SIA(Symverse Identifier & Account)

1. Introduction

SIA(Symverse Identifier & Account)는 블록체인 내에서 고유한 식별자인 SymID와 각 SymID의 정보를 담고 있는 Account로 구성된다. SymID는 발급 주체에 대한 정보와 개인 식별 번호, 개인 당 발급한 계정 index를 포함하며, Account는 각 SymID의 자기 정보이다.

Symverse에서는 SIA를 블록체인 내에서 거래뿐만 아니라 자격 증명과 자격 확인 등의 영역으로 확장하고자 체계를 잡았으며, SIA 설계는 향후 이런 영역에 대한 서비스를 유연하게 지원할 수 있도록 하는 데 목적이 있다.

2. SIA(Symverse Identifier & Account) 구조

SIA 기본 구조는 아래와 같다. 자격 증명, 자격 확인 등으로 확장 시 Account 필드를 경우에 따라 변경하여 적용한다.

B:Byte(s), b:bit(s)

SIA (Symverse Identifier & Account)				
Field			Size	Description
SymID	Ver		2 b	0: version 1
	Citizen ID	CA ID	14 b	0x0001 : Master CA 0x0002 ~ 0x30FF : Trusted CA 0x3100 ~ 0x3EFF : Public CA 0x3F00 ~ 0x3FFF : Self CA
		Random	6 B	0x00...01 : CA Random Number : 일반 사용자
	SeqNum.		2 B	1 : Reserved 2 ~ 9999 : Account 10000 이상 : Reserved
Account	PubKeyHash		20 B	Hashed Public Key
	Role		2 B	0x0001 : General (default) ... 0xF0F0 : Master CA 0xF0F1 : CA
	Verification Flag		3 b	Reserved
			1 b	Deposit (보증금 예치)
			1 b	Face-to-Face (대면 확인)
			1 b	National Identity Card (국가 신분증 확인)
			1 b	Cell phone number (전화번호 확인)
			1 b	E-mail (이메일 확인)
	State		1 B	0x01 : Active (default) 0x02 : Revoked 0x03 : Locked 0x04 : Holding // holding for new account 0x05 : Marked // 재단 설정(오라클)
	Credit		1 B	신용도 (0~15) // 재단 설정(오라클)
	Country		2 B	국가 구분 코드
	Ref. code		4 B	발급자 참조 코드
	Issued		7 B	생성일시 (YY YY MM DD HH MM SS, 숫자 표기)
CA Signature			65 B	ECDSA(symid + classifier)

1) Symverse Identifier

SymID(Symverse Identifier)란?

SymID는 Symverse Blockchain에 접근하기 위한 식별자로 Symverse Network를 이용할 때 사용되는 ID이다. Symverse Network를 이용하려는 사용자가 CA(Citizen Alliance)에게 ID 발급을 요청하면 CA는 CitizenID를 발급하고 이를 구분할 sequence number를 붙여 SymID를 발급하여 준다. 하나의 SymID는 하나의 Account와 짝을 이룬다.

SymID 구성 요소

10 Bytes로 구성된 SymID는 단순히 식별자(Identity)로만 사용되지 않는다. SymID의 10Bytes에는 다양한 정보를 담고 있으며, 구성은 다음과 같다.

Field			Size	Description
SymID	Ver		2 b	0: version 1
	Citizen ID	CA ID	14 b	0x0001 : Master CA 0x0002 ~ 0x30FF : Trusted CA 0x3100 ~ 0x3EFF : Public CA 0x3F00 ~ 0x3FFF : Self CA
		Random	6 B	0x00...01 : CA Random Number : 일반 사용자
	SeqNum.		2 B	1 : Reserved 2 ~ 9999 : Account 10000 이상 : Reserved

- Version (2bits): SymID 구조에 대한 버전 표기이며 0부터 시작한다. 현재는 버전 1이다.
- CitizenID (62bits): CA가 발급하는 ID로 한 CA당 281,474,976,710,656개(2^48개)의 ID를 발급할 수 있다.
  - CAID (14bits): 해당 CitizenID를 발급한 CA의 식별 번호이다.
  - Random (48bits): 실질적으로 CA가 발급하는 유저의 식별번호와 같다.
- SeqNum(16bits): Sequence number. 계정번호로 각 CitizenID 마다 발급된 Account 의 순서이다.

SymID 구성 예

SymID Example	
Master CA's 1st Account	0x0001 000000000001 0002
Master CA's 2nd Account	0x0001 000000000001 0003
1st CA's 1st Account	0x0002 000000000001 0002
1st CA's 2nd Account	0x0002 000000000001 0003
1st CA's 1st User's 1st Account	0x0002 XXXXXXXXXXX 0002
1st CA's 1st User's 2nd Account	0x0002 XXXXXXXXXXX 0003
1st CA's 2nd User's 1st Account	0x0002 YYYYYYYYYYY 0002

SymID 특징

SymID는 Symverse Blockchain Network의 기본이다. SymID를 통해 Symverse가 추구하는 DID, SSI, 영지식증명, PKI, 자격증명, KYC, AML, Network 등 다양 한 주제를 다룰 수 있다. SymID는 다음과 같은 특징이 있다.

- 존재증명(Existence): 사용자의 신원을 증명한다.
- 탈중앙화(Decentralization): DID의 특징인 식별자 관리의 탈중앙화를 통해 단일 지점 장애 문제를 해결한다.
- 자기주권성(Self-Sovereignty): 개인정보의 통제권을 사용자가 가질 수 있게 한다.
- 개인정보(Privacy): 개인정보 노출 없는 서비스를 제공하고 노출 시에는 선택적 노출 기능을 제공한다.
- 보안(Security): 소유자, 발행자, 검증자에게 암호학적 증명을 기반으로 하여 충분한 보안을 제공한다.
- 상호운용성(Interoperability): 기존 ID 시스템과의 연동 및 Symverse Blockchain 참여자 간에 상호 연동할 수 있는 기반을 제공한다.
- 휴대성(Portablity): SymWallet을 이용하여 SymID를 지원하는 모든 시스템에 이용이 가능하다.
- 간결성(Simplicity): 10 Bytes로 사용자의 다양한 계좌 정보, 필수 인증 정보 및 거래 내역 등의 자료를 관리할 수 있다.
- 확장성 (Extensibility): Symverse Blockchain의 기반 기술 중 하나인 Fractal Network 기술을 이용하여 다른 네트워크 참여자와 통신이 가능하다.
- 보호(Protection): SymID를 사용하는 참여자 간에 충돌이 있을 때 서로의 권리를 보호한다.
- 지속성(Persistence): 사용자가 원하는 한 영구 사용가능 하다.
- 신뢰성 통신(Trusted Network): SymID 사용자 간에 PKI 기반 신뢰성 네트웍 구성을 지원한다.
- 실명제(KYC, AML): 사용자의 신뢰성을 확보하여 부정 거래를 방지한다.
- 익명성(Anonymity): 참여자(서비스 제공자 및 이용자)가 원할 경우 익명성을 보장한다.
- 자격증명(Credential): 사용자의 신원 증명 및 자격 증명을 다루며 서비스 제공자가 이용자의 자격을 판별하기 위한 정보를 제공 (성인인증, 운전면허, 졸업증명 등)
- 자격확인(Stamp): 자격증명에서 개인정보를 제거하고 자격여부만 판별

2) Account

계정(Account)은 SymID의 상세 정보로서 사용되며 SymID : Account = 1 : 1 로 짝을 이룬다. Account는 해당 SymID의 공개키, 역할, 신원확인 여부, 상태, 국가 등의 정보로 구성되어 있다. SymID 발급 요청 시 사용자가 Wallet을 통해 CA로 public key hash 값을 보내면 CA는 Account를 구성하고 해당 정보를 Citizen Chain에 등록한다.

Account 구성 요소

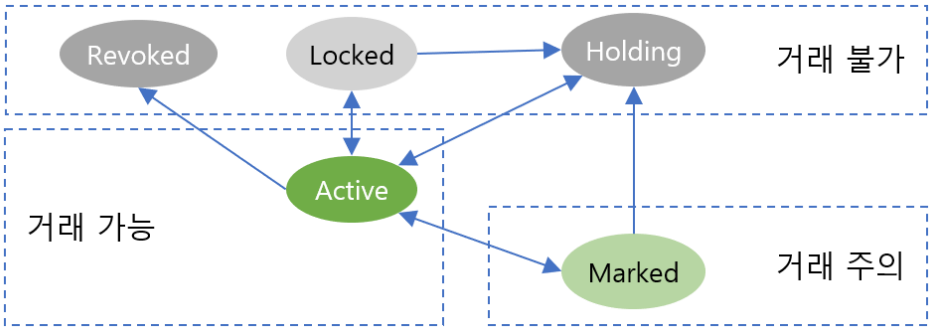
Account는 SymID의 정보를 표현하며, 자격 증명, 자격 확인 등으로 확장 시 각 경우의 포맷으로 변경하여 적용한다.

Account의 구성은 다음과 같다.

Account	PubKeyHash	20 B	Hashed Public Key
	Role	2 B	0x0001 : General (default) ... 0xF0F0 : Master CA 0xF0F1 : CA
	Verification Flag	3 b	Reserved
		1 b	Deposit (보증금 예치)
		1 b	Face-to-Face (대면 확인)
		1 b	National Identity Card (국가 신분증 확인)
		1 b	Cell phone number (전화번호 확인)
		1 b	E-mail (이메일 확인)
	State	1 B	0x01 : Active (default) 0x02 : Revoked 0x03 : Locked 0x04 : Holding // holding for new account 0x05 : Marked // 재단 설정(오라클)
	Credit	1 B	신용도 (0~15) // 재단 설정(오라클)
	Country	2 B	국가 구분 코드
	Ref. code	4 B	발급자 참조 코드
	Issued	7 B	생성일시 (YY YY MM DD HH MM SS, 숫자 표기)

- PubKeyHash (160bits): 유저가 입력한 Public key hash 의 lower 20bytes. 트랜잭션에 대한 서명 검증 시 사용되는 정보이다.
- Role (16bits): SymID 의 역할을 뜻한다. 현재는 Master CA(0xf0f0), CA(0xf0f1) 그리고 일반 유저(0x0001)의 역할이 존재한다.
- Verification Flag (8bits): SymID 가 어느 정도의 강도로 검증받고 등록되었는지에 대한 정보이다. Bit 각각의 자리마다 의미를 가지고 있다.

- State (8bits): SymID 의 상태에 대한 정보이다. 상태는 Active(default), Revoked, Locked, Holding, Marked 등이 있다. 각 상태에 대한 의미는 다음과 같다.



- Credit (8bits): SymID 의 신용 등급에 대한 평가지표이다.
- Country (16bits): SymID 소유자의 국적을 의미한다.
- Ref. code (32bits): CA 가 SymID 발급시 그 SymID 에 대한 특징이나 용도 등과 같이 CA 가 입력하고 싶은 내용을 입력 할 수 있도록 할당된 공간이다.
- Issued (48bits): SymID 의 생성일시 이며 YY YY MM DD HH MM SS 순으로 숫자로 표기한다.

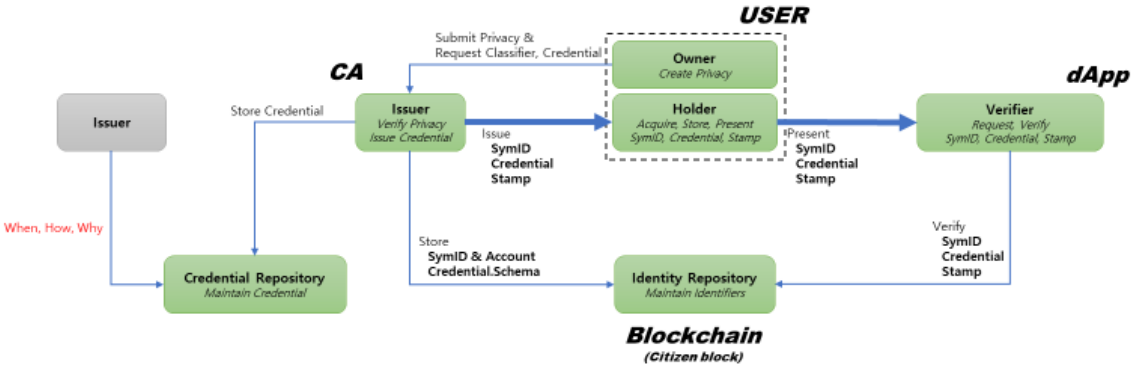
3) CA Signature

SymID를 발급한 CA의 서명으로 ECDSA(SymID + Account)로 생성된다.

3. Actor & Role

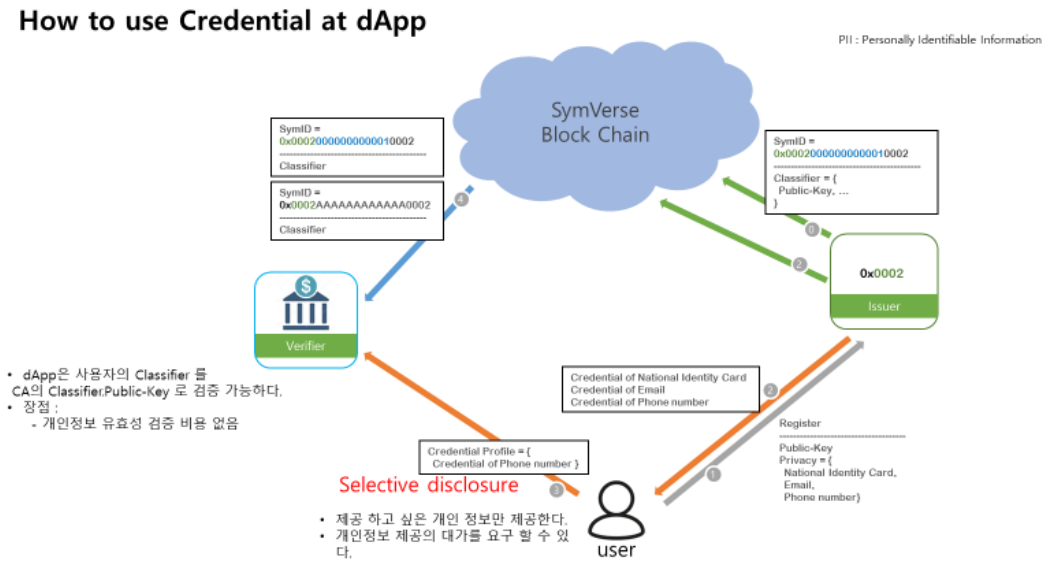
SymID를 활용하는 전체적인 시스템은 SymID를 발급하는 발급자, 정보를 제공하고 사용하는 사용자, 정보를 이용한 서비스 제공자 등으로 구성된다. 거래 또는 자격 증명, 자격 확인 등에서 SymID를 통해 각 주체는 각자의 역할을 수행하고, 원활하게 원하는 서비스를 얻으며, 이익을 극대화할 수 있다.

SymID를 발급하고 Account 또는 자격 정보를 활용하는 주체와 역할은 아래와 같다.



4. SIA 활용

1) 자격 증명 (Credential)

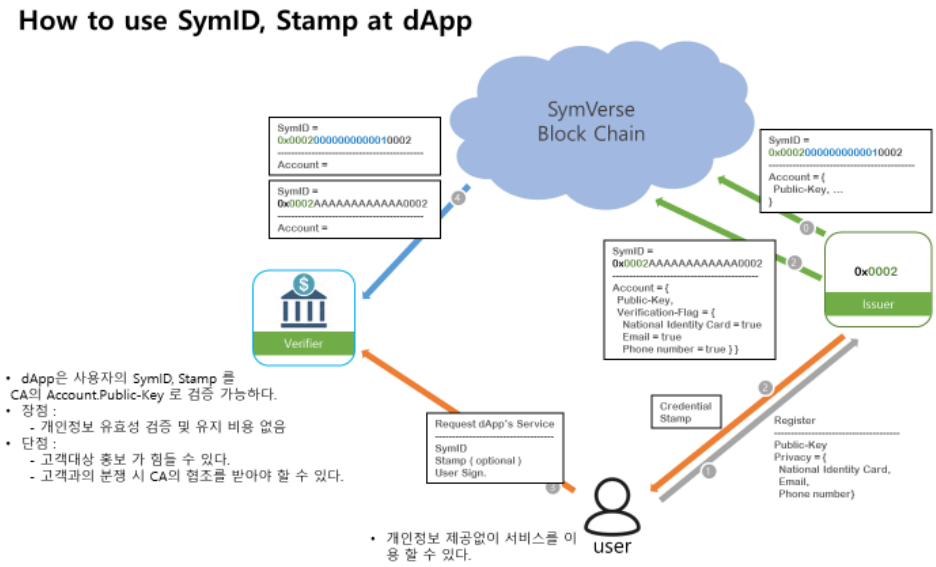


사용자는 자신의 개인 정보 중 제공하고 싶은 정보만을 선별적으로 Credential document 로 작성하여 CA 를 통해 블록체인에 등록할 수 있다. 이 경우 서비스 제공자는 서비스를 요청하는 사용자에 대해 블록체인에서 개인정보 제공 여부를 확인하고, 사용자의 자격 확인을 위해 서명 검증 이외에 개인 정보를 요청할 수 있다.

서비스 제공자는 개인 정보를 제공하는 사용자들에게는 별도의 홍보를 제공할 수 있으므로 다양한 서비스가 가능하고, 사용자는 개인 정보 제공의 대가로 더 높은 수준의 서비스를 제공받을 수 있다.

개인 정보의 제공 여부는 사용자에 의해 결정되어 블록체인에 Credential document 로 기록되므로 사용자는 자신의 신원에 주권을 가지며 언제든지 자신의 개인 정보 제공 여부를 CA 를 통해 블록체인에 기록함으로써 변경할 수 있다.

2) 자격 확인 (Stamp)



서비스를 받고자 하는 사용자가 개인 정보 제공을 원하지 않을 경우 사용자는 Credential document 를 개인정보 미제공으로 작성하여 CA 를 통해 블록체인에 등록할 수 있다. 이 경우 서비스 제공자는 서비스를 요청하는 사용자에 대해 블록체인에 기록된 SymID 의 Credential document 와 계정 정보를 활용하여 사용자에 대한 자격을 검증할 수 있다.

블록체인에 등록된 SymID 는 CA 에 의해 검증되어 계정 정보로 public key hash 를 등록한 상태이고, 서비스 제공자는 public key hash 를 통해 서명 검증만으로 사용자의 자격 여부를 판단한다.

1. Appendix

Terminology

약어/약자 abbreviation	본딧 말 (the original word)	한국어 Korean	설명 Description
SSI	Self Sovereign Identity	자기주권형 식별자	
DID	Decentralized Identifier	분산 식별자	새로운 형태의 전역 고유 식별자(GUI - Globally Unique Identifier)
CA	Citizen Alliance		SymID를 발급한다.
CAID	Citizen Alliance server ID		
	Citizen ID		사용자의 고유 식별자
SymID	Symverse ID		SymVerse blockchain 및 ID 시스템의 식별자(모든 정보는 SymID를 기반으로 하여 기록된다._
	entity	개체	사람, 조직, 개념 또는 장치 등 뚜렷하고 독립적인 존재가 있는 것.
id	***identity***	식별자	***entity*** 의 특정 부분을 식별하는 데 사용할 수 있는 정보 집합. ***entity***는 여러 개의 ***identity***와 연결될 수 있다.
	identity repository	식별자 저장소	
	subject	주제(대상)	***credential*** 이 만들어 질 수 있는 ***entity***. Ex)사람
	credential	자격증명	***Issuer*** 가 claim 을 검증하여 생성한 것이다. 사실상 조작이 불가능 하고 암호학적으로 검증 할 수 있다.
stamp	***credential stamp***	증명확인	***credential*** 을 소유하고 있음에 대한 확인
	credential profile	자격증명 집합	동일한 개체(***entity***)가 한 주제(***subject***)에 대해 주장한 여러 ***credential*** 의 집합 각 개체(***entity***)는 다양한 ***credential profile*** 을 가질 수 있다. ***credential profile*** 은 복수의 ***issuer*** 에서 발행한 ***credential*** 을 포함한다.
	credential repository	자격증명 저장소	A program, such as a storage vault or personal verifiable claim wallet, that stores and protects access to a holder's credentials
	holder	보유자	특정 ***credential*** 의 통제권을 가진 개체.
	issuer	발행자	특정 주제(***subject***)와 연관이 있는 c***redential*** 을 발행(issue) 하고 ***holder*** 에게 전달한다.
	verifier	검증자	대상(***subject***)에 대한 프로파일(profile)을 요청. 프로파일은 다수의 ***credential*** 로 구성될 수 있음. ***Verifier***는 제공받은 프로파일에 포함된 ***credential*** 이 목적에 적합한지 검토함
	Privacy	개인정보	