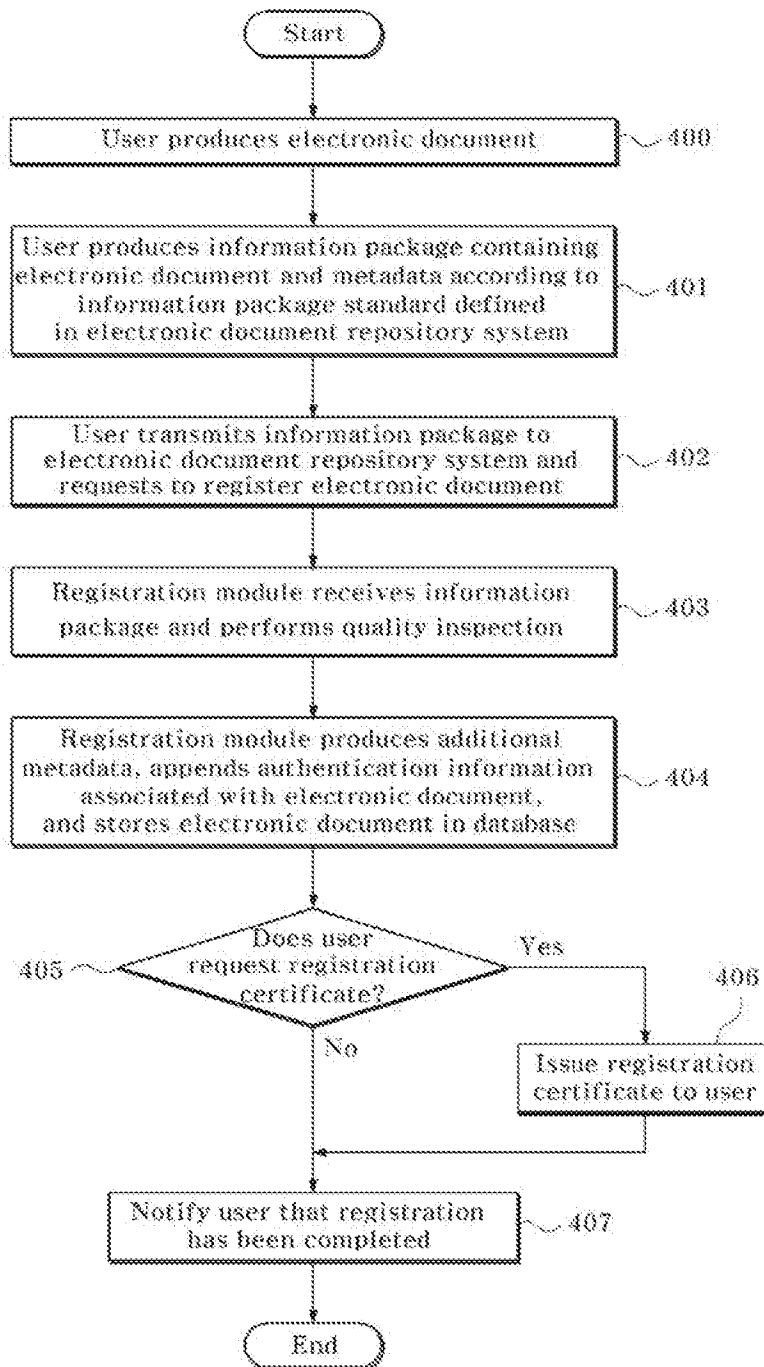
[Fig. 3]



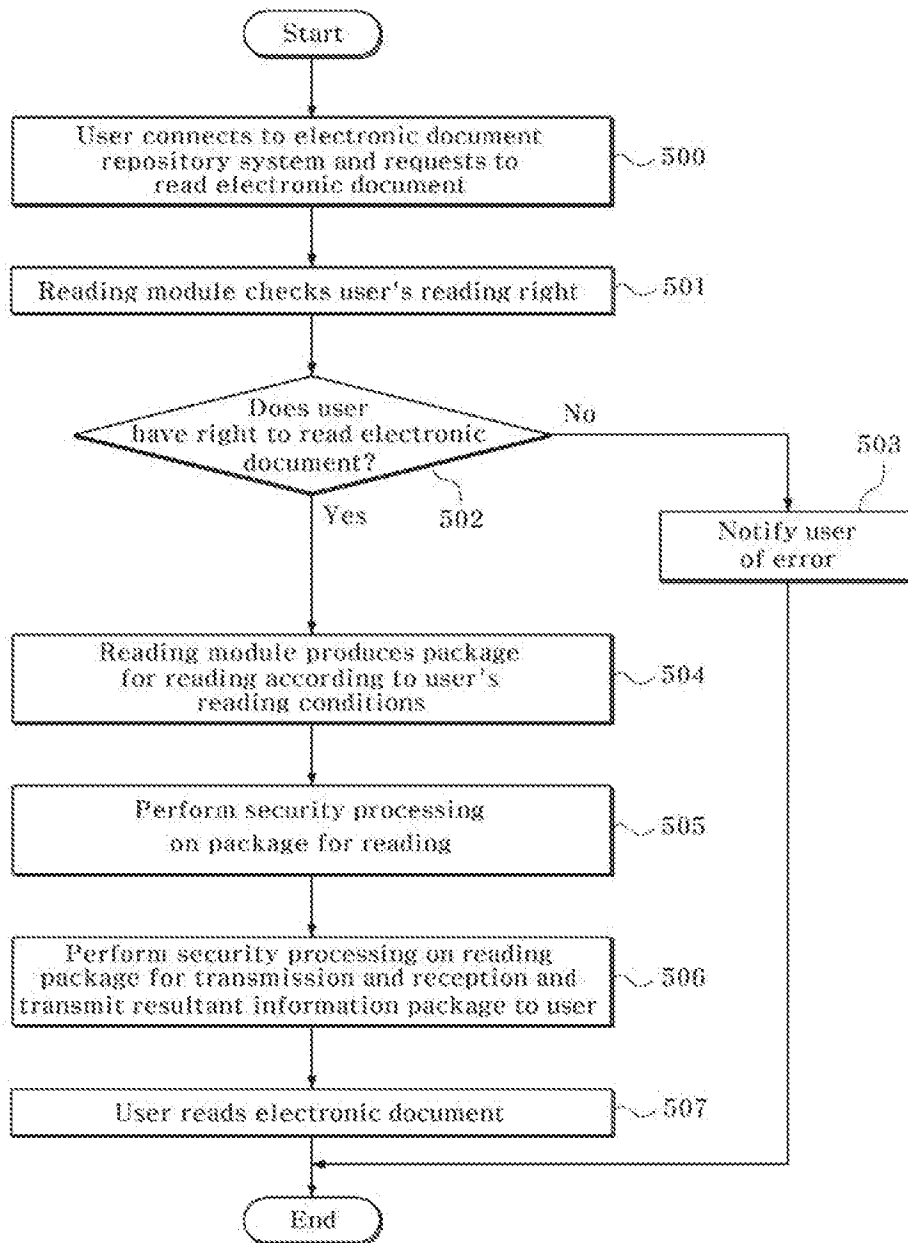
[Fig. 4]



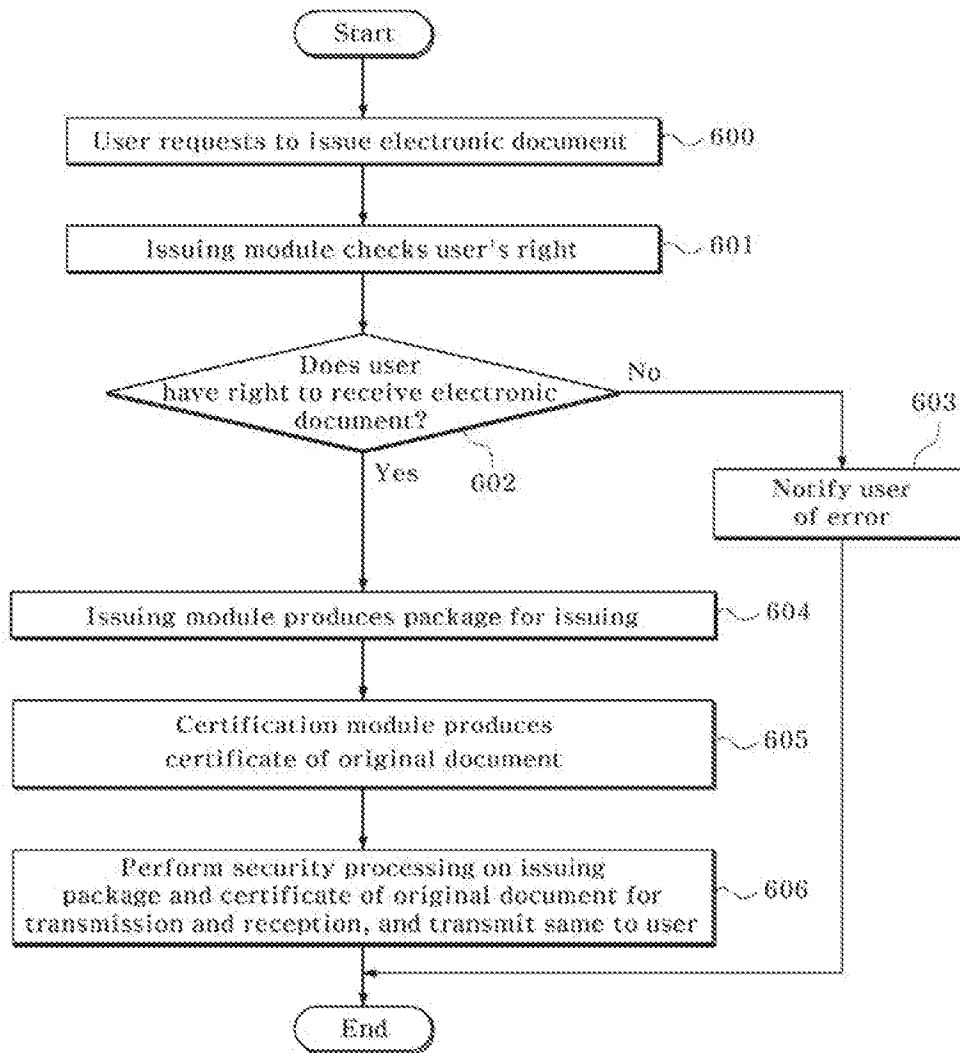
[Fig. 5]



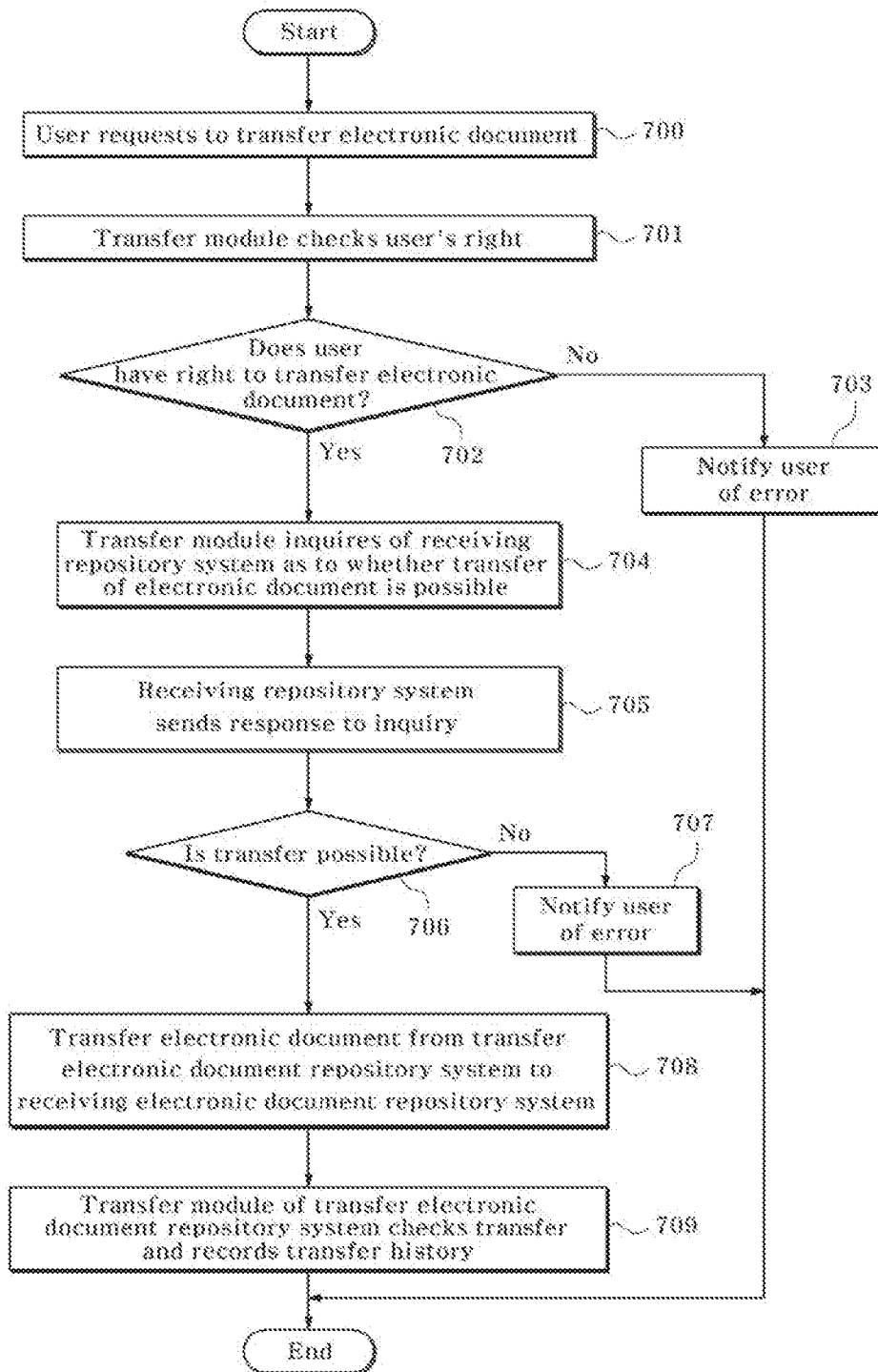
[Fig. 6]



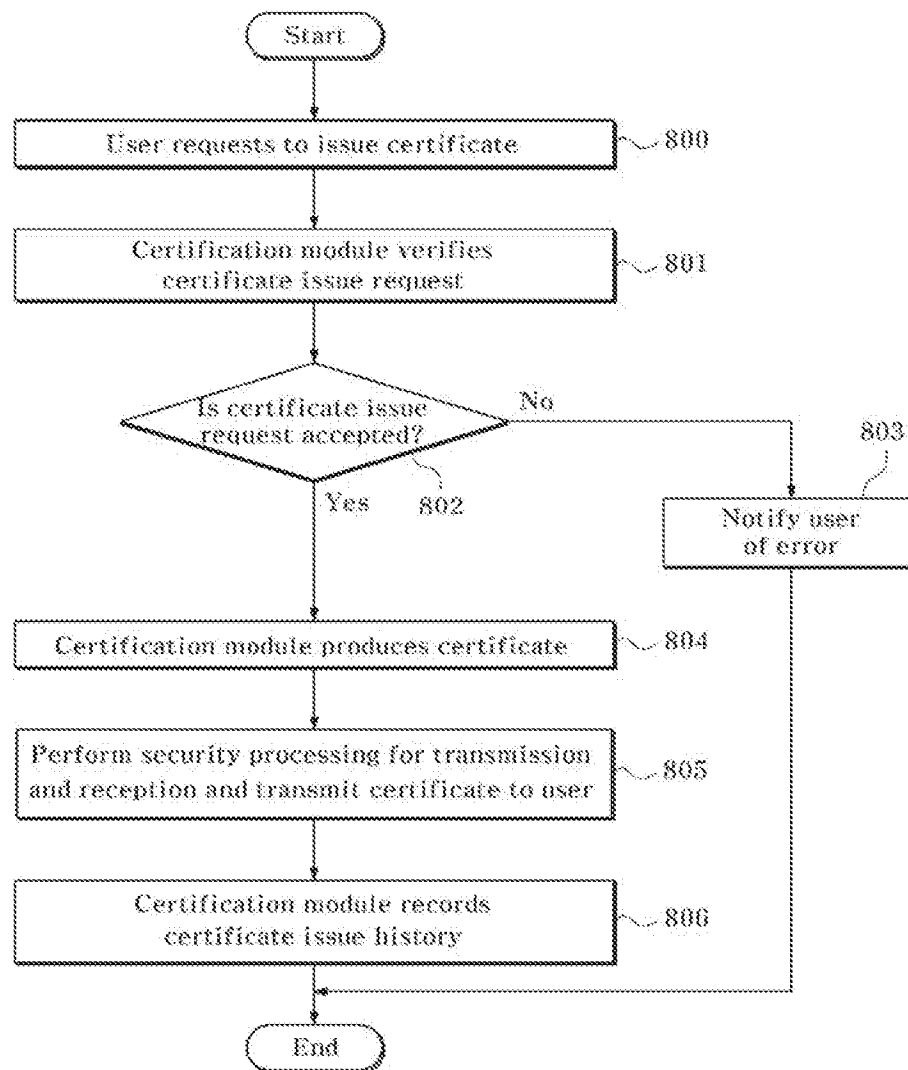
[Fig. 7]



[Fig. 8]



[Fig. 9]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2007/003802**A. CLASSIFICATION OF SUBJECT MATTER***G06F 17/00(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)

IPC 8 G06F 17/00, G06F 17/30

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 since 1975

Japanese Utility models and applications for Utility Models since 1975

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

eKIPASS(KIPO) "electronic, document, repository, and certificate"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 6289460 B1 (JIAJMIKAGHA, M.) 11 September 2001 See the abstract; figure 2; column 3, line 8 - column 5, line 14, claims 1-20	1-6, 9-18, 21, 23
Y	KR 10-2006-0084032 A (OSS INC.) 21 July 2006 See the abstract; figure 1; claims 1-15	1-6, 9-18, 21, 23
A	KR 10-2005-0078402 A (DREAM TO REALITY INC.) 5 August 2005 See the abstract; figure 4; claims 1-10	1-23
A	US 2005-0038756 A1 (NAGEL, R. H.) 17 February 2005 See the abstract; figure 1; paragraphs [0232]-[0248]; claims 1-71	1-23
A	US 2002-0016910 A1 (WRIGHT, R. P. et al.) 7 February 2002 See the abstract; figure 5; paragraphs [0077]-[0079]; claims 1-13	1-23

☐ 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 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

13 NOVEMBER 2007 (13.11.2007)

Date of mailing of the international search report

13 NOVEMBER 2007 (13.11.2007)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
920 Dunsan-dong, Seo-gu, Daejeon 302-701,
Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

YU, Jin Tae

Telephone No. 82-42-481-8542



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/KR2007/003802

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US06289460B1	11.09.2001	AU200073780A1 CA2384944A1 EP01222774A1 JP15509784 NZ517849A WO200120843A1	17.04.2001 22.03.2001 17.07.2002 11.03.2003 27.02.2004 22.03.2001
KR1020060084032A	21.07.2006	None	
KR1020050078402A	05.08.2005	None	
US20060038756A1	17.02.2005	US7080041B9	18.07.2006
US20020016910A1	07.02.2002	None	

이동 통신 단말기의 개인 정보 서비스 방법

METHOD FOR SERVICING PERSONAL INFORMATION OF MOBILE COMMUNICATION TERMINAL

(51) Int. CL. H04W 12/06(2009.01) H04W 8/20(2009.01)

(52) CPC

(21) Application No.(Date) 1020060014686 (2006.02.22)

(71) Applicant LG Electronics Inc.

(11) Registration No.(Date) 1010914100000 (2011.12.01)

(65) Unex. Pub. No.(Date) 1020060093594 (2006.08.25)

(11) Publication No.(Date) (2011.12.07)

(86) Int'l Application No.(Date)

(87) Int'l Unex. Pub. No.(Date)

(30) Priority info.

(Country / No. / Date)

Legal Status Registered

Examination Status Decision to grant (General)

Trial Info

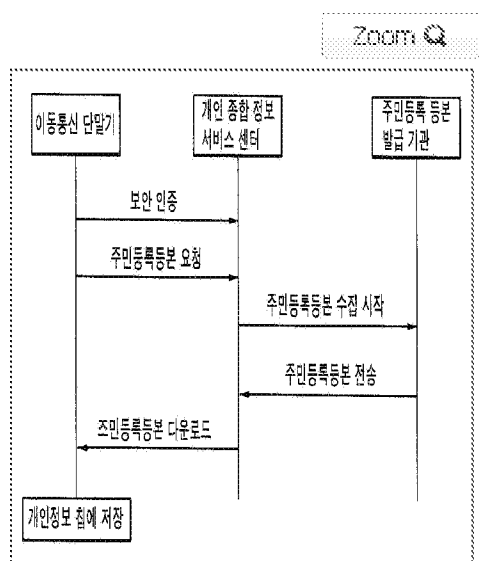
Kind/Right of Org. Application /

Right of Org. Application No.(Date)

Related Application No.

Request for an examination(Date) Y(2010.02.12)

Number of examination claims 3



KIPA (Korea Patent Abstract)

PURPOSE: A personal information service method of a mobile terminal is provided to allow a user to obtain a required certificate through a terminal without having to visit a corresponding agency.

CONSTITUTION: A mobile terminal performs security authentication at a service center by using an ID of a user inputted in a personal information chip of the mobile terminal and requests a certificate. An integrated personal information service center collects certificate information of the user from a pertinent certificate issuance agency and transmits the collected personal information to the mobile terminal. The certificate issuance agency searches a certificate of the user and transmits it including the information available period to the integrated personal information service center. The mobile terminal downloads the certificate of the user from the integrated personal information service center and stores it in the personal information chip.

© KIPO 2006



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2011년12월07일
(11) 등록번호 10-1091410
(24) 등록일자 2011년12월01일

(51) Int. Cl.

H04W 12/06 (2009.01) H04W 8/20 (2009.01)

(21) 출원번호 10-2005-0014686

(22) 출원일자 2005년02월22일

심사청구일자 2010년02월12일

(65) 공개번호 10-2006-0093594

(43) 공개일자 2006년08월25일

(56) 선행기술조사문헌

KR1020020089205 A*

KR1020050007618 A

KR1020040104768 A

*는 심사관에 의하여 인용된 문헌

(73) 특허권자

엘지전자 주식회사

서울특별시 영등포구 여의도동 20번지

(72) 발명자

육경준

서울 금천구 가산동 459-9

(74) 대리인

박장원

전체 청구항 수 : 총 3 항

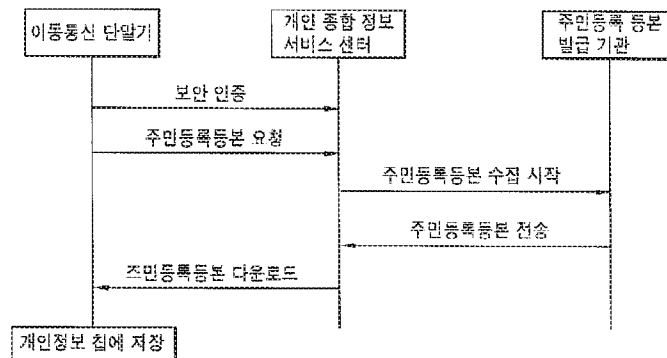
심사관 : 장상배

(54) 이동 통신 단말기의 개인 정보 서비스 방법

(57) 요약

본 발명은 이동 통신 단말기의 개인 정보 서비스 방법에 관한 것으로, 종래 현대인에게서는 각종 자격증과 의료 기록 등이 한 곳에 모여 있지 않아 이러한 기록들을 조회시 여러 기관을 직접 방문하여 확인하는 수밖에 없는 문제점이 있었다. 이러한 문제점을 감안한 본 발명은 이동 통신 단말기에서 개인 정보 칩에 입력된 사용자의 신분증으로 개인종합정보 서비스 센터에 보안 인증을 수행하고 증명서를 요청하는 단계와; 개인종합정보 서비스 센터에서 해당 증명서 발급 기관으로부터 사용자의 증명서 정보를 수집하고 수집된 개인 정보를 이동 통신 단말기로 전송하는 단계와; 증명서 발급 기관에서 사용자의 증명서를 검색하고 정보 유효 기간을 포함하여 사용자의 증명서를 개인종합정보 서비스 센터로 전송하는 단계와; 이동 통신 단말기에서 개인종합정보 서비스 센터로부터 사용자의 증명서를 다운로드하고 개인 정보 칩에 저장하는 단계로 이루어져 사용자는 증명서를 발급할 때마다 해당 기관에 방문하지 않고 단말기를 통해 필요한 증명서를 발급하고, 증명서 발급 기관에 방문하는 시간을 절약하여 증명서를 발급할 때마다 기관을 방문해야 하는 불편함을 해소하는 효과가 있다.

도 2



특허청구의 범위

청구항 1

이동 통신 단말기에서 개인 정보 칩에 입력된 사용자의 신분증으로 개인종합정보 서비스 센터에 보안 인증을 수행하고 증명서를 요청하는 단계와;

상기 개인종합정보 서비스 센터에서 해당 증명서 발급 기관으로부터 상기 사용자의 상기 증명서 정보를 수집하고 수집된 개인 정보를 상기 이동 통신 단말기로 전송하는 단계와;

상기 증명서 발급 기관에서 상기 사용자의 상기 증명서를 검색하고 정보 유효 기간을 포함하여 상기 사용자의 상기 증명서를 상기 개인종합정보 서비스 센터로 전송하는 단계와;

상기 이동 통신 단말기에서 상기 개인종합정보 서비스 센터로부터 상기 사용자의 상기 증명서를 다운로드하고 상기 개인 정보 칩에 저장하는 단계와;

상기 이동 통신 단말기에서 상기 증명서 출력 요청 시 정보 유효 기간을 판단하고 출력할 상기 증명서를 선택하는 단계와;

상기 이동 통신 단말기에서 출력 단말기를 선택하고 상기 개인종합정보 서비스 센터로 출력할 정보를 전송하는 단계와;

상기 개인종합정보 서비스 센터에서 상기 이동 통신 단말기의 정보 출력 요청에 의해 상기 사용자의 상기 증명서를 상기 선택된 출력 단말기로 전송하여 출력하는 단계로 이루어진 것을 특징으로 하는 이동 통신 단말기의 개인 정보 서비스 방법.

청구항 2

제1항에 있어서, 상기 증명서는 의료 기록, 보험 정보, 성적증명서, 졸업증명서, 자격증, 운전면허정보, 공인 연이 점수의 개인 정보인 것을 특징으로 하는 이동 통신 단말기의 개인 정보 서비스 방법.

청구항 3

삭제

청구항 4

제1항에 있어서,

상기 출력 단말기는 상기 증명서를 팩스로 출력하거나, 이메일 서버에 수신된 상기 증명서를 프린터로 출력하도록 이루어진 것을 특징으로 하는 이동 통신 단말기의 개인 정보 서비스 방법.

발명

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

- [0004] 본 발명은 이동 통신 단말기의 개인 정보 서비스 방법에 관한 것으로, 특히 분산된 개인 정보를 한 곳으로 통합하여 단말기를 통해 조회하고 발급할 수 있게 한 이동 통신 단말기의 개인 정보 서비스 방법에 관한 것이다.
- [0005] 현대인은 누구나 주민등록증을 소지하고 운전 자격을 획득 시에는 운전면허증을 소지하고, 언어 검증 시험이 통과하면 시험 전수 통지서를 소지한다. 그밖에 현대인은 경제 활동에 필요한 각종 자격증, 신분증 등 자신을 대변할 증명서를 소지한다.
- [0006] 현대인은 각종 자격증, 운전면허증, 신분증 등 자신의 신상 정보를 나타내는 증명서를 소지하고, 증명서 필요시 각 증명서 발급 기관에 방문하여 필요한 증명서를 발급받는다. 현대인은 필요한 때에 증명서를 발급받아 증명서를 요구하는 곳에 제출한다.

등록번호 10-1091410

[0007] 원대인에게는 각종 저작권의 의료 기록 등이 한 곳에 모여 있지 않아 이러한 기록들을 조화시켜 여러 기능을 직접 방문하여 확인하는 수밖에 없다. 예를 들어 회사에서 주민등록증 발급을 요구한다고 가정하면 사용자는 주민등록증 발급받기 위해 동사무소나 해당 발급기관을 방문하여 증명서를 발급받아야 한다.

원대인이 제공하는 기록의 이해

[0008] 따라서 본 발명은 상기와 같은 문제점을 감안하여 창안한 것으로, 분산된 개인 정보를 한 곳으로 통합하여 단편 기록을 통해 조회하고 발급할 수 있도록 한 이동 통신 단말기의 개인 정보 서비스 방법을 제공함에 그 목적이 있다.

발명의 구성 및 작용

[0009] 상기와 같은 목적을 달성하기 위한 본 발명은, 이동 통신 단말기에서 개인 정보 칩에 입력된 사용자의 신원정보로 개인종합정보 서비스 센터에 보안 인증을 수행하고 증명서를 요청하는 단계와; 개인종합정보 서비스에 해당 증명서 발급 기관으로부터 사용자의 증명서 정보를 수집하고 수집된 개인 정보를 이동 통신 단말기로 전송하는 단계와; 증명서 발급 기관에서 사용자의 증명서를 검색하고 정보 유효 기간을 포함하여 사용자의 증명서를 개인종합정보 서비스 센터로 전송하는 단계와; 이동 통신 단말기에서 개인종합정보 서비스 센터로부터 사용자 증명서의 증명서 발급 기관(31-34)으로부터 보험, 의료, 교육, 증명서 등의 정보를 수집하여 관리한다. 개인종합정보 서비스 센터(20)는 수집된 개인 정보를 팩스, 이메일로 전송하여 사용자에게 제공한다.

[0010] 이하, 본 발명에 따른 실시 예를 첨부한 도면을 참조하여 상세히 설명하면 다음과 같다.

[0011] 도 1은 본 발명을 설명하기 위한 이동 통신 단말기의 개인 정보 수신 통신 환경의 구성을 보인 예시도이다.

[0012] 이동 통신 단말기(10)는 개인종합정보 서비스 센터(20)에 연결하여 사용자의 주민등록증 또는 자동차 운전면허증으로 보안 인증을 수행하고 필요한 개인 신상 정보를 확인하고 다음으로 하여 저장한다.

[0013] 개인종합정보 서비스 센터(20)는 각종 증명서 발급 기관(31-34)으로부터 보험, 의료, 교육, 증명서 등의 정보를 수집하여 관리한다. 개인종합정보 서비스 센터(20)는 수집된 개인 정보를 팩스, 이메일로 전송하여 사용자에게 제공한다.

[0014] 보험, 의료, 교육 등의 정보를 조회하고 싶은 사용자는 해당 기관에 정보를 요청하고 해당 기관은 보안 인증을 받아 개인 신상 확인 후 요청한 정보를 개인종합정보 서비스 센터(20)를 통해 사용자에게 소지한 이동 통신 단말기(10)로 전송한다.

[0015] 이동 통신 단말기(10)는 개인종합정보 서비스 센터(20)로부터 수신한 정보를 저장하고 정보 출력 필요시 정보 요청자가 자동한 연계를 지시된 정보를 컴퓨터로 옮겨 보편으로 출력한다.

[0016] 도 2는 본 발명의 실시 예에 따른 이동 통신 단말기의 개인 정보 서비스 방법의 개인 정보 수신 방법의 동작 흐름도로서, 이에 도시된 바와 같이 이동 통신 단말기에서 개인 정보 칩에 입력된 주민등록증 또는 운전면허증으로 개인종합정보 서비스에 보안 인증을 수행하고 주민등록증 발급을 요청하는 단계와; 개인종합정보 서비스 센터에서 주민등록증 발급 기관으로부터 사용자의 주민등록증 정보를 수집하고 수집된 개인 정보를 이동 통신 단말기로 전송하는 단계와; 주민등록증 발급 기관에서 사용자의 주민등록증 검색하고 정보 유효 기간을 포함하여 사용자의 주민등록증 발급을 개인종합정보 서비스 센터로 전송하는 단계와; 이동 통신 단말기에서 개인종합정보 서비스 센터로부터 사용자 증명서의 증명서 발급 기관으로부터 보험, 의료, 교육, 증명서 등의 정보를 수집하여 관리한다. 개인종합정보 서비스 센터(20)는 수집된 개인 정보를 팩스, 이메일로 전송하여 사용자에게 제공한다.

[0017] 사용자가 주민등록증 또는 이동 통신 단말기에서 저장하고 저장된 주민등록증을 출력하여 사용한다고 가정하자.

[0018] 이동 통신 단말기는 개인 정보 칩에 입력된 주민등록증 또는 운전면허증으로 개인종합정보 서비스 센터에 보안 인증을 수행하고 주민등록증 발급을 요청한다. 이동 통신 단말기는 보안 인증에 필요한 사용자의 주민등록증 또는 운전면허증에 대한 정보를 사용자에게 요청하여 입력하고 개인 정보 칩에 사용자의 주민등록증 또는 운전면허증에 입력하여 개인종합정보 서비스 센터의 칩속에 필요한 보안 인증에 사용한다.

[0019] 개인종합정보 서비스 센터는 주민등록증 발급 기관으로부터 사용자의 주민등록증 정보를 수집하고 수집된 개인 정보를 이동 통신 단말기로 전송한다. 개인종합정보 서비스 센터는 이동 통신 단말기의 주민등록증 발급에 응답하여 주민등록증 발급 기관에 사용자의 주민등록증 발급을 요청하여 수집한다.

[0020] 주민등록증 발급 기관은 개인종합정보 서비스 센터의 주민등록증 발급 요청에 응답하여 사용자의 주민등록증 발급을 데이터베이스에서 검색하고 정보 유효 기간을 포함하여 사용자의 주민등록증 발급을 개인종합정보 서비스 센터로

전송한다. 개인종합정보 서비스 센터는 주민등록등본 발급 기관으로부터 사용자의 주민등록등본 정보를 수신하고 수신된 개인 정보를 이동 통신 단말기로 전송한다.

- [0021] 이동 통신 단말기는 개인종합정보 서비스 센터로부터 사용자의 주민등록등본을 다운로드하고 개인 정보 칩이 저장한다. 이동 통신 단말기는 개인 정보 칩에 사용자의 주민등록등본 정보를 유효기간까지 저장하고 유효기간이 지니면 주민등록등본 정보를 삭제한다.
- [0022] 도 3은 본 발명을 설명하기 위한 이동 통신 단말기의 개인 정보 송신 통신 환경의 구성을 보인 예시도이다.
- [0023] 이동 통신 단말기(10)는 사용자의 출력 요청시 정보 유효 기간동안 언제든지 개인 정보 칩에 저장된 정보를 팩스로 전송하여 출력하거나 이메일, 컴퓨터로 전송하여 프린터로 출력한다.
- [0024] 이동 통신 단말기(10)는 사용자의 정보 출력 요청시 출력 단말기로 팩스, 이메일, 컴퓨터를 선택하고 개인종합정보 서비스 센터(20)로 출력할 정보를 전송한다.
- [0025] 개인종합정보 서비스 센터(20)는 이동 통신 단말기(10)의 정보 출력 요청에 의해 사용자의 정보를 선택된 출력 단말기로 전송하여 출력한다. 예를 들어, 출력 단말기인 팩스(41)는 주민등록등본을 개인종합정보 서비스 센터로부터 수신하여 출력하거나, 컴퓨터는 이메일(42) 서버에 수신된 주민등록등본을 이메일 확인하고 프린터로 출력한다.
- [0026] 다른 실시 예로, 개인종합정보 서비스는 주민등록등본뿐만 아니라 운전면허정보, 공인 언어 점수, 의료 기록 등 개인 정보를 수집 관리한다. 예를 들어 개인 정보 칩이 운전면허정보를 저장하고 있으면 칩 리더기는 개인정보 칩에 저장된 운전면허정보를 참조하여 해당 기관의 정보 센터에 접속하여 사용자의 인적사항과 교통기록을 직접 조회한다.
- [0027] 운전면허증에 개인정보 칩이 장착되어 있으면 이동 통신 단말기를 이용하지 않고 카드 리더기에서 운전면허증에 저장된 운전면허정보를 읽어 들여 해당 기관의 정보 센터에 접속하여 사용자의 인적사항과 교통기록을 직접 조회한다.
- [0028] 병원에서는 의료 기록을, 보험 회사에서는 보험 정보를, 학교에서는 성적증명서와 졸업증명서를, 자격증 발급기관에서는 각종 자격증을 개인종합정보 서비스 센터에 제공하여 이동 통신 단말기에서 개인종합정보 서비스 센터에 각종 증명서 발급을 요청하여 증명서를 다운로드하여 확인하고 개인종합정보 서비스 센터를 통해 정보 유효기간까지 언제든지 증명서를 출력한다.

발명의 효과

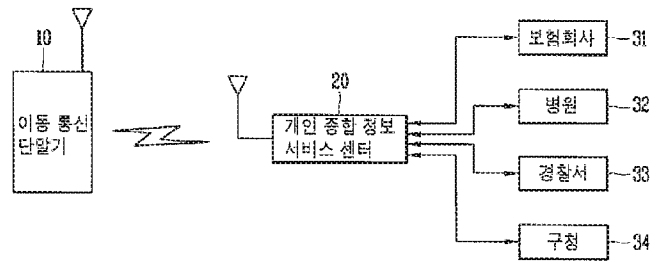
- [0029] 이상에서 상세히 설명한 바와 같이, 본 발명은 분산된 개인 정보를 한 곳으로 통합하여 단말기를 통해 조회하고 발급함으로써 사용자는 증명서를 발급할 때마다 해당 기관에 방문하지 않고 단말기를 통해 필요한 증명서를 발급하고, 증명서 발급 기관에 방문하는 시간을 절약하여 증명서를 발급할 때마다 기관을 방문해야 하는 불편함을 해소하는 효과가 있다.

도면의 간단한 설명

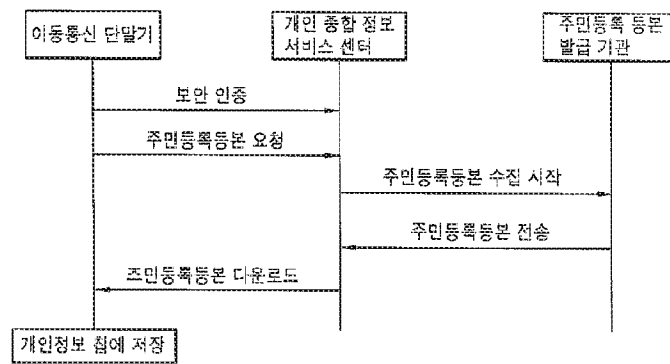
- [0001] 도 1은 본 발명을 설명하기 위한 이동 통신 단말기의 개인 정보 수신 통신 환경의 구성을 보인 예시도.
- [0002] 도 2는 본 발명의 실시 예에 따른 이동 통신 단말기의 개인 정보 서비스 방법의 개인 정보 수신 방법의 동작 흐름도.
- [0003] 도 3은 본 발명을 설명하기 위한 이동 통신 단말기의 개인 정보 송신 통신 환경의 구성을 보인 예시도.

도면

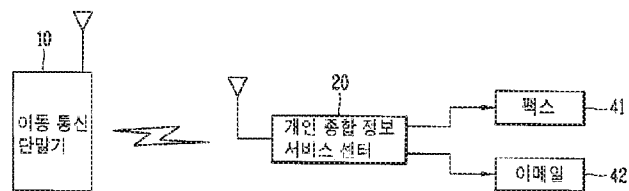
도면1



도면2



도면3





- (51) **International Patent Classification:**
G06F 21/30 (2013.01) *G06F 17/21* (2006.01)
- (21) **International Application Number:**
PCT/US2013/077010
- (22) **International Filing Date:**
20 December 2013 (20.12.2013)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
61/740,731 21 December 2012 (21.12.2012) US
13/794,878 12 March 2013 (12.03.2013) US
- (71) **Applicant:** CORTEX MCP, INC. [US/US]; 35 Terrastar Lane, Ladera Ranch, CA 92694 (US).
- (72) **Inventor:** SARKISSIAN, Shaunt M.; 35 Terrastar Lane, Ladera Ranch, CA 92694 (US).
- (74) **Agents:** TARR, Daniel J. et al.; K&L Gates LLP, K&L Gates Center, 210 Sixth Avenue, Pittsburgh, PA 15222-2613 (US).
- (81) **Designated States** (*unless otherwise indicated, for every kind of national protection available*): 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, KR, 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) **Designated States** (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (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).

Published:

- with international search report (Art. 21(3))
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))

(54) **Title:** FILE FORMAT AND PLATFORM FOR STORAGE AND VERIFICATION OF CREDENTIALS

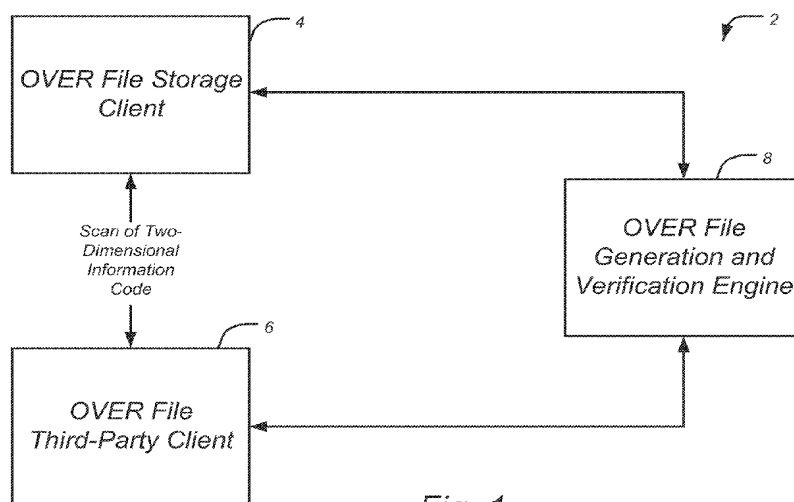


Fig. 1

(57) **Abstract:** In various embodiments, a computer-implemented method for generating and verifying officially verifiable electronic representations may be disclosed. The method may comprise receiving, by a credential database, a request for a credential action. The credential database may be configured to store one or more credentials comprising a status indicator. The method may further comprise determining, by the credential database, a response to the credential action based on the one or more user credentials stored in the credential database and transmitting, by the credential database, the response to a client device.

**FILE FORMAT AND PLATFORM FOR STORAGE AND VERIFICATION OF
CREDENTIALS**

CROSS-REFERENCE TO RELATED APPLICATIONS

5 This application claims the benefit of United States Provisional Patent Application No. 61/740,731, filed December 21, 2012, entitled "FILE FORMAT AND PLATFORM FOR STORAGE AND VERIFICATION OF CREDENTIALS" and U.S. Patent Application No. 13/794,878, filed on March 12, 2013, entitled "FILE FORMAT AND PLATFORM FOR STORAGE AND VERIFICATION OF CREDENTIALS".

10

TECHNICAL FIELD

The present disclosure relates to electronic transactions, and more particularly to systems, methods, and apparatuses for securely storing and displaying user credentials.

BACKGROUND

15 The rapid growth and evolution of traditional and electronic commerce markets has resulted in a wide-spread demand for monetary payments by digital transactions. However, currently payment systems are highly fragmented and insecure, which creates a threat of data compromise and theft during the transfer and use of electronic commerce data. This threat may result in losses for corporations as well as users of such systems, and these
20 losses factor into escalating fees and client costs.

 Additionally, as more users move to a digital transaction model, the need for digital identification also increases. As fewer users carry wallets or traditional payment forms, traditional forms of ID will become less common. Current platforms are insecure and carrying digital credentials increases the risk of identity theft or fraud in transactions. What is
25 needed is secure system for storing and displaying user credentials.

SUMMARY

 In various embodiments, a computer-implemented method for generating and verifying officially verifiable electronic representations may be disclosed. The method may
30 comprise receiving, by a credential database, a request for a credential action. The credential database may be configured to store one or more credentials comprising a status indicator. The method may further comprise determining, by the credential database, a response to the credential action based on the one or more user credentials stored in the

credential database and transmitting, by the credential database, the response to a client device.

In various embodiments, a computer-implemented method for requesting an officially verifiable electronic representation is disclosed. The method may comprise generating, by a processor, a request for a credential action. The request may comprise a credential identifier. The processor may transmit the request for the credential action to a credential database and receive a response to the request for the credential action.

In various embodiments, an apparatus for generating and verifying officially verifiable electronic representations is disclosed. The apparatus may comprise a processor and a memory unit operatively coupled to the processor. The memory unit may be configured to store a plurality of instructions, wherein the instructions are configured to program the processor. The processor may be programmed to maintain a credential database. The credential database may be configured to store one or more credentials comprising a status indicator. The processor may further receive a request for a credential action and determine a response to the credential action based on the one or more user credentials stored in the credential database. The processor may be programmed to transmit the response to a client device. In various embodiments, a credential database may store the one or more credentials in an encrypted format which can only be decrypted by the apparatus. In various embodiments, the credential database may access additional information via a network to complete a verification of a credential. In various embodiments, the credential database may use additional information provided by a client, such as, for example, passwords, biometric information, client GPS location information, and/or a unique device identifiers, to complete the verification.

BRIEF DESCRIPTION OF THE FIGURES

The features of the various embodiments are set forth with particularity in the appended claims. The various embodiments, however, both as to organization and methods of operation, together with advantages thereof, may best be understood by reference to the following description, taken in conjunction with the accompanying drawings as follows:

Fig. 1 illustrates one embodiment of a virtual credential management platform.

Fig. 2 illustrates one embodiment of an Officially Verifiable Electronic Representation (OVER) File generation process.

Fig. 3 illustrates one embodiment of an OVER File verification process.

Fig. 4 illustrates one embodiment of a virtual wallet platform.

Fig. 5 illustrates one embodiment of an OVER File storage client component of the virtual wallet platform of Fig. 4.

Fig. 6 illustrates one embodiment of a credential type display of the OVER File storage client.

Fig. 7 illustrates one embodiment of a displayed OVER File credential oriented horizontally.

5 Fig. 8 illustrates one embodiment of a displayed OVER File credential oriented vertically.

Fig. 9 illustrates one embodiment of an OVER File generation screen.

Fig. 10 illustrates one embodiment of a information code for generation or verification of an OVER File.

10 Fig. 11 illustrates one embodiment of a credential presentation and verification process.

Fig. 12 illustrates one embodiment of a computing environment for implementing an OVER File management platform.

15 DESCRIPTION

In various embodiments, a computer-implemented method for generating and verifying officially verifiable electronic representations may be disclosed. The method may comprise receiving, by a credential database, a request for a credential action. The credential database may be configured to store one or more credentials comprising a status
20 indicator. The credential database may further be configured to store one or more methods for accessing one or more status indicators on a network, such as, for example, via web-service or access to a second data store. The method may further comprise determining, by the credential database, a response to the credential action based on the one or more user credentials stored in the credential database and transmitting, by the credential database,
25 the response to a client device. The method may further incorporate additional information submitted by a client, such as, for example, passwords, device identifiers, client GPS location, and/or biometric data, in conjunction with the stored credential, to determine a response to the request for a credential action.

In various embodiments, a computer-implemented method for requesting an officially
30 verifiable electronic representation is disclosed. The method may comprise generating, by a processor, a request for a credential action. The request may comprise a credential identifier. The request may further comprise additional information to verify the credential. The processor may transmit the request for the credential action to a credential database and receive a response to the request for the credential action. In various embodiments, the
35 processor may incorporate additional information submitted by a client, such as, for example, passwords, device identifiers, GPS location information, and/or biometric

information, to determine a response. In various embodiments, the processor may access other data stores available via a network to determine a response.

In various embodiments, an apparatus for generating and verifying officially verifiable electronic representations is disclosed. The apparatus may comprise a processor and a
5 memory unit operatively coupled to the processor. The memory unit may be configured to store a plurality of instructions, wherein the instructions are configured to program the processor. The processor may be programmed to maintain a credential database. The credential database may be configured to store one or more credentials comprising a status indicator. The processor may access other data stores via a network. The processor may
10 access remote functionality via a network. The processor may further receive a request for a credential action and determine a response to the credential action based on the one or more user credentials stored in the credential database. The processor may be programmed to transmit the response to a client device.

Reference will now be made in detail to several embodiments, including
15 embodiments showing example implementations of systems and methods for generating, storing, and displaying OVER File credentials. Wherever practicable similar or like reference numbers may be used in the figures and may indicate similar or like functionality. The figures depict example embodiments of the disclosed systems and/or methods of use for purposes of illustration only. One skilled in the art will readily recognize from the following
20 description that alternative example embodiments of the structures and methods illustrated herein may be employed without departing from the principles described herein.

In some embodiments, an Officially Verifiable Electronic Representation (OVER) File may provide a secure file format and platform for the storage and verification of key user or consumer credentials. As shown in Fig. 1, in one embodiment, an OVER File management
25 platform 2 may comprise three main components, an OVER File storage client 4, an OVER File third party client 6, and an OVER File generation and authorization engine 8. The OVER File storage client 4 may be executed by a user device to store generated OVER Files representative of the user's credentials. The OVER File storage client 4 may be included as part of a virtual wallet platform or may comprise a stand-alone user application.
30 The OVER File storage client 4 may initiate generation of new OVER Files and may comprise a display function for displaying stored user credentials for third-party verification. The OVER File credentials may comprise any officially verifiable electronic credential, such as, for example, a government issued identification such as a driver's license, non-driver's identification card, or professional license. The OVER File credentials may also comprise
35 privately issued credentials, such as, for example, employee identification cards, merchant loyalty cards, access cards, insurance credentials, transportation credentials, or any other credential that may be electronically verified by an issuing agency.

In some embodiments, an OVER File third party client 6 may be executed by a third party device to verify the existence and validity of OVER File credentials presented by a user. The OVER File third party client 6 may allow a third party to scan or otherwise interact with OVER File credentials displayed on a user device. The OVER File third party client 6 may contact a remote server, such as the OVER File generation and verification engine 8, for verification of the displayed user credential, as explained in more detail below. The OVER File third party client 6 may further allow a third party to request generation of an OVER File credential for delivery to an OVER File storage client 4. In some embodiments, the OVER File third party client 6 may comprise a stand alone application executed by the third party device. In other embodiments, the OVER File third party client 6 may comprise an application program interface (API) configured to provide OVER File credential verification through a third party application.

In some embodiments, an OVER File generation and authorization engine 8 may generate OVER File credentials in response to requests from an OVER File storage client 4 or an OVER File third party client 6. The OVER File credentials may be generated from data provided by a user, a third party, or an issuing agency or authority. The OVER File generation and authorization engine 8 may further provide authorization of OVER File credentials requested by third parties. The OVER File generation and authorization engine 8 may operate on a remote server. Client devices, such as the user device or the third party device, may communicate with the OVER File generation and authorization engine 8 using any suitable network or communication system. In some embodiments, the OVER File generation and verification engine 8 may generate and maintain a status indicator for each stored OVER File credential configured to indicate whether the OVER File credential is currently valid.

Fig. 2 illustrates one embodiment of a process 100 for generating and storing an Officially Verifiable Electronic Representation (OVER) File credential. OVER File generation may be performed by the OVER File generation and verification engine 8. An engine may comprise computer program that drives the functionality of a system or process, such as, for example, the process 100 for generating and storing an OVER File credential. A user may open 102 an application for generating and/or displaying OVER Files, such as the OVER File storage client 4. In some embodiments, the application may be a stand-alone application. In other embodiments, the OVER File storage client 4 may be included in an integrated application.

A user may access 104 the OVER File credential features of an OVER File storage client to add 106 a new credential to the OVER File storage client 4. The user may be presented with a credential generation screen, such as the credential generation screen 518 shown in Fig. 7. A credential may be added manually by a user or automatically by the

application. In some embodiments, a user may select 108 the method of entering the credential, for example, manual or automated entry, using the credential generation screen. In some embodiments, a user may select 110 manual entry of the credential. The user may interact with the credential generation screen to enter 112 information about the credential, such as, for example, the issuing agency, a credential identifier such as a credential identification number, or any other information associated with the credential. For example, in one embodiment, a user may choose to manually enter a credential representing a rewards card for a retailer. The user may be prompted to identify the retailer, a rewards card identification number, and a name associated with the rewards card.

In some embodiments, information for generating an OVER File credential may be automatically added to the OVER File storage client 4. For example, information necessary for the generation of an OVER File credential may be entered by scanning an information code. The information code may be represented, for example, by a quick-response (QR) Code, standard one dimensional bar code, alpha numeric bar code (for example, Type-128), and/or other suitable information codes. The information code may be represented data sent by a radio transmission or by an electronic transmission broadcast over a network. In some embodiments, a user device may scan an information code provided by an issuing agency. The information code may comprise information, such as a credential identifier, necessary for generating an OVER File and contacting an issuing agency database 130 for verification of the credential. The information code may be provided by the issuing agency during creation of the credential and may be scanned by a user using a scan function of the user device.

In some embodiments, the information code may comprise information necessary for the generation of a credential by a third party. A user may select 114 a third-party scan option for generation and delivery of a new credential. The OVER File storage client 4 may generate a information code on the user device for scanning by the third party. The information code may comprise any necessary information for generation and delivery of the OVER File credential to the user device, such as, for example, the user's name, contact information, social security number, biometric information, location information, user-selected password, and/or a device identifier to identify the user device. The information code may be displayed 120 on the user device and may be scanned 122 by a third-party using a third-party device. The third party device may execute an application, such as the OVER File third party client 6, for scanning the information code and contacting an OVER File generation and verification engine 8. The OVER File generation and verification engine 8 may be executed by any suitable system. The OVER File generation and verification engine 8 may comprise a credential data store, such as, for example, a database, a web service, a flat file configured to store data, and/or any other suitable datastore. The

credential datastore may comprise a memory unit formed integrally with the system configured to execute the OVER File generation and verification engine 8 or may comprise a remote storage device, such as, for example, a database connected to the OVER File generation and verification engine 8 through a local area network (LAN), wide area network (WAN), or Internet connection. Although the various embodiments of the OVER File generation and verification engine 8 are discussed with respect to an OVER File database, those skilled in the art will recognize that any suitable architecture and/or datastore may be employed by the OVER File generation and verification engine.

In some embodiments, an issuing agency may set one or more business rules that a user may be required to meet prior to verification of the OVER File credential by the issuing agency, such as being required to verify the user's identity prior to generation of the OVER File credential. For example, a user attempting to add a driver's license credential may be required to visit a state DMV office. After verifying the identity of the user, the DMV office may provide the user with a scannable information code for generation of an OVER File credential for the user's driver's license. The information code may comprise a credential identifier and an authorization code to enable the OVER File database 128 to generate the OVER File credential. In some embodiments, a physical credential issued by the issuing agency may contain an information code that may be scanned by the user at any time to add the credential to the OVER File storage client 4. For example, a retailer loyalty card may comprise a scannable quick-response (QR) code that a user may scan to add an OVER File credential of the loyalty card to a user device.

After the necessary information has been entered to generate an OVER File credential, either manually or through an automated process such as scanning, the generating device may contact an application gateway 124 to deliver an OVER File generation request to an OVER File database 128. The OVER File database 128 may comprise an OVER File generation and verification engine 8. The application gateway may request 126 generation of an OVER File and verification of the generated OVER File credential. The OVER File database 128 may be configured to create a new OVER File containing the entered credential information. The OVER File database 128 may contact an issuing agency datastore, such as, for example, an issuing agency database 130, to verify the information contained in the OVER File generation request and to obtain additional credential information stored by the issuing agency database 130. Issuing agencies may comprise, for example, government entities such as States or licensing agencies, corporations issuing credentials to employees, retailers issuing loyalty or other customer identifiers, or any other suitable agency for issuing credentials. Although the various embodiments are generally described as communicating with an issuing agency database,

those skilled in the art will recognize that issuing agencies may utilize any suitable datastore to store one or more credentials generated by the issuing agency.

The additional credential information may comprise any information stored by the issuing agency database but not provided in or contradictory to the OVER File generation request. For example, in one embodiment, a user may generate a credential representative of a driver's license. The user device may provide a driver's license identification number and an issuing state to the OVER File database 128 for generation of the OVER File. The OVER File database 128 may contact the issuing agency database 130, such as a state DMV database, and provide the driver's license identification number to the issuing agency database 130. The issuing agency database may respond by indicating the validity of the requested credential containing the driver's license identification number and may provide the legal name, address, and birth date of the person associated with the driver's license identification number. The issuing agency database may also provide an image of the requested credential for display on the user device. Once the information has been verified, the OVER File database 128 may generate a new OVER File containing the entered credential information. In some embodiments, the OVER file may be generated by the issuing agency database 130 and sent to the OVER File database 128 for storage and distribution to the user device. The issuing agency may also provide a status indicator for the generated OVER File credential.

In some embodiments, the OVER File may be delivered to a device identified in the OVER File generation request for storage. For example, generated OVER File credential may be delivered to the device requesting generation of the OVER File generation, such as a user device. As another example, if a user provides a information code to a third party for scanning and generation of a credential, the information code may contain a device identifier identifying the user device as the destination for the generated OVER File credential. Copies of the OVER File credential may be stored on both a user device and in the OVER File database 128. The delivered OVER File credential may be tied to a specific user device. For example, the OVER File credential may contain a device identifier identifying the user device or application and/or the OVER File may be encrypted in a format which requires the device identifier and/or a user-provided password to decrypt. The OVER File may include a hash value which requires the device identifier and/or a user-provided password to verify. The OVER File credential may only be usable by a device matching the device or application identifier. By tying the OVER File credential to a specific device, the security of the credential is increased, as an OVER File delivered to a device other than the user device, for example through network snooping, may be prevented from working on a device other than the user device. The delivered OVER File credential may execute a device check to verify the current device matches the specific device identifier. If the current

device and the device identifier are the same, the OVER File credential may be stored 136 on the user device. If the specific device identifier and the current device are not the same, the OVER File credential may be inaccessible or destroyed. In some embodiments, the OVER File may require user-specific information, such as, for example, biometric
5 information, location information, and/or passwords, to decrypt the file or to verify the OVER File credential.

Fig. 3 illustrates one embodiment of an OVER File verification process 200. A user may begin 202 the verification process by opening 204 an OVER File storage client, accessing 206 the credential features of the OVER File storage client, and selecting 208 a
10 stored OVER File credential for display 210 on the user device. The user may select the OVER File credential from a list of credentials stored on the user device, such as, for example, the credential category screen 514 shown in Fig. 6. Credential information stored in the OVER File may be displayed on the user device. In some embodiments, the displayed information may comprise some or all of the information stored in the OVER File
15 credential. For example, a stored OVER File credential may be displayed as shown in Figs. 18 and 19, and may comprise one or more text fields, an image field, a title field, and a information code field. The user may present 212 the displayed credential to a third party for verification. The displayed information code may comprise a credential identifier, such as, for example, a credential identification number.

The third-party may initiate a third party verification process by opening 216 a
20 verification application, such as the OVER File third party client 8, for verifying credentials displayed on a user device. In some embodiments, the verification application may be a stand-alone application specifically configured for verification of OVER File credentials. In other embodiments, the verification application may comprise an application capable of
25 verification of OVER Files through an application programming interface (API). The third party may use the verification application to select a scanning option 218 to scan 220 the information code displayed on the user device. After scanning the information code, the third-party verification application may contact an application gateway 224 to provide verification of the scanned OVER File credential. The third-party verification application may
30 transmit the information contained in the information code displayed on the user device, such as the credential identifier. For example, an information code may comprise an issuing agency identifier and a credential identifier for the displayed credential.

The application gateway 224 may communicate with a verification server 226 and an OVER File database 228. The verification server 226 may comprise the OVER File
35 generation and verification engine 8. Although the application gateway 224, the verification server 226 and the OVER File database 228 are shown as separate systems in Fig. 2, those skilled in the art will recognize that the application gateway 224, the verification server 226

and the OVER File database 228 may be combined into a single system. The OVER File database 228 may store copies of all generated OVER File credentials. The OVER File credentials may be stored in any suitable manner, such as, for example, on a memory unit or other suitable storage device. In some embodiments, the OVER File credentials may be stored on a remote device, such as a networked database, and may be accessed by a reference stored in an OVER File datastore, such as, for example, the OVER File database. In various embodiments, the reference may comprise a hash code, a pointer, network address, and/or any other suitable reference to a remotely stored file. The OVER File database 228 may compare information received from the third-party verification application, such as, for example, a credential identifier, with the OVER File credentials stored in the OVER File database 228. A status indicator providing the validity of the OVER File credential may be sent to the OVER File third party client. If the OVER File database determines 230 that the credentials are valid, the verification server 226 may provide a valid status indicator to the third party device. The verification server 226 may further provide a portion of the stored OVER File credential, such as a credential image, to the third party device. In some embodiments, the status indicator and a portion of the stored OVER File credential may be displayed on the third-party device. If the OVER File verification server 226 determines 230 that the credentials are invalid, the OVER File verification server 226 may transmit a status indicator indicating an invalid credential and may provide the reason for the invalid status indicator to the third party device.

The OVER File database 228 may be in communication with one or more issuing agency databases 230. The issuing agency database 230 may be maintained by an issuing agency authorized to issue one or more credentials. For example, a state Department of Motor Vehicles may maintain a database comprising all driver's licenses issued by the state.

The OVER File database 228 may receive periodic updates from the issuing agency database 230 for the OVER File credentials stored in the OVER File database 228. The update period may depend on the type of credential, requirements of the issuing agency, frequency of verification requests, or other factors affecting the security requirements for a specific credential type. For example, the OVER File database 228 may receive updates on a daily basis for high-security credentials, such as, for example, driver's licenses. The OVER File database 228 may receive updates on a weekly basis for credentials requiring a lower security level, such as merchant loyalty cards. In some embodiments, the OVER File database 228 may contact the issuing agency database 230 to begin the update process. In some embodiments, the issuing agency database 230 may initiate the update process. The OVER File database 228 may be updated for individual OVER File credentials or may receive a batch update from an issuing agency for all OVER File credentials issued by the issuing agency.

A status indicator may be sent to the third party device to indicate the validity status of an OVER File credential matching the credential identifier associated with the OVER File credential displayed on the user device. The status indicator may comprise a valid indicator if the verification server 226 determines that a valid OVER File credential matching the credential identifier received from the third party verification application is stored in the OVER File database 228 and the OVER File database 228 indicates that the OVER File credential is currently valid. The verification server 226 may provide a response 232 to the third party device comprising the status indicator indicating a valid credential and may provide a portion of the credential information stored in the OVER File database 228. For example, in response to a verification request for an OVER File credential of a driver's license, the verification server 226 may provide a valid status indicator and may provide an image of the driver's license to the third party device. As another example, in response to the same request, the verification server 226 may provide a valid status indicator, an image of the credential holder provided by the issuing agency, and the birth date of the credential holder. Those skilled in the art will recognize that the response to the verification request may be customized based on each type of credential and by each issuing agency.

In some embodiments, the verification server 226 may determine 222 that a requested credential is invalid. For example, the credential verification request may be considered invalid if an OVER File credential matching the provided credential identifier was not located in the OVER File database 228. In another embodiment, an OVER File credential matching the provided credential identifier may be stored in the OVER File database 228 but may be expired. In another embodiment, an OVER File credential matching the provided credential identifier may be stored in the OVER File database but may not match a provided device identifier, provided biometric data, and/or a provided password. The verification server 226 may provide a status indicator indicating an invalid credential. The invalid status indicator may indicate why 234 the credential is considered invalid. For example, an invalid status indicator may indicate 236 an expired credential and may display 238 a response on the third-party device that the requested credential exists but has expired. As another example, the invalid status indicator may indicate 240 that the requested credential does not exist. An invalid status indicator may be displayed 242 on the third party device stating that there is no data available for the requested OVER File. As another example, additional information submitted by the client, such as, for example, a password, biometric information, and/or location information, may not match information stored with the credential.

Fig. 4 illustrates one embodiment of a virtual wallet platform 300. The virtual wallet platform may provide an electronic platform for payment and credential storage. The virtual wallet platform 300 may provide electronic replacement for credit cards, cash, identification,

or other cards traditionally carried in a wallet. In some embodiments, the virtual wallet platform may provide a Reducing Currency Denomination (RCD) payment platform and an OVER File credential storage client 4. Fig. 4 shows a logon screen for a virtual wallet platform 300. In some embodiments, the virtual wallet platform 300 may require a username 304 and a password 306 be provided prior to accessing the RCD payment platform or the OVER File credential platform. After entering a username 304 and password 306, a user may submit the username 304 and password 306 for verification using a send button 308. The username 304 and password 306 may be verified by a local processor and memory or may be sent to a remote server for verification. The logon screen may comprise a logo 302 of the virtual wallet platform 300. An RCD payment platform is described in more detail in U.S. Patent Application No. 11/851,215, entitled "SYSTEMS, METHODS, AND APPARATUSES FOR SECURE DIGITAL TRANSACTIONS," which is hereby incorporated by reference in its entirety.

Fig. 5 illustrates one embodiment of an Officially Verifiable Electronic Representation (OVER) File storage client 500. The OVER File storage client 500 may provide storage and retrieval of one or more OVER File credentials associated with a user device. Fig. 5 illustrates one embodiment of an OVER File storage client 500 home screen 502. The home screen 502 may provide access to one or more OVER File credentials stored by the OVER File storage client 500 as part of the virtual wallet platform 300. A primary ID 506 may be displayed on the home screen 502 to allow quick and convenient access to the primary ID 506. The primary ID 506 may be selectable by the user, and may comprise, for example, a government issued driver's license or an employer issued employee ID. In some embodiments, the primary ID 506 may be accessible from any screen of the OVER File storage client 500, for example, through a predetermined user gesture, such as swiping the top of the screen down.

The home screen 502 may further provide one or more credential buttons 508a-508f for accessing a specific category of credentials, such as, for example, insurance credentials 508a, access credentials 508b, electronic coupons 508c, loyalty card credentials 508d, transportation credentials 508e, or miscellaneous credentials 508f. The user credentials may displayed in a wallet card design 504. A user may select one of the credential buttons 508a-508f to access OVER File credentials stored on the user device and classified in the selected category. For example, a user may select the loyalty credentials button 508d and may be presented with a list of OVER File credentials stored on the user's device that have been categorized as loyalty credentials, such as, for example, retailer loyalty cards, frequent buyer cards, retailer discount cards, or any other type of loyalty credential. The home screen 502 may further comprise a new button 510 for adding one or more new credentials

and a manage button 512 for accessing a screen for managing the OVER File credentials stored on the user device.

Fig. 6 illustrates one embodiment of a credential category screen 514 configured to display stored OVER File credentials classified in the selected category. The credential category screen 514 may be accessed by selecting one of the credential buttons 508a-508f displayed on the home screen 502. The credential category screen 514 may display one or more available credentials that have been categorized in the selected category. For example, credential category screen 514 illustrates one embodiment of an insurance and automobile credential category displaying OVER File credentials 516a-516h classified as insurance or automobile credentials. For example, the OVER File credentials 516a-516h may comprise auto insurance credentials, home insurance credentials, or medical insurance credentials. Additionally, the OVER File credentials may comprise automobile credentials, such as, for example, a registration card, inspection documents, or an automobile club member card. The OVER File credentials 516a-516h may be associated with a single category, such as the insurance category, or may be associated with multiple categories.

Fig. 7 illustrates one embodiment of a credential generation screen 518. The credential generation screen 518 may be accessed by selecting the new credential button 510 displayed on the home screen 502. The credential generation screen 518 may be configured to allow a user to request the generation of a new OVER File by an OVER File generation and verification engine 8. The credential generation screen 518 may allow a user to input information necessary for the generation of a new credential either manually or through an automated process. If a user wishes to enter the information manually, the user may enter the necessary credential information in credential fields 520-528. Necessary credential information may comprise a credential name 520, a credential category 522, an issuer type 524, an issuer 526, and a credential number 528. The credential category 522 and the issuer type 524 may be automatically set by the OVER File generation and verification engine 8 or may be manually set by the user. The credential number 528 may comprise a unique credential identifier generated by the issuing agency. The credential number 528 may be used by the OVER File generation and verification engine 8 to verify the validity of the requested credential and to obtain additional information associated with the generated OVER File credential not entered by the user. For example, a loyalty credential may have a certain number of loyalty points associated with the credential. The OVER File generation and verification engine 8 may use the credential number 528 to query the issuing agency regarding the current value of loyalty points associated with the credential. After entering the required credential information, a user may transmit the input information for the generation of a new OVER File credential to the OVER File generation and verification engine 8. The user may transmit the information using the add button 532.

In some embodiments, the credential generation screen 518 may allow a user to automatically enter a credential by scanning an information code, such as a barcode or quick response (QR) code. A user may access the scanning functionality by selecting the scan to add button 530. After selecting the scan to add button 530, the scanning function of a user device may be activated to allow the user to scan an information code provided by an issuing agency. The information code may comprise the information necessary for the OVER File server to contact an issuing agency database to verify the scanned credential and to obtain additional credential information. For example, in one embodiment, a user may wish to add a driver's license to the stored OVER File credentials on the user device. The user may be required to go to a state department of motor vehicle (DMV) location to verify the user's identity. After verifying the user's identity, the DMV may generate an information code for the user to scan containing the user's driver's license identification number and an authorization number.

Once the necessary information has been entered, either manually or automatically, the OVER File storage client 500 may contact the OVER File generation and verification engine 8 to generate the requested OVER File credential. The OVER File generation and verification engine 8 may contact the issuing agency database to verify the credential using the provided information as discussed above with respect to Fig. 2. The issuing agency database may provide additional information associated with the requested credential and not provided during the initial entry of the credential information. For example, a user request to add a driver's license may comprise a driver's license identification number. The issuing agency database may provide additional information such as the user's photo, address information, age information, or license class information. The use of an information code for adding a user credential provides convenience and security, as the user does not have to manually enter the credential information and an issuing agency can control the generation of OVER Files associated with the issuing agency's credentials.

In some embodiments, a user may present a stored OVER File credential to a third party for verification. For example, a user may wish to gain access to an age restricted location or purchase an age restricted product. A third party may require a user to present identification to verify the user's age prior to allowing the user access to the age restricted location or product. A user may choose to present a stored OVER File containing the user's age information, such as, for example, an OVER File credential representative of the user's driver's license. A third party may be required to verify the validity of the presented credential. The OVER File storage client 500 may generate a scannable information code for scanning by the third party to provide verification of the credential, as described in more detail above. In another embodiment, the OVER File storage client may generate an information code in the form of a networked or radio transmission, such as, for example, a

Near Field Communication (NFC) or Bluetooth, or in the form of sensor information, such as, for example, a bump. A credential code screen 536 may be generated on the user device.

The credential code screen 536 may comprise a scannable information code 538

representative of the selected OVER File credential. The third party may scan the

5 information code 538 using an OVER File third party client 6. The OVER File third party client 6 may use the information contained in the information code 538 to contact an OVER File generation and verification engine 8 to verify the validity of the presented OVER File credential. In some embodiments, the information code 538 may be presented on the user device for a predetermined period of time at which point the user device may revert to a
10 previously displayed screen, such as the credential category screen 514. In some embodiments, the user may be able to revert to the previous screen by pressing a back button 534.

When presenting a credential to a third party for verification, the OVER File storage client 500 may display a scannable information code, as described above. In some
15 embodiments, a portion of the stored OVER File may be displayed on the user device for presentation to the third party. Fig. 9 illustrates one embodiment of a credential display 600. The credential display 600 may be configured to display a selected OVER File credential on a user device. The credential display 600 may be standardized, such that each stored OVER File credential utilizes the same fields in a similar manner. In some embodiments, the
20 credential display may be standardized based on the category in which the OVER File credential is stored. For example, a first standardized display may be used for all insurance credentials and a second standardized display may be used for all loyalty credentials. A credential title field 602 may display the name of the displayed credential. The credential name may be set by the issuing agency, by the user, or by the OVER File generation and verification engine 8. As shown in Fig. 9, the credential display 600 may comprise three text
25 sections, text section A 606, text section B 608, and text section C 610. Each text section may be configured to display textual information based on the type of credential selected for presentation. For example, a user may select a driver's license as the displayed OVER File credential. Text section A 606 may be configured to display the user's name as it appears
30 on the user's driver license. Text section B 608 may be configured to display the user's home address and birth date. Text section C 610 may be configured to display a driver's license identification number. Those skilled in the art will recognize that any suitable textual information may be displayed in any of the available text sections 606, 608, 610. In some embodiments, one or more of the text sections 606, 608, 610 may be configured to display
35 the same information regardless of the type of credential displayed. For example, text section C 610 may be configured to always display a credential identification number associated with the credential by the issuing agency. In some embodiments, an image field

604 may be included in the credential display 600. The image field 604 may be configured to display an image selected by the issuing agency, such as, for example, an image of a physical credential which forms the basis of the OVER File credential such as a driver's license, a logo of the issuing agency such as a corporate logo for a loyalty card, or any other image selected by the issuing agency. The image field 604 may display the selected image as a further validity check for the displayed OVER File credential.

An information code section 612 may be included in some embodiments of the credential display 600. As discussed above, an information code may be displayed by the OVER File storage client 500 for third-party verification of stored OVER File credentials. An information code, such as the information code 538 shown in Fig. 8, may be displayed with the selected OVER File credential in the information code section 612. By displaying the information code with other available credential information, the OVER File platform may facilitate easier verification, such as allowing a merchant to quickly establish whether an age restriction has been met prior to scanning the displayed information code. In addition, a third-party may ensure that the credential information received from the OVER File generation and verification engine 8 matches the OVER File credential displayed on the user device.

In some embodiments, one or more functions of the user device may be disabled when an OVER File credential is displayed on the user device. For example, a user device may be capable of taking a screenshot of the content displayed on the device screen. In order to prevent duplication of an OVER File credential outside of the OVER File management platform 2, the OVER File storage client 500 may disable the screenshot capability of the user device during the time that the OVER File credential is displayed on the user device. In some embodiments, all functions, with the exception of the display function, may be disabled for a predetermined period of time while the OVER File credential is displayed on the screen. For example, the OVER File credential may be displayed for a predetermined time period, such as 20 seconds, during which time all functions of the user device may be disabled. After the predetermined time period, the credential display 600 may revert to a previously displayed screen, such as the home screen 502, at which point the functions of the user device may be re-enabled.

Fig. 10 illustrates another embodiment of a credential display 700. The credential display 700 is similar to the credential display 600 shown in Fig. 9. The credential display 700 comprises the same fields as the credential display 600, such as the credential title 702, the image field 704, text section A 706, text section B 708, text section C 710, and information code section 712. The credential display 700 is oriented horizontally. In some embodiments, the OVER File storage client 500 may switch between the credential display 600 and the credential display 700 depending on the orientation of the user device. For

example, a user may hold a user device such that the user device is horizontally oriented. The credential display 600 may be displayed to match the orientation of the user device. If a user rotates the user device such that the user device is vertically oriented, the OVER File storage client 500 may display the credential display 700 to match the new orientation of the user device.

Fig. 11 illustrates one embodiment of a credential presentation and verification process 800. As discussed above, a user may display a selected credential on a user device 804 using the OVER File storage client 4. The displayed user credential may comprise a information code 838 and an image field 808. The image field 808 may display an image provided by the issuing agency, such as, for example, an image of a physical credential, an image of a user, or a logo of the issuing agency. The information code 806 may comprise a scannable code such as, for example, a barcode or a QR code, comprising a credential identifier. A third-party may use a third-party device 806 comprising the OVER File third party client 6 to scan the displayed information code 806. The third-party device 806 may contact the application gateway 824 to request verification of the OVER File credential identified by the credential identifier contained in the scanned information code 838. The application gateway 824 may contact the OVER File database 828 to verify the existence and validity of the requested OVER File. The OVER File database 828 may comprise the OVER File generation and verification engine 8. The OVER File database 828 may be in contact with an issuing agency database 830 to periodically update the validity and status of the OVER Files stored in the OVER File database 828. The application gateway 824 may provide a status indicator to the third-party device 804 indicating the validity of the requested credential. In one embodiment, if the status indicator indicates a valid credential, a response to the third party device 804 may comprise an image displayed in the image field 810 on the third party device 806. The displayed image may be the same image as displayed in the image field 808 of the user device 802. The third-party device may display the status indicator 812. A valid status indicator may be displayed as, for example, a checkmark indicating that the requested credential exists and is valid. In some embodiments, if the status indicator indicates an invalid credential, a response to the third party device may comprise a reason for the invalid response. The reason for the invalid response may be displayed in the image field 810. The status indicator 812 may display as, for example, an X indicating that the requested credential is invalid.

Fig. 12 illustrates one embodiment of a computing device 900 which can be used in one embodiment of the system and method for generating, storing, and displaying OVER Files and associated credentials. For the sake of clarity, the computing device 900 is shown and described here in the context of a single computing device. It is to be appreciated and understood, however, that any number of suitably configured computing devices can be

used to implement any of the described embodiments. For example, in at least some implementation, multiple communicatively linked computing devices are used. One or more of these devices can be communicatively linked in any suitable way such as via one or more networks (LANs), one or more wide area networks (WANs) or any combination thereof.

5 In this example, the computing device 900 comprises one or more processor circuits or processing units 902, on or more memory circuits and/or storage circuit component(s) 904 and one or more input/output (I/O) circuit devices 906. Additionally, the computing device 900 comprises a bus 908 that allows the various circuit components and devices to communicate with one another. The bus 908 represents one or more of any of several types
10 of bus structures, including a memory bus or local bus using any of a variety of bus architectures. The bus 908 may comprise wired and/or wireless buses.

 The processing unit 902 may be responsible for executing various software programs such as system programs, applications programs, and /or module to provide computing and processing operations for the computing device 900. The processing unit 902 may be
15 responsible for performing various voice and data communications operations for the computing device 900 such as transmitting and receiving voice and data information over one or more wired or wireless communication channels. Although the processing unit 902 of the computing device 900 includes single processor architecture as shown, it may be appreciated that the computing device 900 may use any suitable processor architecture
20 and/or any suitable number of processors in accordance with the described embodiments. In one embodiment, the processing unit 900 may be implemented using a single integrated processor.

 The processing unit 902 may be implemented as a host central processing unit (CPU) using any suitable processor circuit or logic device (circuit), such as a as a general-
25 purpose processor. The processing unit 902 also may be implemented as a chip multiprocessor (CMP), dedicated processor, embedded processor, media processor, input/output (I/O) processor, co-processor, microprocessor, controller, microcontroller, application specific integrated circuit (ASIC), field programmable gate array (FPGA), programmable logic device (PLD), or other processing device in accordance with the
30 described embodiments.

 As shown, the processing unit 902 may be coupled to the memory and/or storage component(s) 904 through the bus 908. The memory bus 908 may comprise any suitable interface and/or bus architecture for allowing the processing unit 902 to access the memory and/or storage component(s) 904. Although the memory and/or storage component(s) 904
35 may be shown as being separate from the processing unit 902 for purposes of illustration, it is worthy to note that in various embodiments some portion or the entire memory and/or storage component(s) 904 may be included on the same integrated circuit as the processing

unit 902. Alternatively, some portion or the entire memory and/or storage component(s) 904 may be disposed on an integrated circuit or other medium (e.g., hard disk drive) external to the integrated circuit of the processing unit 902. In various embodiments, the computing device 900 may comprise an expansion slot to support a multimedia and/or memory card, for example.

The memory and/or storage component(s) 904 represent one or more computer-readable media. The memory and/or storage component(s) 904 may be implemented using any computer-readable media capable of storing data such as volatile or non-volatile memory, removable or non-removable memory, erasable or non-erasable memory, writeable or re-writeable memory, and so forth. The memory and/or storage component(s) 904 may comprise volatile media (e.g., random access memory (RAM)) and/or nonvolatile media (e.g., read only memory (ROM), Flash memory, optical disks, magnetic disks and the like). The memory and/or storage component(s) 904 may comprise fixed media (e.g., RAM, ROM, a fixed hard drive, etc.) as well as removable media (e.g., a Flash memory drive, a removable hard drive, an optical disk, etc.). Examples of computer-readable storage media may include, without limitation, RAM, dynamic RAM (DRAM), Double-Data-Rate DRAM (DDRAM), synchronous DRAM (SDRAM), static RAM (SRAM), read-only memory (ROM), programmable ROM (PROM), erasable programmable ROM (EPROM), electrically erasable programmable ROM (EEPROM), flash memory (e.g., NOR or NAND flash memory), content addressable memory (CAM), polymer memory (e.g., ferroelectric polymer memory), phase-change memory, ovonic memory, ferroelectric memory, silicon-oxide-nitride-oxide-silicon (SONOS) memory, magnetic or optical cards, or any other type of media suitable for storing information.

The one or more I/O devices 906 allow a user to enter commands and information to the computing device 900, and also allow information to be presented to the user and/or other components or devices. Examples of input devices include a keyboard, a cursor control device (e.g., a mouse), a microphone, a scanner, biometric sensors, and the like. Examples of output devices include a display device (e.g., a monitor or projector, speakers, a printer, a network card, etc.). The computing device 900 may comprise an alphanumeric keypad coupled to the processing unit 902. The keypad may comprise, for example, a QWERTY key layout and an integrated number dial pad. The computing device 900 may comprise a display coupled to the processing unit 902. The display may comprise any suitable visual interface for displaying content to a user of the computing device 4000. In one embodiment, for example, the display may be implemented by a liquid crystal display (LCD) such as a touch-sensitive color (e.g., 76-bit color) thin-film transistor (TFT) LCD screen. The touch-sensitive LCD may be used with a stylus and/or a handwriting recognizer program.

The processing unit 902 may be arranged to provide processing or computing resources to the computing device 900. For example, the processing unit 902 may be responsible for executing various software programs including system programs such as operating system (OS) and application programs. System programs generally may assist in the running of the computing device 900 and may be directly responsible for controlling, integrating, and managing the individual hardware components of the computer system. The OS may be implemented, for example, as a Microsoft® Windows OS, Symbian OSTM, Embedix OS, Linux OS, Binary Run-time Environment for Wireless (BREW) OS, JavaOS, Android OS, Apple OS or other suitable OS in accordance with the described embodiments. The computing device 900 may comprise other system programs such as device drivers, programming tools, utility programs, software libraries, application programming interfaces (APIs), and so forth.

The computer 900 also includes a network interface 910 coupled to the bus 908. The network interface 910 provides a two-way data communication coupling to a local network 912. For example, the network interface 910 may be a digital subscriber line (DSL) modem, satellite dish, an integrated services digital network (ISDN) card or other data communication connection to a corresponding type of telephone line. As another example, the communication interface 910 may be a local area network (LAN) card effecting a data communication connection to a compatible LAN. Wireless communication means such as internal or external wireless modems may also be implemented.

In any such implementation, the network interface 910 sends and receives electrical, electromagnetic or optical signals that carry digital data streams representing various types of information, such as the selection of goods to be purchased, the information for payment of the purchase, or the address for delivery of the goods. The network interface 910 typically provides data communication through one or more networks to other data devices. For example, the network interface 910 may effect a connection through the local network to an Internet Host Provider (ISP) or to data equipment operated by an ISP. The ISP in turn provides data communication services through the internet (or other packet-based wide area network). The local network and the internet both use electrical, electromagnetic or optical signals that carry digital data streams. The signals through the various networks and the signals on the network interface 910, which carry the digital data to and from the computer system 400, are exemplary forms of carrier waves transporting the information.

The computer 900 can send messages and receive data, including program code, through the network(s) and the network interface 910. In the Internet example, a server might transmit a requested code for an application program through the internet, the ISP, the local network (the network 912) and the network interface 910. In accordance with the invention, one such downloaded application provides for the identification and analysis of a

prospect pool and analysis of marketing metrics. The received code may be executed by processor 904 as it is received, and/or stored in storage device 910, or other non-volatile storage for later execution. In this manner, computer 900 may obtain application code in the form of a carrier wave.

5 In various embodiments, a computer-implemented method for generating and verifying officially verifiable electronic representations may be disclosed. The method may comprise receiving, by a credential database, a request for a credential action. The credential database may be configured to store one or more credentials comprising a status indicator. The method may further comprise determining, by the credential database, a
10 response to the credential action based on the one or more user credentials stored in the credential database and transmitting, by the credential database, the response to a client device. The credential action may comprise generating a credential. The credential may be generated when the credential database determines that no matching credential is stored in the credential database.

15 In some embodiments, generation of a credential may comprise requesting, by the credential database, the credential from an issuing agency database. The issuing agency database may be configured to store credentials issued by an issuing agency. The method may further comprise receiving, by the credential database, the status indicator and credential information associated with the credential transmitted by the issuing agency
20 database and storing the credential and the status indicator in the credential database. The credential information may comprise the credential, and wherein the status indicator indicates a valid credential. The response transmitted to the user device may comprise the credential and a copy of the credential may be stored in the credential database. The credential database may generate a device identifier for the credential. The device identifier
25 may limit the credential to the client device. The status indicator may indicate an invalid credential. When the status indicator indicates an invalid credential, the response transmitted to the user device may comprise the status indicator. In some embodiments, the validity of the credential may additionally depend upon other information submitted by the client, such as, for example, biometric, location, password, device identifiers, and/or other
30 user-specific information.

 The credential action may comprise checking a status indicator of a stored credential. The request for the credential action may comprise a credential identifier. The credential response may be determined by comparing the credential identifier with the one or more credentials stored in the credential database. When the credential identifier matches a
35 stored credential, the response to the request for the credential action may comprises the status indicator of the stored credential and may further comprise a portion of the stored

credential. When the credential identifier does not match a stored credential, the response to the request for the credential action comprises an invalid credential response.

In various embodiments, a computer-implemented method for requesting an officially verifiable electronic representation is disclosed. The method may comprise generating, a
5 processor, a request for a credential action. The request may comprise a credential identifier. The method may further comprise transmitting, by the processor, the request for the credential action to a credential database and receiving, by the processor, a response to the request for the credential action. The request for credential action may comprise a credential generation.

10 In some embodiments a scanner may scan an information code comprising the credential identifier. The response to the request for the credential action may comprise a generated credential. The generated credential may comprise the credential identifier and additional credential information. The additional credential information may be obtained, for example, from the issuing agency database. The generated credential may comprise a
15 device identifier. The device identifier may limit the generated credential to the processor. The request for the credential action may comprise a credential verification request. The response to the request for the credential action may comprise a status indicator. When the status indicator indicates a valid credential, the response to the request for the credential action may comprise a credential image. When the status indicator indicates an invalid
20 credential, the response to the request for the credential action may comprise an invalidity response identifying a reason for the invalid credential.

In various embodiments, an apparatus for generating and verifying officially verifiable electronic representations is disclosed. The apparatus may comprise a processor and a memory unit operatively coupled to the processor. The memory unit may be configured to
25 store a plurality of instructions, wherein the instructions are configured to program the processor. The processor may be programmed to maintain a credential database. The credential database may be configured to store one or more credentials comprising a status indicator. The credential database may be configured to store pointers to other data stores and/or services accessible via a network. The processor may further receive a request for a
30 credential action and determine a response to the credential action based on the one or more user credentials stored in the credential database. The processor may be programmed to transmit the response to a client device.

In some embodiments, generation of a credential may comprise generating a request for the credential from an issuing agency database. The issuing agency database may be
35 configured to store credentials issued by an issuing agency. The processor may receive the status indicator and credential information associated with the credential transmitted by the issuing agency database and may store the credential and the status indicator in the

memory unit. The credential information may comprise the credential when the status indicator indicates a valid credential. The response transmitted to the user device may comprise the credential and a copy of the credential may be stored in the memory unit. The processor may generate a device identifier for the credential. The device identifier may limit
5 the credential to the client device. The status indicator may indicate an invalid credential. When the status indicator indicates an invalid credential, the response transmitted to the user device may comprise the status indicator.

The credential action may comprise checking a status indicator of a stored credential. The request for the credential action may comprise a credential identifier. The credential
10 response may be determined by comparing the credential identifier with the one or more credentials stored in the memory unit. In some embodiments, the response may additionally be determined by comparing other information submitted by the client, such as, for example, location, biometric information, and/or device identifiers, with stored credentials. When the credential identifier matches a stored credential, the response to the request for the
15 credential action may comprise the status indicator of the stored credential and may further comprise a portion of the stored credential. When the credential identifier does not match a stored credential, the response to the request for the credential action comprises an invalid credential response.

Various embodiments may be described herein in the general context of computer
20 executable instructions, such as software, program modules, and/or engines being executed by a computer. Generally, software, program modules, and/or engines include any software element arranged to perform particular operations or implement particular abstract data types. Software, program modules, and/or engines can include routines, programs, objects, components, data structures and the like that perform particular tasks or implement
25 particular abstract data types. An implementation of the software, program modules, and/or engines components and techniques may be stored on and/or transmitted across some form of computer-readable media. In this regard, computer-readable media can be any available medium or media useable to store information and accessible by a computing device. Some embodiments also may be practiced in distributed computing environments where
30 operations are performed by one or more remote processing devices that are linked through a communications network. In a distributed computing environment, software, program modules, and/or engines may be located in both local and remote computer storage media including memory storage devices.

Although some embodiments may be illustrated and described as comprising
35 functional components, software, engines, and/or modules performing various operations, it can be appreciated that such components or modules may be implemented by one or more hardware components, software components, and/or combination thereof. The functional

components, software, engines, and/or modules may be implemented, for example, by logic (e.g., instructions, data, and/or code) to be executed by a logic device (e.g., processor).

Such logic may be stored internally or externally to a logic device on one or more types of computer-readable storage media. In other embodiments, the functional components such as software, engines, and/or modules may be implemented by hardware elements that may include processors, microprocessors, circuits, circuit elements (e.g., transistors, resistors, capacitors, inductors, and so forth), integrated circuits, application specific integrated circuits (ASIC), programmable logic devices (PLD), digital signal processors (DSP), field programmable gate array (FPGA), logic gates, registers, semiconductor device, chips, microchips, chip sets, and so forth.

Examples of software, engines, and/or modules may include software components, programs, applications, computer programs, application programs, system programs, machine programs, operating system software, middleware, firmware, software modules, routines, subroutines, functions, methods, procedures, software interfaces, application program interfaces (API), instruction sets, computing code, computer code, code segments, computer code segments, words, values, symbols, or any combination thereof. Determining whether an embodiment is implemented using hardware elements and/or software elements may vary in accordance with any number of factors, such as desired computational rate, power levels, heat tolerances, processing cycle budget, input data rates, output data rates, memory resources, data bus speeds and other design or performance constraints.

In some cases, various embodiments may be implemented as an article of manufacture. The article of manufacture may include a computer readable storage medium arranged to store logic, instructions and/or data for performing various operations of one or more embodiments. In various embodiments, for example, the article of manufacture may comprise a magnetic disk, optical disk, flash memory or firmware containing computer program instructions suitable for execution by a general purpose processor or application specific processor. The embodiments, however, are not limited in this context.

The functions of the various functional elements, logical blocks, modules, and circuits elements described in connection with the embodiments disclosed herein may be implemented in the general context of computer executable instructions, such as software, control modules, logic, and/or logic modules executed by the processing unit. Generally, software, control modules, logic, and/or logic modules comprise any software element arranged to perform particular operations. Software, control modules, logic, and/or logic modules can comprise routines, programs, objects, components, data structures and the like that perform particular tasks or implement particular abstract data types. An implementation of the software, control modules, logic, and/or logic modules and techniques may be stored on and/or transmitted across some form of computer-readable media. In this regard,

computer-readable media can be any available medium or media useable to store information and accessible by a computing device. Some embodiments also may be practiced in distributed computing environments where operations are performed by one or more remote processing devices that are linked through a communications network. In a distributed computing environment, software, control modules, logic, and/or logic modules may be located in both local and remote computer storage media including memory storage devices.

Additionally, it is to be appreciated that the embodiments described herein illustrate example implementations, and that the functional elements, logical blocks, modules, and circuits elements may be implemented in various other ways which are consistent with the described embodiments. Furthermore, the operations performed by such functional elements, logical blocks, modules, and circuits elements may be combined and/or separated for a given implementation and may be performed by a greater number or fewer number of components or modules. As will be apparent to those of skill in the art upon reading the present disclosure, each of the individual embodiments described and illustrated herein has discrete components and features which may be readily separated from or combined with the features of any of the other several aspects without departing from the scope of the present disclosure. Any recited method can be carried out in the order of events recited or in any other order which is logically possible.

It is worthy to note that any reference to “one embodiment” or “an embodiment” means that a particular feature, structure, or characteristic described in connection with the embodiment is comprised in at least one embodiment. The appearances of the phrase “in one embodiment” or “in one aspect” in the specification are not necessarily all referring to the same embodiment.

Unless specifically stated otherwise, it may be appreciated that terms such as “processing,” “computing,” “calculating,” “determining,” or the like, refer to the action and/or processes of a computer or computing system, or similar electronic computing device, such as a general purpose processor, a DSP, ASIC, FPGA or other programmable logic device, discrete gate or transistor logic, discrete hardware components, or any combination thereof designed to perform the functions described herein that manipulates and/or transforms data represented as physical quantities (e.g., electronic) within registers and/or memories into other data similarly represented as physical quantities within the memories, registers or other such information storage, transmission or display devices.

It is worthy to note that some embodiments may be described using the expression “coupled” and “connected” along with their derivatives. These terms are not intended as synonyms for each other. For example, some embodiments may be described using the terms “connected” and/or “coupled” to indicate that two or more elements are in direct

physical or electrical contact with each other. The term “coupled,” however, also may mean that two or more elements are not in direct contact with each other, but yet still co-operate or interact with each other. With respect to software elements, for example, the term “coupled” may refer to interfaces, message interfaces, application program interface (API), exchanging
5 messages, and so forth.

CLAIMS

What is claimed is:

1. A computer-implemented method for generating and verifying officially verifiable
5 electronic representations, the method comprising:
receiving, by a credential engine executed by a processor, a request for a credential
action;
determining, by the credential engine, a response to the credential action based on
the one or more user credentials; and
10 transmitting, by the processor, the response to the credential action.
2. The computer-implemented method of claim 1, comprising storing, by the credential
engine, one or more credentials.
- 15 3. The computer-implemented method of claim 2, generating, by the credential engine,
a credential, wherein the credential is generated when the credential engine determines that
no matching credential is stored.
4. The computer-implemented method of claim 3, comprising:
20 requesting, by the credential engine, the credential from an issuing agency, wherein
the issuing agency stores credentials issued by the issuing agency;
receiving, by the credential engine, the status indicator and credential information
associated with the credential transmitted by the issuing agency;
storing, by the credential engine, the status indicator.
25
5. The computer-implemented method of claim 4, receiving, by the credential engine,
credential information comprising the credential, wherein the status indicator indicates a
valid credential.
- 30 6. The computer-implemented method of claim 5, comprising storing, by the credential
engine, the credential, and wherein the response transmitted to the client device comprises
the credential.
7. The computer-implemented method of claim 6, comprising generating, by the
35 credential engine, a device identifier for the credential, wherein the device identifier limits the
credential to the client device.

8. The computer-implemented method of claim 4, wherein the status indicator indicates an invalid credential and the credential information indicates the reason for the invalid credential, and wherein the response transmitted to the client device comprises the status indicator and the credential information.

5

9. The computer-implemented method of claim 2, comprising generating, by the credential engine, a reference to a remotely stored credential, wherein the one or more credentials stored by the credential engine comprise the reference to the one or more remotely stored credentials.

10

10. The computer-implemented method of claim 2, comprising storing, by the credential engine, user-specific information.

11. The computer-implemented method of claim 10, comprising storing, by the credential engine, the user specific-information selected from the group consisting of: biometric information, location information, a password, a device identifier.

15

12. The computer-implemented method of claim 1, comprising checking, by the credential engine, a status indicator of a stored credential, wherein the request for the credential action comprises a credential identifier.

20

13. The computer-implemented method of claim 12, comprising determining, by the credential engine, the credential response by comparing the credential identifier with the one or more stored credentials.

25

14. The computer-implemented method of claim 13, comprising generating, by the credential engine, the response to the request for the credential action comprising the status indicator of the stored credential when the credential identifier matches a stored credential.

15. The computer-implemented method of claim 14, comprising generating, by the credential engine, the response to the request for the credential action comprising a portion of the stored credential.

30

16. The computer-implemented method of claim 13, comprising generating, by the credential engine, the response to the request for the credential action comprising an invalid credential identifier when the credential identifier does not match a stored credential,.

35

17. A computer-implemented method for requesting an officially verifiable electronic representation, the method comprising:

generating, by a processor, a request for a credential action comprising a credential identifier;

5 transmitting, by the processor, the request for the credential action to a credential engine;

receiving, by the processor, a response to the request for the credential action.

18. The computer-implemented method of claim 17, wherein the requested credential
10 action comprises generating a credential.

19. The computer-implemented method of claim 18, comprising scanning, by a scanner, an information code comprising the credential identifier.

15 20. The computer-implemented method of claim 18, wherein the response to the request for the credential action comprises a generated credential comprising the credential identifier and additional credential information.

21. The computer-implemented method of claim 20, wherein the generated credential
20 comprises a device identifier, wherein the device identifier limits the generated credential to the processor.

22. The computer-implemented method of claim 17, comprising:

collecting, by the processor, user-specific information; and

25 transmitting, by the processor, the user-specific information to a credential engine, wherein the user-specific information is included in the request for a credential action.

23. The computer-implemented method of claim 17, wherein the request for the credential action comprises a credential verification request, and wherein the response to the request for the credential action comprises a status indicator.

30

24. The computer-implemented method of claim 23, wherein when the status indicator indicates a valid credential, the response to the request for the credential action comprises a credential image.

35 25. The computer-implemented method of claim 23, wherein when the status indicator indicates an invalid credential, the response to the request for the credential action comprises a reason for the invalid credential.

26. An apparatus for generating and verifying officially verifiable electronic representations, the apparatus comprising:

a processor;

a memory unit operatively coupled to the processor, the memory unit configured to
5 store a plurality of instructions, wherein the instructions are configured to program the processor to:

execute a credential engine, wherein the credential engine is configured to receive a request for a credential action;

receive the request for a credential action;

10 determine a response to the credential action based on one or more stored user credentials; and

transmit the response to a client device.

27. The apparatus of claim 26, wherein the credential action comprises generating a
15 credential, wherein the credential is generated when the processor determines that no matching credential is stored.

28. The apparatus of claim 27, wherein the instructions are configured to program the processor to:

20 request the credential from an issuing agency, wherein the issuing agency stores credentials issued by an issuing agency;

receive the status indicator and credential information associated with the credential transmitted by the issuing agency; and

store the credential and the status indicator.

29. The apparatus of claim 28, wherein the credential information comprises the credential, and wherein the status indicator indicates a valid credential.

30. The apparatus of claim 28, wherein the credential information comprises user-specific information.

31. The apparatus of claim 30, wherein the user-specific information is selected from the group consisting of: biometric information, location information, a password, a device identifier.

32. The apparatus of claim 29, wherein the response transmitted to the user device comprises the credential.

33. The apparatus of claim 32, wherein the instructions are configured to program the processor to generate a device identifier for the credential, wherein the device identifier limits the credential to the client device.

5

34. The apparatus of claim 28, wherein the status indicator indicates an invalid credential, and wherein the response transmitted to the user device comprises the status indicator.

10

35. The apparatus of claim 28, wherein the stored credential comprises a reference to a remotely stored credential.

15

36. The apparatus of claim 28, wherein the credential action comprises checking, by the processor, a status indicator of a stored credential, wherein the request for the credential action comprises a credential identifier.

37. The apparatus of claim 36, wherein the credential response is determined by comparing the credential identifier with the one or more stored credentials.

20

38. The apparatus of claim 37, wherein when the credential identifier matches a stored credential, the response to the request for the credential action comprises the status indicator of the stored credential.

25

39. The apparatus of claim 38, wherein when the credential identifier does not match a stored credential, the response to the request for the credential action comprises an invalid credential response.

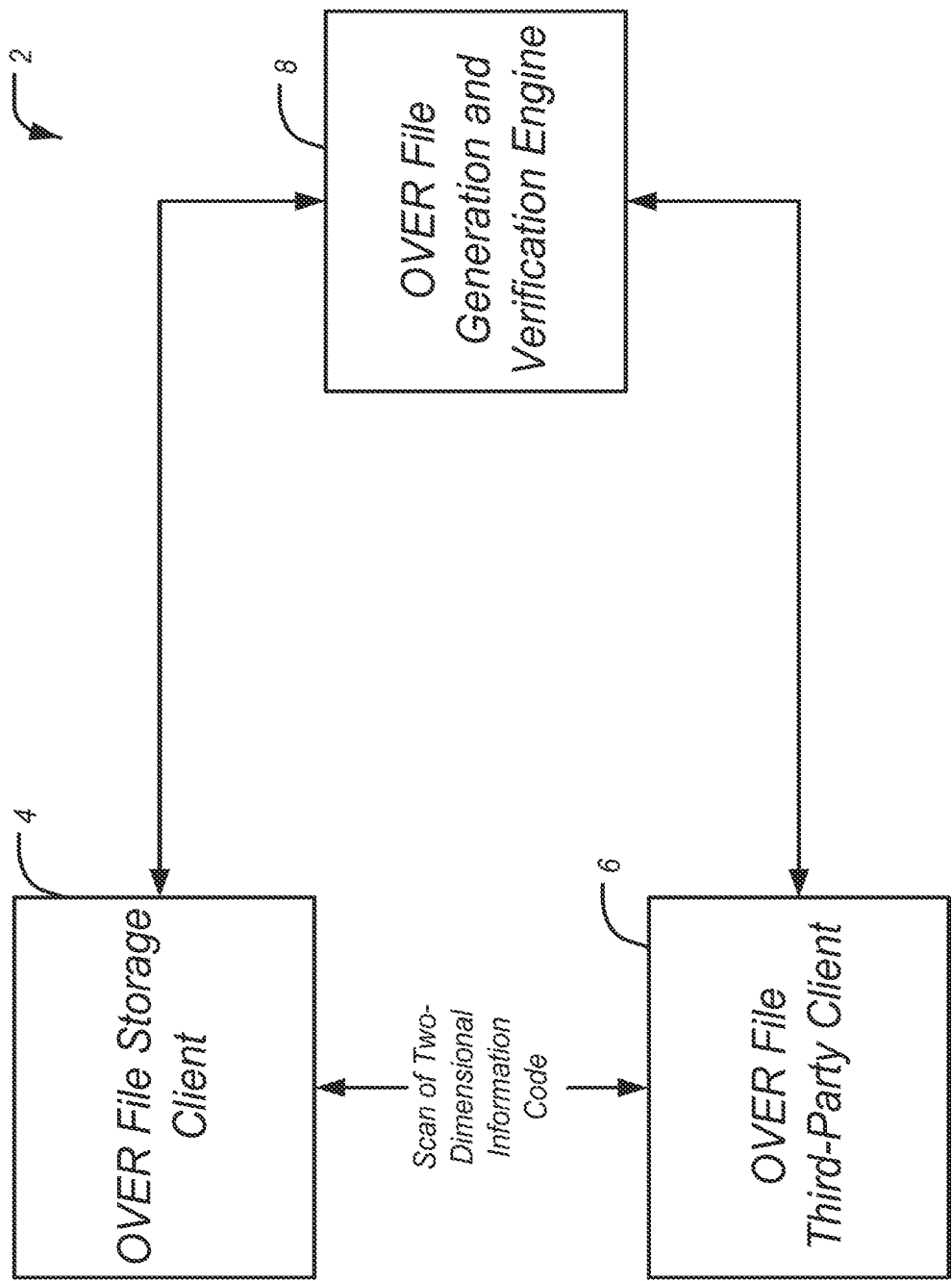


Fig. 1

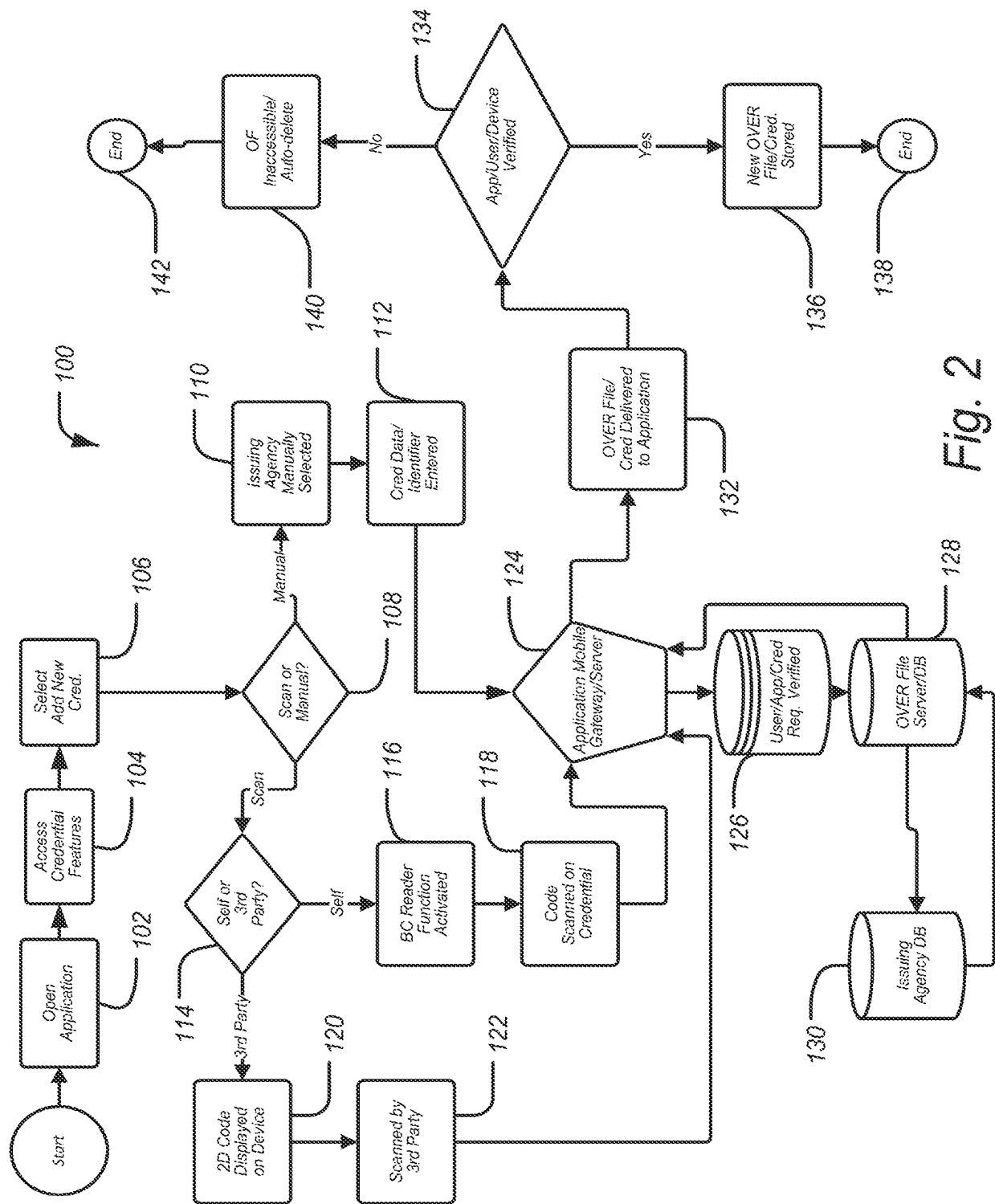
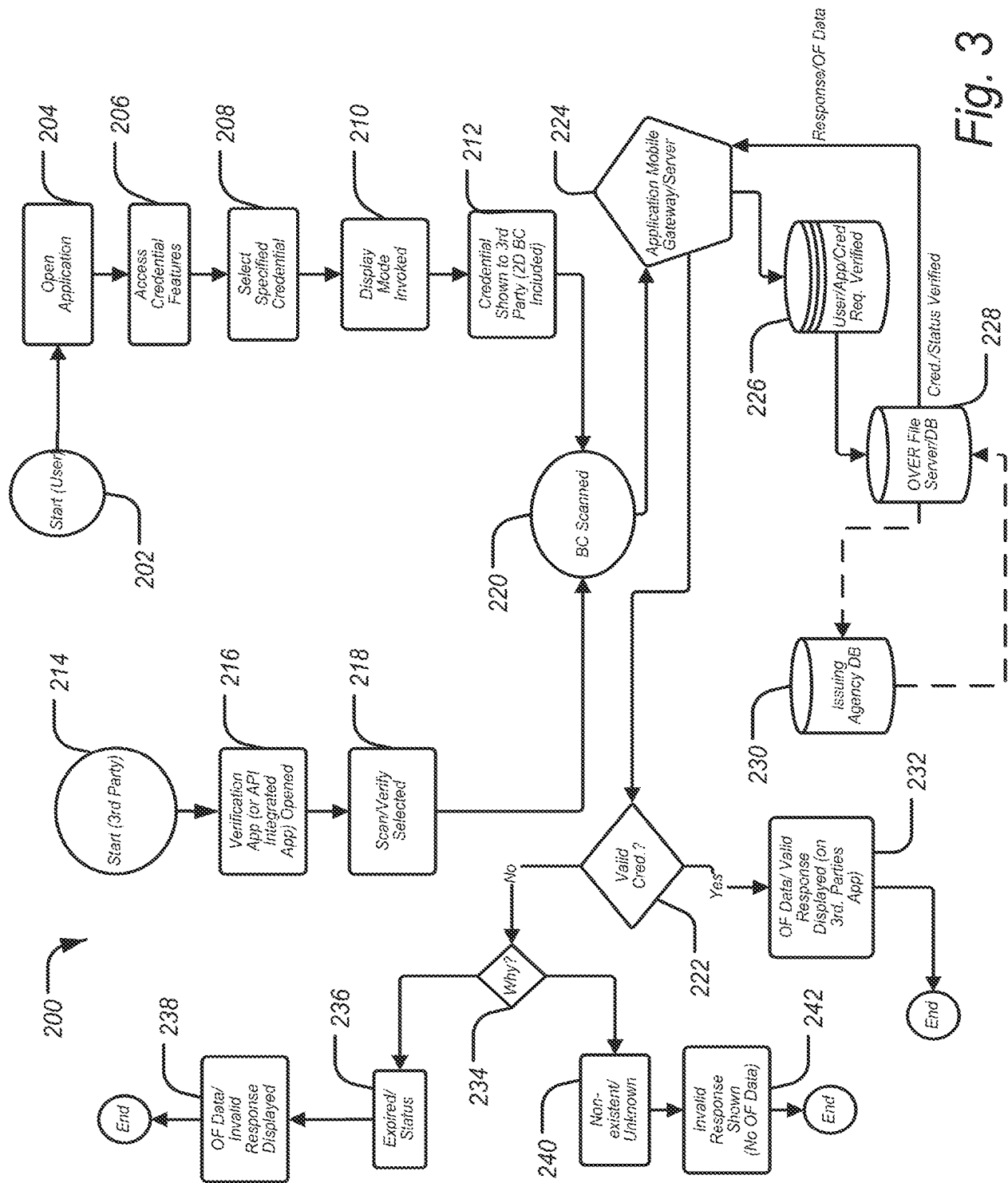


Fig. 2



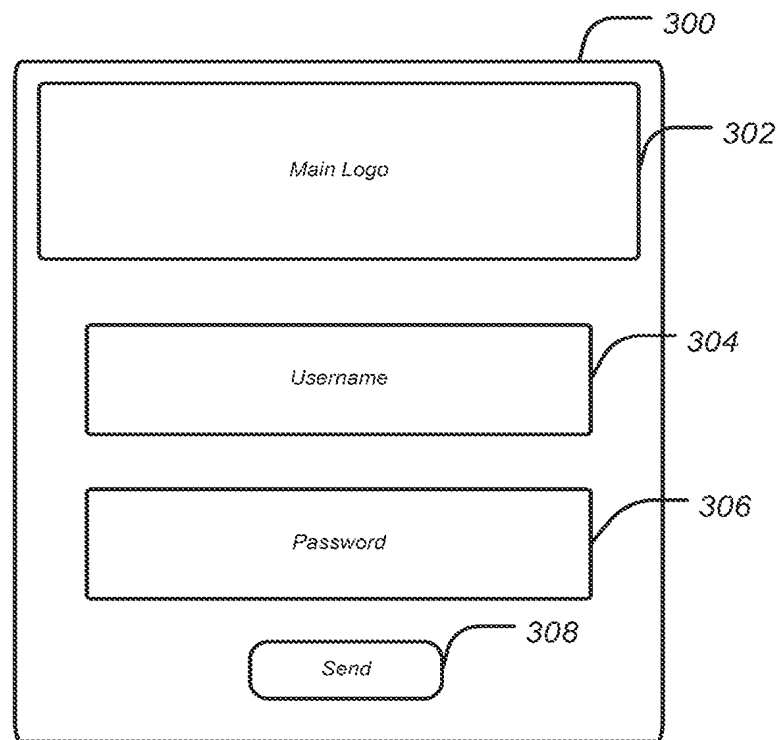


Fig. 4

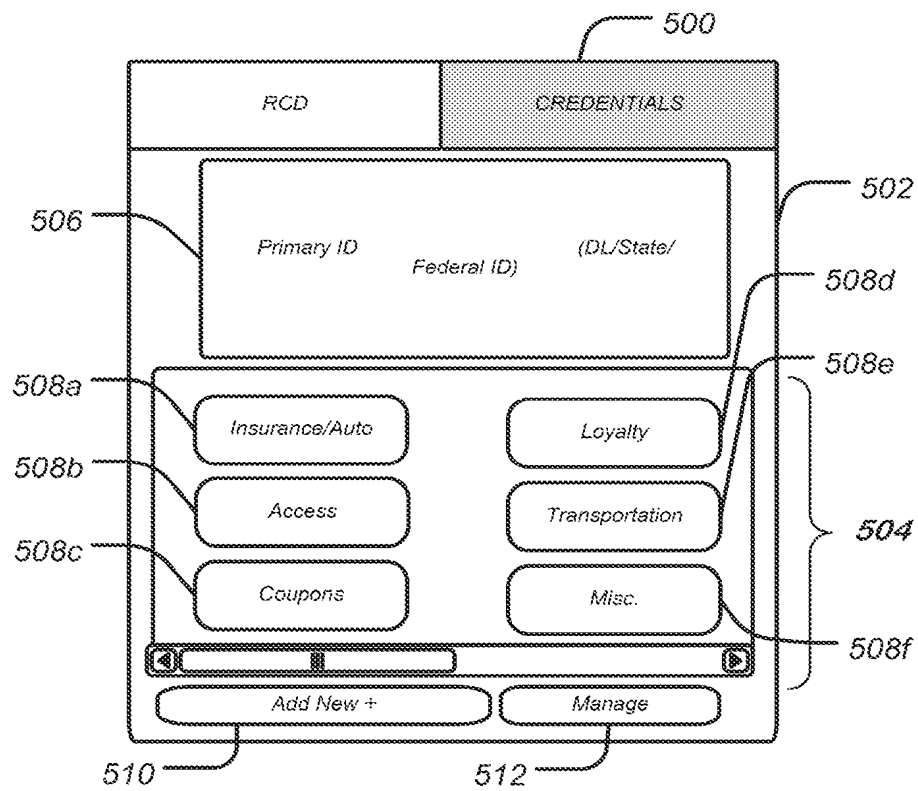
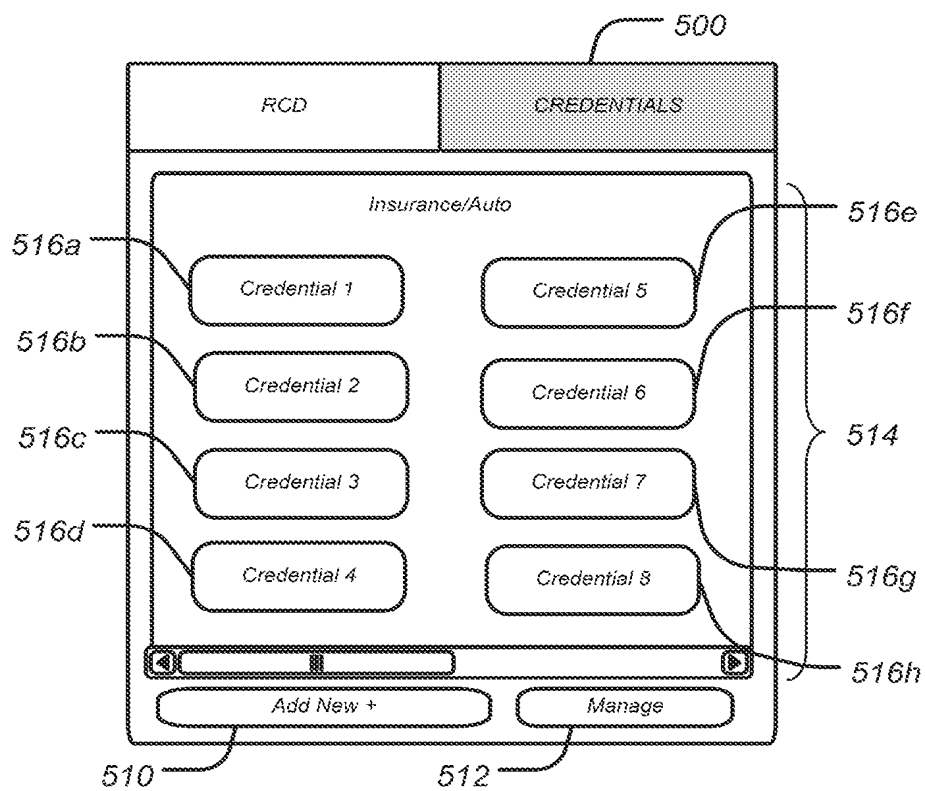


Fig. 5

*Fig. 6*

500

RCD	CREDENTIALS
Credential Name	User Selected Name
Category	Automatic
Issuer Type	Restaurant
Issuer	Submart
Credential Number	Text
518	
530	532
Scan to Add	Add
	534
	Back

Fig. 7

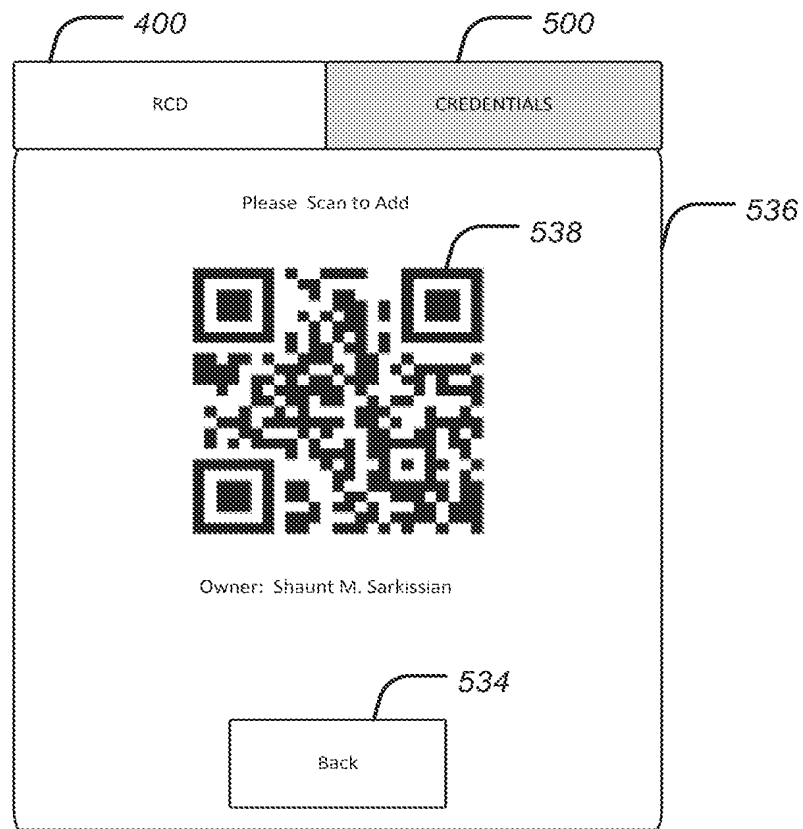


Fig. 8

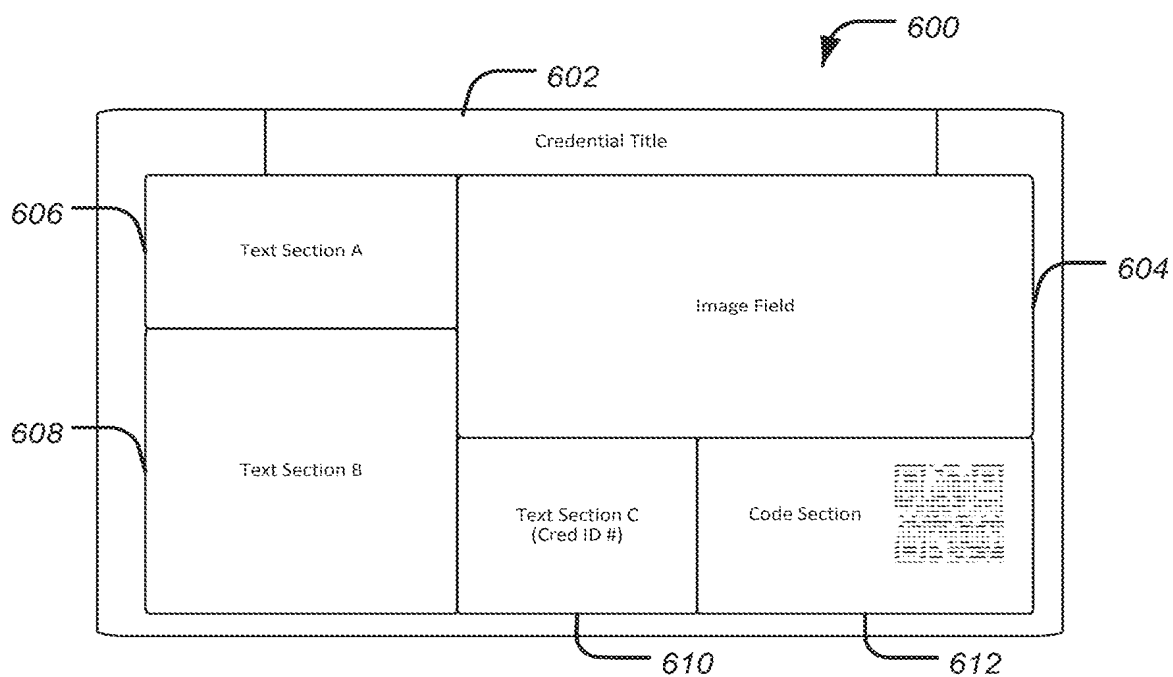
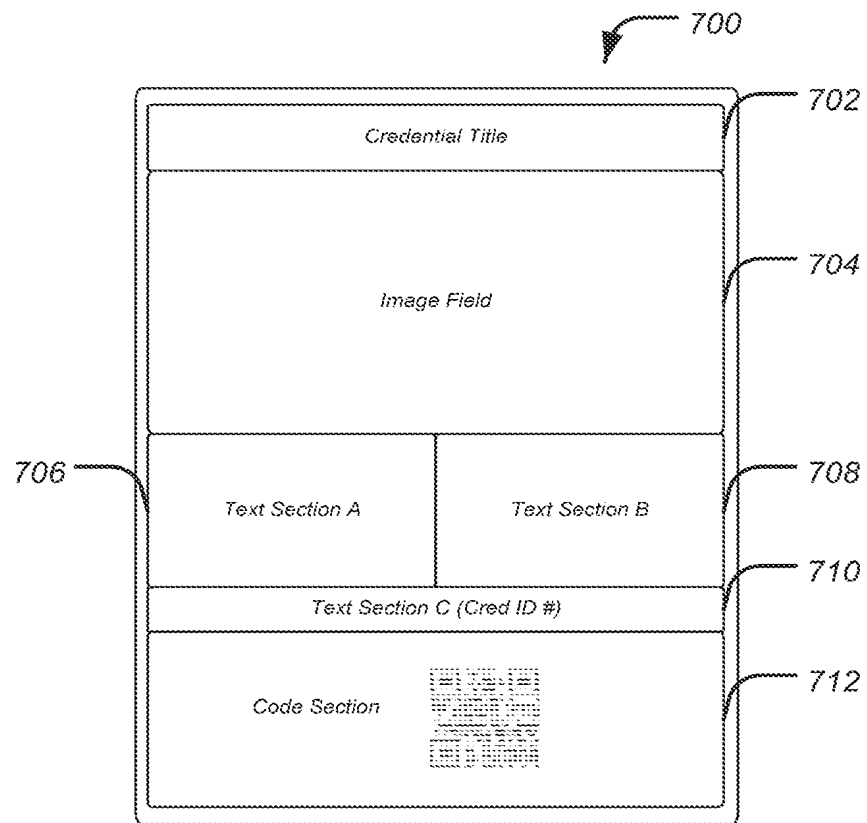


Fig. 9

*Fig. 10*

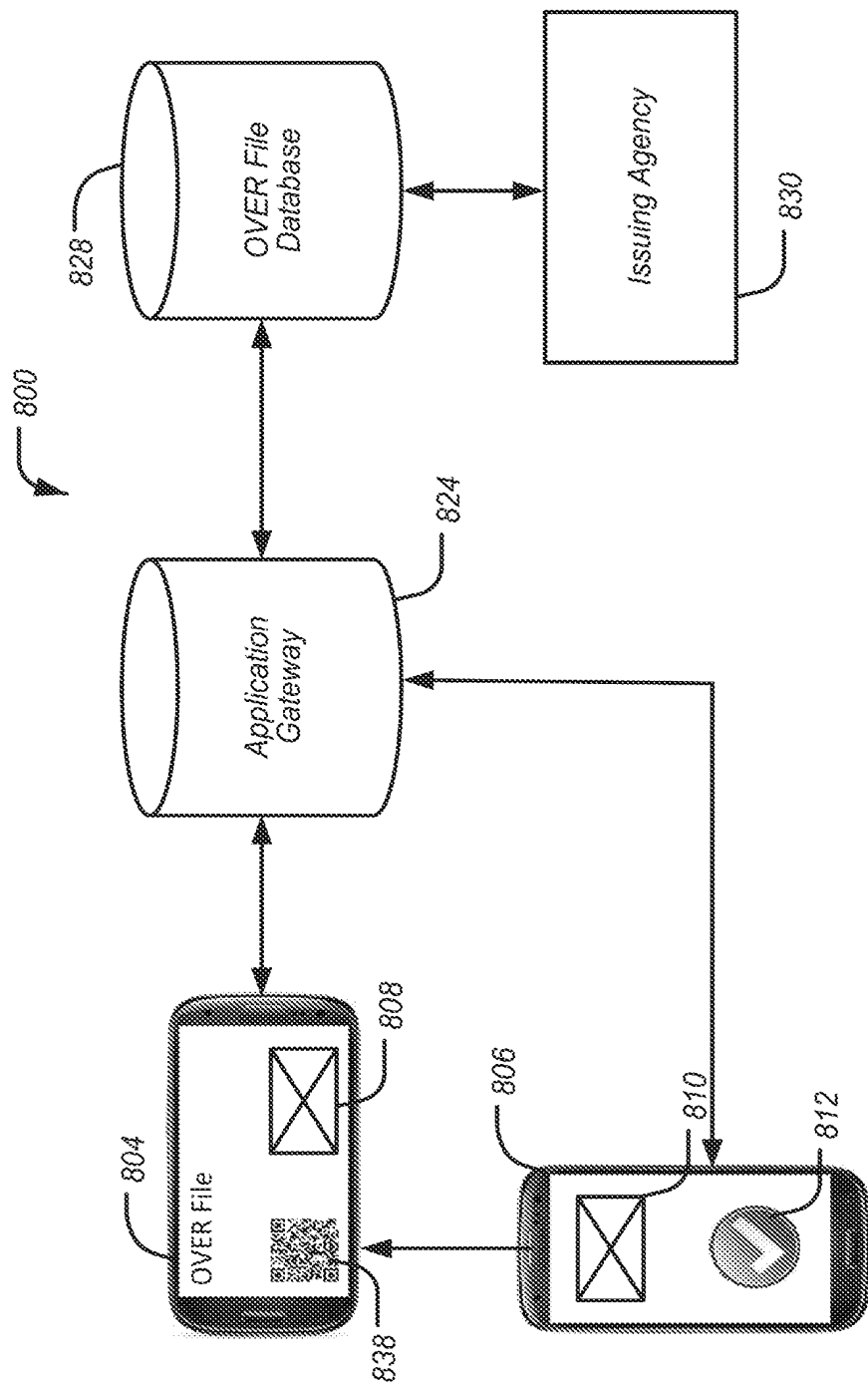
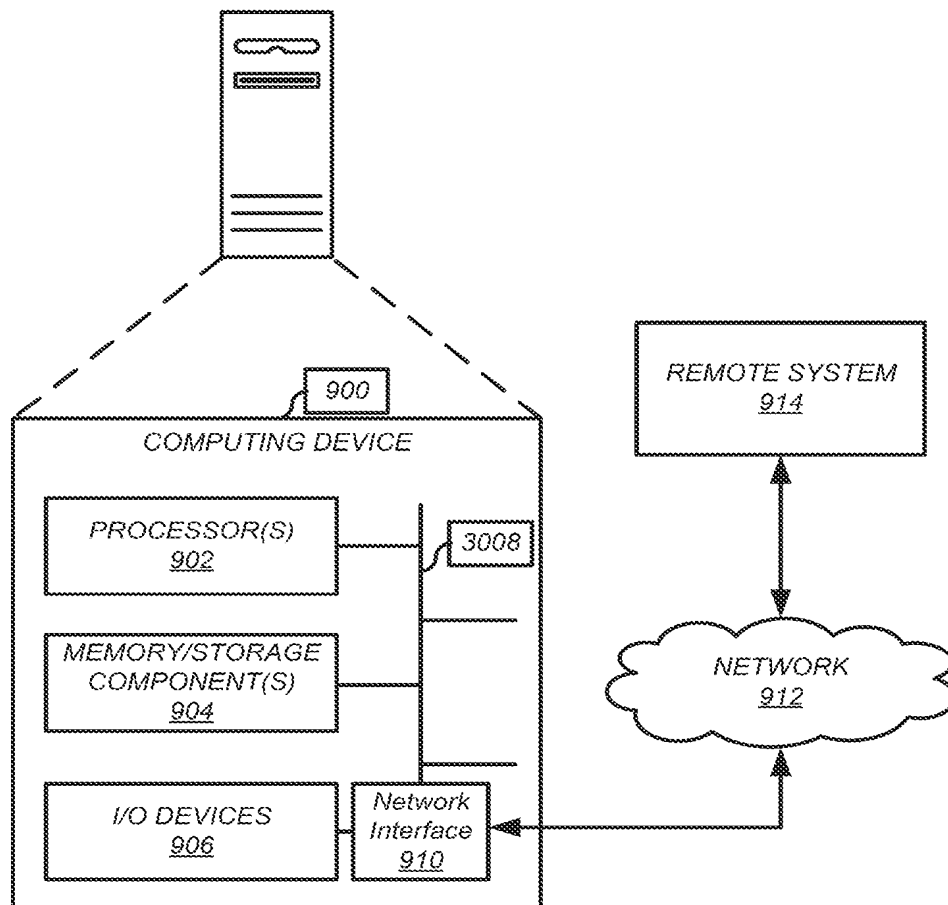


Fig. 11

*Fig. 12*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2013/077010**A. CLASSIFICATION OF SUBJECT MATTER****G06F 21/30(2013.01)i, G06F 17/21(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)

G06F 21/30; H04L 9/14; H04W 8/20; G06F 17/00; G06Q 30/00; H04L 9/32; H04W 12/06; G06F 21/22; G06F 17/21

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

Japanese utility models and applications for utility models

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

eKOMPASS(KIPO internal) & keywords: credential engine, verifying, user credential, store, request, matching, issuing agency, status indicator, identifier

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	KR 10-2011-0130002 A (KOREA FINANCIAL TELECOMM. & AMP.) 05 December 2011 See paragraphs [0026]–[0046]; and figure 1.	17–25
Y		1–16, 26–39
Y	KR 10-2011-0126269 A (SAMSUNG SDS CO., LTD.) 23 November 2011 See paragraphs [0016]–[0020]; claim 1; and figure 1.	1–16, 26–39
A	US 2010-0250389 A1 (THOMAS AUGUSTIN et al.) 30 September 2010 See paragraphs [0046]–[0059]; and figure 2.	1–39
A	KR 10-1091410 B1 (LG ELECTRONICS INC.) 07 February 2011 See paragraphs [0011]–[0021]; and figures 1–2.	1–39
A	WO 2008-018744 A1 (KOREA INSTITUTE FOR ELECTRONIC COMMERCE) 14 February 2008 See paragraphs [0044]–[0062]; and figure 1.	1–39

☐ 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

"I" 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

16 April 2014 (16.04.2014)

Date of mailing of the international search report

17 April 2014 (17.04.2014)

Name and mailing address of the ISA/KR

International Application Division
Korean Intellectual Property Office
189 Cheongsu-ro, Seo-gu, Daejeon Metropolitan City, 302-701,
Republic of Korea

Facsimile No. +82-42-472-7140

Authorized officer

AHN, Jeong Hwan

Telephone No. +82-42-481-8440



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2013/077010

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
KR 10-2011-0130002 A	05/12/2011	None	
KR 10-2011-0126269 A	23/11/2011	None	
US 2010-0250389 A1	30/09/2010	CN 101854245 A EP 2237182 A1 JP 2010-244542 A KR 10-2010-0109472 A	06/10/2010 06/10/2010 28/10/2010 08/10/2010
KR 10-1091410 B1	07/12/2011	None	
WO 2008-018744 A1	14/02/2008	CN 101326517 A CN 101326517 B EP 1917604 A1 EP 1917604 A4 JP 04918092 B2 JP 2009-512001 A KR 10-0816184 B1 KR 10-2008-0014194 A US 2009-0307756 A1 US 8132237 B2	17/12/2008 02/06/2010 07/05/2008 09/03/2011 18/04/2012 19/03/2009 21/03/2008 14/02/2008 10/12/2009 06/03/2012

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

RECEIVED

To:

TARR, DANIEL J

K&L GATES LLP K&L GATES CENTER 210 SIXTH
AVENUE PITTSBURGH PENNSYLVANIA 15222-2613 USA

PCT

APR 23 2014

NOTIFICATION OF TRANSMITTAL OF
THE INTERNATIONAL SEARCH REPORT AND
THE WRITTEN OPINION OF THE INTERNATIONAL
SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

Date of mailing
(day/month/year) 17 April 2014 (17.04.2014)

Applicant's or agent's file reference

120393PCT

FOR FURTHER ACTION See paragraphs 1 and 4 below

International application No.

PCT/US2013/077010

International filing date
(day/month/year)

20 December 2013 (20.12.2013)

Applicant

CORTEX MCP, INC.

1. ☒ The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

Filing of amendments and statement under Article 19:

The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):

When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes
1211 Geneva 20, Switzerland, Facsimile No.: +41 22 338 82 70

For more detailed instructions, see *PCT Applicant's Guide*, International Phase, paragraphs 9.004 - 9.011.

2. ☐ The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. ☐ **With regard to any protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:
☐ the protest together with the decision thereon has been transmitted to the International Bureau together with any request to forward the texts of both the protest and the decision thereon to the designated Offices.

☐ no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. Reminders

The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. Following the expiration of 30 months from the priority date, these comments will also be made available to the public.

Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau before the completion of the technical preparations for international publication (Rules 90bis.1 and 90bis.3).

Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

For details about the applicable time limits, Office by Office, see www.wipo.int/pct/en/texts/time_limits.html and the PCT Applicant's Guide, National Chapters.

Name and mailing address of the ISA/KR



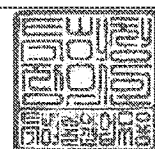
International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701,
Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

COMMISSIONER

Telephone No. 82-42-481-5875



* Attention

Copies of the documents cited in the international search report can be searched in the following Korean Intellectual Property Office English website for six months(expire date : **2014.10.18**) from the date of mailing of the international search report.

<http://www.kipo.go.kr/en/> => PCT Services => PCT Services

ID : PCT international application number

PW : **BAQ9PNF5**

Inquiries related to PCT International Search Report or Written Opinion prepared by KIPO as an International Searching Authority can be answered not only by KIPO but also through IPKC (Intellectual Property Korea Center), located in Vienna, VA, which functions as a PCT Help Desk for PCT applicants.

Homepage: <http://www.ipkcenter.com>

Email: ipkc@ipkcenter.com

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 120393PCT	FOR FURTHER ACTION		see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US2013/077010	International filing date (<i>day/month/year</i>) 20 December 2013 (20.12.2013)	(Earliest) Priority Date (<i>day/month/year</i>) 21 December 2012 (21.12.2012)	
Applicant CORTEX MCP, INC.			

This International search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 3 sheets.

☐ It is also accompanied by a copy of each prior art document cited in this report.

1. Basis of the report

a. With regard to the **language**, the international search was carried out on the basis of:

- ☒ the international application in the language in which it was filed
- ☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))

b. ☐ This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6bis(a)).

c. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. ☐ **Certain claims were found unsearchable** (See Box No. II)

3. ☐ **Unity of invention is lacking** (See Box No. III)

4. With regard to the **title**,

- ☒ the text is approved as submitted by the applicant.
- ☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,

- ☒ the text is approved as submitted by the applicant.
- ☐ the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the **drawings**,

- a. the figure of the **drawings** to be published with the abstract is Figure No. 1
- ☐ as suggested by the applicant.
- ☒ as selected by this Authority, because the applicant failed to suggest a figure.
- ☐ as selected by this Authority, because this figure better characterizes the invention.
- b. ☐ none of the figures is to be published with the abstract.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2013/077010**A. CLASSIFICATION OF SUBJECT MATTER****G06F 21/30(2013.01)i, G06F 17/21(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)

G06F 21/30; H04L 9/14; H04W 8/20; G06F 17/00; G06Q 30/00; H04L 9/32; H04W 12/06; G06F 21/22; G06F 17/21

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

Japanese utility models and applications for utility models

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

eKOMPASS(KIPO internal) & keywords: credential engine, verifying, user credential, store, request, matching, issuing agency, status indicator, identifier

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	KR 10-2011-0130002 A (KOREA FINANCIAL TELECOMM. & AMP.) 05 December 2011 See paragraphs [0026]-[0046]; and figure 1.	17-25
Y		1-16, 26-39
Y	KR 10-2011-0126269 A (SAMSUNG SDS CO., LTD.) 23 November 2011 See paragraphs [0016]-[0020]; claim 1; and figure 1.	1-16, 26-39
A	US 2010-0250389 A1 (THOMAS AUGUSTIN et al.) 30 September 2010 See paragraphs [0046]-[0059]; and figure 2.	1-39
A	KR 10-1091410 B1 (LG ELECTRONICS INC.) 07 February 2011 See paragraphs [0011]-[0021]; and figures 1-2.	1-39
A	WO 2008-018744 A1 (KOREA INSTITUTE FOR ELECTRONIC COMMERCE) 14 February 2008 See paragraphs [0044]-[0062]; and figure 1.	1-39

☐ 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

16 April 2014 (16.04.2014)

Date of mailing of the international search report

17 April 2014 (17.04.2014)

Name and mailing address of the ISA/KR



International Application Division
Korean Intellectual Property Office
189 Cheongsu-ro, Seo-gu, Daejeon Metropolitan City, 302-701,
Republic of Korea

Facsimile No. +82-42-472-7140

Authorized officer

AHN, Jeong Hwan

Telephone No. +82-42-481-8440



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2013/077010

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
KR 10-2011-0130002 A	05/12/2011	None	
KR 10-2011-0126269 A	23/11/2011	None	
US 2010-0250389 A1	30/09/2010	CN 101854245 A EP 2237182 A1 JP 2010-244542 A KR 10-2010-0109472 A	06/10/2010 06/10/2010 28/10/2010 08/10/2010
KR 10-1091410 B1	07/12/2011	None	
WO 2008-018744 A1	14/02/2008	CN 101326517 A CN 101326517 B EP 1917604 A1 EP 1917604 A4 JP 04918092 B2 JP 2009-512001 A KR 10-0816184 B1 KR 10-2008-0014194 A US 2009-0307756 A1 US 8132237 B2	17/12/2008 02/06/2010 07/05/2008 09/03/2011 18/04/2012 19/03/2009 21/03/2008 14/02/2008 10/12/2009 06/03/2012

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

TARR, DANIEL J

K&L GATES LLP K&L GATES CENTER 210 SIXTH
AVENUE PITTSBURGH PENNSYLVANIA 15222-2613
USA

PCT

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

(PCT Rule 43bis.1)

Date of mailing
(day/month/year) **17 April 2014 (17.04.2014)**

Applicant's or agent's file reference
120393PCT

FOR FURTHER ACTION

See paragraph 2 below

International application No.

PCT/US2013/077010

International filing date (day/month/year)

20 December 2013 (20.12.2013)

Priority date(day/month/year)

21 December 2012 (21.12.2012)

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

G06F 21/30(2013.01)i, G06F 17/21(2006.01)i

Applicant

CORTEX MCP, INC.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1 bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA/KR
International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon
Metropolitan City, 302-701, Republic of Korea
Facsimile No. +82-42-472-7140

Date of completion of this opinion

16 April 2014 (16.04.2014)

Authorized officer

AHN, Jeong Hwan

Telephone No. +82-42-481-8440



**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.
PCT/US2013/077010

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of :
 - ☒ the international application in the language in which it was filed
 - ☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))
3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:
 - a. (means)
 - ☐ on paper
 - ☐ in electronic form
 - b. (time)
 - ☐ in the international application as filed.
 - ☐ together with the international application in electronic form.
 - ☐ subsequently to this Authority for the purposes of search.
4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.
5. Additional comments:

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.

PCT/US2013/077010

Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-39	YES
	Claims	NONE	NO
Inventive step (IS)	Claims	NONE	YES
	Claims	1-39	NO
Industrial applicability (IA)	Claims	1-39	YES
	Claims	NONE	NO

2. Citations and explanations :

Reference is made to the following documents:

D1: KR 10-2011-0130002 A (KOREA FINANCIAL TELECOMM. & AMP.) 05 December 2011

D2: KR 10-2011-0126269 A (SAMSUNG SDS CO., LTD.) 23 November 2011

1. Novelty and Inventive Step

1.1. Independent Claim 1 and its Dependent Claims 2-16

1.1.1. D1, which is considered to be the closest prior art to the subject matter of claim 1, discloses a method comprising: receiving a request for issuing a certificate (see paragraph [0039]); and transmitting certificate information (see paragraph [0039]).

The subject matter of claim 1 differs from that of D1 in determining, by a credential action, a response to the credential action based on one or more user credentials. However, the different feature of the invention defined in claim 1 can be easily derived from the feature of D2 that comprises sending a pre-stored certificate in a certificate management server to a user terminal (see paragraph [0018]). Accordingly, it would be obvious to a person skilled in the art to combine the disclosures of D1 and D2, thereby arriving at the claim. Therefore, claim 1 lacks an inventive step under PCT Article 33(3).

1.1.2. The additional feature of claim 2, dependent on claim 1, can be easily conceived from the feature of D2 that comprises the pre-stored certificate in the certificate management server (see paragraph [0018]). Therefore, claim 2 lacks an inventive step under PCT Article 33(3).

1.1.3. The additional feature of claim 3, dependent on claim 2, can be easily conceived from the feature of D1 that comprises generating the certificate information (see paragraph [0040]). Therefore, claim 3 lacks an inventive step under PCT Article 33(3).

Continued on Supplemental Box

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of: Box No. V

1.1.4. The additional feature of claims 4-5, directly or indirectly dependent on claim 3, can be easily conceived from the feature of D1 that the certificate information comprises expiration date information of the certificate (see paragraph [0042]). Therefore, claims 4-5 lack an inventive step under PCT Article 33(3).

1.1.5. The additional feature of claim 6, dependent on claim 5, can be easily conceived from the feature of D1 that comprises storing the certificate information (see paragraph [0044]). Therefore, claim 6 lacks an inventive step under PCT Article 33(3).

1.1.6. The additional feature of claim 7, dependent on claim 6, can be merely a variation of user identification in D1 (see paragraph [0035]). Therefore, claim 7 lacks an inventive step under PCT Article 33(3).

1.1.7. The additional feature of claim 8, dependent on claim 4, can be merely a matter of design option in view of the feature of D1 that comprises the expiration date information of the certificate (see paragraph [0042]). Therefore, claim 8 lacks an inventive step under PCT Article 33(3).

1.1.8. The additional feature of claim 9, dependent on claim 2, can be easily conceived from the feature of D1 that comprises storing the certificate information in a storage medium (see paragraph [0044]). Therefore, claim 9 lacks an inventive step under PCT Article 33(3).

1.1.9. The additional feature of claims 10-11, directly or indirectly dependent on claim 2, can be easily conceived from biometric information in D1 (see paragraph [0036]). Therefore, claims 10-11 lack an inventive step under PCT Article 33(3).

1.1.10. The additional feature of claim 12, dependent on claim 1, can be easily conceived from the expiration date information of the certificate in D1 (see paragraph [0042]). Therefore, claim 12 lacks an inventive step under PCT Article 33(3).

1.1.11. The additional features of claims 13-14, 16, directly or indirectly dependent on claim 12, can be easily conceived from the user identification in D1 (see paragraph [0035]) and the pre-stored certificate in the certificate management server in D2 (see paragraph [0018]). Therefore, claims 13-14, 16 lack an inventive step under PCT Article 33(3).

Continued on The Next Page

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.
PCT/US2013/077010

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of : Previous Page

1.1.12. The additional feature of claim 15, dependent on claim 14, can be easily conceived from the feature of D1 that comprises generating the certificate information (see paragraph [0040]). Therefore, claim 15 lacks an inventive step under PCT Article 33(3).

1.2. Independent Claim 17 and its Dependent Claims 18-25

1.2.1. D1, which is considered to be the closest prior art to the subject matter of claim 17, discloses a method comprising: transmitting a request for issuing a certificate identifying a user (see paragraphs [0029], [0039]); and receiving certificate information (see paragraph [0039]).

The subject matter of claim 17 differs from that of D1 in generating, by a processor, a request for a credential action comprising a credential identifier. However, the different feature of the invention defined in claim 17 can be easily derived from the feature of D1 that comprises the request for issuing the certificate and identifying the user (see paragraphs [0029], [0039]). Accordingly, claim 17 would have been obvious over D1. Therefore, claim 17 lacks an inventive step under PCT Article 33(3).

1.2.2. The additional feature of claim 18, dependent on claim 17, can be easily conceived from the request for issuing the certificate in D1 (see paragraph [0040]). Therefore, claim 18 lacks an inventive step under PCT Article 33(3).

1.2.3. The additional features of claims 19-20, dependent on claim 18, can be easily conceived from a user identification in D1 (see paragraph [0035]). Therefore, claims 19-20 lack an inventive step under PCT Article 33(3).

1.2.4. The additional feature of claim 21, dependent on claim 20, can be merely a variation of the user identification in D1 (see paragraph [0035]). Therefore, claim 21 lacks an inventive step under PCT Article 33(3).

1.2.5. The additional feature of claim 22, dependent on claim 17, can be easily conceived from biometric information in D1 (see paragraph [0036]). Therefore, claim 22 lacks an inventive step under PCT Article 33(3).

1.2.6. The additional feature of claims 23-25, directly or indirectly dependent on claim 17, can be merely matters of design option in view of the feature of D1 that comprises

Continued on The Next Page

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.
PCT/US2013/077010

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of: Previous Page

expiration date information of the certificate (see paragraph [0042]). Therefore, claims 23-25 lack an inventive step under PCT Article 33(3).

1.3. Independent Claim 26 and its Dependent Claims 27-39

1.3.1. The features of claim 26 are substantially the same as those of claim 1 except the category of the invention and additional features. However, the additional features of claim 26 are considered to be a minor difference over the disclosure of D1 that falls under the general knowledge of a person skilled in the art. Accordingly, the same reasoning as in claim 1 applies to claim 26. Therefore, claim 26 lacks an inventive step under PCT Article 33(3).

1.3.2. The additional features of claims 27-29, directly or indirectly dependent on claim 26, are substantially the same as those of claims 3-5 except the category of the invention, respectively. Accordingly, the same reasoning as in claims 3-5 applies to claims 27-29, respectively. Therefore, claims 27-29 lack an inventive step under PCT Article 33(3).

1.3.3. The additional features of claims 30-31, directly or indirectly dependent on claim 28, can be easily conceived from biometric information in D1 (see paragraph [0036]). Therefore, claims 30-31 lack an inventive step under PCT Article 33(3).

1.3.4. The additional feature of claim 32, dependent on claim 29, can be easily conceived from the transmitting the certificate information in D1 (see paragraph [0039]). Therefore, claim 32 lacks an inventive step under PCT Article 33(3).

1.3.5. The additional feature of claim 33, dependent on claim 32, can be merely a variation of user identification in D1 (see paragraph [0035]). Therefore, claim 33 lacks an inventive step under PCT Article 33(3).

1.3.6. The additional feature of claim 34, dependent on claim 28, can be merely a matter of design option in view of the feature of D1 that comprises expiration date information of the certificate (see paragraph [0042]). Therefore, claim 34 lacks an inventive step under PCT Article 33(3).

1.3.7. The additional feature of claim 35, dependent on claim 28, can be easily conceived from the feature of D1 that comprises storing the certificate information in a storage

Continued on The Next Page

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2013/077010

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of: Previous Page

medium (see paragraph [0044]). Therefore, claim 35 lacks an inventive step under PCT Article 33(3).

1.3.8. The additional feature of claim 36, dependent on claim 28, can be easily conceived from the expiration date information of the certificate in D1 (see paragraph [0042]). Therefore, claim 36 lacks an inventive step under PCT Article 33(3).

1.3.9. The additional features of claims 37-39, directly or indirectly dependent on claim 36, can be easily conceived from the user identification in D1 (see paragraph [0035]) and a pre-stored certificate in a certificate management server in D2 (see paragraph [0018]). Therefore, claims 37-39 lack an inventive step under PCT Article 33(3).

2. Industrial Applicability

Claims 1-39 are industrially applicable under PCT Article 33(4).

ADVANCE E-MAIL

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION CONCERNING
TRANSMITTAL OF COPY OF INTERNATIONAL
PRELIMINARY REPORT ON PATENTABILITY
(CHAPTER I OF THE PATENT COOPERATION
TREATY)

(PCT Rule 44bis.1(c))

To:

TARR, Daniel J.
K&L Gates LLP
K&L Gates Center
210 Sixth Avenue
Pittsburgh, PA 15222-2613
ETATS-UNIS D'AMERIQUE

Date of mailing (day/month/year) 02 July 2015 (02.07.2015)			IMPORTANT NOTICE
Applicant's or agent's file reference 120393PCT			
International application No. PCT/US2013/077010	International filing date (day/month/year) 20 December 2013 (20.12.2013)	Priority date (day/month/year) 21 December 2012 (21.12.2012)	
Applicant CORTEX MCP, INC.			

The International Bureau transmits herewith a copy of the international preliminary report on patentability (Chapter I of the Patent Cooperation Treaty)

RECEIVED

JUL 06 2015

K & L GATES
PITTSBURGH, PA

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Authorized officer

Lingfei Bai

Facsimile No. +41 22 338 82 70

e-mail: pt02.pct@wipo.int

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
TARR, DANIEL J

K&L GATES LLP K&L GATES CENTER 210 SIXTH
AVENUE PITTSBURGH PENNSYLVANIA 15222-2613
USA

PCT

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

(PCT Rule 43bis.1)

Date of mailing
(day/month/year) **17 April 2014 (17.04.2014)**

Applicant's or agent's file reference
120393PCT

FOR FURTHER ACTION

See paragraph 2 below

International application No.

PCT/US2013/077010

International filing date (day/month/year)

20 December 2013 (20.12.2013)

Priority date(day/month/year)

21 December 2012 (21.12.2012)

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

G06F 21/30(2013.01)i, G06F 17/21(2006.01)i

Applicant

CORTEX MCP, INC.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. FURTHER ACTION

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.
For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA/KR
International Application Division
Korean Intellectual Property Office
189 Cheongsu-ro, Seo-gu, Daejeon
Metropolitan City, 302-701, Republic of Korea
Facsimile No. +82-42-472-7140

Date of completion of this opinion

16 April 2014 (16.04.2014)

Authorized officer

AHN, Jeong Hwan

Telephone No. +82-42-481-8440



**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.
PCT/US2013/077010

Box No. 1 Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of :

- ☒ the international application in the language in which it was filed
- ☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43bis.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:

a. (means)

- ☐ on paper
- ☐ in electronic form

b. (time)

- ☐ in the international application as filed.
- ☐ together with the international application in electronic form.
- ☐ subsequently to this Authority for the purposes of search.

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.
PCT/US2013/077010

Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-39	YES
	Claims	NONE	NO
Inventive step (IS)	Claims	NONE	YES
	Claims	1-39	NO
Industrial applicability (IA)	Claims	1-39	YES
	Claims	NONE	NO

2. Citations and explanations :

Reference is made to the following documents:

D1: KR 10-2011-0130002 A (KOREA FINANCIAL TELECOMM. & AMP.) 05 December 2011

D2: KR 10-2011-0126269 A (SAMSUNG SDS CO., LTD.) 23 November 2011

1. Novelty and Inventive Step

1.1. Independent Claim 1 and its Dependent Claims 2-16

1.1.1. D1, which is considered to be the closest prior art to the subject matter of claim 1, discloses a method comprising: receiving a request for issuing a certificate (see paragraph [0039]); and transmitting certificate information (see paragraph [0039]).

The subject matter of claim 1 differs from that of D1 in determining, by a credential action, a response to the credential action based on one or more user credentials. However, the different feature of the invention defined in claim 1 can be easily derived from the feature of D2 that comprises sending a pre-stored certificate in a certificate management server to a user terminal (see paragraph [0018]). Accordingly, it would be obvious to a person skilled in the art to combine the disclosures of D1 and D2, thereby arriving at the claim. Therefore, claim 1 lacks an inventive step under PCT Article 33(3).

1.1.2. The additional feature of claim 2, dependent on claim 1, can be easily conceived from the feature of D2 that comprises the pre-stored certificate in the certificate management server (see paragraph [0018]). Therefore, claim 2 lacks an inventive step under PCT Article 33(3).

1.1.3. The additional feature of claim 3, dependent on claim 2, can be easily conceived from the feature of D1 that comprises generating the certificate information (see paragraph [0040]). Therefore, claim 3 lacks an inventive step under PCT Article 33(3).

Continued on Supplemental Box