W3C 분산 식별자 (Decentralized ID) 표준화 동향

이원석 _ ETRI 지능정보산업표준연구실 책임연구원
이강찬 _ ETRI 지능정보산업표준연구실 실장

1. 머리말

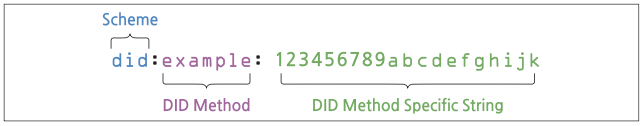
W3C(World Wide Web Consortium)[1]는 웹에 대한 모든 표준 및 기술개발 등을 총괄해 국제표준화를 주도하는 비영리단체로 HTML5(HyperText Markup Language 5), HTTP(HyperText Transfer Protocol), URL(Uniform Resource Locator) 및 XML(eXtensible Markup Language) 등을 표준화하는 등 인터넷 기술의 국제표준을 개발하였으며, 현재는 웹을 기반으로 자동차, 결제, 머신러닝, 블록체인 등의 영역으로 표준 개발을 확장하고 있다. 최근 사물인터넷, 자율주행차 등 모든 개체들이 인터넷에 연결되면서 온라인상에서 중요한 문서나 정보의 교환에 고신뢰성의 보장은 필수적으로 요구되고 있다. 이러한 요구에 따라 최근 DID(Decentralized Identifier) 기술 및 표준이 주목을 받고 있다. 이와 관련하여 W3C는 2017년 Credentials CG(Community Group)[2]를 중심으로 DID 표준 개발을 본격적으로 시작하였고 2019년에 DID WG(Working Group)[3]을 설립하여 DID 표준을 빠르게 개발하고 있다. 본고에서는 DID 국제표준과 관련하여 W3C DID 개념과 DID 상호운용성의 의미를 소개한다. 또한 W3C DID 표준화 현황 및 계획을 소개한다.

2. W3C DID 개념 및 상호운용성

2.1 디지털 아이덴티티 개념 및 모델[4]

디지털 아이덴티티는 온라인에 존재하는 개인, 조직 또는 디바이스를 고유하게 식별할 수 있는 식별자 정보를 의미하며, 디지털 아이덴티티에는 중앙집중형 아이덴티티, 제 삼자 아이덴티티 제공자 기반의 아이덴티티, 분산원장 혹은 블록체인 기반의 자기주권 아이덴티티 세 가지 모델로 구분할 수 있다.

① **중앙집중형 아이덴티티**: 사용자가 외부 사이트에 이름과 비밀번호로 계정을 만들고 두 당사자가 기밀성과 데이터 무결성이 보장된 상태로 서로 식별 및 인증하여 통신할 수 있는 암호화 프로토콜로써 Transport Layer Security(TLS) 프로토콜과 SSL 프로토콜이 있다. 두 프로토콜의 기본적인 주요 목표는 기밀성(때로는 사생활 보호), 데이터 무결성, 아이덴티티 및 디지털 인증서를 사용한 인증을 제공하는 것이다.



[그림 1] DID 표기 방법

② **아이덴티티 제공자 기반의 아이덴티티**: 두 당사자 중간에 아이덴티티의 신뢰를 보장하는 아이덴티티 제공자가 있는 것으로 Security Assertion Markup Language(SAML), OAuth, Open ID connect 등의 표준이 있다.

③ **분산원장 혹은 블록체인 기반의 자기 주권 아이덴티티**: 최근에 연구/개발 중인 자기 주권을 보장하는 블록체인 기반 아이덴티티는 두 당사자의 신뢰를 블록체인 기반으로 인증하는 것이다.

2.2 W3C DID 개념 및 표기 방법

W3C에서 DID는 중앙화된 등록 기관에 등록이 필요하지 않은 글로벌한 식별자로 정의하고 있으며, 사용자가 개인정보를 생성하고, 사용하고, 삭제하는 등 개인정보를 관리할 수 있으며, 내가 나를 증명할 수 있는 방법을 제공할 수 있어야 한다.

DID 표기 방법은 URN(Unified Resource Name) 규격을 참고하여 유사한 방식으로 설계되었으며 [그림 1]과 같이 세 부분의 문자열로 구성된다.

- **Scheme**: DID 식별자임을 표시하는 것으로 모든 DID는 'did'로 시작한다.
- **DID Method**: DID가 생성되고 읽어지고 업데이트되는 등의 CRUD(Create, Read, Update, Delete)를 수행할 수 있는 방법을 지정하는 것이다. 현재 다양한 방법의 DID 메소드(Method)가 제안되어 있으며, 현재까지 did:web(URI를 DID로 사용), did:git(개발자를 위한 DID), did:ipid(분산 파일 시스템 기반 DID), did:PROPRIETARY(특정 사업자가 제공하는 DID), did:peer(P2P 관계를 위한 DID), did:key(공개키 기반 DID) 등이 제안되었다.
- **DID Method Specific String**: DID 메소드에 해당하는 ID 문자열이다.

실제로 DID는 DID 문서로 해석된다. DID 문서는 공개키, 유사생체인식과 같은 메커니즘을 포함하여 DID를 인증하고 DID 관련을 입증하는 데 사용할 수 있는 DID 주제를 설명하는 데이터 세트이다. DID 문서는 식별 대상을 설명하는 다른 속성이나 식별 대상을 포함할 수 있으며, 일반적으로 JSON-DL을 사용하여 표준되는 그래프 기반 데이터 구조를 따르거나 다른 호환 가능한 그래프 기반 데이터 형식을 사용하여 표현할 수 있다. DID 문서는 DID에 대한 식별 및 검증에 핵심적인 요소이다. [그림 2]는 DID 문서에 대한 예를 보여준다.

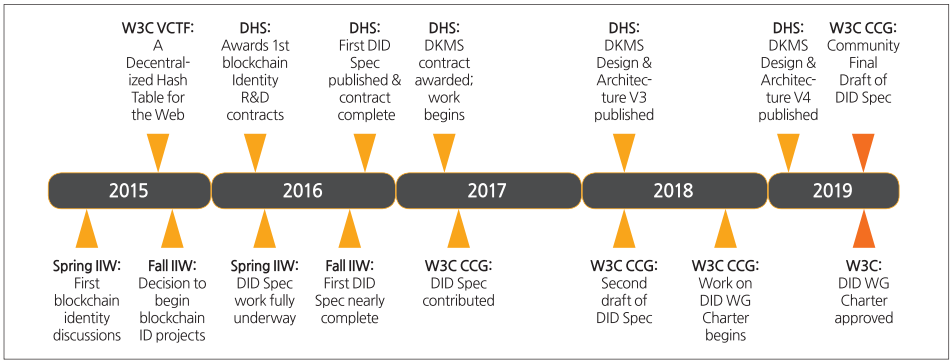
2.3 W3C DID 상호운용성

DID 및 DID 문서에 대한 상호운용성은 스펙을 준수하는 DID 및 DID 문서를 작성하고, 이 DID 및 문서를 분석하는 구현 기능에 대한 테스트가 필요하다. 또한 DID 메소드에 대한 상호운용성은 각 DID 메소드의 사양을 평가하여 최소한 다음의 사항을 만족하여야 한다.

- DID 메소드 이름이 고유하며 기존의 호환되지 않는 DID 메소드에서 사용되지 않아야 한다.
- DID 메소드에 요구되는 연산이 지원되어야 한다.
- 연산에 대한 설명이 기술되어야 한다.
- 스펙은 구체적이고 자세히 기술되어야 하고 독립적인 구현을 위해 충분히 설명되어야 한다.
- 스펙에는 보안 및 개인정보보호에 대한 고려사항을 설명하는 섹션이 포함되어 있어야 한다.

```
[최소자체관리 DID 문서] - 인증정보(컨트롤러, 공개키등) 서비스제공하는 DID 문서
{
 "@context": "https://www.w3.org/2019/did/v1",
 "id": "did:example:123456789abcdefghi",
 "authentication": [{
   // used to authenticate as did:...fghi
   "id": "did:example:123456789abcdefghi#keys-1",
   "type": "RsaVerificationKey2018",
   "controller": "did:example:123456789abcdefghi",
   "publicKeyPem": "-----BEGIN PUBLIC KEY...END PUBLIC KEY-----\r\n"
 }],
 "service": [{
   // used to retrieve Verifiable Credentials associated with the DID
   "id":"did:example:123456789abcdefghi#vcs",
   "type": "VerifiableCredentialService",
   "serviceEndpoint": "https://example.com/vc/"
 }]
}
```

[그림 2] DID 문서 예



[그림 3] W3C DID WG 신설 과정

즉, DID 및 DID 문서의 생산자와 소비자를 위한 상호운용성은 DID와 DID 문서가 일치하도록 보장함으로써 제공되며, 메소드 사양의 상호운용성은 사양의 세부사항에 의하여 제공되어야 한다.

3. W3C DID 표준화 현황

3.1 DID WG 설립

2017년 W3C CCG(Credentials Community Group)에서 DID 명세 개발을 시작하였고 2018년 말부터 DID WG 설립을 준비하여 2019년 9월에 DID WG을 설립하였다. 또한 2019년 11월 초 DID WG에서 첫 번째 DID 1.0 스펙 초안을 공식적으로 공개하였다. 이렇게 빠르게 스펙을 준비할 수 있었던 것은 DID CCG에서 개발 중에 있던 DID 스펙을 WG 설립과 함께 인수인계받아 준비했기 때문이다.

3.2 DID 표준 개발 계획

최근 신설된 DID WG은 [그림 4]와 같이 2021년 말까지 2건의 W3C 노트(Note)와 1건의 권고안(Recommendation) 개발을 목표로 하고 있다.

Specification	FPWD	CR	PR	Rec
Decentralized Identifier Use Cases & Requirements (NOTE)	November 2019			August 2021
Decentralized Characteristics Rubric (NOTE)	December 2019			September 2021
Decentralized Identifiers Data Model and Syntax(es)	November 2019	November 2020	July 2021	August 2021
Note: The group will document significant changes from this initial schedule on the group home page.				

[그림 4] DID WG 표준 개발 일정

- **Decentralized Identifier Use Cases and Requirements:** DID로 수행할 수 있는 작업과 DID를 사용해야 하는 이유를 사례(엔터프라이즈, 교육, 헬스케어, 법률, 보안)별로 정리한 문서
- **Decentralized Characteristics Rubric:** DID 메소드 및 서로 다른 분산 식별자에 대한 평가 방법 제시
- **Decentralized Identifiers Data Model and Syntax(es):** DID 문법 및 DID 문서에 대한 기술 방법에 대한 표준

W3C에서는 CR(Candidate Recommendation)에서 PR(Proposed Recommendation) 단계로 넘어가기 위한 조건으로 스펙에 대한 두 개 이상의 구현을 시험한 구현 리포트가 있다. 따라서 스펙에 대한 테스트 케이스(Test Cases) 개발, 두 건 이상의 구현물 그리고 시험 보고서 작성이 필요하여 일반적으로 PR 진입에 많은 시간이 필요하다.

4. 맺음말

DID는 온라인에 존재하는 개인, 조직 또는 디바이스를 고유하게 식별할 수 있는 식별자를 표현하기 위한 표준 표기법을 정의하고, 이러한 온라인상의 개체를 검증할 수 있는 기반을 제공하는 핵심적인 표준이다. 즉, DID를 통해서 보다 안전하게 대학교 졸업증명서, 학위증명서 같은 인증이 필요한 사회의 모든 증명서를 포함하여 디바이스에 대한 인증, 응용에 대한 인증 등 온라인상의 모든 개체에 대한 고신뢰 서비스 환경을 제공할 수 있다.

W3C는 2019년 9월 DID WG을 설립하고 DID 표현 방법 및 DID 문서에 대한 표준 개발을 빠르게 진행하고 있으며, 2019년 11월 초에 DID 핵심 표준에 대한 초안을 공개하였다. 이러한 DID 국제표준 개발과 함께 업계의 블록체인 플랫폼 활성화 및 DIF(Decentralized identity Foundation)[5] 등 DID 생태계 확산 노력으로 DID 활용은 빠르게 늘어날 것으로 기대된다. 따라서 국내에서도 DID와 관련한 IPR 및 국제 표준화에 대한 전략적 선점을 위한 노력이 절실히 요구되는 시점이라고 생각된다. 또한 이러한 관점에서 우리가 강점을 지닌 DID 관련 기술 개발이 필요하며, 더불어 이와 관련된 국제 표준화 전략을 새롭게 고민해 볼 시점이라고 할 수 있다.

※ 본 연구는 2019년도 과학기술정보통신부의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임[2018-0-01537, 고신뢰 서비스 생태계 구축을 위한 블록체인 표준 개발].

[참고문헌]

[1] W3C, 2019. https://www.w3.org/
[2] W3C Credentials CG, 2019. https://www.w3.org/community/credentials/
[3] W3C DID WG, 2019. https://www.w3.org/2019/did-wg/
[4] 권동승, 이현, 박종대, '디지털 신뢰 사회 실현을 위한 디지털 아이덴티티 동향', ETRI 전자통신동향분석, 2019.
[5] Decentralized identity Foundation, 2019. https://identity.foundation/