(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2025년06월11일
(11) 등록번호 10-2819698
(24) 등록일자 2025년06월09일

(51) 국제특허분류(Int. Cl.)
H04L 9/40 (2022.01)
(52) CPC특허분류
H04L 63/0442 (2013.01)
H04L 63/065 (2013.01)
(21) 출원번호 10-2024-7042421
(22) 출원일자(국제) 2023년05월19일
심사청구일자 2024년12월20일
(85) 번역문제출일자 2024년12월20일
(65) 공개번호 10-2025-0005528
(43) 공개일자 2025년01월09일
(86) 국제출원번호 PCT/FI2023/050281
(87) 국제공개번호 WO 2023/227828
국제공개일자 2023년11월30일
(30) 우선권주장
22175341.1 2022년05월25일
유럽특허청(EPO)(EP)
(56) 선행기술조사문헌
EP04283918 B1
(뒷면에 계속)

(73) 특허권자
구루로직 마이크로시스템스 오이
핀란드 투르쿠 20100 린난카투 34
(72) 발명자
카에르카에이넨 투오마스
핀란드 20400 투르쿠 티카아잔카투 7
(74) 대리인
김태홍, 김진희

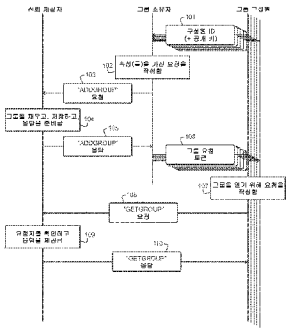
전체 청구항 수 : 총 14 항 심사관 : 이준석

(54) 발명의 명칭 **그룹 중의 보안 디지털 통신을 가능하게 하기 위한 방법 및 장치**

(57) 요 약

디지털 암호화 그룹을 확립하기 위한 장치는 주어진 입력 데이터로부터 암호화 제품을 생성하도록 구성된 암호화 엔진을 포함한다. 상기 암호화 엔진은 암호화 제품을 생성함으로써 사용자 식별자를 포함하는 요청을 보안 전송 메커니즘을 통해 수신하는 것에 응답한다. 암호화 엔진은 또한 상기 보안 전송 메커니즘을 통해 상기 암호화 제품을 송신함으로써, 상기 복수의 사용자 식별자 중 하나를 포함하는 후속 제2 요청을 상기 보안 전송 메커니즘을 통해 수신하는 것에 응답한다. 상기 암호화 제품은, 상기 복수의 사용자 식별자 및 상기 복수의 사용자 식별자에 의해 식별되는 사용자들 간의 대칭 암호화에 사용하기 위한 공통 암호화 키 및/또는 상기 복수의 사용자 식별자에 의해 식별되는 사용자들 간의 통신에서 비대칭 암호화에 사용하기 위한 사용자 특유 및 사용자 식별자 관련 공개 키를 포함하는 디지털 암호화 그룹이다.

대 표 도



(52) CPC특허분류
H04L 63/123 (2013.01)

(56) 선행기술조사문헌
US20110320815 A1
US20150281372 A1
US20090222668 A1
US20220069984 A1
KR1020200055672 A

명 세 서

청구범위

청구항 1

디지털 암호화 그룹을 확립하기 위한 장치(arrangement)에 있어서,

- 주어진 입력 데이터로부터 암호화 제품(cryptoproduct)을 생성하도록 구성된 암호화 엔진, 및

- 상기 암호화 엔진에 결합된 보안 전송 메커니즘의 수신단 및 송신단

을 포함하고,

상기 암호화 엔진은, 암호화 제품을 생성함으로써 복수의 사용자 식별자를 포함하는 제1 요청을 상기 보안 전송 메커니즘을 통해 수신하는 것에 응답하도록 구성되고,

상기 암호화 엔진은, 상기 보안 전송 메커니즘을 통해 상기 암호화 제품을 송신함으로써 상기 복수의 사용자 식별자 중 하나를 포함하는 후속 제2 요청을 상기 보안 전송 메커니즘을 통해 수신하는 것에 응답하도록 구성되고;

상기 암호화 제품은, 상기 복수의 사용자 식별자 및

- 상기 복수의 사용자 식별자에 의해 식별되는 사용자들 간의 대칭 암호화에 사용하기 위한 공통 암호화 키,

- 상기 복수의 사용자 식별자에 의해 식별되는 사용자들 간의 통신에서 비대칭 암호화에 사용하기 위한 사용자 특유 및 사용자 식별자 관련 공개 키 중, 적어도 하나를 포함하는 디지털 암호화 그룹인 것인, 디지털 암호화 그룹을 확립하기 위한 장치.

청구항 2

제1항에 있어서,

- 상기 장치는 상기 제1 요청이 상기 복수의 사용자 식별자 각각에 대해 각각의 사용자 특유 암호화 키를 포함했는지 여부를 확인하도록 구성되고,

- 상기 장치는 상기 제1 요청에서 수신된 데이터를 상기 복수의 사용자 식별자 각각에 대해 각각의 사용자 특유 암호화 키를 포함하도록 증강함으로써, 상기 복수의 사용자 식별자 각각에 대해 상기 제1 요청이 각각의 사용자 특유 암호화 키를 포함하지 않았다는 발견에 응답하도록 구성되는 것인, 디지털 암호화 그룹을 확립하기 위한 장치.

청구항 3

제2항에 있어서, 상기 장치는 상기 장치 외부의 소스로부터 각각의 사용자 특유 암호화 키를 요청하고 수신함으로써 상기 증강을 수행하도록 구성되는 것인, 디지털 암호화 그룹을 확립하기 위한 장치.

청구항 4

제1항 내지 제3항 중 어느 한 항에 있어서, 상기 장치는 상기 제1 요청에서 수신된 사용자 관련 정보의 조각(piece)을 또 다른 소스로부터의 사용자 관련 정보 조각의 대응 조각에 대조 확인하여, 사용자 관련 정보의 이들 조각이 서로 매칭되는지 여부를 발견하도록 구성되는 것인, 디지털 암호화 그룹을 확립하기 위한 장치.

청구항 5

제4항에 있어서, 상기 장치는 상기 디지털 암호화 그룹의 확립이 계속되도록 허용되는지에 대한 결정을 내림으로써 사용자 관련 정보의 상기 조각들이 서로 매칭되지 않는다는 발견에 응답하도록 구성되는 것인, 디지털 암호화 그룹을 확립하기 위한 장치.

청구항 6

제1항 내지 제3항 중 어느 한 항에 있어서, 상기 장치는 자신이 상기 암호화 그룹에 포함하는 정보 요소를 디지털 서명하기 위해 서명 키를 사용하도록 구성되는 것인, 디지털 암호화 그룹을 확립하기 위한 장치.

청구항 7

제1항 내지 제3항 중 어느 한 항에 있어서, 상기 장치는 상기 요청이 자기 자신에게 향하는 것인지 또는 추가 수신자에게 향하는 것인지를 상기 후속 제2 요청으로부터 확인하고, 상기 후속 제2 요청을 추가 수신자에게 전달함으로써 상기 요청이 상기 추가 수신자에게 향하는 것이라는 발견에 응답하도록 구성되는 것인, 디지털 암호화 그룹을 확립하기 위한 장치.

청구항 8

제7항에 있어서, 상기 장치는 상기 전달 이전에, 상기 후속 제2 요청의 원래의 인증을 상기 장치 자체의 인증으로 대체하도록 구성되는 것인, 디지털 암호화 그룹을 확립하기 위한 장치.

청구항 9

디지털 암호화 그룹을 확립하기 위한 방법에 있어서,

- 복수의 사용자 식별자를 포함하는 제1 요청을 보안 전송 메커니즘을 통해 수신하는 단계,

- 상기 제1 요청을 수신하는 것에 대한 응답으로, 암호화 제품을 생성하는 단계,

- 상기 복수의 사용자 식별자 중 하나를 포함하는 후속 제2 요청을 상기 보안 전송 메커니즘을 통해 수신하는 단계, 및

- 상기 제2 요청을 수신하는 것에 대한 응답으로, 상기 보안 전송 메커니즘을 통해 상기 암호화 제품을 송신하는 단계

를 포함하고;

상기 암호화 제품은, 상기 복수의 사용자 식별자 및

- 상기 복수의 사용자 식별자에 의해 식별되는 사용자들 간의 대칭 암호화에 사용하기 위한 공통 암호화 키,

- 상기 복수의 사용자 식별자에 의해 식별되는 사용자들 간의 통신에서 비대칭 암호화에 사용하기 위한 사용자 특유 및 사용자 식별자 관련 공개 키 중, 적어도 하나를 포함하는 디지털 암호화 그룹인 것인, 디지털 암호화 그룹을 확립하기 위한 방법.

청구항 10

제9항에 있어서,

- 상기 제1 요청이 상기 복수의 사용자 식별자 각각에 대해 각각의 사용자 특유 암호화 키를 포함했는지 여부를 확인하는 단계, 및

- 상기 제1 요청에서 수신된 데이터를 상기 복수의 사용자 식별자 각각에 대해 각각의 사용자 특유 암호화 키를 포함하도록 증강함으로써, 상기 복수의 사용자 식별자 각각에 대해 상기 제1 요청이 각각의 사용자 특유 암호화 키를 포함하지 않았다는 발견에 응답하는 단계를 포함하는, 디지털 암호화 그룹을 확립하기 위한 방법.

청구항 11

제9항에 있어서,

- 상기 암호화 그룹을 생성할 때, 상기 암호화 그룹에 포함된 정보 요소를 디지털 서명하기 위해 서명 키를 사용하는 단계를 포함하는, 디지털 암호화 그룹을 확립하기 위한 방법.

청구항 12

제9항에 있어서,

- 상기 요청이 장치에게 향하는 것인지 또는 추가 수신자에게 향하는 것인지를 상기 후속 제2 요청으로부터 확인하는 단계, 및

- 상기 후속 제2 요청을 추가 수신자에게 전달함으로써 상기 요청이 상기 추가 수신자에게 향하는 것이라는 발견에 응답하는 단계를 포함하는, 디지털 암호화 그룹을 확립하기 위한 방법.

청구항 13

제12항에 있어서,

- 상기 전달 이전에, 상기 후속 제2 요청의 원래의 인증을 상기 방법을 실행하는 상기 장치의 인증으로 대체하는 단계를 포함하는, 디지털 암호화 그룹을 확립하기 위한 방법.

청구항 14

하나 이상의 프로세서에 의해 실행될 때, 상기 하나 이상의 프로세서로 하여금 제9항 내지 제13항 중 어느 한 항에 따른 방법을 실행하게 하도록 구성되는 하나 이상의 기계 실행 가능 명령어(machine-executable instruction)의 하나 이상의 세트를 포함하는 프로그램이 저장된 컴퓨터 판독 가능 기록 매체.

발명의 설명

기 술 분 야

[0001] 본 발명은 일반적으로 둘 이상의 당사자의 그룹 중에서 디지털 서비스를 사용하는 데 필요한 보안의 기술적 분야에 관한 것이다. 특히, 본 발명은 당사자들 간의 신뢰를 중앙적으로 확립하는 작업에 관한 것이며, 그 후 이들 당사자들은 그룹 통신 또는 다른 종류의 그룹 관련 디지털 서비스 사용에서 중앙적으로 확립된 신뢰에 의존할 수 있다.

배 경 기 술

[0002] 디지털 통신의 보안은 기밀성(인가된 당사자만 한 조각(piece)의 정보에 액세스할 수 있음), 인증(통신 당사자는 자신이 누구와 통신하고 있는지 확인해야 함), 무결성(한 조각의 정보가 허용되지 않게 수정되지 않았음). 및 부인 방지(당사자는 특정 조각의 정보를 송신한 것을 성공적으로 부인할 수 없음)와 같은 다수의 양상을 수반한다. 디지털 통신의 아속(subgenus)은 그룹 통신, 즉 디지털 통신 및/또는 사전 정의된 그룹의 구성원들 간의 다른 디지털 서비스의 사용이다. 그룹의 구성원은 가능한 한 쉽고 신뢰할 수 있게 그룹 특유 통신에 액세스할 수 있어야 하며, 동시에 그룹 외부의 당사자가 통신에 액세스하거나 그 외 다른 방식으로 통신을 방해할 수 없도록 해야 한다. 암호화 애플리케이션에 대한 고유한 종속성으로 인해 여기에서 의미되는 임의의 종류의 그룹을 디지털 암호화 그룹이라고 할 수 있다.

[0003] 그룹 통신에 대해 적어도 두 가지 기본 접근법이 알려져 있다. 중앙 집중형 솔루션에서 그룹의 구성원들 간의 모든 통신은 서버 또는 유사한 중앙 집중형 서비스 지점을 통해 라우팅된다. 이러한 경우 서버는 참가자를 인증하고 필요한 암호화 및 복호화 동작을 수행하는 데 상당한 책임을 질 수 있다. 다른 접근법은 분산형 솔루션이며, 여기서 통신은 구성원들 간에 직접 이루어질 수 있다. 분산형 솔루션을 사용하려면 필요한 보안을 제공하기 위해 사용자 디바이스가 특정 공유 시크릿(secret)(들)에 액세스할 수 있어야 한다.

[0004] 중앙 집중형 솔루션은 그룹의 모든 활성 구성원에 대해 서버에 대한 지속적인 액세스에 완전히 의존한다는 단점을 적어도 가진다. 반면에 분산형 솔루션에서, 공유 시크릿을 배포하는 비용 효율적이고 계산적으로 합리적인 방식을 찾는 것이 문제가 있는 것으로 입증되었다. 예를 들어, 알려진 디피-헬먼 방법(Diffie-Hellman method)에서는 각 당사자가 그룹에 공통된 공유 시크릿을 계산할 수 있도록 공개 키가 처리를 위해 제공되는 순서에 당사자들이 동의해야 한다. 또한, 많은 알려진 분산형 솔루션은 당사자들 간에 충분한 수준의 신뢰를 확립하는 방식에 있어 비효율적이므로 이러한 솔루션을 악의적인 공격에 취약하게 할 수 있다. 많은 분산형 솔루션의 또 다른 단점은 확립된 디지털 암호화 그룹을 사용할 때 특정 기술에 대한 의존성과 관련이 있다. 디지털 암호화 그룹이 기술에 구애받지 않는(technology-agnostic) 경우, 즉 그룹의 소유자와 구성원이 그 그룹을 미래에 사용할 계획인 방식과 관련하여 임의의 특정 기술에 의존하지 않는 것이 더 좋을 것이다.

종래 기술 문헌 US 2019/0305940 A1은 제2 사용자로부터 그룹 자격 증명 요청을 수신하면 자격 증명 시스템이 제1 사용자의 공개 키로 요청이 합법적인지 확인한 다음 그룹 자격 증명을 전송하여 요청에 응답하는 방법을 개시한다.

또 다른 종래 기술 문서 US 2015/0195261 A1은 네트워크 노드가 네트워크 노드 그룹의 멤버를 위한 보안 세션을

생성하고 가입할 수 있는 방법을 공개한다.

또 다른 선행 기술 문서 US 2010/0329463 A1은 모바일 애드혹 네트워크에서 그룹 키를 관리하는 방법을 공개한다.

발명의 내용

[0005] 본 개요는 하기의 발명을 실시하기 위한 구체적인 내용에서 추가로 설명되는 엄선된 개념을 간소화된 형태로 소개하기 위해 제공된다. 본 개요는, 청구된 주제의 주요한 피처(feature) 또는 본질적인 피처를 식별하도록 의도되지 않으며, 청구된 주제의 범위를 제한하는 데 사용되도록 의도되지도 않는다.

[0006] 앞에서 약술한 종래 기술의 단점 없이 디지털 암호화 그룹의 활용을 확립, 활용, 및 활성화하기 위한 방법과 장치(arrangement)를 제공하는 것이 목적이다.

[0007] 제1 양상에 따르면, 디지털 암호화 그룹을 확립하기 위한 장치가 제공된다. 장치는 주어진 입력 데이터로부터 암호화 제품(cryptoproduct)을 생성하도록 구성된 암호화 엔진, 및 상기 암호화 엔진에 결합된 보안 전송 메커니즘의 수신단 및 송신단을 포함한다. 상기 암호화 엔진은 암호화 제품을 생성함으로써, 복수의 사용자 식별자를 포함하는 제1 요청을 상기 보안 전송 메커니즘을 통해 수신하는 것에 응답하도록 구성된다. 상기 암호화 엔진은 상기 보안 전송 메커니즘을 통해 상기 암호화 제품을 송신함으로써, 복수의 사용자 식별자 중 하나를 포함하는 후속 제2 요청을 보안 전송 메커니즘을 통해 수신하는 것에 응답하도록 구성된다. 상기 암호화 제품은, 상기 복수의 사용자 식별자 및 상기 복수의 사용자 식별자에 의해 식별되는 사용자들 간의 대칭 암호화에 사용하기 위한 공통 암호화 키 및/또는 상기 복수의 사용자 식별자에 의해 식별되는 사용자들 간의 통신에서 비대칭 암호화에 사용하기 위한 사용자 특유 및 사용자 식별자 관련 공개 키를 포함하는 디지털 암호화 그룹이다.

[0008] 일 실시예에 따르면, 장치는, 상기 제1 요청이 상기 복수의 사용자 식별자 각각에 대해 각각의 사용자 특유 암호화 키를 포함하고 있는지 여부를 확인(check)하도록 구성된다. 그 후, 장치는, 상기 제1 요청에서 수신된 데이터를 상기 복수의 사용자 식별자 각각에 대해 각각의 사용자 특유 암호화 키를 포함하도록 증강함으로써, 상기 복수의 사용자 식별자 각각에 대해 상기 제1 요청이 각각의 사용자 특유 암호화 키를 포함하지 않았다는 발견에 응답하도록 구성될 수 있다. 이것은 장치가 모든 사용자 특유 암호화 키가 제1 요청에 포함되지는 않는 상황에 유연하게 적응할 수 있다는 이점을 적어도 수반한다.

[0009] 일 실시예에 따라, 장치는 장치 외부의 소스로부터 각각의 사용자 특유 암호화 키를 요청하고 수신함으로써 상기 증강을 수행하도록 구성된다. 이것은, 장치가 누락된 사용자 특유 암호화 키를 자체적으로 소유하지 않는 상황에서 동작하고 이 상황에 유연하게 적응할 수 있다는 이점을 적어도 수반한다.

[0010] 일 실시예에 따라, 장치는 제1 요청에서 수신된 사용자 관련 정보의 조각을 또 다른 소스로부터의 사용자 관련 정보 조각의 대응하는 조각에 대조 확인하여, 사용자 관련 정보의 이들 조각이 서로 매칭되는지 여부를 발견하도록 구성된다. 이것은 사용자 관련 정보의 사기 또는 그 외 부적절한 사용이 검출되고 대응할 수 있는 이점을 적어도 수반한다.

[0011] 일 실시예에 따라, 장치는 디지털 암호화 그룹의 확립이 계속되도록 허용되는지에 대한 결정을 내림으로써, 사용자 관련 정보의 상기 조각들이 서로 매칭되지 않는다는 발견에 응답하도록 구성된다. 이것은 정보의 각 조각이 얼마나 정확해야 하는지에 관한 상이한 종류들의 요구에 장치의 동작이 유연하게 적응될 수 있는 이점을 적어도 수반한다.

[0012] 일 실시예에 따라, 장치는 자신이 상기 암호화 그룹에 포함하는 정보 요소를 디지털 서명하기 위해 서명 키를 사용하도록 구성된다. 이것은 그러한 정보 요소가 나중에 사용될 때 신뢰할 수 있는 정보로서 특별한 가치를 가질 수 있다는 이점을 적어도 수반한다.

[0013] 일 실시예에 따라, 장치는 요청이 자기 자신에게 향하는 것인지 또는 추가 수신자에게 향하는 것인지를 상기 후속 제2 요청으로부터 확인하고, 상기 후속 제2 요청을 상기 추가 수신자에게 전달함으로써, 요청이 추가 수신자에게 향하는 것이라는 발견에 응답하도록 구성된다. 이것은 상이한 사용자들이 상이한 신뢰 제공자들의 관리되는 도메인에 속할 수 있는 환경에서 동작할 때 동일한 원칙이 준수될 수 있다는 이점을 적어도 수반한다.

[0014] 일 실시예에 따라. 장치는 상기 전달 이전에, 상기 후속 제2 요청의 원래의 인증을 장치 자체의 인증으로 대체하도록 구성된다. 이것은 정보가 더 멀리 전달되는 경우에도 당사자들 간의 신뢰 관계가 적절하게 유지되고 사용될 수 있다는 이점을 적어도 수반한다.

[0015] 제2 양상에 따르면, 디지털 암호화 그룹을 확립하기 위한 방법이 제공된다. 이 방법은 보안 전송 메커니즘을 통해 복수의 사용자 식별자를 포함하는 제1 요청을 수신하는 단계와, 응답으로서 암호화 제품을 생성하는 단계를 포함한다. 이 방법은 상기 복수의 사용자 식별자 중 하나를 포함하는 후속 제2 요청을 상기 보안 전송 메커니즘을 통해 수신하는 단계와, 상기 보안 전송 메커니즘을 통해 상기 암호화 제품을 송신함으로써 응답하는 단계를 포함한다. 상기 암호화 제품은, 상기 복수의 사용자 식별자 및 상기 복수의 사용자 식별자에 의해 식별되는 사용자들 간의 대칭 암호화에 사용하기 위한 공통 암호화 키 및/또는 상기 복수의 사용자 식별자에 의해 식별되는 사용자들 간의 통신에서 비대칭 암호화에 사용하기 위한 사용자 특유 및 사용자 식별자 관련 공개 키를 포함하는 디지털 암호화 그룹이다.

[0016] 일 실시예에 따라, 방법은 상기 제1 요청이 상기 복수의 사용자 식별자 각각에 대해 각각의 사용자 특유 암호화 키를 포함했는지 여부를 확인하는 단계, 및 상기 제1 요청에서 수신된 데이터를 상기 복수의 사용자 식별자 각각에 대해 각각의 사용자 특유 암호화 키를 포함하도록 증강함으로써, 상기 복수의 사용자 식별자 각각에 대해 상기 제1 요청이 각각의 사용자 특유 암호화 키를 포함하지 않았다는 발견에 응답하는 단계를 포함한다. 이는 모든 사용자 특유 암호화 키가 제1 요청에 포함되지는 않는 상황에 대해 이 방법이 유연하게 적용될 수 있다는 이점을 적어도 수반한다.

[0017] 일 실시예에 따라, 방법은 상기 암호화 그룹을 생성할 때, 상기 암호화 그룹에 포함된 정보 요소를 디지털 서명하기 위해 서명 키를 사용하는 단계를 포함한다. 이것은, 방법을 실행하는 장치가 누락된 사용자 특유 암호화 키를 자체로 소유하지 않는 상황에서 방법이 동작 가능하고 이 상황에 유연하게 적응할 수 있다는 이점을 적어도 수반한다.

[0018] 일 실시예에 따라, 방법은, 요청이 방법을 실행하는 장치에게 향하는 것인지 또는 추가 수신자에게 향하는 것인지를 상기 후속 제2 요청으로부터 확인하는 단계, 및 상기 후속 제2 요청을 상기 추가 수신자에게 전달함으로써 상기 요청이 추가 수신자에게 향하는 것이라는 발견에 응답하는 단계를 포함한다. 이는 상이한 사용자들이 상이한 신뢰 제공자들의 관리되는 도메인에 속할 수 있는 환경에서 동작할 때 동일한 원칙이 준수될 수 있다는 이점을 적어도 수반한다.

[0019] 일 실시예에 따라, 방법은 상기 전달 이전에, 상기 후속 제2 요청의 원래의 인증을 상기 방법을 실행하는 상기 장치의 인증으로 대체하는 단계를 포함한다. 이것은 정보가 더 멀리 전달되는 경우에도 당사자들 간의 신뢰 관계가 적절하게 유지되고 사용될 수 있다는 이점을 적어도 수반한다.

[0020] 제3 양상에 따라, 하나 이상의 프로세서에 의해 실행될 때, 상기 하나 이상의 프로세서로 하여금 전술한 종류의 방법을 실행하게 하도록 구성되는 하나 이상의 기계 실행 가능 명령어(machine-executable instruction)의 하나 이상의 세트를 포함하는 컴퓨터 프로그램 제품이 제공된다.

도면의 간단한 설명

[0021] 도면들에서,

도 1은 실시예에 따라 동작할 때의 정보의 교환을 예시하고,

도 2는 실시예에 따라 동작할 때의 정보의 교환을 예시한다.

발명을 실시하기 위한 구체적인 내용

[0022] 다음의 설명에서, 첨부된 도면들에 대한 참조가 이루어지며, 이들은 개시내용의 일부를 형성하고, 그 안에서, 예시로서, 본 개시내용이 배치될 수 있는 특정 양상이 도시된다. 다른 양상이 활용될 수 있으며, 본 개시내용의 범위를 벗어나지 않으면서 구조적 변경 또는 논리적 변경이 이루어질 수 있음을 이해한다. 따라서, 본 개시내용의 범위는 첨부된 청구항들인 것으로 정의되므로, 이하의 상세한 설명은 제한적인 의미로 받아들여져서는 안 된다.

[0023] 예를 들어, 설명된 방법과 관련된 개시내용은 방법을 수행하도록 구성된 대응 디바이스 또는 시스템에 대해서도 적용될 수 있으며 그 반대의 경우도 마찬가지인 것으로 이해된다. 예를 들어, 특정 방법 단계가 설명되는 경우, 설명된 방법 단계를 수행하는 유닛이 도면에서 명시적으로 설명되거나 예시되지 않더라도 대응 디바이스는 이러한 유닛을 포함할 수 있다. 반면에, 예를 들어, 특정 장치가 기능 유닛에 기초하여 설명되는 경우, 대응 단계는 도면에서 명시적으로 설명되거나 예시되지 않더라도, 설명된 기능성을 수행하는 단계를 포함할 수 있다. 또한, 본 명세서에서 설명되는 다양한 예시적인 양상의 피처는 특별히 다르게 언급되지 않는 한, 서로 결합될 수 있다

는 것이 이해된다.

[0024] 디지털 암호화 그룹의 예는 디지털로 송신된 정보를 서로 안전하게 공유하고자 하는 적어도 두 명의 사용자, 예를 들어(반드시 그런 것은 아님) 개인으로 구성된 그룹인데, 즉, 그 결과 그룹의 모든 사람이 다른 사람들을 그들이 보이는 것처럼 그들이 맞다고 신뢰할 수 있고 그룹의 구성원이 아닌 당사자가 공유된 정보에 액세스할 수 없다. 상기 사용자들 중 한 명은 그룹의 소유자 또는 설립자 역할을 할 수 있다.

[0025] 디지털 암호화 그룹을 활용하는 또 다른 예는 개별 사용자가 디지털 속성을 안전하게 소유하고 필요할 때 확인을 위해 제시할 수 있도록 하는 것이 목적이다. 예를 들어, 운전 면허증을 부여할 책임이 있는 국가 기관은 유효한 운전 면허증의 각 소지자별로 그러한 그룹을 설정하고 관리할 수 있다. 경찰관은 그러한 그룹의 (바람직하게는 임시) 구성원으로 간주될 수 있으며, 이 경우 경찰관은 사용자의 디지털 지갑과의 보안 디지털 통신을 수행하기 위한 수단을 갖게 된다. 특정 종류의 차량을 운전할 수 있는 사용자의 권리는 속성으로 저장되었을 수 있으며, 사용자의 디지털 지갑은 검사를 위해 경찰관에게 제시할 수 있다. 또 다른 예로서, 그룹의 소유자는 영리 기업일 수 있고, 구성원은 로열티 카드를 소유한 사용자 및 그의 또는 그녀의 가족 구성원일 수 있으며, 이들은 종래 기술 시스템에서 주 사용자의 로열티 카드와 연관된 종속 카드(subordinate card)의 소유자로 나타났다.

[0026] 이 명세서에 사용된 일반적인 정의에서, 디지털 암호화 그룹의 소유자 또는 설립자는 소유자 또는 설립자로서의 상기 역할을 가지고 있음에도 불구하고 반드시 그룹의 구성원인 것은 아니다. 상황은 판독할 권리와 기록할 권리의 개념으로 시각화될 수 있다. 디지털 암호화 그룹의 구성원은 항상 판독할 권리를 가진다; 즉, 구성원은 구성원으로 남아 있는 한 그룹에 대해 저장된 속성에 지속적으로 액세스할 수 있다. 소유자는 기록 권한, 즉 그룹에 대해 저장될 속성을 결정할 수 있는 권한을 가지고 있지만, 그룹을 설정한 후 소유자는 나중에 저장된 속성이나 구성원들 간의 통신에 반드시 액세스할 수 있는 것은 아니다. 그러나 대부분의 경우 소유자가 또한 그룹의 구성원이 되는 것이 가장 실용적일 수 있다.

[0027] 디지털 암호화 그룹의 구성원은 사용자일 수 있지만 적어도 일부 경우에서 조직 및/또는 디바이스일 수도 있다. 구성원이 사용자인 경우, 엄밀한 의미에서 실제 디지털 통신에서 발생하는 당사자가 상기 사용자와 그룹 소유자에 의해 운영되는 전자 디바이스일지라도 사용자를 그룹의 구성원(및 그룹 소유자)으로 지칭하는 것이 일반적이다. 이러한 전자 디바이스는 예를 들어, 컴퓨터, 랩톱, 태블릿, 스마트폰, 휴대용 디지털 비서, 또는 처리 및 통신에 필요한 수단을 포함하는 어떤 다른 전자 디바이스일 수 있다. 일부 경우에, 사용자의 프로그래밍 가능한, 이식 가능한 전자 디바이스가 그러한 전자 디바이스로서 작용할 수 있다.

[0028] 단수인 디바이스에 대한 모든 참조는 동일한 사용자의 감독하에 함께 작동하는 두 개 이상의 디바이스의 그룹도 포괄하기 위한 것이다. 두 개 이상의 디바이스의 이러한 그룹은 사용자가 함께 연결한 디바이스들로 구성되는 것으로 설명될 수 있다. 자기 주권 신원(Self-Sovereign Identity; SSI)의 개념은 사용자가 관리 권한, 취급 권한 등과 같은 권리를 비롯하여, 그룹에 생성된 정보에 대한 제어를 암호학적으로 확립했음을 의미한다. 암호학적으로 확립된 제어는 단순히 특정 사용자 ID에 바인딩된 일부 저장된 권한을 기반으로 하는 권한과 다르다: 이는 사용자가 적절한 정보를 판독하고/하거나 기록하는 데 필요한 암호화 요소를 소유하고 있음을 의미한다. 암호화 그룹을 확립하는 것은 그룹의 구성원에게 그러한 필요한 암호화 요소를 소유할 수 있도록 하는 것을 목표로 한다.

[0029] 도 1은 실시예에 따른 방법을 실행할 때 신뢰 제공자, 그룹 소유자, 및 하나 이상의 그룹 구성원 사이의 일부 통신 및 이들에 의해 수행되는 일부 동작을 예시한다. 신뢰 제공자는 금고라고도 불릴 수 있으며, 이는 매우 높은 수준의 디지털 보안을 가진 기관을 대표한다는 가정을 강조한다. 신뢰 제공자에 대해서도 사용될 수 있는 유사한 지정(designation)으로는 지갑 제공자와 CA(Certification Authority) 및/또는 VA(Validation Authority)의 약어가 있다. 신뢰 제공자는 사적으로 운영될 수도 있고, 당국에 속하고/속하거나 당국의 감독하에 운영될 수도 있다.

[0030] 그룹 설정을 시작하려면 그룹 소유자는 형성될 그룹의 각 구성원을 디지털 방식으로 식별하기 위한 적어도 일부 수단을 보유하고 있어야 한다. 나중에 더 많은 구성원이 그룹에 추가될 수 있지만, 여기서는 미리 정의된 수의 알려진 사용자에 대해 그룹을 설정하는 경우가 먼저 고려될 것이다. 나중에 추가될 새 구성원과 관련하여, 이전의 기존 그룹에 새 구성원을 추가하는 것은 새 구성원을 추가하기 전에 새 구성원이 그룹에서 처리된 정보에도 액세스할 수 있음을 의미할 수 있음을 유의해야 한다. 이전에 처리된 정보는 그룹 내에서 별도로 암호화하거나, 기존 구성원이 시크릿 키를 자체로 보관하면서 서로에게 공개 키를 배포했을 수 있는 소위 PGP 키와 같이 그룹의 이전 구성원들 간에 교환되는 키로 암호화하여 새 구성원이 액세스할 수 없도록 할 수 있다. 또 다른 가능성

은 이전 구성원에게 알려진 키를 사용하여 이전 정보를 한 번만 암호화하고 각 이전 구성원에 대해 상기 키를 별도로 암호화하는 것이다. 이 마지막 가능성은 그룹 내에서 공유되는 정보의 양이 구성원 수에 비례하여 증가하지 않기 때문에 가장 비용 효율적인 방법일 수 있다; 각 이전 구성원은 그룹 내의 암호화된 정보에 대한 자신의 키를 안전하게 저장하기만 하면 된다. 새 구성원이 단정적으로(categorically) 이전에 처리된 정보에 액세스할 필요가 없는(또는 액세스하지 않아야 하는) 경우 새 구성원이 또한 속한 새 그룹을 설정하는 것이 더 간단할 수 있다. 기존 그룹 구성원은 나중에 그룹에서 제거될 수도 있다; 이를 위해서는 일반적으로 그룹과 관련된 정보를 안전하게 처리하는 데 사용되는 키들 중 적어도 일부를 갱신해야 한다.

[0031] 도 1은 사용자가 그룹 소유자에게 그룹 내에서 알려지기를 원하는 식별자를 전달하는 단계(101)를 개략적으로 도시한다. 그러나, 다음 설명의 목적상, 그룹 소유자가 그룹 구성원의 구성원 ID 또는 다른 식별자를 어떻게 그리고 언제 획득했는지는 의미가 없다는 점에 유의해야 한다. 그룹 소유자가 예를 들어, 연락처 정보 카탈로그, 인구 정보의 공식 등록부 또는 고객 데이터베이스를 유지 관리하는 경우 거기에서 그룹 구성원의 식별자를 판독할 수 있다. 그룹 내에 i명의 구성원이 있을 수 있으므로, i는 인덱스로 사용되는 양의 정수이며, 그룹 구성원(들)의 사용자 식별자(들)는 일반적으로 UID_i로 지칭될 수 있다.

[0032] 단계(101)에서(또는 임의의 다른 이전 단계에서) 그룹 소유자는 또한 설정될 그룹의 각 구성원으로부터, 비대칭 암호화 시스템의 사용자-특유 키 쌍의 절반을 구성하는 각각의 공개 키를 획득할 수 있다. 그러나 이것은, 이 명세서의 뒷부분에서 설명되는 바와 같이 그룹 구성원의 공개 키가 나중에 작동할 수도 있으므로 필요하지 않는다. 그룹 내 i번째 구성원의 공개키는 PK_{UIDi}로 지칭될 수 있다.

[0033] 단계(102)에서, 그룹 소유자는 AddGroup 요청, 즉 디지털 암호화 그룹을 설정하기 위한 요청을 작성한다. AddGroup 요청은 신뢰 제공자로 전달되며, 적어도 그룹 구성원의 식별자와 그룹 구성원에 의해 나중에 사용되도록 의도된 하나 이상의 속성을 포함해야 한다. 속성의 예로, 여기서는 P_{G0}이라는 사전 공유 키(pre-shared key; PSK)가 고려된다. 이러한 PSK는 그룹 구성원들 간의 공유되는 시크릿으로서, 예를 들어, 대칭 암호화 방법의 암호화 및 복호화 키로서 사용하기 위한 것일 수 있다. PSK 및/또는 다른 속성은 KGA라는 약어로 알려진 키스토어 그룹 아카이브(Keystore Group Archive)라는 데이터 구조의 일부로서 처리된다. 공식 지정에 따라,

[0034] $KGA(P_{G0},...)$이 있으며,

[0035] 여기서 3개의 마침표는 KGA가 그룹 구성원의 식별자 UID_i 및/또는 그룹 구성원(중 적어도 일부)의 공개 키 PK_{UIDi}와 같은 다른 속성도 포함할 수 있음을 나타낸다. 이들이 명시적으로 나열되어야 하는 경우, 공식적인 지정은

[0036] $KGA(P_{G0},UID_i,PK_{UIDi},...)$일 수 있다.

[0037] KGA에서 가능한 기타 속성의 예로는 디지털 암호화 그룹의 명칭 및/또는 다른 식별자, 예를 들어, 디지털 암호화 그룹의 생성 시간 및 수정 시간을 표시하는 타임스탬프, 디지털 암호화 그룹이 유효하게 유지되어야 하는 기간을 보여주는 만료 데이터, 요청이 전달될 신뢰 제공자의 식별자, 및 디지털 암호화 그룹의 임의의 양상(들)과 관련된 메타데이터를 포함하지만 이에 제한되지 않는다.

[0038] 보안을 위해 단계(102)는 KGA를 암호화하는 것을 포함해야 한다. 암호화 키 K_{KGA}를 생성하는 유리한 방식은

[0039] $K_{KGA} = SHA2(X25519(SK_{UID},PK_{VID})||PK_{VID}||PK_{UID}||n)$이며,

[0040] 여기서 SHA2()는 괄호 안의 인수에 대해 수행된 보안 해시 알고리즘 2를 수행하는 것을 나타내고 X25519()는 괄호 안의 인수에 대해 Curve25519 타원 곡선 디피-헬먼 방법(Elliptic Curve Diffie-Hellman method)을 적용하는 것을 나타낸다. 문자 n은 암호화 난스(cryptographic nonce), 예를 들어, 12 비트의 고유한 난스를 나타낸다. 이중 수직선 ||은 비트 논리 OR 연산을 의미한다. PK_{VID} 키 및 PK_{UID} 키는 각각 신뢰 제공자(PK_{VID})와 그룹 소유자(PK_{UID})의 공개 키이다.

[0041] KGA의 암호화는 예를 들어, 갈루와/카운터 모드(Galois/Counter Mode)에서 256 비트 AES를 의미하는 AES256-GCM 방법을 사용하여 수행될 수 있다. 지금까지 소개된 표기법을 사용하여 암호화된 KGA는

[0042] $Enc(K_{KGA}, KGA(P_{G0},UID_i,PK_{UIDi},...))$

[0043] $= AES256\text{-}GCM(SHA2(X25519(SK_{UID},PK_{VID})$

[0044] ||PK_{VID}||PK_{UID}||n),m,n, KGA(P_{GO},UID_i,PK_{UIDi},...))와 같이 표현될 수 있으며,

[0045] 여기서 문자 m은 암호화 인증 태그에 대해 MAC 또는 메시지 인증 코드를 나타낸다.

[0046] 또한, 단계(102)가 비대칭 암호화 방법의 임시 키(ephemeral key)쌍의 생성을 포함하도록 하는 것이 유리하다. 이러한 임시 키는 여기서 PK_{GRT} 및 SK_{GRT}라고 하며, 여기서 PK는 공개 키를 의미하고, SK는 시크릿 키를 의미하고, 아래 첨자 GRT는 그룹 요청 토큰이라는 단어에서 유래한다. 그룹 소유자는 시크릿 키 SK_{GRT}를 저장된 상태로 유지하고 AddGroup 요청에서 공개 키 PK_{GRT}를 신뢰 제공자에게 제공할 것이다. 이러한 방식으로 신뢰 제공자는 공개 키 PK_{GRT}를 사용하여 최종 응답을 암호화할 수 있으므로 그룹 소유자만 최종 응답을 복호화할 수 있을 것이다. 이러한 키의 임시 특성은 필수는 아니지만 나중에 이러한 키들 중 하나를 손에 넣을 악의적인 당사자가 그것을 거의 사용하지 않을 것이기 때문에 보안을 추가한다.

[0047] 그룹 소유자로부터 신뢰 제공자에게 완료된 AddGroup 요청을 송신하는 단계는 도 1에 단계(103)로서 도시된다. AddGroup이라는 지정 및 도 1의 모든 다른 특정 지정은 예시적인 것일 뿐이며, 어떠한 의미에서도 제한적으로 해석되어서는 안 된다; 당연히 메시지에 어떤 다른 명칭이 사용될 수 있다. 또한, 여기서 설명되는 모든 정보를 단일 메시지로 전달할 필요는 없지만, 공통 통신 채널 또는 복수의 채널을 통한 다중 송신이 사용될 수 있다. 위에서 소개된 표기법을 사용하여, 단계(103)에서의 AddGroup 요청은 적어도 임시 공개 키 PK_{GRT} 및 암호화된 KGA를 포함할 수 있다.

[0048] 보안 전송 메커니즘은 단계(103)에서 그룹 소유자로부터 신뢰 제공자에게 AddGroup 요청을 전달하기 위해 가장 유리하게 사용된다. 이러한 보안 전송 메커니즘의 비제한적인 예는 TLS(Transport Layer Security) 프로토콜이 사용될 수 있는 디지털 통신 채널이다. 여기서 신뢰 제공자로 지칭되는 장치(arrangement)는 암호화 동작을 수행할 수 있는 암호화 엔진에 결합된 이러한 보안 전송 메커니즘의 수신단 및 송신단을 포함한다. 보안 전송 메커니즘을 통한 수신 및 송신이 반드시 동일하거나 유사한 채널 또는 연결을 거치는 것은 아니지만, 보안 전송 메커니즘을 통한 수신 및 송신이 동일하거나 유사한 채널 또는 연결을 거치는 것이 제외되지도 않는다.

[0049] 도 1의 단계(104)는 일반적으로 신뢰 제공자가 요청된 디지털 암호화 그룹을 설정하는 것, 및 이를 나중에 요청에 따라 그룹의 구성원에게 전달될 수 데이터 구조의 형태로 저장하는 것으로 특징지어질 수 있다. 단계(104)는 또한 신뢰 제공자의 장치 내의 암호화 엔진이 암호화 제품을 생성함으로써, 복수의 사용자 식별자(UID_i)를 포함하는 제1 요청(즉, AddGroup 요청(103))을 상기 보안 전송 메커니즘을 통해 수신하는 것에 응답하도록 특징지어질 수 있다. 여기서 암호화 제품이라는 단어는 디지털 암호화 그룹을 지칭하며, 이는 그룹 구성원들 간의 보안 통신을 가능하게 하기 위한 키 또는 키들뿐만 아니라 그룹 구성원의 사용자 식별자를 적어도 포함한다. 디지털 암호화 그룹은 또한 다양한 다른 정보를 포함할 수 있으며, 이는 이 명세서의 뒷부분에서 더 자세히 설명될 것이다.

[0050] KGA가 암호화된 형태로 AddGroup 요청(103)에서 도착했으므로 신뢰 제공자의 장치는 먼저 이를 복호화해야 한다. 그룹 소유자가 AddGroup 요청(103)에서 KGA를 암호화하기 위한 암호화 키를 생성하기 위해 전술한 방법을 사용했다고 가정하면, 신뢰 제공자의 장치는 키를

[0051] K_{KGA} = SHA2(X25519(SK_{VID},PK_{UID})||PK_{VID}||PK_{UID}||n)과 같이 재생성하고

[0052] 재생성된 키를 사용하여 KGA를 복호화한다.

[0053] 전술한 바에 따르면, AddGroup 요청(103)을 구성할 때, 그룹 소유자는 자신이 소유하고 있는 모든 그룹 구성원들(또는 심지어 그들 중 임의의 그룹 구성원)의 사용자 특유 (공개) 암호화 키를 반드시 가지고 있지는 않다. 이러한 이유로, 단계(104)의 일부로서, 수신된 AddGroup 요청(103)이 각 사용자 식별자에 대해 각각의 사용자 특유 암호화 키를 포함했는지 여부를 확인하도록 신뢰 제공자의 장치를 구성하는 것이 유리하다. 그렇지 않다면, 신뢰 제공자의 장치는 상기 복수의 사용자 식별자 각각에 대해 각각의 사용자 특유 암호화 키를 포함하도록 상기 제1 요청에서 수신된 데이터를 증강하도록 구성될 수 있다.

[0054] 한 가지 가능성은 신뢰 제공자가 예를 들어, 상기 사용자와 가진 일부 이전 통신을 기반으로 각각의 사용자 특유 (공개) 암호화 키를 이미 알고 있다는 것이다. 또 다른 가능성으로서, 신뢰 제공자의 장치는 장치 외부의 소스로부터 각각의 사용자 특유 암호화 키를 요청하고 수신함으로써 상기 증강을 수행하도록 구성될 수 있다. 예를 들어, 두 개 이상의 신뢰 제공자가 서로 연결된 경우를 고려할 수 있다. 각각의 이러한 신뢰 제공자는 자신

에게 이전에 알려진 사용자의 데이터베이스를 가지고 있다: 신뢰 제공자는 예를 들어, 특정 사용자가 이전에 통신한 적이 있는 다른 기관, 및/또는 각각 자체 고객 데이터베이스를 가진 다른 영리 기업일 수 있다. 사용자 특유 암호화 키, 특히 공개 키는 이러한 데이터베이스에 일상적으로 저장된 것처럼 보일 수 있으며, 각각의 이러한 저장된 암호화 키는 AddGroup 요청에 사용된 것과 유사한 종류의 각각의 사용자 식별자와 명확한 관계를 갖는다. 신뢰 제공자의 장치는 하나 이상의 이러한 연결된 신뢰 제공자에게 요청을 송신하고, 이에 응답하여 요청된 사용자 특유 암호화 키를 획득할 수 있다.

[0055] 유사한 원칙이 암호화 그룹에 포함될 다른 데이터에 대해서도 적용될 수 있다: 신뢰 제공자의 장치는 자체 또는 연결된 다른 소스로부터의 요청, 또는 둘 다에 의해 임의의 누락된 정보 요소를 생성함으로써 암호화 그룹의 미래의 콘텐츠(contents-to-be)를 증강할 수 있다. 신뢰 제공자의 장치는 필요한 경우 암호화 그룹의 생성 및 처리를 관리하는 사전 정의된 사양에 따라 임의의 이러한 증강을 수행한다.

[0056] 신뢰 제공자의 장치는 AddGroup 요청(103)에서 수신된 정보의 임의의 조각, 예를 들어, 사용자 관련 정보를 또 다른 소스로부터의 (사용자-관련) 정보의 대응 조각에 대조 확인하도록 구성될 수 있다. 실행되는 경우 이러한 확인의 목적은 사용자 관련 정보의 이러한 조각들이 서로 매칭되는지 여부를 발견하는 것이다. 예를 들어, AddGroup 요청(103)이 하나 이상의 사용자 특유 (공개) 암호화 키를 포함한 경우, 신뢰 제공자의 장치는 이것들을 자신의 데이터베이스와 비교하거나, 또는 - 자신의 데이터베이스에서 발견되지 않는 경우 - 전술한 사용자 특유 암호화 키를 요청하는 경우에서와 아주 유사하게, 아마도 연결된 다른 신뢰 제공자에게 다시 요청을 할 수 있다.

[0057] 각 사용자(또는 그룹 내의 멤버십에 대해 자격이 있는 다른 당사자)는 일부 신뢰 제공자에게 "속하거나" 일부 신뢰 제공자에 의해 원래 안전하게 식별된 것으로 간주될 수 있다. 자신의 장치가 AddGroup 요청(103)을 수신한 신뢰 제공자는 새로운 그룹에 구성원으로서 포함될 모든 그러한 사용자를 원래 안전하게 식별한 신뢰 제공자가 아닐 수 있다. 다시 말하면, AddGroup 요청(103)은 장치가 AddGroup 요청을 수신한 신뢰 제공자와는 다른 하나 이상의 신뢰 제공자에게 "속하는" 그룹의 하나 이상의 의도된 구성원의 UID를 포함할 수 있다. 이러한 경우, 한 가지 가능성은 신뢰 제공자의 장치가 "자신의" 사용자들 중 한 명이 문제가 될 경우 사용자 특유 암호화 키를 사용할 빈 공간을 단지 남겨 두는 것이다. 이러한 동작 방식, 즉 "외부" 사용자의 사용자 특유 암호화 키를 비워 두는 것은 이 명세서의 뒷부분에서 설명되는 특정 추가 결과를 가질 수 있다.

[0058] 사용자 관련 정보의 상기 조각들이 서로 매칭되지 않는 경우, 신뢰 제공자의 장치는 디지털 암호화 그룹의 확립이 계속되도록 허용되는지 여부에 대한 결정을 내릴 수 있다. 신뢰 제공자의 장치가 어떻게 동작하도록 프로그래밍되어 있는지, 그리고 어떤 종류의 결정 기준을 그 장치가 적용하는지에 따라 긍정적 결정과 부정적 결정이 모두 가능하다.

[0059] 위에서 사용자 식별자 외에도 디지털 암호화 그룹이 완료되면 그룹 구성원들 간의 보안 통신을 가능하게 하는 키 또는 키들을 포함하여야 한다는 점이 이미 지적되었다. 사용자 특유 (공개) 암호화 키는, 각 사용자가 대응 시크릿 키가 안전하게 저장되게 한다고 가정할 수 있으므로 이 요건을 충족할 수 있다. 이러한 키의 또 다른 예는 일반적으로 사용자 식별자에 의해 식별되는 사용자들 간의 대칭 암호화에 사용하기 위한 공통 암호화 키로서 정의되는, 위에서 P_{GO}라고 하는 사전 공유된 키(pre-shared key; PSK)이다. 그룹 소유자가 이미 P_{GO}를 생성한 경우, 신뢰 제공자의 장치는 단순히 복호화된 KGA로부터 이를 판독하고 디지털 암호화 그룹의 일부로 이것을 저장할 수 있다. 또 다른 대안으로, 신뢰 제공자의 장치는 이러한 PSK를 생성하고 디지털 암호화 그룹의 일부로서 이것을 저장할 수 있다.

[0060] P_{GO} 또는 다른 PSK는 그룹 구성원이 나중에 완전히 의존할 수 있어야 하는 암호화 그룹에 포함된 속성(또는 정보 요소)의 예이다. 이러한 보안을 제공하기 위해서는, 그룹 소유자에 의해(그룹 소유자가 이미 P_{GO}를 생성한 경우) 그리고/또는 신뢰 제공자의 장치에 의해 P_{GO} 또는 다른 PSK가 디지털로 서명되게 하는 것이 유리하다. 알려진 원칙에 따라, 서명 당사자는 디지털 서명을 위해 자신의 시크릿 서명 키를 사용하므로 나중에 다른 당사자가 서명 당사자의 대응 공개 검증 키를 사용하여 해당 정보 요소의 무결성을 검증할 수 있다.

[0061] 방법의 후속 단계에서 추가적인 보안을 제공하기 위해, 단계(104)의 일부로서, 비대칭 암호화 방법의 추가적인 임시 키 쌍을 생성하도록 신뢰 제공자의 장치를 구성하는 것이 유리하다. 이 임시 키 쌍은 여기에서 그룹 액세스 토큰을 의미하는 아래 첨자 GAT와 함께 참조된다. 비제한적인 예로서, 신뢰 제공자의 장치는 시크릿 GAT 키 SK_{GAT}를

[0062] SK_{GAT} = RNG(256)와 같이 생성할 수 있으며,

[0063] 여기서 연산자 RNG()는 괄호 안의 (10진법) 숫자만큼 많은 비트를 가진 랜덤 2진수를 생성하는 것을 의미한다. 이후, 대응 공개 키 PK_{GAT}는 예를 들어, scalarbasemult(SK_{GAT})로부터 공개 키로서 생성될 수 있다. 여기서 scalarbasemult()는 예를 들어, Curve 25519와 같은 타원 곡선을 기반으로 시크릿 키가 입력으로 주어졌을 때 대응 공개 키를 결정론적으로 반환하는 함수이다. 함수의 이름은 사용된 소스에 따라 변경될 수 있지만, 본 명세서를 작성하는 시점에서 원래 scalarmult() 함수에 대한 문서는 https://doc.libsodium.org/에서 찾아볼 수 있다. 시크릿 키와 공개 키 쌍이 생성되어야 할 때마다 두 키를 모두 출력으로 제공하는 적절한 단일 함수를 사용하여 이것이 수행될 수도 있다.

[0064] 신뢰 제공자의 장치는, 단계(104)에서 이것이 그룹 소유자에게 응답을 송신하기 전에 이 디지털 암호화 그룹을 생성하는 경우(또는 이전에 생성된 디지털 암호화 그룹을 갱신하지만 다른 그룹 구성원들 중 임의의 그룹 구성원과 통신하기 전에 갱신하는 경우)였는지, 또는 암호화가 그룹 소유자 이외의 그룹 구성원과의 통신과 연관되어 수행되는지에 따라, 생성되거나 갱신된 KGA를 약간 다른 방식으로 암호화하도록 구성될 수 있다; 도 1의 단계(109)가 참조된다. 첫 번째로 언급된 경우에서, 그룹 소유자에 특유한 이전에 획득된 키를 활용하는 것이 유리한 가능성이다. 이러한 키를 생성하고 처리하는 유리한 방법은 공동 계류 중인 특허 출원 제EP22157019.5호에 설명되었으며, 이는 이 명세서의 출원일에 일반에 공개되어 있지 않다. 문제의 키는 상기 방법에서 SK_{UAT}라고 하며, 여기서 아래 첨자 UAT는 사용자 액세스 토큰(User Access Token)으로부터 유래한다. 새로 생성된 KGA를 암호화하는 프로세스는

[0065] SS_{GAK} = scalarmult(SK_{GAT}, PK_{GRT})와 같이 공유 시크릿 SS_{GAK}를 생성하는 것을 수반할 수 있으며,

[0066] 여기서 아래 첨자 GAK는 그룹 아카이브 키(Group Archive Key)로부터 유래한다. 함수 scalarmult()는 예를 들어, Curve 25519와 같은 타원 곡선을 기반으로 두 당사자 간에 계산적으로 공유된 시크릿을 반환하는 함수이며, 수학적으로 연결된 키 쌍들에 의해 확립된 보안에 의존하면서 실제 키를 송신할 필요가 없게 한다. 그런 다음, 새로 생성된 KGA는

[0067] Enc(SS_{GAK}, KGA(...))와 같이 암호화될 수 있으며,

[0068] 여기서 세 기간은 KGA에 포함되는 모든 정보를 다시 일반적으로 나타낸다. 이 경우가 SS_{GAK}를 키로서 사용해 이전에 암호화된 KGA를 갱신하는 경우들 중 하나였지만, 그룹 소유자 이외의 임의의 그룹 구성원과 통신하기 전에 갱신하는 경우였으면, 갱신 동작은

[0069] Update(Dec(SS_{GAK}, KGA(...)))와 같이 설명될 수 있으며,

[0070] 그 후 새로운 암호화는 위와 유사하게 발생할 수 있다.

[0071] 단계(109)의 일부로서 암호화가 수행되는 경우, 그룹 소유자 이외의 그룹 구성원과의 통신과 연관되어, 이 명세서의 앞부분에서 소개된 시크릿 GAT 키 SK_{GAT}를 활용하여 추가된 보안이 획득될 수 있다. 이 경우, 공유 시크릿 SS_{GAK}은

[0072] SS_{GAK} = scalarmult(SK_{GAT}, PK_{GRT})와 같이 획득될 수 있으며,

[0073] 여기서 아래 첨자 GAK는 그룹 아카이브 키로부터 유래한다. 그런 다음, KGA는

[0074] Enc(SS_{GAK}, KGA(...))와 같이 암호화될 수 있다.

[0075] 이러한 방식으로 신뢰 제공자의 장치에 KGA를 SS_{GAK}로 암호화된 형태로 저장하면, 저장된 KGA를 복호화하기 위해 신뢰 제공자 외부의 소스로부터 도달하는 키가 항상 필요하다는 목적에 부합한다. 따라서 신뢰 제공자에서의 보안이 손상되고, 저장된 KGA가 노출되더라도, 그룹 소유자 또는 다른 그룹 구성원들 중 한 명으로부터 도달해야 하는 그러한 키 구성 요소 없이는 신뢰 제공자조차도 자신의 암호화된 콘텐츠에 액세스할 수 없기 때문에 이러한 손상 및 노출은 공격자에게는 거의 쓸모가 없을 것이다.

[0076] 전술한 절차적 단계들의 결과로서, KGA(즉, 단계(104)에서 신뢰 제공자의 장치의 암호화 엔진이 생성한 암호화 제품)는 예를 들어,

[0077] $KGA(P_{GO},UID_i,PK_{UIDi},PID,GID,GMD,...)$로서 설명될 수 있으며,

[0078] 여기서 P_{GO}는 그룹을 위한 PSK이고, UID_i는 나열된 그룹 구성원(그룹 소유자를 포함함)을 식별자로 표시하고, PK_{UIDi}는 그룹 구성원의 (공개) 사용자 특유 암호화 키를 표시하고, PID 또는 제공자 ID는 신뢰 제공자의 공개 식별자이고, GID 또는 그룹 ID는 그룹의 공개 식별자이고, GMD 또는 그룹 메타데이터는 그룹과 연관된 모든 가능한 메타 데이터를 표시한다. 그룹 소유자의 식별자 및/또는 공개 키는 이들 중 하나 또는 모두를 UID_i 및 PK_{UIDi}의 나머지 부분과 구별할 수 있도록 선별될 수 있다.

[0079] 암호화 그룹에 있는 속성의 신뢰성을 향상시키기 위해, 신뢰 제공자의 장치는 자신이 암호화 그룹에 포함하는 정보 요소를 디지털 서명하기 위해 소유 중인 서명 키를 사용하도록 신뢰 제공자의 장치를 구성하는 것이 유리하다. 이렇게 하면 그룹의 모든 구성원이 나중에 암호화 그룹으로부터 판독된 속성이 올바른지, 즉 원본성과 무결성이 손상되지 않았는지 보장할 수 있다.

[0080] 신뢰 제공자의 장치가 AddGroup 응답을 그룹 소유자에게 송신하는 단계는 도 1의 단계(105)로서 도시된다. 이전에 단계(103)에서의 AddGroup 송신과 유사하게, 신뢰 제공자의 장치는 AddGroup 응답(105)에서 그룹 소유자에게 KGA를 송신하기 전에 KGA를 유리하게 암호화한다. 이러한 암호화의 유리한 형태는

[0081] $Enc(K_{KGA}, KGA(...))$

[0082] $= AES256\text{-}GCM(SHA2(X25519(SK_{VID},PK_{UID})$

[0083] $||PK_{VID}||PK_{UID}||n),m,n, KGA(...))$이다.

[0084] 단계(105) 이후에, 그룹 소유자는 단계(104) 동안에 신뢰 제공자가 자신의 모션에 대해 제공하고/하거나 연결된 다른 신뢰 제공자 또는 다른 소스로부터 요청한 증강된 정보를 비롯하여, 그룹에 대한 모든 필요한 정보를 갖는다. 또한 그룹 소유자는 그룹에 대한 모든 필요한 정보가 신뢰 제공자의 장치에 안전하게 저장되며 거기로부터 그룹의 구성원에게 배포될 준비가 되어 있음을 알고 있다.

[0085] 단계(106)는 그룹 소유자가 그룹 구성원에게 신뢰 제공자에게 연락하고 신뢰 제공자의 장치로부터 KGA를 다운로드하도록 지시하는 것을 나타낸다. 그룹 구성원이 그렇게 할 수 있도록 하는 한 가지 유리한 방식은 그룹 요청 토큰의 복사본, 즉 임시 공개 키 PK_{GRT}를 그룹 구성원에게 송신하는 것이다. 추가적으로 또는 대안적으로, 그룹 소유자는 단계(106)에서 그룹에 대한 다른 정보를 그룹 구성원에게 송신할 수 있다.

[0086] 도 1에 도시된 나머지 단계들은 그래픽 명확성을 유지하기 위해 하나의 그룹 구성원에 대해서만 도시된다. 그룹이 완전히 동작하도록 하려면 모든 그룹 구성원에 대해 유사한 단계들이 실행되어야 한다. 그러나 하나 이상의 그룹 구성원이 자신의 역할을 수행하지 못하더라도 대응 단계의 실행을 완료한 그룹의 구성원은 이미 그룹을 활용할 수 있다. 여기서, 그룹의 한 구성원만이 실제로 이러한 단계를 수행하고 미래에 암호화 그룹을 활용하더라도, 신뢰 제공자를 그룹과 관련된 정보 요소의 보안 저장소로서 사용함으로써 특정 이점이 얻어질 수 있다는 것을 주목할 수 있다.

[0087] 단계(107)는 그룹 구성원이 그룹에 관한 필요한 정보를 획득하기 위한 요청을 작성하는 것을 나타내고, 단계(108)는 그룹 구성원이 여기서는 GetGroup 요청이라고 불리는 요청을 신뢰 제공자에게 송신하는 것을 나타낸다. 단계(108)에서의 송신은 TLS(Transport Layer Security) 프로토콜이 사용될 수 있는 디지털 통신 채널과 같은 보안 전송 메커니즘을 활용할 수 있다는 점에서 이전 단계(103)에서의 송신과 유사하다.

[0088] GetGroup 요청(108)은 신뢰 제공자가 송신자, 즉 그룹 구성원이 그룹의 구성원으로서 동작하기 위해 필요한 KGA를 수신하도록 허용되는 구성원들 중 하나임을 보장할 수 있도록 허용해야 한다. 바람직하게는, 그러므로 GetGroup 요청(108)은 적어도 사용자 식별자 UID를 포함하며, 그 후 신뢰 제공자는 이것을 자신이 그룹 소유자로부터 이전에 수신한 사용자 식별자 UID_i의 목록과 비교할 수 있다. GetGroup 요청(108)이 사용자 식별자 UID를 포함하게 하는 한 가지 유리한 방식은 GetGroup 요청(108)이 요청 당사자의 인증서를 포함하게 하는 것인데, 이 인증서는 UID와 요청 당사자의 공개 키를 모두 포함한다. 이 경우, 위에 언급된 목적을 위해 UID와, 요청 당사자에게 응답으로서 송신할 KGA를 보호하기 위한 공개키를 사용할 수 있다.

[0089] 또한, GetGroup 요청(108)은 그룹 요청 토큰, 즉 임시 공개 키 PK_{GRT}를 포함하는 것이 유리하다. GetGroup 요청이 포함할 수 있는 다른 가능한 정보 요소는, 적어도 요청하는 그룹 구성원이 이전에 그룹 소유자로부터 이러한

정보 요소를 얻은 경우, 그룹 식별자 GID, 그룹 소유자의 식별자에 대한 참조, 다양한 유형의 서명되거나 서명되지 않은 속성, 및/또는 그룹과 관련된 임의의 메타데이터를 포함하지만 이들에 제한되지는 않는다.

[0090] 도 1의 단계(109)는 일반적으로 신뢰 제공자의 장치가 GetGroup 요청(108)을 수신하는 것에 응답하여 수행하도록 구성되는 모든 확인을 나타낸다. 기본적으로, 신뢰 제공자의 장치 내의 암호화 엔진은, 이전에 생산된 암호화 제품, 즉, 디지털 암호화 그룹을 보안 전송 메커니즘을 통해 송신함으로써, GetGroup 요청(108)(AddGroup 요청(103)에서 이전에 수신된 복수의 사용자 식별자들 중 하나를 포함함)을 상기 보안 전송 메커니즘을 통해 수신하는 것에 응답하도록 구성된다.

[0091] KGA가 신뢰 제공자의 장치에 암호화된 형태로 이전에 저장되었다는 점을 감안할 때, 이 장치는 먼저

[0092] SS_{GAK} = scalarmult(SK_{GAT}, PK_{GRT})와 같이 복호화에 필요한 키 SS_{GAK}를 재생성하고,

[0093] 그런 다음, 복호화 Dec(SS_{GAK}, KGA(...))를 수행한다.

[0094] 그런 다음, 장치는

[0095] n = RNG(96)를 난스로서 그리고

[0096] K_{KGA} = SHA2(X25519(SK_{VID},PK_{UID})||PK_{VID}||PK_{UID}||n)를

[0097] (인증서가 GetGroup 요청에서 수신된 경우 인증서로부터 판독된 이 특정 사용자의 PK_{UID}를 사용하여) 암호화 키로서 제공함으로써, 그리고 그런 다음,

[0098] Enc(K_{KGA}, KGA(...))

[0099] = AES256-GCM(SHA2(X25519(SK_{VID},PK_{UID})

[0100] ||PK_{VID}||PK_{UID}||n),m,n, KGA(...))를 암호화함으로써, 이번에 요청 그룹 구성원으로의 송신을 위해 KGA를 다시 암호화하도록 진행할 수 있다.

[0101] 보안의 관점에서, 단계(109)에서 (그리고 나중에 도 2의 단계(210)에서) 키스토어 그룹 아카이브가 특정 사용자의 공개 키 PK_{UID}에 대해 사용자를 위해 보안되기 때문에, 위에서 언급된 인증서가 항상 요청자로부터 유래하도록 요구하는 것이 특히 유리하다. 인증서는 위에서 언급된 것처럼 GetGroup 요청에서 도달할 수 있지만, 예를 들어, 동일한 출원인의 공동 계류 중인 유럽 특허 출원 제EP22157019.5호에 설명된 방법에 따라 어떤 다른 PKI 기반 솔루션을 통해 신뢰 제공자의 장치를 알게 되었을 수도 있다. 추가적으로 또는 대안적으로, 적절한 지능형 ID 카드, 여권 또는 대응 문서가 존재하는 경우, 신뢰 제공자의 장치는 그것으로부터 인증서를 사양 X.509에 따라 RSA 또는 ECC 인증서로서 판독할 수 있다.

[0102] 마찬가지로, 보안의 관점에서도 신뢰 제공자의 장치에 의해, 또는 여러 개의 상호 연결된 신뢰 제공자의 경우 이러한 상호 연결된 신뢰 제공자들 중 하나의 장치에 의해 인증서가 서명되도록 요구하는 것이 매우 유리하다. 그런 다음, 인증서를 수신하는 임의의 당사자는 인증서의 무결성과 인증성을 확인하고 신뢰할 수 있는 당사자에 의해(즉, 신뢰 제공자 또는 상호 연결된 신뢰 제공자들 중 하나에 의해) 그것이 서명되었는지 확인할 수 있다. 이는 결국 인증서에 포함된 공개 키가 신뢰될 수 있음을 증명한다.

[0103] 난스 n에 대해 이것이 IETF에 의해 허용되는 AES-256 GCM 알고리즘의 요건과 관련이 있음을 알 수 있다. 특히 이것은 장기간 사용하는 경우 최대 350 GB까지 32개의 추가적인 비트의 향상된 보안을 암호화 키에 제공한다.

[0104] 도 1의 단계(110)는 신뢰 제공자의 장치가 암호화된 KGA를 그것을 요청한 그룹 구성원에게 송신하는 것을 나타낸다. 송신은 선행의 GetGroup 요청(108)과의 연관성을 강조하기 위해 도 1에서 GetGroup 응답으로 레이블링된다. 이전의 지정 AddGroup과 마찬가지로 지정 GetGroup은 당연히 예시일 뿐이며 다른 지정이 사용될 수 있다.

[0105] 도 1에 도시된 종류의 방법을 적용하는 예로서, 일상적인 순찰 중인 경찰관이 시민을 멈춰 세우고 그 특정한 종류의 차량을 운전할 수 있는 시민의 권리를 확인하고자 하는 상황을 고려할 수 있다. 운전 면허증 발급을 담당하는 국가 기관이 그룹 소유자 역할을 할 수 있다. 이미 이전에, 현재 유효한 운전 면허증을 부여할 때, 기관은 그 자체가 그룹 소유자이고 시민이 구성원인 디지털 암호화 그룹을 구성했을 수 있다. 그룹을 형성할 때 기관은 허용되는 차량 유형을 신뢰 제공자에게 속성으로서 전달했을 수 있고 신뢰 제공자에게 이러한 속성을 디지털 서명하도록 요청했을 수 있다. 그런 다음, 시민이 대응 GetGroup 요청을 송신하여 그룹에 가입하면 디지털 서명된

속성은 "디지털 지갑", 즉 시민의 사용자 디바이스에 있는 전용 저장 위치에 저장되었다. 속성은 기본 문서(이 예에서는 운전 면허증)가 유효한 기간 동안 유효할 수 있다.

[0106] 시민으로부터 (공개) 사용자 식별자를 알게 된 후 경찰관은 자신의 사용자 ID(및 아마도 공개 키)를 제공하고 시민의 사용자 식별자를 요청에 속성으로서 또한 추가하여 기관에 요청을 송신할 수 있다. 그런 다음, 기관은 신뢰 제공자에게 AddGroup 요청을 송신할 수 있으며, 기본적으로 시민으로부터 "허용되는 차량 유형" 속성을 수신하기 위한 권리와 함께 이전에 형성된 디지털 암호화 그룹에 경찰관이 임시로 추가되도록 요청한다. 대안으로, 경찰관(또는 근무 중일 때 개별 경찰관에 대한 대응 파생 권리를 갖는, 기관으로서의 경찰력)은 시민의 운전 면허증을 오프라인에서도 검사할 수 있도록 이미 이전에 그룹의 (영구 또는 적어도 장기) 구성원이 되게 되었을 수 있다.

[0107] 신뢰 제공자의 장치는 디지털 암호화 그룹에 대한 요청된 추가를 수행할 수 있다. 그런 다음, 그룹 요청 토큰을 포함하는, 경찰관의 사용자 디바이스에 해당 표시가 도달할 것이다. 그런 다음, 경찰관의 사용자 디바이스가 신뢰 제공자에게 GetGroup 요청을 송신하면 결국 필요한 정보를 포함하는 GetGroup 응답을 수신한다. 이 통신 라운드 동안에, 하나 이상의 속성이 디지털 암호화 그룹에 추가되었을 수 있다: 예를 들어, 경찰관의 사용자 디바이스가 짧은 기간 동안만 그룹의 구성원으로 유지되도록 허용하는 시간 제한 유효성 정보.

[0108] 경찰관이 디지털 암호화 그룹의 구성원이 되면, 시민과 경찰관의 사용자 디바이스는 시민의 사용자 디바이스가 이전에 획득되고 디지털 서명된 속성인 "허용되는 차량 유형"을 경찰관의 사용자 디바이스에 제시하는 로컬 통신에 진입할 수 있다. 디지털 서명으로 인해 후자는 제시된 속성이 유효한지 검증할 수 있다. 모든 확인이 완료되면 경찰관의 사용자 디바이스는 추가되었을 때와 유사한 통신 라운드를 통해 디지털 암호화 그룹으로부터 제거되거나 단순히 이전에 언급된 시간 정보에 의존하여 디지털 암호화 그룹 내의 경찰관의 멤버십이 만료되게 할 수 있다. 또 다른 대안으로, 이 그룹에서 경찰의 영구적인 멤버십 또는 적어도 장기 멤버십이 있다.

[0109] 위와 같은 예시 사례에서 기관은 오래된 속성(또는 적어도 심하게 오래된 속성은 아님)이 사용자의 디바이스에 저장된 상태로 남아 있지 않도록 하기 위해 암호화 그룹의 속성을 정기적으로 갱신하길 원할 수 있다. 시민의 사용자 디바이스는 알려진 갱신 일정에 따라 그리고/또는 당국에 의해 갱신하도록 프롬프트됨에 따라 신뢰 제공자로부터 갱신된 암호화 그룹을 가져올 수 있다.

[0110] 도 2는 실시예에 따른 방법을 실행할 때 2명의 신뢰 제공자, 그룹 소유자, 및 하나 이상의 그룹 구성원 사이의 일부 통신 및 이들에 의해 수행되는 일부 동작을 예시한다. 이러한 실시예의 배경으로서, 각 사용자가 자신의 선택된 신뢰 제공자에게 "속할" 수 있다는 가정을 상기할 수 있다. 이 예에서 중간에 있는 두 개의 세로줄은 신뢰 제공자의 장치를 나타내고 오른쪽과 왼쪽에 있는 두 개의 세로줄은 그에 따라 그룹 소유자와 그룹 구성원을 나타낸다. 예시를 위해, 도 2에 도시된 예는 그룹 소유자가 그룹 구성원에게 보호된 전화 통화를 설정하고자 하는 실제 사용 사례와 관련된 것으로 간주될 수 있다.

[0111] 도 2의 단계(201)는 그룹 소유자가 어떤 방식으로든 그룹 구성원의 식별자를 획득했어야 한다는 점에서 도 1의 단계(101)와 유사하다. 이 단계는 예를 들어, 사용자 디바이스에 서로의 전화번호를 저장하는 사용자에게 일반적으로 나타나는 것처럼 심지어 매우 오래 전에 수행되었을 수 있다.

[0112] 단계(202)는 또한 그룹 소유자의 사용자 디바이스가 보호된 호출을 설정하는 것을, 즉 보호된 통화가 발생할 수 있는 암호화 그룹을 생성하는 것을 목표로 하는 단계를 수행하는 것을 나타낸다는 점에서 도 1의 대응 단계(102)와 유사하다. 작성된 요청은 단계(203)로서 도시되고, 도 1의 단계(103)와 매우 유사하게, AddGroup 요청으로 명명된다. 그룹 소유자는 AddGroup 요청(203)을 자기 "자신의" 신뢰 제공자에게 송신한다. 가장 유리하게는, AddGroup 요청(203)은 암호화된 KGA(Keystore Group Archive) 및 그룹 요청 토큰 PK_{GRT}를 포함하며, 그 중 KGA는 다른 것들 중에서도, 보호된 호출이 이루어져야 하는 그룹 구성원의 사전 공유 키(이 명세서에서 앞에서 PSK 또는 P_{G0} 라고 불림) 및 식별자 UID(및 아마도 공개 키 PK_{UID})를 포함한다.

[0113] 도 2의 단계(204)는, 그것이 신뢰 제공자(그룹 소유자가 "속하는" 신뢰 제공자)가 요청된 암호화 그룹을 설정하고 그것을 나중에 요청 시 그룹 구성원에게 전달될 수 있는 데이터 구조 형태로 저장하는 것을 나타내는 점에서 도 1의 단계(104)와 유사하다. 이러한 신뢰 제공자의 장치에 있는 암호화 엔진은 암호화 제품을 생성함으로써, 즉 요청된 암호화 그룹을 생성함으로써, 복수의 사용자 식별자(그룹 소유자 및 그룹 구성원의 UID)를 포함하는 AddGroup 요청(203)을 보안 전송 메커니즘을 통해 수신하는 것에 응답한다. 단계(205)는 신뢰 제공자의 장치가 그룹 소유자에게 다시 송신하는 AddGroup 응답이며, 이 경우에도 도 1의 단계(105)와 매우 유사하다.

[0114] 단계(206)에서, 그룹 소유자의 사용자 디바이스는 그룹 구성원의 사용자 디바이스에게 적어도 그룹 요청 토큰 PK_{GRT} 및 그룹 소유자의 신뢰 제공자의 식별자 VID를 송신한다. 도 2에서 별도의 단계로 명시적으로 도시되지는 않았지만, 그룹 구성원의 사용자 디바이스는 이 정보를 사용하여 암호화 그룹(의 암호화된 KGA)을 얻기 위한 요청을 작성한다. 그러나, 그룹 구성원이 그룹 소유자와는 다른 신뢰 제공자에 속하기 때문에, 단계(207)의 GetGroup 요청은 암호화 그룹의 저장된 데이터를 현재 보유하고 있는 해당 신뢰 제공자에게 송신되지 않는다. 대신에, 그룹 구성원의 사용자 디바이스는 GetGroup 요청(207)을 자신의 신뢰 제공자에게 송신한다.

[0115] 사용자와 그 신뢰 제공자 사이의 기존 관계는 대응 디바이스 및 장치가 도 2에 도시된 요청 및 응답을 송신하는 데 사용되는 보안 전송 메커니즘을 설정하고 활용하는 것이 특히 쉽고 간단하다는 것을 의미한다. 일부 이전 단계에서, 각 사용자와 각각의 신뢰 제공자 간에 충분한 키 및/또는 다른 공유 시크릿 정보가 교환되었을 수 있으므로, 이러한 통신 연결이 필요할 때 빠르고 안전하게 설정될 수 있다. 이것은 신뢰 제공자들 간의 통신에도 동일하게 적용된다. 따라서 여기서 의미하는 대로 공유 시크릿에 의존하는 것은 이를 확립하는 데 사용되는 기술에 구애받지 않는다. PKI(Public Key Infrastructure)와 마찬가지로 어떤 종류의 암호화(ECC, RSA 또는 기타) 및 알고리즘이 사용되는지는 중요하지 않는다. 예를 들어, 기관은 가장 진보된 개인 사용자 및 민간 기업보다 오래된 암호화 기술에 의존하는 경우가 많으므로 가장 유리한 경우 시스템 및 방법은 임의의 종류의 PK 키로 동작할 수 있어야 한다.

[0116] 위의 공유 시크릿에 대한 언급은 유리하게는 수학적으로 연결된 키 쌍들 간의 계산 시크릿을 의미할 수 있으며, 이는 예를 들어, ECC 알고리즘 또는 RSA 알고리즘에 따라 자신의 시크릿 키(SK)와 다른 사람의 공유 키(PK)의 곱으로부터 유래한다.

[0117] 단계(208)에서, 그룹 구성원의 신뢰 제공자는 GetGroup 요청(207)을 수신하고, 이것이 그룹 요청 토큰 이외에 외부 VID를 포함하고 있음을 주목한다. 즉, GetGroup 요청(207)의 VID는 그룹 구성원의 신뢰 제공자의 VID가 아니라 그룹 소유자의 신뢰 제공자를 식별한다. 신뢰 제공자들 간에 이전에 확립된 연결된 관계에 기초하여, 그룹 구성원의 신뢰 제공자는 도 2의 단계(209)에 도시된 바와 같이, 그룹 소유자의 신뢰 제공자에게 GetGroup 요청을 전달할 수 있다. 그러나 그룹 구성원의 신뢰 제공자는 (그룹 구성원의 자격 증명 대신) 자체 자격 증명을 사용하여 자신이 그룹 소유자의 신뢰 제공자에게 전달하는 GetGroup 요청(209)을 인증한다.

[0118] 도 2의 단계(210)는 그룹 소유자의 신뢰 제공자의 장치에 있는 암호화 엔진이 (신뢰 제공자들 간에 통신하기 위해 사용되는) 보안 전송 메커니즘을 통해 GetGroup 요청(209)을 수신하는 것에 응답한다는 점에서 도 1의 단계(109)와 유사하다. 상기 요청은 AddGroup 요청(203)에서 이전에 수신된 복수의 사용자 식별자 중 하나, 즉, 그룹 구성원의 식별자를 포함한다. 그룹 소유자의 신뢰 제공자의 장치는 이전에 생성된 암호화 제품, 즉 디지털 암호화 그룹을 보안 전송 메커니즘을 통해 그룹 구성원의 신뢰 제공자 쪽으로 송신함으로써 응답한다(도 2의 단계(211) 참조).

[0119] 그룹 구성원의 신뢰 제공자는 자신이 수신하는 GetGroup 응답(211)의 어떤 내용도 인식할 필요가 없다. 대신, 두 신뢰 제공자 간에 사용된 인증 메커니즘을 그룹 구성원의 신뢰 제공자와 그룹 구성원 간에 사용된 인증 메커니즘으로 대체하는 것으로 충분하다. 이에 대응하여 전달된 GetGroup 응답은 도 2의 단계(212)와 같이 도시되어 있다. 이 응답을 수신하고 그 내용을 복호화한 후, 그룹 구성원의 사용자 디바이스는 도 2의 단계(213)에 도시된 바와 같이, 그룹 소유자의 사용자 디바이스와의 보안 통신에 참여할 준비가 된다.

[0120] 전술한 방법 및 장치와 연관된 중요한 이점들 중 하나는 일반적으로 DID라고 하는 분산형 식별자의 관행을 적용할 수 있다는 것이다. 디지털 통신에 대한 신뢰 관계를 확립하기 위해 신뢰 제공자는 상이한 목적들을 위해 상이한 (공개) 암호화 키들 및 사용자의 사인-인(sign-in) 정보를 가질 수 있다. 이의 한 가지 유리한 결과는 상이한 수준들에서 제어를 적용할 수 있다는 것이다. 또 다른 하나는 그룹 구성원의 익명 및/또는 가명 출연(anonymous and/or pseudonymous appearance)의 가능성이다. 사용 사례에 따라 그룹의 구성원들은 서로에게 익명으로 출현하거나 가명으로 동작할 수 있지만 신뢰 제공자에 의해 보장되는 신뢰 관계(들)에 전적으로 의존할 수 있다. 마찬가지로 그룹의 구성원들은 서로를 식별할 수 있지만 비구성원에게는 식별되지 않은 상태로 남아 있다.

[0121] 여기에 제공된 임의의 범위 또는 디바이스 값은 원하는 효과를 잃지 않고 확장되거나 변경될 수 있다. 또한, 임의의 실시예는 명시적으로 허용되지 않는 한 또 다른 실시예와 결합될 수 있다.

[0122] 비록 주제가 구조적 피처 및/또는 행위에 특유한 언어로 설명되었지만, 첨부된 청구항들에 정의된 주제가 반드시 전술한 특정 피처 또는 행위에 한정되는 것은 아니라는 점을 이해해야 한다. 오히려, 전술한 구체적인 피처

및 행위는 청구항을 구현하는 예로서 개시된 것이며, 다른 동등한 피처 및 행위는 청구항의 범위 내에 있도록 의도된 것이다.

[0123] 전술한 혜택 및 이점은 하나의 실시예에 관련될 수 있거나 여러 실시예에 관련될 수 있다는 것이 이해될 것이다. 실시예는 명시된 문제들 중 어느 하나 또는 모두를 해결하는 것들 또는 언급된 혜택들 및 이점들 중 어느 하나 또는 모두를 갖는 것들에 제한되지 않는다. 또한, 단수형('an') 항목에 대한 언급은 이들 항목 중 하나 이상을 지칭할 수 있음이 추가적으로 이해할 것이다.

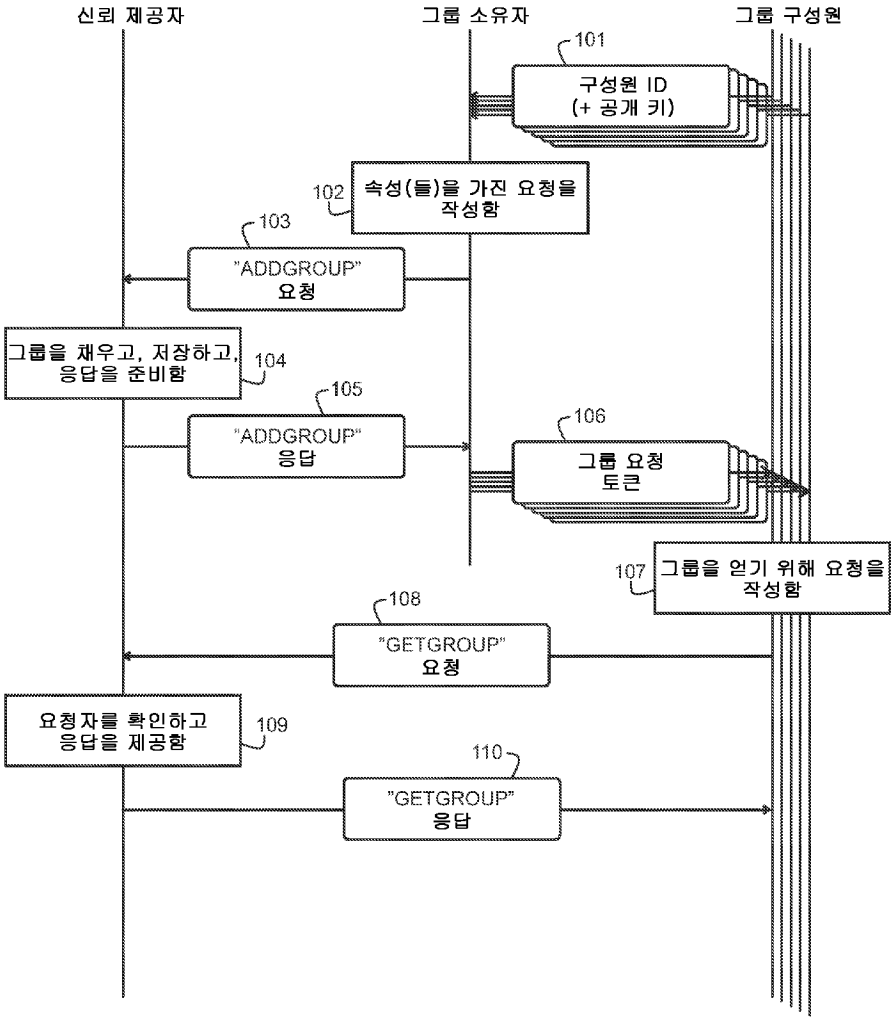
[0124] 본원에 설명된 방법들의 단계들은 임의의 적절한 순서로, 또는 적절한 경우 동시에 수행될 수 있다. 또한, 개별 블록은 본 명세서에 설명된 주제의 정신 및 범위를 벗어나지 않는 범위 내에서 어떠한 방법으로부터도 삭제될 수 있다. 전술한 실시예들 중 어느 하나의 양상들은, 추구되는 효과를 잃지 않으면서 추가적인 실시예들을 형성하기 위해 설명된 다른 실시예들 중 어느 하나의 양상들과 결합될 수 있다.

[0125] 본 명세서에서 '포함하는'이라는 용어는 식별된 방법, 블록 또는 요소를 포함하는 것을 의미하기 위해 사용되지만, 이러한 블록 또는 요소는 배타적 목록을 포함하지 않으며, 방법 또는 장치는 추가적인 블록 또는 요소를 포함할 수 있다.

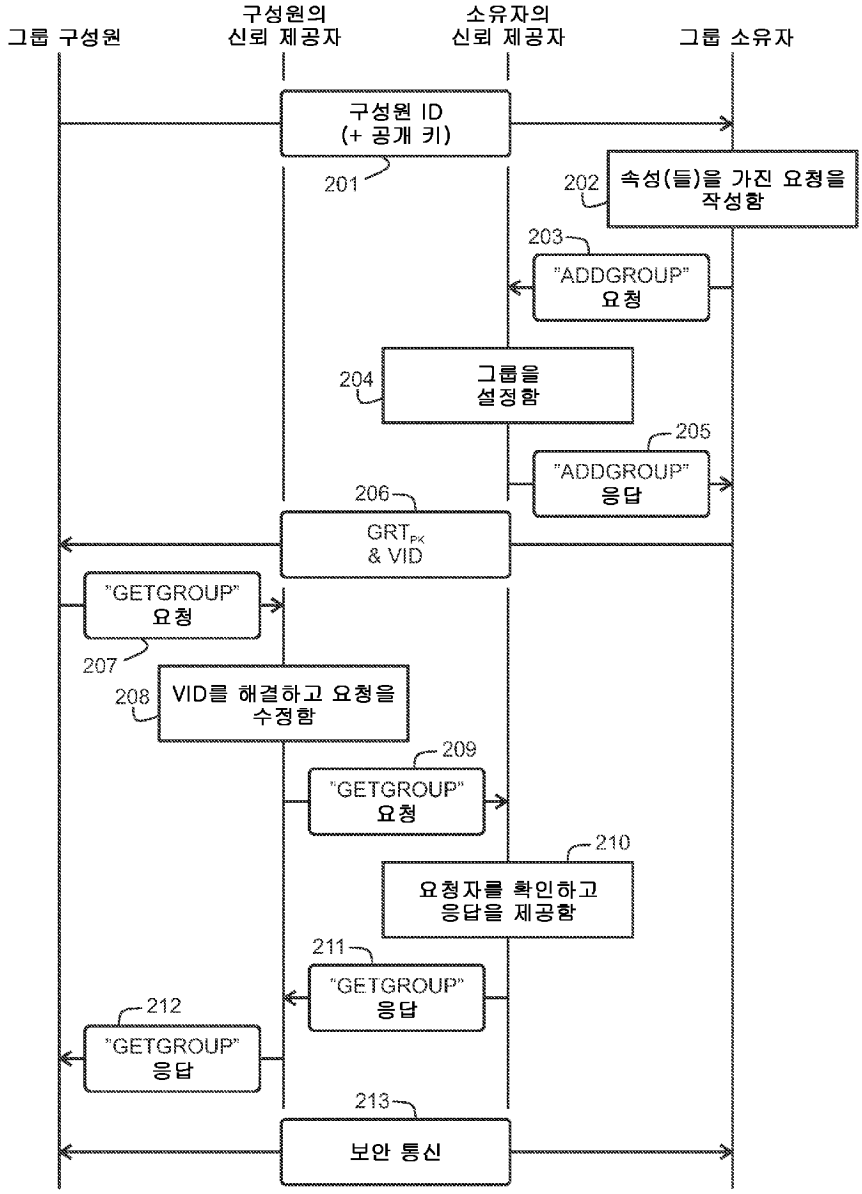
[0126] 전술한 설명은 단지 예시로서 주어진 것이며, 당업자에 의해 다양한 수정이 이루어질 수 있음을 이해할 수 있을 것이다. 상기 명세서, 예시 및 데이터는 예시적인 실시예의 구조 및 사용에 대한 완전한 설명을 제공한다. 다양한 실시예들이 어느 정도의 특수성을 가지고 또는 하나 이상의 개별적인 실시예와 관련하여 앞에서 설명하였지만, 당업자는 본 명세서의 사상 또는 범위를 벗어나지 않으면서 개시된 실시예에 수많은 변경을 할 수 있을 것이다.

도면

도면1


신뢰 제공자
그룹 소유자
그룹 구성원
101
구성원 ID
(+ 공개 키)
102
속성(들)을 가진 요청을
작성함
103
"ADDGROUP"
요청
그룹을 채우고, 저장하고,
응답을 준비함
104
105
"ADDGROUP"
응답
106
그룹 요청
토큰
107
그룹을 얻기 위해 요청을
작성함
108
"GETGROUP"
요청
요청자를 확인하고
응답을 제공함
109
110
"GETGROUP"
응답

도면2


그룹 구성원
구성원의 신뢰 제공자
소유자의 신뢰 제공자
그룹 소유자
구성원 ID (+ 공개 키)
201
202
속성(들)을 가진 요청을 작성함
203
"ADDGROUP" 요청
204
그룹을 설정함
205
"ADDGROUP" 응답
206
GRT$_{PK}$ & VID
"GETGROUP" 요청
207
208
VID를 해결하고 요청을 수정함
209
"GETGROUP" 요청
210
요청자를 확인하고 응답을 제공함
211
"GETGROUP" 응답
212
"GETGROUP" 응답
213
보안 통신