



GADI 소개

분산ID 시스템을 위한 진정한 상호호환성의 실현



CONTENTS

GADI 소개	1
소개	1
Digital Identity의 당면 과제	2
신뢰와 책임	
분할 및 복제 (Fragmentation & Duplication)	3
Digital Identity의 소유권 및 통제 결여	
실제 Identity와 Digital Identity간의 바인딩 결여	5
GADI 소개 - 신뢰의 비전	6
소개	
GADI - 비전 및 효용	8
소개	
신뢰 기반 프레임워크 (Trust Sourcing)	9
이기종 거래 지원 (Cross-ledger transaction support)	
포용성	12
GADI Digital Address	
요약	14
Goode Intelligence 소개	16
DID Alliance 소개	16

GADI 소개



Goode Intelligence가 발행한 본 백서는 DID Alliance 글로벌 신뢰 플랫폼인 GADI (Global Association for Digital Identity)를 소개하는 문서입니다. [1] DID Alliance는 Digital Identity에 대해 확립된 신뢰를 보장하기 위해, 탈중앙화된 Identity 서비스(DID, Decentralized Identity)를 위한 표준화되고 상호 호환이 가능한 프레임워크 개발을 추진하기 위해 만들어진 개방형 비영리 재단입니다.

본 연구는 DID Alliance의 협력으로 개발되었으며, DID Alliance의 회원사들을 포함한 업계의 선도적인 글로벌 이해관계자들과의 인터뷰가 포함되어 있습니다. 분할(Fragmentation), 복제(Duplication), Identity의 소유권 및 통제 부족, 실제 Identity와 Digital Identity간의 약한 바인딩 등 Digital Identity와 관련된 당면 과제를 살펴봅니다.

먼저, Digital Identity란 무엇인지 정의하는 것이 중요합니다.

[1] <https://www.didalliance.org/>

Digital Identity는 무엇인가?

온라인 Digital Identity를 정의하는 것은 어렵습니다. 美 국립표준기술원(NIST)에 따르면, Digital Identity를 제대로 정의하기 위해서는, “모든 것을 만족시키는 단일 정의에 도달하기 위한 사용 맥락”에 대한 지식이 필요하다고 합니다. [2]

Digital Identity를 구성하는 정보는 디지털 속성과 디지털 활동이라는 두 가지 상위 범주로 분류할 수도 있습니다.

첫째, 고유의(Inherent) 속성에 해당하는 디지털 속성에는 이름, 생년월일, 사회보장번호 그리고 주민등록번호와 같은 국가 ID 번호, 생체 데이터 및 은행 세부 정보가 포함됩니다. 둘째, 유전적(Inherent) 속성이나 행동(behaviour) 속성에 해당하는 디지털 활동에는 소셜 네트워크 상호작용, 금융 거래 내역, 검색 내용 등이 포함됩니다.

[2] NIST Special Publication 800-63 Revision 3 Digital Identity Guidelines. <https://pages.nist.gov/800-63-3/sp800-63-3.html>

DIGITAL IDENTITY의 당면과제

Digital Identity는 상당한 진전이 있었음에도 불구하고, 업계에서는 신뢰와 책임, 분할, 복제, 소유권 및 통제 부족, 실제 Identity 과 Digital Identity 간의 바인딩 결여 등 다양한 문제로 여전히 어려움을 겪고 있습니다.

Identity 문제를 해결하고자 하는 기관들은 그들이 특정 솔루션에 종속될 수 있고, 미래를 위한 바람직한 선택이 아닐 수 있음에도 불구하고 현재 경쟁력 있는 모델 중 하나를 선택하려는 오류를 종종 범하고 있습니다.

본 연구는 다음 섹션에 걸쳐 Digital Identity와 관련된 몇 가지 주요 이슈들을 살펴보고자 합니다.

신뢰와 책임



신뢰와 책임은 사회의 기반 요소입니다. 그러나 현재 온라인에서 Identity를 관리하는 방법에 있어서 신뢰와 책임 두 요소 모두, 많은 측면에서 부족합니다. 전 세계 주요 소셜 미디어 및 메시징 서비스에서 계정을 만들 때 Identity 검증이 거의 이루어지지 않습니다.

가짜 뉴스의 시대에는, 뉴스 출처에 대한 신뢰가 떨어지며, 특히 인기 있는 소셜 미디어 사이트에 뉴스가 실릴 때에도 누가 실제로 많은 뉴스를 게재하고 있는지 책임감이 결여되어 있습니다.

인터넷이 보다 빨라지면서, 신원을 알 수 없는 저자가 진위를 파악하기 힘든 새로운 뉴스들을 생성하더라도 소셜 미디어 플랫폼을 통해 빠르게 전파되고 있습니다.

소셜 미디어 플랫폼은 활성 사용자 수를 늘리기를 원하지만, 계정 보유자 신원을 충분히 검증할 만한 제어 메커니즘이 거의 전무하며, 계정 개설 시 강력한 신원 검증을 강제하기 위해 연동된 규정 또한 제한적입니다.

분할 및 복제 (Fragmentation & Duplication)

Digital Identity의 분할 및 복제는 사용자에게 혼란을 야기하고 Issuer(발급기관) 및 SP(서비스 제공자)가 실행 방법을 선택하는데 있어서 복잡한 요소로 작용합니다.

Digital Identity는 사용자가 누구이며, 무엇을 할 수 있는지, 또 할 수 없는 것은 무엇인지 등에 대한 고유한 프로필을 생성하는 수천 개의 데이터 포인트로 구성됩니다. 우리의 Digital Identity는 정부, 금융 기관, 대형 기술 회사, 신용 조사 기관 및 소셜 네트워크 제공업체를 포함한 여러 데이터 소유자들이 보유하고 있는 인터넷 전반에 걸쳐 분할되어 흩어져 있습니다.

이는 이러한 데이터 포인트를 검증하려는 기관들(Entities)이 분할된 Identity 정보 지점에 접근하는 비용과, 수많은 다른 개체들에 의해 저장된 수많은 개인 데이터로 인한 데이터 유출 위험을 포함하여 일련의 문제를 야기합니다.

또한, Identity 정보는 여러 개체들에 걸쳐 과도하게 복제되어 사용자에게 부담이 되는 매우 비효율적인 시스템을 만들게 됩니다. SP가 Digital Identity를 검증하고 생성할 때마다 이름, 생년월일, 주소, 사회보장번호 및 주민등록번호 등 유사 신원 정보가 수집됩니다. 이러한 상황에서는 User와 SP 모두에게 비용이 발생합니다. SP의 경우 새 계정과 Digital Identity를 생성할 때마다 신원 검증에 소요되는 재정적 비용이 발생하는 한편, User의 경우에는 가끔씩 기억하기 어려운 Identity 정보를 제공해야 하는 마찰 비용을 지불하게 됩니다.

2020년 7월에 발표된 한 연구에 따르면, 최소 39개의 서로 다른 기관이 일반 영국 시민의 개인 데이터를 보유하고 있으며, 영국 시민의 약 25%는 얼마나 많은 기관들이 자신의 개인 데이터를 보유하고 있는지 모르는 것으로 나타났습니다.[3]

이미 다른 곳에서 수집되고 검증된 신원 문서 및 정보들을, 추가적으로 수집해야 하는 이유가 무엇인지에 관한 근본적인 질문이 제기되는 것입니다.

Digital Identity의 소유권 및 통제 결여

오늘날 Identity 와 관련된 대부분의 상호작용은, User에게 민감하고 상업적으로 가치 있는 개인 정보를 공개하도록 요구하는 중앙화된 기관에 의해 통제됩니다. 이러한 관계는 종종 고객의 프라이버시를 희생하면서 해당 정보를 이용하려는 Identity 제공자에게 유리하게 작용하는 경우가 많습니다.

개인정보 규정은 강화되고 있지만, 개인정보가 요청 기관으로 전달된 후 그 정보가 어디까지 유출될 지에 대한 통제력은 더 이상 개인에 있지 않으며, 많은 인터넷 회사에서 개인정보를 사업화하는 현상은 이미 보편화 되어있습니다.

이러한 불균형적인 관계는 User와 신원 제공자 모두에게 상당한 비용 부담을 초래합니다. 신원 도용, 스팸 이메일, 피싱 공격 및 사기는 모두 이러한 시스템 장애의 직접적인 산물입니다.

**[Verizon에 따르면 2018년 미국에서
1,440만 명이 신원 도용의 피해를 받았다고
합니다 [4].]**

탈중앙화된 Identity (Decentralized Identity, DID)로 전환하고 ‘자기주권형 신원 (Self-Sovereign Identity, SSI)’을 개발 하면서, User가 자신의 신원 자산 (Identity 정보 및 Credential)을 관리함으로써, 이러한 문제를 완화하고 제거할 수 있습니다.

그러나, SSI모델은 Identity 업계가 구상했던 만병통치약(Panacea)은 아니며 다음의 자체 도전과제를 제시합니다:

- 탈중앙화된 신원 플랫폼 (Decentralized Identity Platforms, DIPs) 간의 상호 호환성 결여 - 격리된 (siloed) 생태계
- DID는 일반적으로 신뢰 앵커(Trust Anchor) 없이 자체 보증 가능
- 비포용성 - 스마트 기기 사용자만 이용 가능
- Identity Issuer 및 SP는 한 개 승자 (winner)를 선정해야 함 - 한 개의 ‘우승’ 스택과 통합하기를 희망
- 신뢰와 책임이 아닌 보안과 프라이버시를 강조
- 낮은 허용률(acceptance rates)
- 진화가 아닌 혁명적인 것으로 간주됨 - 기존 Identity 제공자 및 네트워크는 제외
- 스마트 기기 변경 시 주요 복구 문제 유발
- 경제적 필요성 결여 - 신기술이 번창하기 위해서는 지속 가능한 새로운 비즈니스 모델이 필요

실제 Identity 와 Digital Identity간의 바인딩 결여

모든 Digital Identity 시스템에서 가장 큰 문제 중 하나는 실제 Identity를 Logical Identity와 연결 혹은 바인딩 하는 것입니다. 어떻게 물리적 개인을 디지털 세상에서 증명할 수 있는지에 관한 질문은 정말 어렵습니다.

Identity 확인 또는 증명은 일반적으로 정부에서 발급하는 신뢰할 수 있는 문서 (여권, 운전면허증 및 주민등록증), 생체 데이터, 안면 인식 및 기타 Identity 정보 조합을 검증 가능한 Digital Identity Credential과 연동함으로써, 실제 신원과 Digital Identity 간의 효과적인 바인딩을 형성할 수 있는 한 가지 방법입니다.

현재 접근 방법 중 중요한 문제는 Digital Identity를 인증할 때 Trust Anchor로 사용할 수 있는, 유일한 Digital Address 정보가 없다는 것입니다. User는 매번 자신의 신원을 증명해야 할 때마다 유사한 프로세스를 반복해야 합니다. 이는 비효율적이고 사용자에게 마찰 비용을 가중시키며, SP는 비용이 많이 듭니다.

[3] <https://www.nomidio.com/>

[4] <https://www.verizon.com/info/digital-security/identity-theft-what-to-do/>



GADI 소개-신뢰의 비전

소개

GADI (Global Association for Digital Identity)는 DID Alliance의 글로벌 신뢰 플랫폼입니다.

DID Alliance는 Digital Identity에 대해 확립된 신뢰를 보장하기 위해, 탈중앙화된 Identity 서비스(DID, Decentralized Identity)를 위한 표준화되고 상호 호환이 가능한 프레임워크 개발을 추진하기 위해 만들어진 개방형 비영리 재단입니다.

DIDA와 GADI가 달성하고자 하는 것의 기초를 형성하는 Digital Identity 문제를 해결하는데 있어서 상당한 투자와 더불어, 차세대 DID 시스템 구축을 위한 많은 양의 우수한 작업들과 표준화 노력들이 진행되고 있습니다.

DIDA의 임무는 모든 사람에게 고유한 Digital Address (DA)를 제공하여 실제 또는 디지털 세계에서 신뢰와 책임을 강화할 수 있는 권한을 부여함으로써, 신뢰할 수 있는 새로운 Identity 프레임워크를 구축하는 것입니다.

DID Alliance는 기술뿐만 아니라 비즈니스 상호 호환 계층을 가능하게 하여 운영과 채택에 관련된 가장 중요한 실질적 문제들을 해결하도록 지원함으로써, DID 시스템의 약속을 이행하고자 합니다.

GADI의 핵심은 Digital Address(DA)로, DA는 KYC (고객 확인) 프로세스를 수행한 후 인증된 DA 발급자가 개인에게 발급하는 특수 GADI 식별자입니다.

신뢰, 책임, 포용성 및 User 소유권은 GADI의 핵심입니다.

본 섹션에서는 GADI의 비전을 소개하고 주요 구성 요소 및 주요 이점을 기술합니다.

[1] <https://www.didalliance.org/>



GADI - 비전 및 효용

소개

FIDO Alliance의 설립자이자 DIDA의 공동 설립자인 Ramesh Kesanupalli는 RaonSecure의 이순형 대표, CVS/Aetna의 Abbie Barbir와 협력하여 GADI를 만드는데 중추적인 역할을 해왔습니다. GADI에 대한 이들의 비전은 W3C, DIF, Hyperledger Aries와 같은 기존의 상호호환성 노력의 범위를 벗어난 필수 기술과 프로세스를 사용하여, DID 시스템간 진정한 상호 호환성을 달성하는 것입니다.

GADI는 이기종 플랫폼 호환성을 지원하여 협업을 통해 글로벌 차원에서 Identity 플랫폼을 제공할 수 있도록 합니다. 이를 통해 SP는 모든 신원 플랫폼의 모든 VC (Verifiable Credential) 및 GADI Token Exchange이라는 프로세스를 통해 거래 비용을 정산하는 메커니즘을 신뢰하게 됩니다.

GADI의 효용성은 다음과 같습니다.

- 모든 사람이 본인의 유일한 Digital Address를 소유함으로써, 전 세계적으로 통용될 수 있는 Digital Identity 문제 해결
- DID 플랫폼 간의 상호 호환성을 위한 메커니즘 제공
 - GADI는 상호 작용하는 모든 시스템에 대해 별도의 ledger 간 호환 기능을 구현할 필요 없이, 각 DID 시스템이 GADI SDK를 통합할 경우 모든 GADI 회원사와 연계 지원 가능
- 정부기관을 포함한 Identity Issuer들은 검증 과정에서 발생하는 GADI의 가치 사슬에 포함되고, 그들이 소유한 모든 개인정보(PID: Personal Identity Data)는 안전하게 유지되며, 국가간에도 유출되지 않음
- Credential 복구에 대한 재등록 문제 해결
 - 스마트폰의 대체
- ZKP를 통한 개인정보보호 - 개인 정보를 공유할 필요 없음
- 포용성 - Digital Address는 다양한 매체에 저장 가능

영지식 증명 (Zero-knowledge proof, ZKP) 정의: ZKP는 한사람(제공자)의 정보를 공개하지 않고, 자신이 일부 정보에 소유권을 가지고 있음을 다른 사람(검증자)에게 증명할 수 있도록 하는 암호법입니다. 예컨대, ID 카드 및 운전면허증과 같은 신원 문서는 종종 나이를 증명하는 수단으로 사용되지만, 동시에 신원 절도범들에게 오용될 수 있는 소유자와 관련된 매우 중요한 다른 개인 신상 정보도 가지고 있습니다. ZKP는 실체가 명확한 생년월일을 제공하지 않고도 개인의 나이 (21세 이상)를 확인할 수 있는 신원 문서의 디지털 사본을 만드는데 사용할 수 있습니다.

이러한 목적을 추구하기 위한 GADI의 노력은 크게 세 가지 영역으로 집약됩니다.

1. 신뢰 기반 프레임워크
2. 이기종 플랫폼 호환성
3. 포용성

Trust Sourcing 신뢰 기반 프레임워크

탈중앙화된 식별자(DID)는 검증 가능한 분산형 Digital Identity을 가능하게 하는 식별자의 한 유형입니다. 기존 표준은 다른 기관에서 발급한 Credential을 정밀 분석하기 위해 탈중앙화된 분산형 Identity 시스템을 지원하는 반면, 신뢰 당사자들은 권한 부여 결정을 내리는데 어려움을 겪습니다. 이는 신뢰 당사자들이 다음과 같은 Credential 발급에 대한 여러 가지 중요한 질문에 답하기 위해 고군분투하고 있기 때문입니다:

- Credential 의 사법권한적 한계는 무엇입니까?
- Credential 발급을 위해 어떤 유형의 신원 검증 (증빙)을 수행했습니까?
- 신뢰 당사자는 어떻게 면책 보상(indemnified) 됩니까?
- Credential 을 사용할 수 있는 트랜잭션 거래 유형은 무엇입니까?
- 신뢰 구축 실패 시 예외 처리 절차는 무엇입니까? GADI는 신뢰할 수 있는 당사자가 이러한 질문에 답변할 수 있도록 신뢰 프레임워크를 제공하고 다음과 같은 방법으로 이를 수행할 것입니다.
- 표준화된 Credential 발급 절차 및 의미 체계 도입
- 특정 Credential 유형에 대해 공개된 요구 사항에 따라 Credential 발급자 인증
- 각 Credential 유형을 실제 계약 집합에 바인딩 이러한 신뢰 기반의 프레임워크를 통해 신뢰 당사자는 GADI가 제공하는 Credential 의 명확한 의미를 알 수 있어 정확한 권한 부여 결정을 내릴 수 있습니다.

이기종 플랫폼 호환성

이기종 DID간의 상호 호환성 결여는 대개 이러한 시스템의 약점으로 언급됩니다. GADI의 주요 목표 중 하나는 회원 시스템 간의 완전한 이기종 플랫폼 호환성을 가능하게 하는 것입니다.

기존 DID 표준화 노력은 이기종 DID 시스템 간의 형식과 프로토콜 레벨의 상호호환성을 제공하는 측면에서 완성도가 높아지고 있지만, 여전히 회원 시스템간 완전한 이기종 플랫폼 호환성을 지원하는 측면에서는 미비한 점이 있습니다.

GADI는 DID관련 거래의 교환 플랫폼 역할을 하는 분산 원장(Distributed Ledger)을 지원하여 이기종 원장간 상호호환성을 실현할 수 있는 수단 제공을 목표로 합니다.

이는 또한, 토큰 유형 간에 유동성을 제공할 수 있는 제 3자의 시장조성자(마켓메이커)들을 통해 원장 간 결제 지원하는 메커니즘을 제공하여 진정한 상호 호환이 가능한 (Agnostic) 생태계 구축을 가능하게 합니다.

GADI는 합의된 프로토콜을 통해 이기종 플랫폼 호환성을 지원할 수 있는 기반을 제공할 뿐만 아니라, 기술을 뒷받침해주는 명확하게 정의된 경제 모델도 만듭니다.

정부 여권 사무소에 새로운 수익원 창출



Digital Identity 검증은 디지털 전환 이니셔티브의 직접적인 산물로 빠르게 성장하고 있으며, COVID-19 비상 사태로 인해 성장을 증가 추이를 보이고 있습니다. 계정 개설이 온라인으로 전환되고 있으며, SP는 Identity 검증을 위한 확실하고 안전한 방법을 요구합니다. 정부가 발급한 ID 증명서, 여권, 운전면허증, 주민등록증 등의 문서 검증은 신원 증명으로 활용되며, 신원 검증에 중요한 요소입니다. 신원 문서는 스마트폰 카메라를 사용하여 원격으로 스캔한 후 위조되지 않고 유효한지 확인하기 위해 인증됩니다. 이는 인쇄된 문서를 스캔하는 것을 포함하기 때문에, 현재 Issuer(정부)의 디지털 인프라에 대한 검증은 거의 또는 전혀 이루어지지 않고 있으며, 더 중요한 것은 문서 발급기관(여권 사무소)이 해당 과정을 통해 수익화 할 수 있는 방법이 없다는 것입니다. 이러한 문서들이 검증 가능한 Digital Credential을 제공하고 해당 Credential의 검증을 지원하기 위한 인프라가 마련되어 있다면, 정부 부처는 신원 확인과 문서 검증을 통해 경제 가치를 창출할 방법이 있을 것입니다. GADI 거래 원장은 이 시나리오를 지원하는 메커니즘을 제공하며, 더 이상 전체 신원 문서를 스캔하지 않을 것이기 때문에, 검증된 개인의 프라이버시를 보호합니다.]

Inclusiveness 포용성

스마트폰 보급률이 100%를 넘는 선진국이 많음에도 불구하고, 여전히 스마트폰 소유권이 없는 세계 인구는 45%에 달합니다.[6] 또한, 세계 경제 포럼(WEF)은 전세계 10억명이 넘는 사람들이 공식 Identity를 가지고 있지 않다고 추산합니다.

기존 DID 시스템의 중요한 단점은 스마트폰을 소유하고 인터넷에 접속하는 기술 의존도가 높다는 점입니다.

포용적 시스템을 설계하는 것은 GADI의 중요한 목적이며 DID Alliance의 핵심 목표입니다.

DID Alliance는 User가 DID 시스템과 상호작용하도록 설계된 프록시 대행 시스템과 상호작용할 수 있는 일련의 프로토콜을 제공하여, 포용성 문제에 대한 솔루션을 개발했습니다.

[6] <https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/>

이 솔루션에는 스마트폰 소유권에 의존하지 않는 다양한 솔루션이 포함되며, Identity 토큰이 템플릿이 없는 알고리즘을 통해 사용자에게 생체 정보를 통해 바인딩되고 잠재적으로 스마트 카드에 저장할 수 있습니다. 사용자의 DA는 SP의 시스템을 사용하여 사용자의 동의 하에 2D 바코드를 통해 모든 표면에 저장할 수 있습니다.

Identity 정보를 확인하기 위해 SP는 사용자를 대신하여 GADI 신뢰 프록시(trust proxy)와 상호 작용하여 User를 대신하여 인증하는 GADI 공인 토큰 판독기를 갖추고 있습니다. 그런 다음 Trust Proxy는 거래에 적합한 데이터를 검색하고 SP의 시스템으로 인증을 수행합니다.

GADI, Digital Address

GADI의 기본은 Digital Address로, 공인된 DA Issuer가 개인에게 발급한 특수 식별자이며, 개인에게는 고유한 정보입니다.

DA 생성은 GADI 생태계 내에서 신뢰와 책임을 모두 보장하는데 있어 매우 중요한 절차입니다.

우리는 태어나면서, 부모나 보호자로부터 이름의 형태로 첫 번째 Identity Credential을 받습니다. 정부는 이러한 출생자들을 등록 명부에 올린 후에, 출생 증명서, 출생일, 부모 이름, 출생지 등과 같은 다른 신원 관련 정보가 포함된 종이 문서를 발급합니다. 이러한 공문서는 의료 서비스 번호, 사회 보장 번호, 여권, 운전 면허증, 주민등록증, 결혼 증명서 등과 같은 다른 Identity Credential을 양성하는 Trust Anchor가 됩니다. 또한, 우리가 교육 수수료증을 받을 때 신분을 증명하고 취업을 위해 사용되는 기초적인 신원 증명 문서입니다. 우리가 새로운 Identity Credential을 발급 받을 때 마다, Trust Anchor와 출생 증명서에 다시 연동될 수 있으며, 일련의 신원 검증 및 Custody에 의해 강화됩니다.

GADI DA는 출생 증명서와 동등한 디지털 주소입니다. 한 사람이 인증된 Issuer로부터 GADI 생태계에 온보딩 되면, 이후 모든 거래에 대해 검증 가능한 Trust Anchor가 되는 DA가 생성됩니다. 이 DA는 인증된 Issuer에 의해 GADI 생태계를 지배하는 법적 프레임 워크에 따라 작성됩니다. DA의 생성은 또한 정부 Identity Credential 발급과 비견할 만한 엄격한 KYC (고객확인) 규칙에도 구속됩니다. Digital Address가 검증될 때마다 Digital Address가 고도화되고, Identity Issuer와 신뢰당사자들과의 상호 작용을 통해 강화됩니다.

DA Issuer는 금융서비스 기관, 정부 기관, 교육 기관 및 기업체, 신뢰 경제의 중심인 조직일 수도 있습니다.

GADI DA가 Issuer에 의해 생성되면 생체 인식 데이터, 이름, 성, 생년월일, 출생 도시 등을 포함한 Identity관련 특성으로 구성됩니다. DA는 해시 알고리즘을 적용하여 생성되며, 참여하는 Digital Address Provider(DAP)와 협력합니다.

DAP은 현재 DID관련 Identity 서비스를 제공하는 솔루션 공급자입니다. DAP은 DA와 GADI 시스템을 사용하여 SP 또는 다른 DID 기반 Identity Chain 또는 이에 상응하는 것에 상주하는 Issuer (혹은 둘 다)를 대신하여 Credential Request를 처리합니다. DA는 GADI DLT (분산원장)에 등록된 고유한 서명과 같습니다.

DA는 스마트폰 단말기, FIDO가 보증하는 Credential Wallet에 전달되거나, 포용성을 위해 스마트 카드에 저장될 수 있습니다. 두 경우 모두, DA는 Issuer가 제공한 Identity 속성과 기타 속성의 조합에 의해 개별 사용자에게 강하게 바인딩됩니다.

DA는 일단 생성이 되면 DA와 연동되는 추가 신원들과 함께 기본 Trust Anchor로 사용됩니다. 연계성 및 상호호환성은 Hyperledger Aries[7] 및 DIF의 DIDCOM을 포함한 기존 통신 프로토콜을 활용하여 달성됩니다. [8]

[7] <https://www.hyperledger.org/use/aries>

[8] <https://identity.foundation/working-groups/did-comm.html>

SUMMARY

요약

Digital Identity는 상당한 진전이 있었음에도 불구하고, 업계에서는 신뢰와 책임, 분할, 복제, 소유권 및 통제 부족, 실제 Identity 과 Digital Identity 간의 바인딩 결여 등 다양한 문제로 여전히 어려움을 겪고 있습니다.

Identity 문제를 해결하고자 하는 기관들은 그들이 특정 솔루션에 종속될 수 있고 미래를 위해 바람직한 선택이 아닐 수 있음에도, 현재 경쟁력 있는 모델 중 하나를 선택하려는 오류를 종종 범하고 있습니다.

GADI (Global Association for Digital Identity)는 DID Alliance의 글로벌 신뢰 플랫폼입니다. DID Alliance는 Digital Identity에 대해 확립된 신뢰를 보장하기 위해, 탈중앙화된 Identity 서비스 (DID, Decentralized Identity)를 위한 표준화되고 상호 호환이 가능한 프레임워크 개발을 추진하기 위해 만들어진 개방형 비영리 재단입니다.

DIDA와 GADI가 달성하고자 하는 것의 기초를 형성하는 Digital Identity 문제를 해결하는데 있어서 상당한 투자와 더불어, 차세대 DID 시스템 구축을 위한 많은 양의 우수한 작업들과 표준화 노력들이 진행되고 있습니다.

DIDA의 임무는 모든 사람에게 고유한 Digital Address (DA)를 제공하여 실제 또는 디지털 세계에서 신뢰와 책임을 강화할 수 있는 권한을 부여함으로써, 신뢰할 수 있는 새로운 Identity 프레임워크를 구축하는 것입니다.

DID Alliance는 기술뿐만 아니라 비즈니스 상호호환 계층을 가능하게 하여 운영과 채택에 관련된 가장 중요한 실질적 문제들을 해결하도록 지원함으로써, DID 시스템의 약속을 이행하고자 합니다.

GADI의 핵심은 Digital Address(DA)로, DA는 KYC(고객확인) 프로세스를 수행한 후 인증된 DA 발급자가 개인에게 발급하는 특수 GADI 식별자입니다.

신뢰, 책임, 포용성 및 User 소유권은 GADI의 핵심입니다.

[9] <https://www.didalliance.org/>

ABOUT GOODE INTELLIGENCE



Goode Intelligence는 영국 런던에 본사를 두고 2007년에 설립된 선도적인 Identity, 인증 및 생체정보 연구, 컨설팅 및 이벤트 조직입니다.

본 연구 또는 기타 연구에 대한 자세한 내용은 www.goodeintelligence.com을 참조하십시오.
Twitter 팔로우 해주세요.

ABOUT DID ALLIANCE



DID Alliance는 Digital Identity에 대해 확립된 신뢰를 보장하기 위해, 탈중앙화된 Identity 서비스(DID, Decentralized Identity)를 위한 표준화되고 상호 호환이 가능한 프레임워크 개발을 추진하기 위해 만들어진 개방형 비영리 재단입니다.

DID Alliance에 대한 자세한 내용은 <https://www.didalliance.org/> 을 참조하십시오.
(한국어 사이트: <http://www.didalliance.or.kr/>)

이 문서의 저작권은 Goode Intelligence에 있으며, Goode Intelligence의 사전 서면 동의 없이 어떠한 형식이나 수단으로도 복제, 배포, 보관 또는 전송할 수 없습니다.

