H. Roßnagel, C.H. Schunck, S. Mödersheim (Hrsg): Open Identity Summit 2022,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2022 137

Combination of x509 and DID/VC for inheritance properties of trust in digital identities

Paul Bastian[1], Carsten Stöcker[2], Steffen Schwalm[3]

Abstract: The proposal for review of the eIDAS Regulation from 2021 has opened strong expectations for a deep change in traditional identity models. The new regulation starts with the creation of European Digital Identity Wallets that will enable citizens' control over their data in identification and authentication processes. Likewise digital identities and digital signatures are in place and interoperability between existing solutions mainly based on x509 certificates and decentralized PKI using DID/VC foreseeable. The paper provides various options in combining x509 and DID/VC approaches.

Keywords: eIDAS, SSI, self-sovereign identity, x509, DID, verifiable credentials, interoperability

1 Introduction

Unique identification of legal or natural entities as well as their objects – the basement for a digital identity – allows the verification of companies (Do they really exist?), the person acting for the company (Do they really exist?) and their authorization (Is Alice authorized to act for company A?). Digital identities and digital signatures are currently typically issued by a centralized authority using [x509] certificates as well as [OIDC] and [OAuth2]-protocols while e.g. DLT follow the DID/VC [W3C]. Both technical approaches are basically possible to execute the new SSI-paradigma but according to the comprehensible dissemination of x509/OIDC-approach the vice-versa interoperability is essential. This paper specifically discusses possible hybrid approaches on how to technically combine x509 and DID/VC. The paper is based on results of research projects from *GAIA-X Federation Services*[4] and *ID Union* where the authors take part in.

2 Hybrid-Approaches x509 and DID/VC

Conceivable hybrid approaches for combination of x509 and DID/VC are Embedding DID in x509 certificate, Derivation DID from x509 key pair, Encapsulated credential during onboarding in use case domain including issuance of identity credential, x509 based wallet and trusted verifier, Signed x509 in DID-Document, Using [eIDASBridge]. This

[1] Bundesdruckerei Group, Kommandantenstraße 18, 10969 Berlin, Germany
[2] Spherity GmbH, Emil-Figge-Straße 80, 44227 Dortmund, Germany
[3] msg group, Robert-Bürkle-Str. 1, 85737 Ismaning, Germany
[4] See https://gaia-x.eu/what-is-gaia-x/federation-services

cbe doi:18.18420/OID2022-13

list is not comprehensible so there are more approaches possible.

3 Discussion of hybrid approaches

3.1 Option 1: Embedding DID in x509 certificate

During issuance of a x509 certificate a signed DID will be embedded in the x509 certificate. It's necessary to ensure that a (qualified) trust service provider acc. [eIDAS] is needed to ensure that the DID is really linked to the identified natural or legal entity. This means basically that the onboarding process for x509 certificates must be changed such that the QTSP as an issuer of x509 certificates validates the signed DID of the identified natural or legal entities using a secure communication channel e.g., TLS acc. [TR02102]. Afterwards the DID will be integrated into the certificate as an x509 extension e.g., by a trusted resolver service so that the verifier gets the information how to resolve the DID from the DID document. This means that in the results the x509 includes a DID which can be resolved by a trusted 3rd party to ensure verifiability and useability of VC of wallet service endpoint of the given holder. Any other identity x509 attributes including the Root-CA can be used as usual without any change needed.

Option	Advantages	Disadvantages
Embedding DID in x509 certificate	Method for combination of x509 certificates with DID for inheritance of properties/credentials of verified entities	Change in x509 issuance process necessary

Table 1: Summary Option 1

3.2 Option 2: Derivation DID from x509 key pair

For the special use case that x509 certificates and DID use the same cryptographic primitives the key material of x509 may be used for evidence of control of the x509 certificate itself as well as the given DID document. Public and private key pair of the x509 certificate will be used for the creation of a new DID and DID document. This approach can be beneficial if dedicated crypto primitives are mandatorily required due to compliance, business or legal needs.

Option	Advantages	Disadvantages
Derivation DID from x509 key pair	Method for combination of x509 certificates with DID for inheritance of	Requires utilisation of same crypto primitives for x509 and DID as well as

	properties/credentials of verified entities	authoritative control for signatures in DID Document

Table 2: Summary Option 2

The picture below illustrates option 1 and 2:

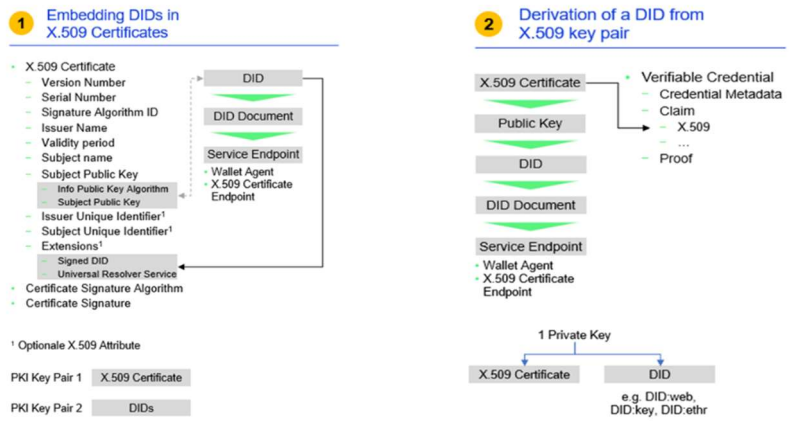

Figure 1: Option 1 and 2

3.3 Option 3: Encapsulated credential during onboarding

The idea of option 3 is that a verification service validates if the holder really owns two private keys so Private key for x509 certificate and Private key of self created (or created by TSP) DID. In this case the holder creates and signs the credential with his private keys to achieve an encapsulated data structure which contains both signatures. The aim is that the verifier is enabled to validate if the holder controls both private keys X509 identity proof, e.g. EV or QWAC, DID control of DID private key. Sequence of encapsulation does not matter and may be designed according to the communication protocols in use. If the verifier is an onboarding or verification service, the signature can be verified directly in the encapsulated credential itself. Additionally, the x509 verification service verifies the validity and trust chain of the x509 certificate. In the next step the can create verifiable credential for the holder where the trust is given by e.g., at the trusted issuer [BaseID], [OCI].

Option	**Advantages**	**Disadvantages**
Encapsulated credential	Method for combination of	Additional verification

Option	Advantages	Disadvantages
during onboarding	x509 certificates with DID for inheritance of properties/credentials of verified entities Encapsulated credentials are established approach No change in x509 specification	service (trusted third party) for issuance of VC

Table 3: Summary Option 3

3.4 Option 4: x509 based wallet and trusted verifier

X509 certificates may also be used to validate if the holder communicates with the infrastructure domain of a verified issuer or verifier. Under the assumption that those systems running in the same infrastructure domain the verifier may assume that the DID-based Wallet hosted in this domain is owned by the given holder. This implies that an SSI agent will create a channel to a service endpoint e.g., using an Aries DIDComm-Channel running over HTTPS. The communication is operated encapsulated with the assumption that if the user the x509 certificate of the outer channel is trustworthy that the endpoint of HTTPS is the mentioned DID subject and consequently the verifier is trustworthy too. The X.509 certificate can be an Extended Validation Certificate (EV).

Option	Advantages	Disadvantages
Wallet infrastructure with an X.509 Certificate (e.g. Extended Validation Certificate)	Easy to implement May solve issuer of trusted verifier	No solution for interoperability between x509 and DID/VC Only works for HTTPS-related communication while DIDComm also supports other channels like Bluetooth or NFC

Figure 5: Summary Option 4

3.5 Option 5: Signed x509 in DID-Document

Another option is to add a signed x509 certificate (e.g., signed by a qualified trust service

provider) in the DID-document of the holder and the certificate end point in the DID-document itself. The result is an encapsulated credential like option 2. During the addition of signed x509 in DID-document this must also be signed with its private key to update the DID-document including the x509 certificate.

Option	Advantages	Disadvantages
Signed x509 in DID-Document	Method for combination of x509 certificates with DID for inheritance of properties/credentials of verified entities	Addition of signed x509 in DID-document is not defined in W3C-DID-Specification, extension allowed Update of DID-document implies no secured link

Table 4: Summary Option 4

3.6 Option 6: eIDAS Bridge

Further option is the utilization of [eIDASBridge]. The [eIDASBridge]. was developed by the European Commission to establish a legal compliant link between SSI based on DID/VC and existing digital identities based on x509. It contains legal reports and technical specifications and ensures legal trust in SSI if [eIDAS2] is not fully applicable. The [eIDASBridge] implies that verifiable credentials are signed with an additional (qualified) electronic signature or seal of the issuer from a qualified trust service provider acc. to [eIDAS]. In result existing validation mechanism acc. [ETSIEN319102] can be used to make the authenticity and integrity of the VC evident against 3rd parties to fulfil the burden of proof and documentation requirements. [Ko20], [We18].

Option	Advantages	Disadvantages
eIDAS Bridge	Ensures legal trust of VC Verifiability of VC by any validation service acc. eIDAS	Less feasible for interoperable attribute exchange between x509- and DID/VC-based environments

Table 5: Summary Option 6

4 Outlook

The interoperability between x509 and DID/VC based digital identities as well as digital signatures can be mentioned as one of the most important success factors for SSI. The

paper discussed roughly different possiblities which will be analyzed in detail by the authors and may be part of further standardization..

Bibliography

[eIDAS1] Regulation (EU) No 910/2014 of the European Parliament and of the Council - of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. eIDAS, 2014.

[eIDAS2] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity {SEC(2021) 228 final} - {SWD(2021) 124 final} - {SWD(2021) 125 final}

[eIDASBridge] Burgos, O. et al: SSI eIDAS Bridge - Use cases and Technical Specifications. Brusssels 2020: https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/document/ssi-eidas-bridge-use-cases-and-technical-specifications

[ETSIEN319102] ETSI EN 319 102-1 Electronic Signatures and Infrastructures (ESI). Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation

[IS20] ISO/IEC 9594-8:2020 Information technology - Open systems interconnection - Part 8: The Directory: Public-key and attribute certificate frameworks

[Ko20] Korte, U. et. al.: Criteria for trustworthy digital transactions – Blockchain/ DLT between eIDAS, GDPR, Data and Evidence Preservation. OpenIdentity Summit 2020. Lecture Notes in Informatics (LNI). Proceedings. Bonn 2020 S. 49-60

[OIC] Hendrix, P et. Al.: Credential Issuer Conformance Criteria v2.0.0. W3C. 2020

[OIDC] OpenID Connect protocol: https://openid.net/connect/

[OAuth2] OAuth2 protocol: https://oauth.net/2/

[RFC5280] Cooper, D. et. Al.: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. 2008

[TR02102] Technical Guideline TR-020159. BSI TR-02102 Cryptographic Mechanisms. Federal Office for Information Security. https://www.bsi.bund.de/EN/Service-Navi/Publications/TechnicalGuidelines/tr02102/tr02102_node.html

[W320] W3C: Decentralized Identifiers (DIDs) v1.0. 2020.

[We18] Weber, M. et al.: Records Management nach ISO 15489. Einführung und Anleitung. Beuth Verlag, Berlin, 2018.