An integrated approach for electronic identification and central bank digital currencies

Received (in revised form): 21st June, 2021

Michael Adams*
Founder, Quali-Sign, UK

Luca Boldrin**
Innovation Manager, InfoCert, Italy

Ralf Ohlhausen***
Founder, PayPractice, Germany

Eric Wagner†
Group Product Owner Compliance Advanced Analytics, Erste Group Bank, Austria

Michael Adams

Luca Boldrin

Ralf Ohlhausen

***Michael Adams** is the founder of Quali-Sign Ltd, a company specialising in mobile apps for electronic identification and strong customer authentication. Michael has participated in the UK and Berlin Group Open Banking forums and the EU/UK Forums on Electronic Identification. He has also provided consultancy services to the European eIDAS enabled i-banking project.*

***Luca Boldrin** investigates innovation trends and manages research initiatives for InfoCert, the EU's largest qualified trust service provider. His specialist areas are trust services, identity management, distributed ledgers and security. He has been involved as a subject expert in many digital transformation projects, both at national and international levels, and regularly takes part in standardisation initiatives in his areas of expertise. He is a member of the EU Blockchain Observatory Expert Group.*

***Ralf Ohlhausen** is founder of PayPractice, an organisation that provides payment service providers, such as PPRO and Tink, with advice about open banking. Ralf chairs the European Third Party Providers Association, co-chairs the Berlin Group's openFinance Advisory Board, and is a member of the European Central Bank's Market Infrastructure Board and alternate member of the Euro Retail Payments Board.*

***Eric Wagner** is responsible for the advanced analytics compliance platform and related services at Erste Group Bank AG. He is also actively involved in a number of national and international expert groups and working groups in various fields relating to financial crime and electronic ID, as well as advanced analytics and emerging technologies.*

Abstract

This paper outlines a proposal for how to implement Central Bank Digital Currencies (CBDC) based on open banking standards and supports both account-based and token-based CBDC models, transacting online and offline with immediate finality, while recognising the European PSD2 requirements, including (multi-factor) strong customer authentication (SCA). The authors recognise the limitations with current smartphone technologies with respect to deploying trusted applications and in performing the role of a qualified signature creation device - highly relevant to offline scenarios. In some cases, the authors recommend regulatory review, in others they recommend taking full advantage of the existing capabilities of the separated secure execution environment by dividing the control of a CBDC transaction between both payee and payer devices, so that if one device was compromised, this does not undermine the whole transaction. It balances the need for anonymity

**Quali-Sign Ltd, Woodview, Hough Lane, Alderley Edge, Cheshire SK9 7JE, UK*
E-mail: michael_adams@quali-sign.com

***InfoCert, P.zza da Porto 3, 35100 Padova, Italy*
E-mail: luca.boldrin@infocert.it

****PayPractice, Neue Str. 17, 73642 Welzheim, Germany*
E-mail: ro@paypractice.com

Journal of Payments Strategy & Systems
Vol. 15, No. 3 2021, pp. 287–304

1750-1806

Eric Wagner

with financial crime regulatory requirements and suggests that a CBDC wallet can be enriched with eID capabilities, or vice versa. The wallet is bound to the person's identity, their device and software via a chain of trust (eIDAS for the EU or similar for non-EU countries). The authors combine this with self-sovereign identity (SSI) principles to maximize privacy and minimize information sharing with a third party

Keywords: CBDC, identity, eID, SCA, electronic signatures, verifiable credentials, offline transactions

BACKGROUND

For many years, payments have been one of the most exciting areas of technological innovation in the financial industry. Market players are continuously rolling out new solutions and services, while authorities are working toward regulations, regulatory standards and guidelines to foster opportunities while reducing systemic threats to the growing ecosystem of payment means. These efforts are geared at making such payments easier and faster and, at the same time, more secure for banks, merchants and their customers.

Among the many innovations ongoing in the payments industry, this paper focuses on two areas that may well determine the next breakthrough:

- *Central bank digital currencies (CBDCs):* According to the Bank for International Settlements (BIS),[1] central banks representing one-fifth of the world's population are likely to issue CBDCs in the near future, while 20 per cent of central banks (by number) are likely to issue a retail CBDC over the medium term. Concurrent with this, a full 80 per cent of central banks are conducting research and development in the area of CBDCs.
- *Electronic identification (eID):* The payments industry is working on solutions that combine modern payment technologies and eID to provide a seamless and secure payment experience, in addition to functions such as the ability to sign third-party contracts.

At present, payments are normally made using physical cash, cards, cheques or credit transfers (account to account). As yet, is unclear whether CBDCs will simply co-exist with these instruments or whether they will significantly reduce the market share and role of certain payment types (notably cash or debit cards).

A comparison of a general-purpose CBDC (available to retail consumers) with existing means of payments across seven categories reveals how an appropriately designed CBDC could provide value for users in certain areas.[2] These technological benefits could include a digital form of a bearer instrument, more cost-effective payment services, greater anonymity than current digital transactions, and a catalyst for greater innovation through programmable money.

There are also use cases where the practical application of CBDC could solve some of today's challenges. The recent economic stimulus packages issued to citizens as part of the coronavirus relief effort provide a case in point.

While previous stimulus efforts reportedly took at least two months to reach recipients and used a combination of direct deposit, paper cheques and prepaid debit cards, CBDC could theoretically be used to remunerate every citizen electronically, thus greatly simplifying and expediting the disbursement process. In such a case, the integration of eID and CBDC would provide confidence vis-à-vis the identity[3] of the citizens receiving such benefits.

As this paper is focused on a specific implementation approach, no further political or strategic topics will be elaborated. Indeed, such aspects have been discussed

†*Erste Group Bank AG, Am Belvedere 1, 1100 Vienna, Austria*
E-mail: eric.wagner@chello.at

extensively elsewhere, including within this very journal.[4]

As identified in the public consultation on a digital euro conducted by the European Central Bank (ECB),[5] data privacy and related aspects such as anonymity or traceability are highly important. Full anonymity, even for small amounts, is simply incompatible with anti-money-laundering (AML) regulations and regulations to counter the financing of terrorism (CFT). Full anonymity would also impact the ability to detect and reverse double-spending conducted offline.

To address these issues, transactions must be traceable in both online and offline use cases — while meeting data privacy and other regulatory requirements. This requires a level of data privacy that supports the auditability legally required for authorised entities while also providing customer consent-based transparency with respect to other market participants.

This paper outlines an approach that fulfils both these aspects through the adoption of electronic identities, which may be provided by one or more identity service providers (either public sector or private sector providers) and be separated or aggregated in one or more wallets. This integration makes auditability feasible without sacrificing privacy, when accompanied with additional adequate data privacy mechanisms, such as key rotation or other privacy enhancement techniques.[6]

This integrated approach enables the full range of non-payment related use cases, such as COVID-19 'vaccination passports', ticketing, travelling, etc, in a secure way, that also includes rare features such as counterparty authentication and complex transaction handling based on countersignatures. Subsequently, more complex transactions, such as cross-border or multi-currency transactions, can be handled once an appropriate payment scheme has been defined, such as SEPA or SWIFT.

The paper also discusses other proposed offline approaches, including the one proposed by Visa.[7] These approaches are identified either as technologically unviable (at present) or integrated to the maximum extent feasible, as is the case with the World Wide Web Consortium's Self Sovereign Identity (W3C SSI) approach. The SSI concepts have been adopted, but in order to support the complex transaction handling and offline trust verification required by CBDC, they have been implemented using eIDAS Advanced Electronic Signatures (AdES) and X.509 Attribute Certificates. The work of the ISO Technical Committee 68 including on ISO24366[8] (Identification of Natural Persons) may also become relevant in this context.

The proposed approach makes use of existing, proven technologies and standards, hence it has been possible to prototype and demonstrate the approach successfully.[9]

DEFINITIONS AND CONTEXT

This section consolidates definitions from various sources in order to use them coherently.

Electronic identification

'Electronic identification' refers to the process of using personal identification data in electronic form to uniquely represent either a natural or legal person, or a natural person representing a legal person.[10]

Electronic signature

'Electronic signature' refers to electronic data attached to or logically associated with other electronic data that a signatory may use to sign.[11]

Identity provider

NIST defines an identity provider as 'The party that manages the subscriber's primary authentication credentials and issues assertions derived from those credentials'.[12]

Identity providers prove the real-world identities of persons and are responsible for issuing or certifying an app/device to be used for eID.

An identity provider issues the person with an electronic wallet that is maintained within the eID app/device. A person can maintain one or more wallets within the same eID app.

Each eID wallet operates a dedicated cryptographic public/private key pair.[13] The identity provider must ensure that the private key (eg stored within the separated secure execution environment[14] of a smartphone) is under the sole control of the person.

The identity provider issues the person with credentials (eg an X.509 certificate[15]) to represent the wallet. These credentials bind the person's real-world identity to the key pair and to the eID app, the device and operating system via Android attestations[16,17] and iOS attestations.[18]

The identity provider can also be or may contract with a qualified trust service provider (QTSP)[19] to support the issuance and management of the eID wallet credentials, represented by a qualified certificate for electronic signatures (in the case of natural persons) or electronic seals (in the case of legal entities). When issuing credentials to the person,[20,21] the identity service provider/QTSP must ensure that a 'high' level of assurance[22,23,24] is achieved.

The identity provider is responsible for suspending or revoking a person's eID wallet credentials.

In a CBDC context, the identity provider would be a payment service provider (PSP) that issues a CBDC app to its payment service users (PSUs). The PSP may contract with a QTSP to issue and manage credentials. While a CBDC app may additionally perform standalone eID functions, the main purpose of the associated wallets would be to store and transact digital currency. Each wallet could be regarded as equivalent to a (bank money) account.

Identity service provider (SSI context)

In the current SSI[25,26] context, the data subject is his own identity provider, ie the person is self-sovereign. There is no role for a third-party provider to manage their identity. Instead, an identity service provider provides ancillary services, such as registration, resolution and documentation services.

The data subject manages and controls his own public/private key pairs without an associated certificate that constitutes the root of trust.

This is inadequate for either an EU eID or a payments context. Therefore, an identity provider role (as defined above) is required for such purposes.

Attribute provider

Attribute providers collect or create pieces of information that describe something about a person.

An attribute provider is responsible for ensuring that an attribute belongs to the correct person; however, the attribute provider relies on the identity provider to bind a person's real-world identity to their wallet (eg eID, CBDC etc).

The attribute provider will also issue the person with credentials (eg in the form of an X.509 certificate), in a verifiable form that describes a person's attribute(s). These credentials are bound to the person's wallet credentials.

The attribute provider is also responsible for suspending or revoking a person's attribute credentials.

In a CBDC context, the PSP/QTSP may perform the role of attribute provider[27] and:

- issue additional PSP-related attribute credentials (eg source of funds, source of wealth, insolvency/bankruptcy risk, bank account code, list of PSP services active, transactional behaviour, banking relationship); and

- import attributes from other (trusted sources) attribute providers (eg proof of age, university qualifications).

A key driver behind the separation of identity and attributes is privacy and data-minimisation. For example, in a CBDC context, when a person (the payer) pays for goods in a shop, they have every right to remain anonymous to the shopkeeper (payee). Therefore, when signing a CBDC transaction, the payer's wallet credentials must not contain a common name (eg Jane Doe). However, in order for the payer to authorise the payment (via strong customer authentication (SCA)) the payee's name must be displayed to the payer. The payee cannot retain their anonymity from the payer. Therefore, when the payee prepares and signs a request for payment (eg an electronic invoice or any other type of payment request not containing debtor/payer information), the payee CBDC app (eg point of sale (POS) or CBDC wallet) must include both the payee's wallet credentials plus an additional attribute credential, to supply their name. This allows a person to reuse the same wallet credentials when performing both payer and payee roles. The parties share additional attribute credentials, as appropriate.

KEY BUSINESS REQUIREMENTS

Legal certainty

For payments, the capture of SCA enables a PSP (eg a bank or CBDC wallet provider) to hold the payer liable in the event of fraud. Therefore, the action of performing SCA transfers liability from the PSP to the payer. In a dispute situation, a court of law may be called to adjudicate. A court-appointed official would be required to evaluate the proof. It is therefore in the interests of the PSP to ensure the SCA proof offers legal certainty. Although the burden of proof is on the PSP in the event that fraud does occur, it is clearly in the interests of the payer for the PSP's SCA procedure to offer the highest level of assurance to minimise the risk of fraud arising in the first place.

To ensure legal certainty in all EU jurisdictions for the finality of payments, it would be ideal if the SCA proof were to involve the creation of a qualified electronic signature, as this provides the highest level of admissibility in the EU courts and has the equivalent legal status as a handwritten signature. In order for a signature to be deemed qualified, the PSU's credentials (linked to a CBDC wallet/account) must be represented by a qualified certificate for electronic signature, issued by a qualified trust services provider. The corresponding private key must reside within a certified qualified electronic signature/seal creation device (QSCD). Figure 1 illustrates how a wallet certificate would reference (indicated by arrows) and thereby bind together the person, their private key and the identity provider.

Currently, however, it is unclear whether/how a smartphone or similar multi-purpose device could be certified as a QSCD. Going forward, this is something for smartphone providers to address, while eIDAS2 and future revisions of the Payment Services Directive (PSD) and Regulatory Technical Standards (RTS) should consider ways to encourage this. In the absence of a smartphone to perform the role of a certified QSCD, for payments it is therefore necessary to target advanced electronic signatures[28] (AdES) instead. A further option might be an advanced electronic signature based on a qualified certificate.

An additional legal issue relates to the mutual identification of the PSPs, for which PSD2 RTS of SCA and Common and Secure Communication (CSC) Article 34(1)[29] state that PSPs shall rely on qualified certificates. In a CBDC context where both payee and payer apps may be offline, it seems reasonable to assume that

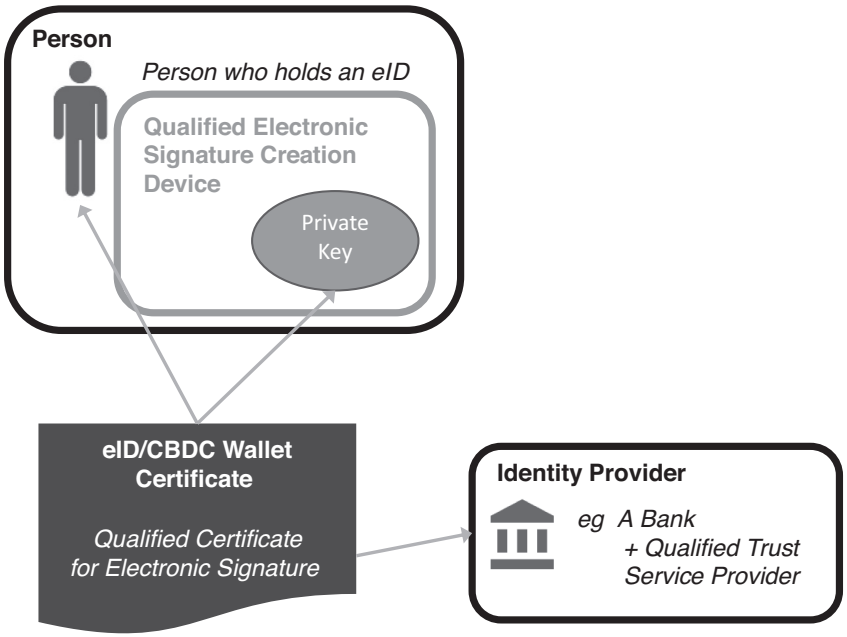

Figure 1: A wallet certificate binds the person to their private key and identity provider

this requirement extends to the mutual identification of the respective CBDC apps. The app-to-app identification would then be based on a qualified certificate. This is not the same certificate as the one mentioned above for SCA, as it is a certificate for the PSP, not for the person (ie the PSU).

European Telecommunications Standards Institute (ETSI) technical specification TS 119 495[30] dictates that qualified certificates under PSD2[31] should be issued under policy QCP-l (for seals) and QCP-w (for website authentication). Neither policy mandates the use of a QSCD (see ETSI EN 319 411-2[32]).

To enable especially secure offline transactions, this paper recommends the provision of guidelines for the creation of qualified certificates for apps on mobile devices (similar to smartcards) with respective private keys residing in the secure element via delegation authority from the CBDC wallet service provider. A procedure could be devised for issuing both the PSU's wallet qualified certificate and the PSP's qualified certificate to the device at the same time. The PSP would play the role of registration authority for the QTSP.

Offline verification

A digital equivalent to physical cash must strive to achieve the same levels of resilience. For this reason, a key requirement of CBDC transactions is to enable funds to be exchanged between parties even in the absence of mains power and/or network communications.

According to the existing PSD2 directive, all electronic payment transactions (CBDC or otherwise) require SCA unless an exemption is available.[33] This applies equally to account-based and token-based CBDC models. Ideally, CBDC transactions should not utilise any SCA exemption. This means that SCA shall be performed for every transaction and be verifiable offline.

Offline verification of electronic signatures can be achieved by the signer

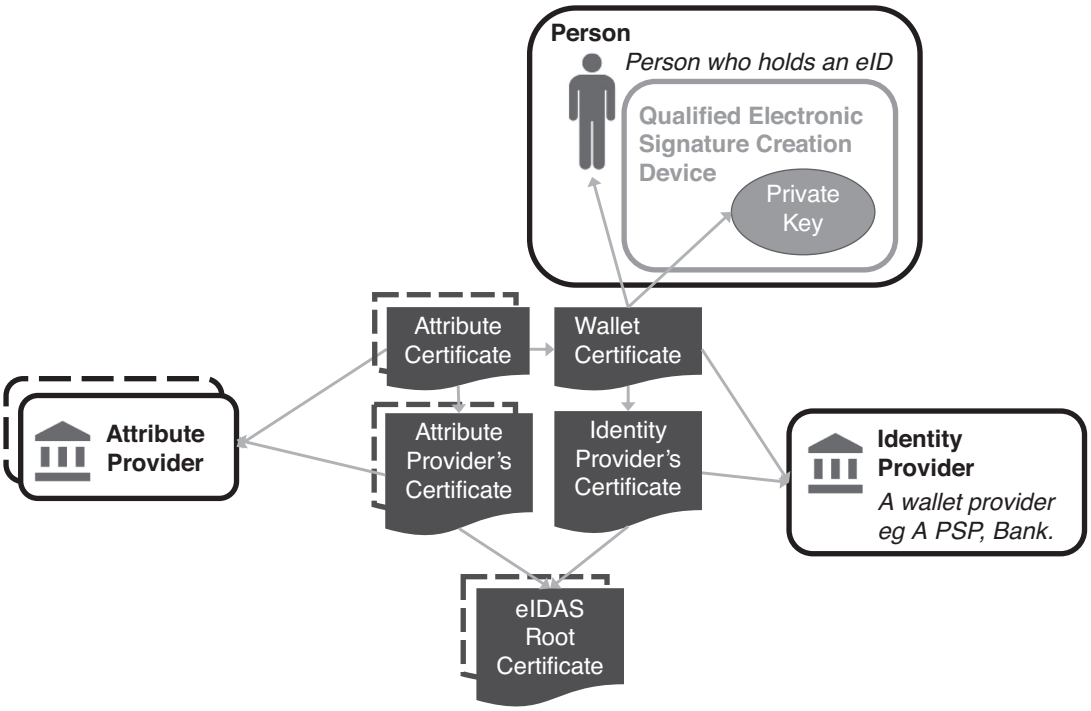

Figure 2: The certificate chain of trust

including the full certificate chains of their wallet (identity) and attribute certificates, up to and including their eIDAS trusted root certificate.

Both payer and payee CBDC apps (wallet/POS) must store offline copies of all related eIDAS trusted lists root certificates, which the app provider can obtain from a trusted source. This paper recommends that eIDAS provide a simple means whereby a CBDC app provider can download the latest copies of all trusted certificates of ECB certified CBDC PSPs. Ideally only one root certificate would be operated for CBDC, similar to the model envisaged for the EU Intelligent Transport System.[34]

To verify their counterparties' signatures, the app must also verify the associated certificate chains. The app must match the root certificate(s) included in the signature to the offline copy. It must not trust any root certificate provided by a counterparty. Figure 2 illustrates the concept.

With respect to checking certificate revocation, it is not possible to conduct a real-time online check of certificate revocation status if both apps are offline. However, if one party's app is online (eg the POS terminal), this app can check the certificate revocation status of the counterparty certificates. This online party's app can include (in the AdES) the real-time certificate revocation information relating to the online party's own certificates, which the counterparty app can then verify offline. In summary, as long as one party is online, both parties can check certificate revocation status for all certificates.

Privacy

To protect the person's privacy, the wallet certificate does not include any personal

information. Instead, it includes the public key and a pseudonym, which the identity provider then links to the person's wallet, their real-world identity, device, operating system and wallet app (via Android and iOS attestation data).

As discussed previously, data-minimisation techniques are recommended to ensure only the minimum necessary information about a person is contained within a transaction, as this is visible to the counterparty (and their PSP).

Another key requirement is that a person's transactions cannot be tracked (eg by a PSP) and their real-life identity derived. Unless changed regularly, the wallet's public key could be used to track the person.

STELLA[35] was the joint research project of the ECB and the Bank of Japan on 'Balancing confidentiality and auditability in a distributed ledger environment'. It considered privacy-enhancing techniques, including a hierarchical deterministic wallet.

It may not be practical to implement the most advanced STELLA recommendations using today's smartphones. Therefore, simpler techniques may need to be considered, for example a wallet's public/private key pair may need to be replaced on a regular basis (eg every seven days) when online. This would also require the wallet certificate (including pseudonym) and potentially all attribute certificates to be replaced to optimise the balance between data privacy and efficient auditability.

Financial crime

The ISO 20022[36] payment initiation formats provide rich structures containing hundreds of elements to convey a variety of information with a payment. This is beneficial from an AML[37] perspective. It is therefore important that any new CBDC transaction structures must not create obstacles that would limit the level of information to be attached to the CBDC structures. The CBDC approach must also allow both the payee and payer to attach the information deemed necessary. The levels of information provided may also depend on the parties involved as well as the purpose and value of the transaction. The approach described below is extensible. It provides for flexibility over the data structures and over which party supplies the information.

Inclusivity

It is an important prerequisite that any proposed CBDC technological approach must enable the CBDC wallet apps to run on contemporary mid-range smartphones. It would not be appropriate to render existing handsets obsolete and require people to purchase new devices. Therefore, any proposed technological solutions for CBDC must not require changes to existing smartphone hardware or operating systems.

The architecture approach recently proposed by Visa[38] includes the deployment of a new trusted application into the smartphone's separated secure execution environment/trusted execution environment (TEE).[39] This may not be practical without changes to smartphone hardware and operating systems and would likely render existing handsets obsolete.

In the approach outlined in what follows, this paper refrains from suggesting that additional functionality be deployed into the TEE. Instead, it focuses on the division of control (between the payee and payer) and the need for a verifiable audit trail, and recommends making full use of existing TEE functionality, available in existing smartphones via current Android and iOS application programming interfaces (APIs). These principles could be combined with the two-tier approach in the future. This would require the deployment of a trusted application into an open TEE,[40,41] with APIs that are accessible to CBDC wallet (Android and iOS) apps.

PROPOSED CBDC TRANSACTION STRUCTURE

The following outlines an option for how a CBCD transaction could be performed. The scope of this paper is not intended to define a 'solution' for CBDC, but to support the CBDC discussion. To avoid double-spending offline, usage is only possible on downloaded and received balances or unspent transaction output (UTXO[42]). These balances are stored in the wallet applications that are secured using industry best practice. The following example uses the ETSI Advanced Electronic Signature standards. This approach builds on a recent change request called 'Signed Payment Request'[43,44] to the Berlin Group NextGenPSD2 standard.

An important aspect of the proposed approach is the use of countersignatures to divide control of the CBDC transaction between both payee and payer devices so that if one device is compromised, this does not undermine the whole transaction. The payee specifies the amount and their public key represents their CBDC account. Therefore, a compromised payer's CBDC app cannot change the amount and the payee. If the payee's device is compromised, and supplies an incorrect amount or payee, the payer's device would likewise display that incorrect amount/payee, thus enabling the payer to reject it before authorising the payment. The payee's name, which is displayed to the payer, is bound to the payee's CBDC wallet via a certificate issued by an attribute provider. This enables the payer's app to verify the payee name without relying on the payee wallet app.

Step 0: The PSP apps authenticate each other

A preliminary step in the procedure involves the PSP wallet apps establishing mutual trust, prior to exchanging payment information. First, an end-to-end encrypted session is established, using Diffie-Hellman techniques.[45] Then each app automatically creates an AdES (signature) and exchanges this with the counterparty app. Assuming each app includes a qualified certificate in its AdES, this would allow each PSP app to authenticate the counterparty PSP app in a manner that aligns with PSD2 RTS Article 34.1.[46] All following steps in the transaction operate within this trusted encrypted session.

Step 1: The payee prepares and signs a request for payment

The next step involves the payee (eg a POS terminal or person in the case of peer-to-peer payments) preparing a request for payment (without debtor/payer information). This is represented in this example by an electronic invoice, where the payee specifies, at the very least, their name, the CBDC wallet to be credited and the amount to be credited.

The payee then signs the e-invoice using their (CBDC wallet) private key that is contained within (and can never leave) the separated secure execution environment of the device. The public key is contained within the payee's wallet credential, which takes the form of qualified certificate for electronic seal (QSEAL, in the case of a POS) or a qualified certificate for electronic signature (QES, in the case of a person).

Included within the electronic signature structure is the payee's (identity) certificate, bound to their CBDC wallet/account. Additional (optional) payee attribute certificate(s) is/are included to supply their name, as a minimum.

A commitment type is assigned to the payee's signature. This is either ProofOfCreation for a QSEAL (machine signature) or ProofOfOrigin (representing creation + approval) for a QES (personal signature). This step is illustrated by Figure 3.

The (AdES) signature file (signatures0) and the e-invoice file are included in an ETSI-associated signature container

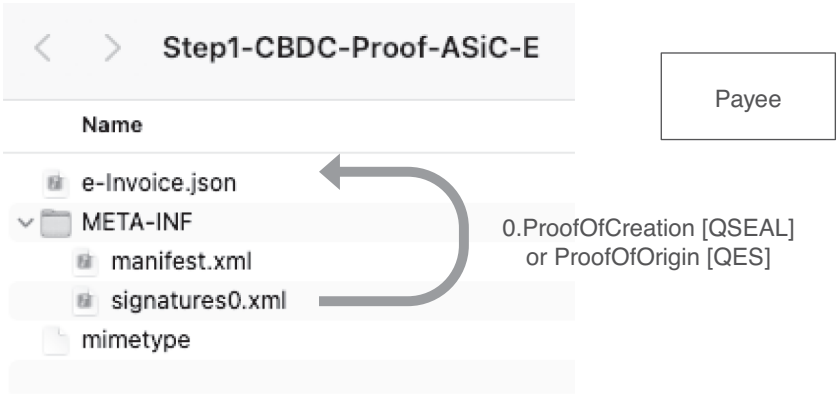

Figure 3: Step 1 — The payee signs an e-invoice

(ASiC-E)[47] structure. An ASiC is simply a ZIP archive created according to rules set forth in the specifications.

The ASiC-E is transmitted to the payer's CBDC wallet app/device via the previously established end-to-end encrypted connection (HTTPS if online or via a proximity protocol, such as Bluetooth, if offline).

Step 2: The payer applies their countersignature

On receipt of the ASiC-E containing the signed e-invoice, the payer's CBDC wallet app verifies the payee's signature, including the full certificate chains of all wallet and attribute certificates. The CBDC wallet app matches the root certificate(s) to local copies stored for offline use by the app. By verifying this signature, the wallet app has authenticated the payee. This is a clear requirement for CBDC. This approach is also in line with the PSD2 RTS on SCA and CSC.

The payer's CBDC wallet app now displays the e-invoice details (including the amount as a minimum) and the payee (eg their name, extracted from the corresponding attribute certificate). Assuming that the payer is using a device that can be used for distance communication (eg a smartphone) to initiate the CBDC transaction, this will be classified as a 'remote payment transaction'[48] under PSD2 and therefore require dynamic linking, including the display of the amount and payee.[49]

When the payer is ready to approve the payment, the CBDC wallet app asks the payer to sign using the private key linked to their qualified certificate. This payer's signature (signatures1) countersigns the payee's signature (signatures0). A commitment type of ProofOfApproval is assigned to the payer's signature.

Multiple central bank CBDC papers include a requirement for a person to be able to receive and reuse funds while offline. One challenge posed by this requirement is to ensure that there is a clear audit trail that provides evidence of the source of the CBDC value that was transferred. It also adheres to other regulatory requirements such as AML, sanctions and embargoes, CFT and respective predicate offences. The funds transferred must be final, even if all previous payers that funded a particular balance subsequently lose or destroy their smartphones. In this event, the final recipient of the funds may be the only one that can connect to their PSP and transmit the transactions accumulated offline to the central bank. Including this history

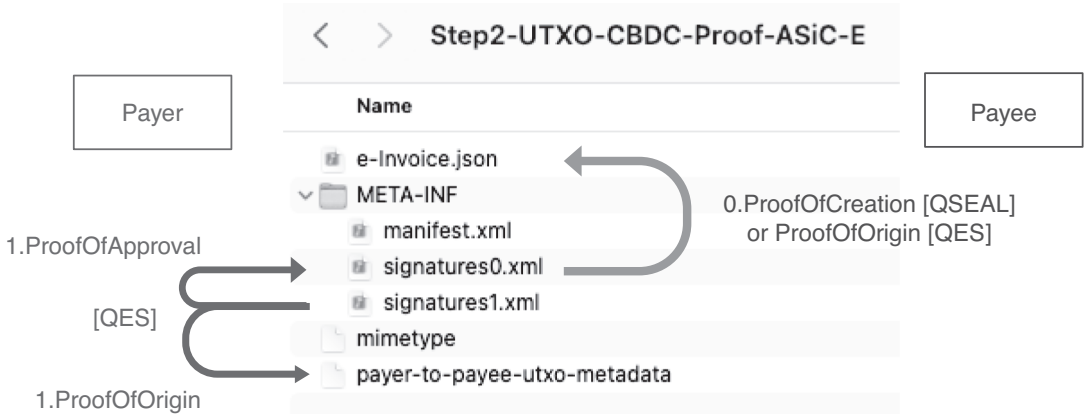

Figure 4: Step 2 — The payer countersigns to approve (UTXO flavour)

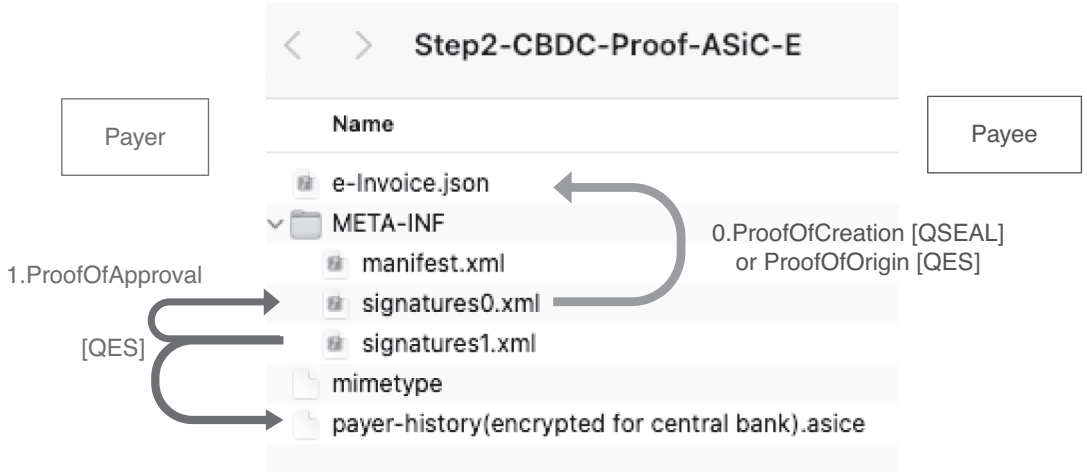

Figure 5: Step 2 — The payer countersigns to approve (account-based flavour)

with subsequent transactions provides necessary redundancy. This approach will not on its own address every issue, such as double-spending, however this evidence will support the central bank in its reconciliation of transactions and its detection of double-spending.

In the UTXO based CBDC model, illustrated by Figure 4, metadata are attached to the payment that provides evidence of how a digital currency (bearer) token was funded.

In the account-based CBDC model, illustrated by Figure 5, one option would be for the payer's CBDC wallet app to attach to the signed proof, the evidence of all historic payments and receipts (that justify the payer's balance). As such data would potentially pass through multiple different PSPs before reaching the central bank, the privacy of all parties must be protected. This can be achieved by each CBDC wallet app encrypting the history using the public key of the central bank.

To reduce network overhead only the new elements of the ASiC-E, as illustrated by Figure 6, are then transmitted to the payee's app.

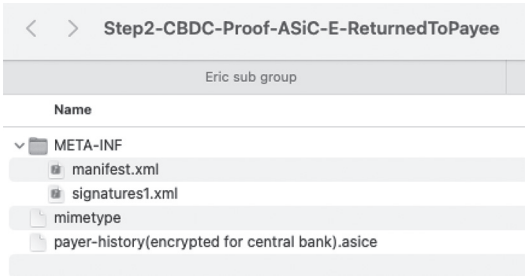

Figure 6: Step 2 — Data returned to payee (account-based flavour)

Step 3: The payee countersigns to provide an e-receipt (and change)

On successful receipt of the payer's countersignature, the payee's CBDC app generates an automatic electronic signature (signatures2) that countersigns the payer's signature (signatures1). A commitment type of ProofOfReceipt is assigned to this payee signature.

This is an automated signature. Where the payee is a person, they must not be asked to touch the fingerprint sensor. As the private key linked to their (QES) qualified certificate would require a biometric prompt, a second (authentication) public/private key pair (bound to their QES credentials) is used instead.

In the UTXO based CBDC model, the payee may be required to provide change to the payer. It is assumed that this transaction would also be automated (ie without a biometric prompt) and therefore also signed by the authentication private key. This element would not constitute SCA. The SCA for this transaction is performed when the payee signs the e-invoice. Figure 7 illustrates the UTXO based model.

Figure 8 illustrates the account-based CBDC model.

To reduce network overhead, only the signatures2 file is transmitted to the payee's app. In the UTXO model, the payee-to-payer UTXO metadata file is also transmitted.

Step 4: Payer countersigns to provide e-receipt (UTXO only)

In the UTXO model, in the circumstances where the payer receives change (digital currency) from the payee, the payer CBDC app generates an automatic electronic signature (signatures3) that countersigns the payer's signature (signature2). This ProofOfReceipt signature is transmitted to the payee. Figure 9 illustrates the CBDC signed proof structure, including the UTXO e-receipt.

Step 5: Both parties transmit to PSP

When each party's CBDC app is next online, they transmit their copy of the full CBDC package (ASiC-E structure) to their PSP, who forwards it to the central bank.

If either party makes a subsequent payment without going online, the details of this transaction (including the encrypted payer history) are included in the payer history of the new transaction, per the account-based model described above. To limit the data size and mitigate the danger of offline CBDC abuse, it may be necessary to cap the number of transactions performed offline (offline-hop maximum).

OPTIONS FOR IMPLEMENTING A SIMPLE EID USE CASE: AUTHENTICATION

Before considering how to implement a complex use case such as CBDC, consider a simpler eID use case, such as authentication. Examples of authentication use cases include:

- a person logging into a third-party website using their eID (app/device);
- a person using their eID to fulfil the know-your-customer requirements when enrolling remotely for a financial services product;
- a person using their eID to prove they are over the legal age to buy alcohol;
- a person using their eID to open their hotel room door or access a secure office location.

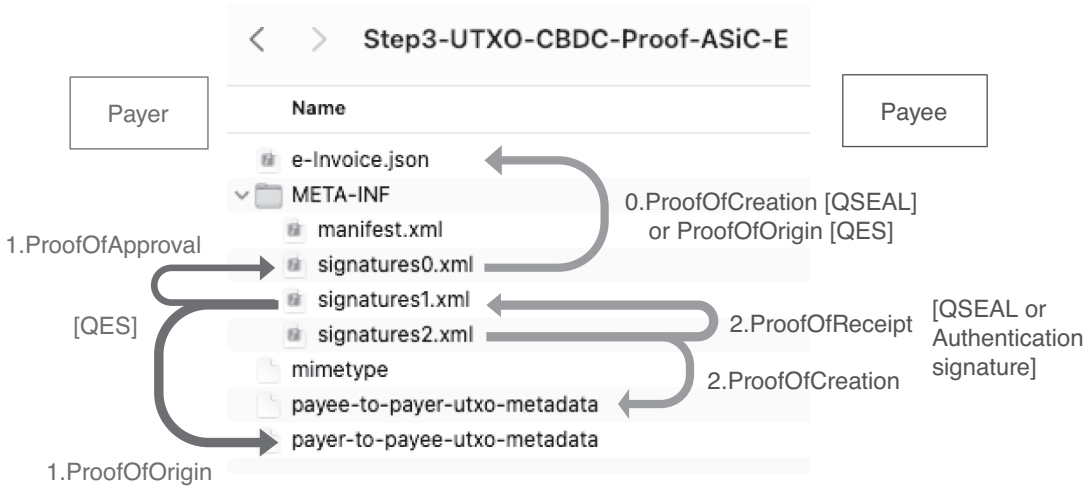

Figure 7: Step 3 — Payee countersigns to provide an e-receipt plus change (UTXO flavour)

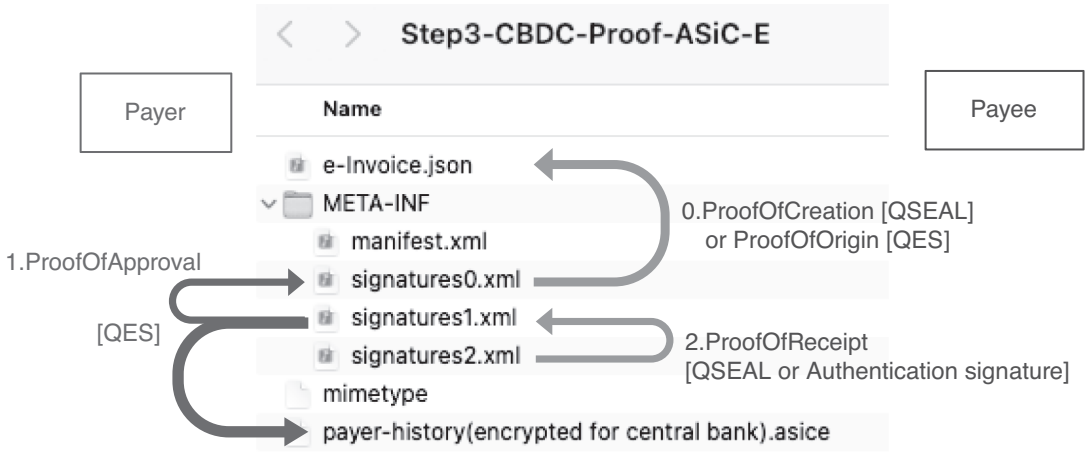

Figure 8: Step 3 — Payee countersigns to provide an e-receipt (account-based flavour)

It is assumed that even these simple use cases would involve the person performing the SCA procedure to create the eID proof.

Creating the eID proof using ETSI advanced electronic signatures

The ETSI AdES structure is the normal standard for creating qualified electronic signatures and is the standard required by public sector bodies. It is a rich and versatile structure that enables multiple data objects to be signed at the same time. It also supports countersignatures. A key advantage of adopting the ETSI standards is the availability of off-the-shelf signature verification software and verification services provided by trust providers. Figure 10 describes this option.

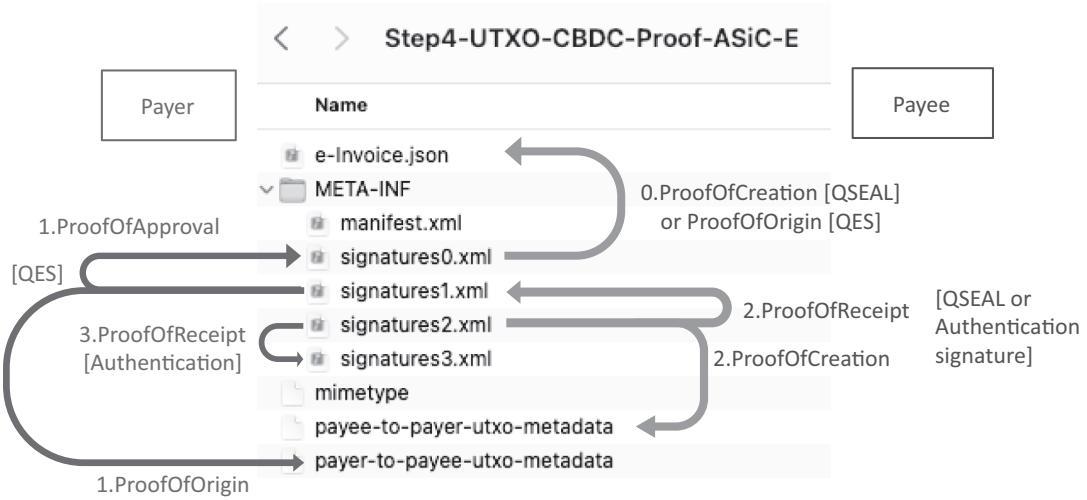

Figure 9: Step 4 — Payer countersigns to provide an e-receipt for the change (UTXO flavour)

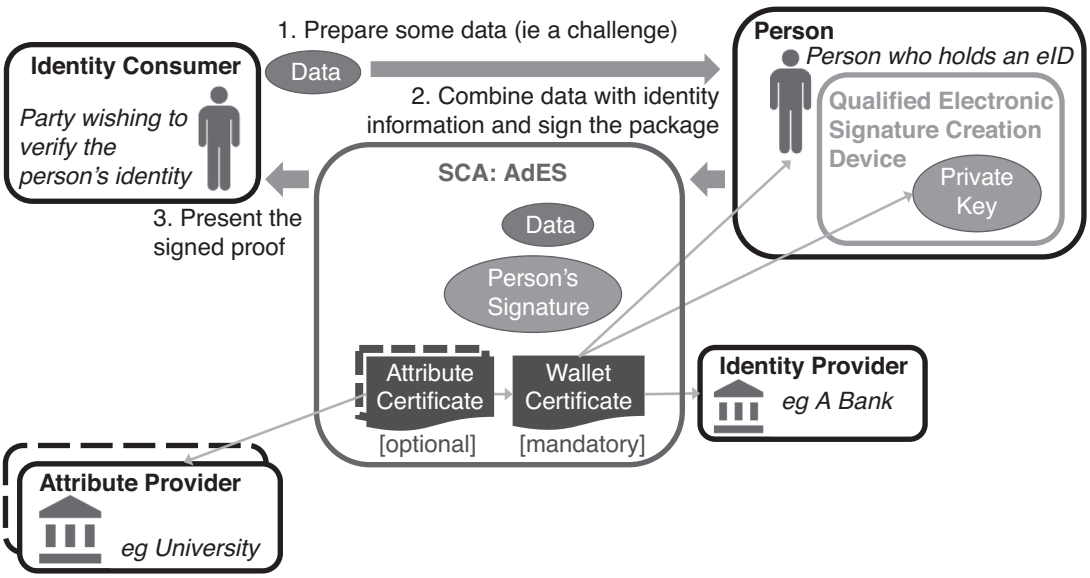

Figure 10: eID proof created in an AdES format

Creating the eID proof with W3C decentralised identifier documents and verifiable credentials

The principal aim of SSI is to put the person (receiver) in control of their identity. In SSI, there is normally no concept of an identity provider. Instead, the person is in charge of their own identity (ie self-sovereign). Their eID wallet credentials take the form of a decentralised identifier document (DID), which is referenced by a decentralised identifier (eg a URI). The person can create multiple versions of their DID, all with the same public key.

The focus is instead on attribute service providers (issuers) who assign attributes to a person in the form of verifiable credentials.

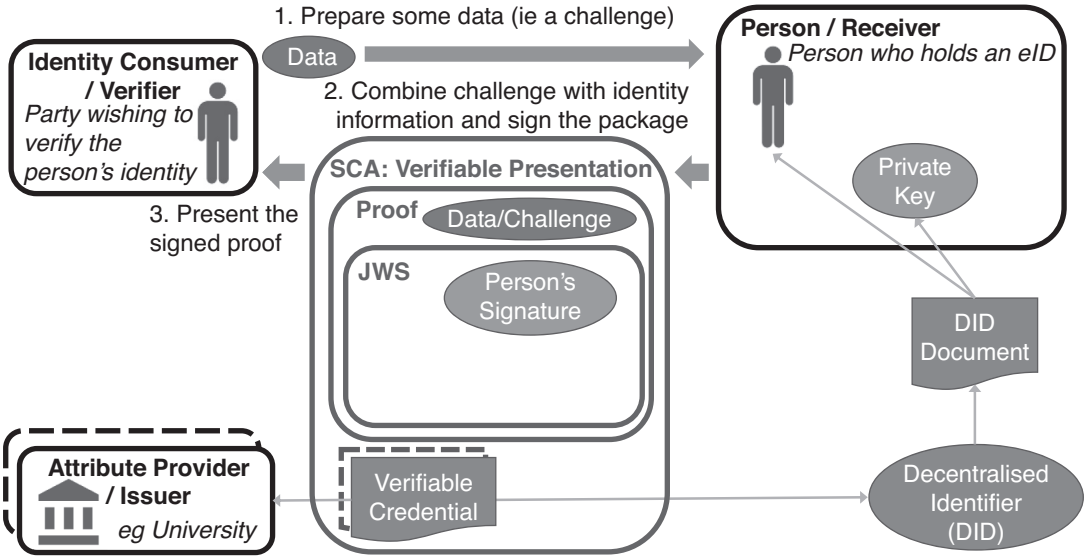

Figure 11: eID proof created in a W3C (SSI) format

The identity consumer (verifier) relies on these credentials to identify and authenticate the person. Figure 11 describes this option.

A proposal to create qualified signatures using SSI structures

As described previously, in order for an electronic signature to be deemed qualified, the person must be issued a qualified certificate for electronic signatures and the related private key must reside in a qualified electronic signature creation device.

The person's eID wallet certificate (ie their qualified certificate) can be included in Java Web Signature (JWS) structure as outlined in Figure 12. In order to support offline verification, the full certificate chain of this certificate would also be included in the JWS.

To support offline verification of the attributes, an attribute certificate that is linked (eg via the verifiable credential ID) to each verifiable credential would also be included in the JWS, together with their full certificate chains.

This approach, described in Figure 12, also enables the verifier to check the revocation status of the verifiable credentials, via its associated attribute certificate.

IMPLEMENTING THE CBDC USE CASE

When comparing the AdES and W3C approaches, both are equally suited to a simple use case, such as authentication, where the challenge can be a simple one-time value (a nonce). However, the W3C approach is less suitable when sophisticated data structures (required by CBDC) must be included instead of a simple challenge data element.

Therefore, to implement the proposed CBDC approach, which involves counter-signatures and multiple data objects, the ETSI AdES structures are currently more suitable for the CBDC transaction process and the W3C SSI approach for the setup and maintenance of the CBDC wallets.

The identity consumer is the party best placed to determine the signature format (AdES or W3C) that they require. As long as

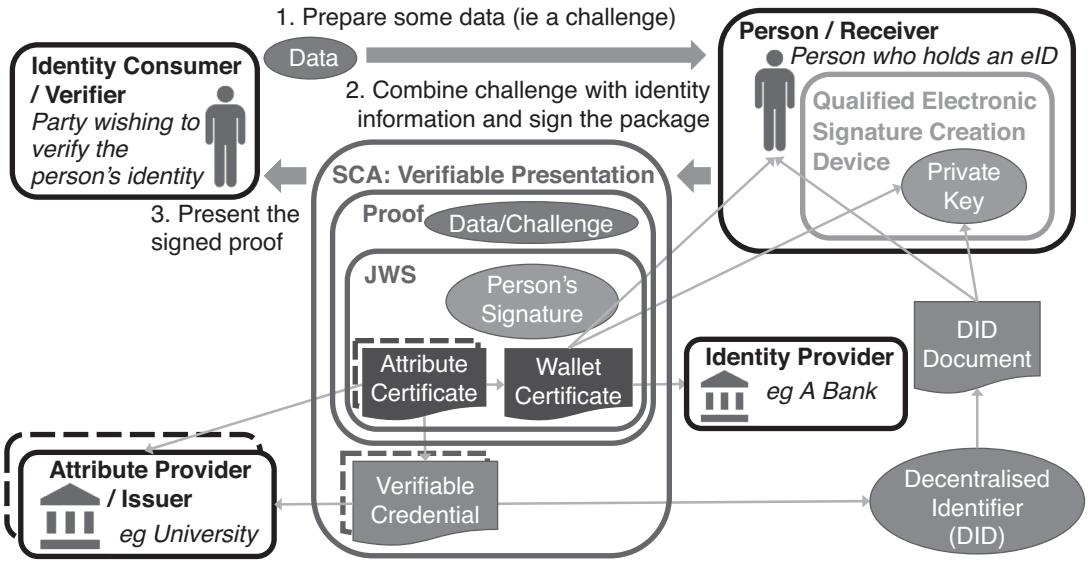

Figure 12: eID qualified signature proof in a W3C (SSI) format

the identity/attribute service providers issue both X.509 and W3C based credentials for the same wallet/private key, the wallet app would be capable of supporting both AdES and W3C approaches.

In the future, the W3C structures could be extended to better handle the signing of transactions, such as CBDC via, for example, extending the DIDComm protocol. This would involve replacing the challenge element with a more sophisticated structure that supports countersignatures and multiple data objects. Once this support is implemented, W3C would become a more viable option for CBDC transactions.

DISCLAIMER

The views expressed in this paper are those of the authors and do not necessarily represent the views of the institutions they work for.

References

(1) Auer, R., Cornelli, G. and Frost, J. (2020) 'Rise of the central bank digital currencies: drivers, approaches and technologies', BIS Working Paper No 880, available at: https://www.bis.org/publ/work880.htm (accessed 1st May, 2021).

(2) Wong, P. and Maniff, J.L. (2020) 'Comparing means of payment: what role for a central bank digital currency?', available at: https://www.federalreserve.gov/econres/notes/feds-notes/comparing-means-of-payment-what-role-for-a-central-bank-digital-currency-20200813.htm (accessed 1st May, 2021).

(3) ABILab (2020) 'eIB-White Paper, Interim Report 2020', available at: https://www.abilab.it/progetti-europei/eIB (accessed 1st May, 2021).

(4) Wagner, E., Bruggink, D. and Benevelli, A. (2021) 'Preparing euro payments for the future: A blueprint for a digital euro', *Journal of Payment Systems & Strategies*, Vol. 15 No. 2.

(5) European Central Bank (2021) 'ECB publishes the results of the public consultation on a digital euro', press release, available at: https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210414~ca3013c852.en.html (accessed 1st May, 2021).

(6) European Central Bank and Bank of Japan (2020) 'Project Stella: the ECB and the Bank of Japan release joint report on distributed ledger technology', available at: https://www.boj.or.jp/en/announcements/release_2020/rel200212a.htm/ (accessed 1st May, 2021).

(7) Christodorescu, M., Gu, W.C., Kumaresan, R., Minaei, M., Ozdayi, M., Price, B., Raghuraman, S., Saad, M., Sheffield, C., Xu, M. and Zamani, M. (2020) 'Towards a two-tier hierarchical infrastructure: an offline payment system for central bank digital currencies', available at: https://arxiv.org/abs/2012.08003 (accessed 1st May, 2021).

(8) International Organization for Standardization (n.d.) 'ISO 24366: Identification of Natural Persons',

briefing note, available at: https://committee.iso.org/files/live/sites/tc68/files/Robin%20Doyle/ISO-TC68-SC8-WG7_NPI_Briefing_Note_Final.pdf (accessed 1st May, 2021).
(9) Quali-Sign Ltd (2020) 'Perform eID at a turnstile to access a sports stadium', available at: https://www.quali-sign.com/resources_demonstration_evaluation.html (accessed 1st May, 2021).
(10) eIDAS (2014) 'Art. 3(1), EU Regulation 910/2014 of 23 July 2014 on electronic identification', available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG (accessed 1st May, 2021).
(11) eIDAS (2014) 'Art. 3(10), EU Regulation 910/2014 of 23 July 2014 on electronic identification', available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG (accessed 1st May, 2021).
(12) Grassi, P., Garcia, M. and Fenton, J. (2020) 'NIST SP 800-63-3,'Digital Identity Guidelines', available at: https://csrc.nist.gov/publications/detail/sp/800-63/3/final (accessed 1st May, 2021).
(13) Wikipedia (n.d.) 'Public key cryptography', available at: https://en.wikipedia.org/wiki/Public-key_cryptography (accessed 1st May, 2021).
(14) Regulatory Technical Standards on Strong Customer Authentication & Common and Secure Communication (2018) 'Art. 9(3)(a), Commission Delegated Regulation (EU) 2018/389 of 27 November 2017', available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R0389 (accessed 1st May, 2021).
(15) Wikipedia (n.d.) 'X509', available at: https://en.wikipedia.org/wiki/X.509 (accessed 1st May, 2021).
(16) Android developers (n.d.) 'SafetyNet device attestation', available at: https://developer.android.com/training/safetynet/attestation (accessed 1st May, 2021).
(17) Android developers (n.d.) 'Key attestation', available at: https://developer.android.com/training/articles/security-key-attestation (accessed 1st May, 2021).
(18) Apple iOS Developer (n.d.) 'Establishing your app's integrity', available at: https://developer.apple.com/documentation/devicecheck/establishing_your_app_s_integrity (accessed 1st May, 2021).
(19) eIDAS (2014) 'Art. 3(20), EU Regulation 910/2014 of 23 July 2014 on electronic identification', available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG (accessed 1st May, 2021).
(20) eIDAS (2014) 'Art. 24, EU Regulation 910/2014 of 23 July 2014 on electronic identification', available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG (accessed 1st May, 2021).
(21) Regulatory Technical Standards on Strong Customer Authentication & Common and Secure Communication (2018) 'Art. 24, Commission Delegated Regulation (EU) 2018/389 of 27 November 2017', available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R0389 (accessed 1st May, 2021).
(22) Commission Implementing Regulation (2015) '(EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means (see Annex)', available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2015_235_R_0002 (accessed 1st May, 2021).
(23) eIDAS (2014) 'Guidance on Levels of Assurance', available at: https://ec.europa.eu/cefdigital/wiki/download/attachments/40044784/Guidance%2Bon%2BLevels%2Bof%2BAssurance.docx (accessed 1st May, 2021).
(24) European Commission, eIDAS/remoteKYC Financial Services Expert Group (2020) 'Accessing portable KYC/CDD solutions in the banking sector', available at: https://ec.europa.eu/info/files/assessing-portable-kyc-cdd-solutions-in-the-banking-sector-December2019_en (accessed 1st May, 2021).
(25) CEF Digital (n.d.) 'European Self-Sovereign Identity Framework (ESSIF)', available at https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=262505734 (accessed 1st May, 2021).
(26) World Wide Web Consortium (n.d.) 'Decentralized Identity', available at: https://decentralized-id.com/web-standards/w3c/ (accessed 1st May, 2021).
(27) European Commission (2020) 'Shaping Europe's digital future, Reports of the expert group on eID and KYC processes', available at: https://ec.europa.eu/digital-single-market/en/news/reports-expert-group-eid-and-kyc-processes (accessed 1st May, 2021).
(28) CEF Digital (n.d.) 'What is eSignature?', available at: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/What+is+eSignature (accessed 16th July, 2021).
(29) Regulatory Technical Standards on Strong Customer Authentication & Common and Secure Communication (2018) 'Art. 34(1), Commission Delegated Regulation (EU) 2018/389 of 27 November 2017', available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R0389 (accessed 1st May, 2021).
(30) European Telecommunications Standards Institute (2019) 'ETSI TS 119 495 V1.4.1, Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366', available at: https://www.etsi.org/deliver/etsi_ts/119400_119499/119495/01.04.01_60/ts_119495v010401p.pdf (accessed 1st May, 2021).
(31) Revised Payments Services Directive (2015) 'Directive (EU) 2015/2366', available at: https://www.eba.europa.eu/regulation-and-policy/single-rulebook/interactive-single-rulebook/5402 (accessed 1st May, 2021).

(32) European Telecommunications Standards Institute (2018) 'ETSI EN 319 411-2 V2.2.2, Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates', available at: https://www.etsi.org/deliver/etsi_en/319400_319499/31941102/02.02.02_60/en_31941102v020202p.pdf (accessed 1st May, 2021).
(33) Revised Payments Services Directive (2015) 'Art. 97(1)(b), Directive (EU) 2015/2366', available at: https://www.eba.europa.eu/regulation-and-policy/single-rulebook/interactive-single-rulebook/8603 (accessed 1st May, 2021).
(34) European Telecommunications Standards Institute (2018) 'ETSI TS 102 941 V1.2.1, Intelligent Transport Systems (ITS); Security; Trust and Privacy Management', available at: https://www.etsi.org/deliver/etsi_ts/102900_102999/102941/01.02.01_60/ts_102941v010201p.pdf (accessed 1st May, 2021).
(35) European Central Bank and Bank of Japan, ref. 6 above.
(36) International Organization for Standardization (n.d.) 'ISO 20022', available at: https://www.iso20022.org/ (accessed 1st May, 2021).
(37) European Commission (n.d.) 'Anti-money laundering and counter terrorist financing', available at: https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/anti-money-laundering-and-counter-terrorist-financing_en (accessed 1st May, 2021).
(38) Christodorescu *et al.*, ref. 7 above.
(39) Wikipedia (n.d.) 'Trusted execution environment', available at: https://en.wikipedia.org/wiki/Trusted_execution_environment (accessed 1st May, 2021).
(40) Open-TEE (n.d.) 'Open-TEE (Github)', available at: https://open-tee.github.io/ (accessed 1st May, 2021).
(41) OP-TEE (n.d.) 'OP-TEE', available at: https://www.op-tee.org/ (accessed 1st May, 2021).
(42) Wikipedia (n.d.) 'Unspent transaction output (UTXO)', available at: https://en.wikipedia.org/wiki/Unspent_transaction_output (accessed 1st May, 2021).
(43) The Berlin Group (2020) 'NextGenPSD2 Change Request 'Signed Payment Request', available at: https://www.quali-sign.com/documents/bg/20201118- NextGenPSD2_Change Request Form - SPR.pdf (accessed 1st May, 2021).
(44) The Berlin Group (2020) 'Annex 'Open Banking PSU Signed Payment Request', available at: https://www.quali-sign.com/documents/bg/CR_SignedPaymentRequest_20201113.pdf (accessed 1st May, 2021).
(45) Wikipedia (n.d.) 'Elliptic-curve Diffie–Hellman', available at: https://en.wikipedia.org/wiki/Elliptic-curve_Diffie%E2%80%93Hellman (accessed 1st May, 2021).
(46) Regulatory Technical Standards on Strong Customer Authentication & Common and Secure Communication (2018) 'Art. 34(1), Commission Delegated Regulation (EU) 2018/389 of 27 November 2017', available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R0389 (accessed 1st May, 2021).
(47) CEF Digital (n.d.) 'ASiC (Associated Signature Container) Baseline Profile', available at: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eSignature+standards#eSignaturestandards-ASiC(AssociatedSignatureContainer)BaselineProfile (accessed 1st May, 2021).
(48) Revised Payments Services Directive (2015) 'Art. 4(6)(b), Directive (EU) 2015/2366)', available at: https://www.eba.europa.eu/regulation-and-policy/single-rulebook/interactive-single-rulebook/8701 (accessed 1st May, 2021).
(49) Regulatory Technical Standards on Strong Customer Authentication & Common and Secure Communication (2018) 'Art. 5, Commission Delegated Regulation (EU) 2018/389 of 27 November 2017', available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R0389 (accessed 1st May, 2021).