DID vs e-Certificate (PDF)

Use DID for identity verification, on/offline verification, data integrity and reliability

Features	DID (Decentralized ID)	e-Certificate (PDF)
Definition	Verifiable **digital credential** using decentralized web technology	**File format** created by Adobe
Purpose of use	Digital credential, user identity verification, authentication, etc.	Keep, share and print document, e-book, report
User's identity verification	Decentralized web technology	Unable to verify user's identity with PDF
On/Offline verification method	**Verify** with the issued VC	**Unable to verify** on/offline
Digital signature and security	Secure integrity and identity	Limited feature of digital signature
Data format and store	Store in blockchain	Text-based
Data reliability	Secure reliability with **blockchain**	Not secure directly
Central agency	**Self verification** with distributed system	**Need a separate institute** or central agency
Privacy	**Owned and managed by the user**	**Add encryption function**
Decentralized web technology	Core technology of VC	General PDF file type
Validity period	Set by the issuer on VC	Not designated

Introduction Method

Category		SaaS (OmniOne Digital ID)
Deployment models	Blockchain node	Use OmniOne Digital ID SaaS service
	Issuing system	Use OmniOne Digital ID SaaS server (ledger DB and simple APIs)
	App	Use OmniOne App (provide SDK when using own App)
	Verification system	Use OmniOne Digital ID SaaS server
Deployment period		Between two and four weeks for service registration and connection
Costs		Basic platform fees and a charge based on usage
Operation		Operated by Cloud SaaS service provider (only need the current system operators)
Scalability		Need to discuss with Cloud SaaS service provider
Introduction organization		For those who need quick deployment

Signup and use OmniOne DigitalID service, a Cloud SaaS, through a simple procedure.

On-Premise is available for enterprises who need closed network, network separation and internal security.

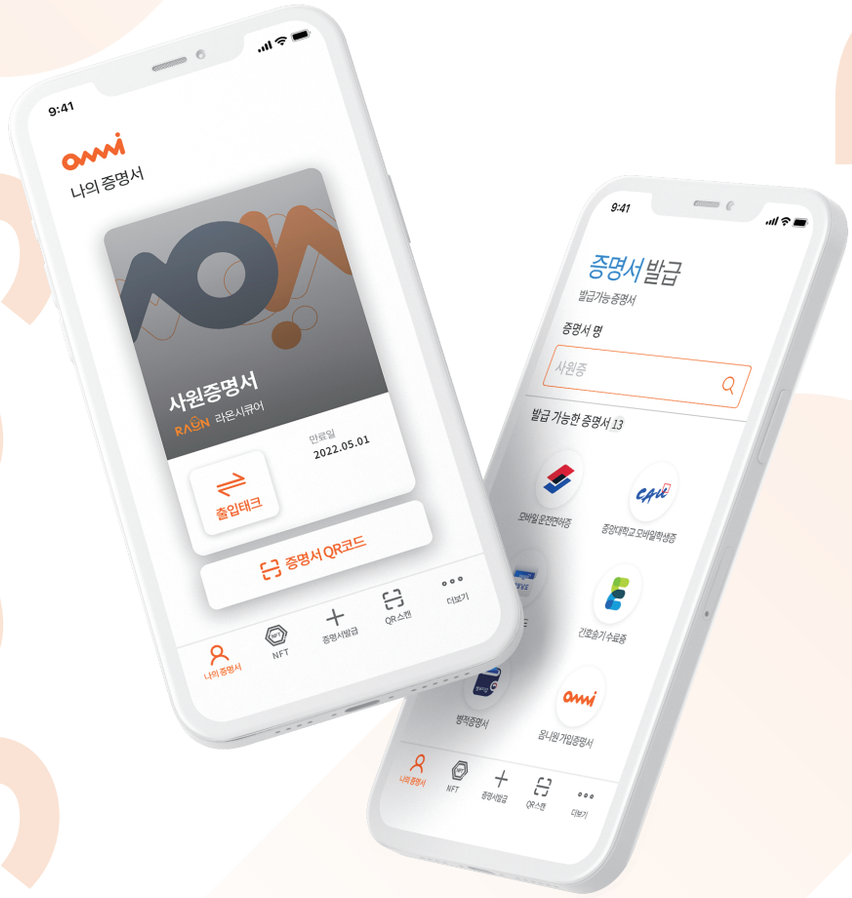
RaonSecure

Head office 47-48F Parc1 Tower 2, 108 Yeoui-daero, Yeongdeungpo-gu, Seoul, Korea
Tel 02-561-4545 **Fax** 02-561-5350 **Inquiry** serviceplan@raoncorp.com
Homepage www.omnione.net

Scan Your QR code

OmniOne Digital ID

Blockchain DID-based integrated SaaS platform for identity verification and credential authentication



RAON

Services

OmniOne Digital ID is Blockchain DID-based integrated SaaS platform for identity verification and credential authentication.

DID
(Decentralized Identity)

Decentralized identity verification management system to realized SSI for users

\+

FIDO
(Fast Identity Online)

Use user's biometric information for authentication without passwords

=

OmniOne Digital ID

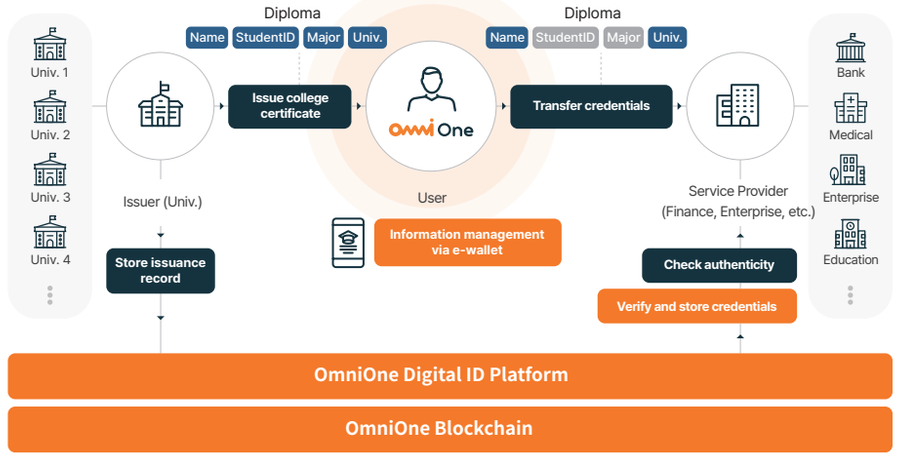
Store the user's decentralized ID and metadata exclusively on the blockchain to eliminate the risk of information leakages.

Differentiators

OmniOne Digital ID provides safe identity verification and credential authentication services under a Cloud SaaS environment.

- Cloud-based service for identity and credential authentication
- Quick and simple signup without system installation
- One Digital ID for both on and offline
- Platform for issuers, service providers and users
- Store Digital ID in TrustZone
- Check the authenticity of DID issuance via blockchain

Service diagram



Features

01 Enroll parties and issue a guarantee

- Enroll parties (issuers, service providers and users). (create a trust chain connecting OmniOne platform, service providers and users)
- Issue a guarantee for parties (issuers, service providers and users).

02 Apply for service and admit

- Apply for OmniOne platform service.
- Automatically allocate a service server when admitted.
- Operate a service server in the cloud for parties.

03 Issue a DA for parties

- Issue a Digital Address (DA) for parties within the domain.
- Get issued multiple DAs (DA consists of unique values for the domain)

04 Issue an identity certificate / credential

- Issue identity certificates and credentials (serve as eKYC and evidence)
- Quickly set based on the standard template for each certificate

05 Authenticate and distribute certificates

- Submit a identity certificate and distribute credentials.
- Simple log-in through decentralized DID-based biometric authentication.

06 Manage service admin and operation

- Separated Admin access for each issuer and service provider.
- Set a certificate template for each issuer.
- Set a certificate list and attribute data for each service provider.