Your views on a digital euro

About the respondent (15781)

I give explicit consent for my personal data to be disclosed together with my reply. (213434)

Type: (M/multiple-opt)

[X]

Yes **(213435)**

I am responding as: (213418)

Type: (!/list-dropdown)

A3 - Company/business organisation

Type of business association: (213419)

Type: (!/list-dropdown)

-

Type of company/business organisation: (213420)

Type: (!/list-dropdown)

A6 - Technology company

Organisation size: (213422)

Type: (!/list-dropdown)

A1 - Micro (1 to 9 employees)

Please specify your activity field(s) or sector(s): (213427)

Type: (!/list-dropdown)

A1 - Payment services

Age group (213430)

Type: (!/list-dropdown)

A5 - 45-54

Gender (213431)

Type: (!/list-dropdown)

A2 - Male

Country of residence (213432)

Type: (!/list-dropdown)

A28 - Other

User perspective (15779)

How would you rank, in order of importance, the features that a digital euro should offer? (213414)

Type: (R/ranking)

Rank #1:

A3 - I want to be able to use it with my smartphone and at payment terminals.

Rank #2:

A4 - I want to be able to pay even when there is no internet or power connection.

Rank #3:

A8 - I want it to be a secure means of payment.

Rank #4:

A9 - I want my transactions to be completed instantaneously.

Rank #5:

A5 - I want it to be easy to use.

Rank #6:

A6 - I want to use a digital euro without having to pay additional costs.

Rank #7:

A1 - I want to be able to use it throughout the euro area.

Rank #8:

-

Rank #9:

-

Do you have any further comments about the ranking that you have indicated above? (213508)

Type: (T/text-long)

In our opinion the payee cannot be anonymous to the payer however the payer can and should be anonymous to the payee. Article 5 of the PSD2 RTS on SCA and CSC requires the the amount and payee to be displayed to the payer at the time they authorise the payment.

Do you envisage any challenges associated with a digital euro that would prevent you or others from using it? If so, what are they? (213415)

Type: (T/text-long)

The biggest challenge lies in a perceived lack of trust in the system. An example would be if there was any risk that the PSU may lose offline value stored in their CBDC wallet if they were to break or lose their smartphone. In our opinion it is acceptable for there to be a short delay (e.g. 2 weeks) for funds to be returned, but there should be no question that the fund will always be returned.

What user features should be considered to ensure a digital euro is accessible for people of all ages, including those who do not have a bank account or have disabilities? (213416)

Type: (T/text-long)

It is important that the digital euro is inclusive. It should not require citizens to purchase a new top of the range smartphone in order to operate a CBDC wallet on their phone. It is important that a CBDC wallet can be installed on an existing (c. 2020) model mid-range (€150) smartphone. It is also important that there should be no requirement for CBDC apps to rely on a data connection. Many citizens do not pay for mobile data and therefore leave this facility permanently turned off on their smartphone.

There are two approaches we can take to make a digital euro work, one that requires intermediaries to process the payment and one that doesn't. If we design a digital euro that has no need for the central bank or an intermediary to be involved in the processing of every single payment, this means that using a digital euro would feel closer to cash payments, but in digital form – you would be able to use the digital euro even when not connected to the internet, and your privacy and personal data would be better protected. The other approach is to design a digital euro with intermediaries recording the transaction. This would work online and allow broader potential for additional services to be provided to citizens and businesses, creating innovation opportunities and possible synergies with existing services. For example, it could make it easier to integrate a digital euro into currently available electronic banking services and applications. From your perspective, which of the following do you find most appealing? (select one): (213417)

Type: (!/list-dropdown)

A3 - a combination of both.

Do you have any further comments regarding your answer to the question above? (213509)

Type: (T/text-long)

In our opinion it is most important that PSUs would be able to make and receive digital euro payments without any connection to the internet. However we do believe that intermediaries (Payment Service Providers) are best placed to provide PSUs with wallet apps and manage their identities. We believe it would also be beneficial for PSPs to route the CBDC transaction data (including SCA proof) to the central bank, rather than for the mobile apps to establish a direct connection to the central bank. We believe it is acceptable for the wallet holder's PSP to have visibility of the CBDC transaction data. The PSP should be responsible for ensuring that the PSU's CBDC balance (online and offline) is consistent with the central bank. If a balance becomes out of sync, the PSP should temporarily suspend or even revoke the PSU's credentials (e.g. represented by a Qualified Certificate for Electronic Signature).

Financial, payment and technology professionals' perspective (15776)

What role do you see for banks, payment institutions and other commercial entities in providing a digital euro to end users? (213354)

Type: (T/text-long)

We believe that banks, payment institutions and other commercial entities should perform the role of Intermediaries. Their role should be to provide the PSU with a front end application (e.g. smartphone CBDC wallet app). They should also perform the role of Identity Provider.

A digital euro may allow banks and other entities to offer additional services, on top of simple payments, which could benefit citizens and businesses. What services, functionalities or use cases do you think are feasible and should be considered when developing a digital euro? (213369)

Type: (T/text-long)

We believe these Intermediaries that provide citizens and business with CBDC wallet apps are ideally placed to perform the role of Identity Providers for EUeID. The citizen or business user could use their Identity and associated Attributes in a general purpose manner to assert their identity and attributes i.e. for authentication. They could also use it for authorisation (i.e. SCA) for example to sign 3rd party contracts. These additional services would allow the CBDC wallet Identity Providers to generate additional sources of revenue that would enable them to provide a CBDC wallet app to citizens and businesses in a low cost manner. Preferably there would be no cost to the PSU to operate their wallet. For example a hotel acting as Identity Consumer could allow their customer to open their hotel room door with their EUeID app. The payment (from Identity Provider to Identity Consumer) could even be incorporated (via a digital euro transaction) into the (offline) authentication procedure. The hotel would cover the (potentially very small) transaction fee through their associated cost savings.

What requirements (licensing or other) should intermediaries fulfil in order to provide digital euro services to households and businesses? Please base your answer on the current regulatory regime in the European Union. (213370)

Type: (T/text-long)

Intermediaries must be financial services regulated Payment Service Providers. These PSPs must carry the liability in the event of fraud for all unauthorised payments.

Which solutions are best suited to avoiding counterfeiting and technical mistakes, including by possible intermediaries, to ensure that the amount of digital euro held by users in their digital wallets matches the amount that has been issued by the central bank? (213373)

Type: (T/text-long)

We believe it is important that any technical solution does not make current smartphones obsolete with respect to being able to operate CBDC wallet app. Some approaches (e.g. Visa) advocate that CBDC functionality be deployed directly into the Trusted Execution Environment (TEE) of a smartphone. This would be accessed via APIs by the CBDC wallet apps. We are concerned that this approach would require changes to both Android and iOS operating systems and may also require the involvement of the smartphone manufacturers. We believe that there are alternative approaches that could mitigate this need. We believe all CBDC transactions should each be represented by a signature followed by (at least) two countersignatures. Firstly, the payee must prepare an eInvoice which specifies the amount. The payee then signs this with their QSEAL or QES credentials, with a commitment type of ProofOfCreation (if QSEAL) or ProofOfOrigin(if QES - representing creation+approval). The signed eInvoice is received (e.g. via a proximity connection) by the payer. The payer must countersign with ProofOfApproval (they potentially should be prevented from changing anything else, including the amount) and return the countersignature to the payer. Finally, the payer's wallet applies an automated ProofOfReceipt electronic seal which is returned to the payer. Both the payee and payer's private key reside within a Qualified Signature/SEAL Creation Device (within the TEE) on the smartphone. A hacker would not be able to change the payee or the payer on either device. If the hacker did change the amount on the payee's device, the payer is expected to review it on their device before providing their approval. With respect to ensuring the integrity of both apps there is Android/iOS attestation data however this may not be available offline. It is best to assume that either app can be compromised. However, this is mitigated by the division of control between both devices and the need to compromise both. With respect to the issue of double spending and whether the balances match, additional measures could be implemented. For example, (for both ‘account based’ and UTXO models) meta-data could be included (encrypted so that only the central back could read it) within every CBDC transaction package to show how the Payer funded their offline balance (last online balance plus all subsequent offline transaction history). Every CBDC transaction package should be transmitted to the central bank by both the payer and payee’s PSP. Therefore, if the payee (e.g a POS terminal) is online and the payer is offline, the payee could receive real time confirmation from the central bank that there is evidence of double spending and reject the transaction.

What technical solutions (back-end infrastructure and/or at device level) could best facilitate cash-like features (e.g. privacy, offline use and usability for vulnerable groups)? (213377)

Type: (T/text-long)

1. With respect to privacy, we believe it is important that the payer must have the option to remain anonymous to the payee however the payee cannot remain anonymous to the payer. We believe it would be ideal if all CBDC transactions were signed with a QSEAL or QES. It is our understanding that Qcerts for ES require the person's name to be included in the common name. So as not to undermine the payer's privacy we believe that instead of the person's name being included in their Identity Qcert, their name and other attributes should instead be included in Attribute Certificates which are bound to the Identity Qcert. In the case of P2P CBDC transactions, where a person performs the role of payee, they must include their respective Attribute Certificate that includes their name in the QES AdES structure in addition to their Identity Qcert. Where a person performs the role of payer, there is no requirement to include any Attribute Certificates, unless, for example, they are required to provide proof that they are above the legal age to buy alcohol. This approach enables data minimisation and protects the privacy of the payer.
2. With respect to offline use, we believe it is essential that even whilst offline it must be possible to verify the SCA proof. It is possible for each CBDC app to verify their counterparties signature even while offline as long as each party includes the certificate chain of all their certificates in their QSEAL/QES AdES structure. Each CBDC app would be responsible for maintaining local copies of all country root certificates. In addition, where one party is online (e.g. the POS terminal), this party can include real time Certificate Revocation information in their AdES. This allows the other party to verify certificate revocation even when their own device is offline. By verifying the counterparty signature, this will authenticate both the person and also their PSP.
3. With respect to usability for vulnerable groups, as discussed previously we believe it is important that any CBDC technical solution must not make existing smartphones obsolete. It is important that PSUs be able to install CBDC wallet apps on existing (circa 2020) mid-range smartphones and not require brand new features that may only be initially available on top of the range devices.

Financial, payment and technology professionals' perspective (15794)

What should be done to ensure an appropriate degree of privacy and protection of personal data in the use of a digital euro, taking into account anti-money laundering requirements, and combating the financing of terrorism and tax evasion? (213382)

Type: (T/text-long)

As mentioned previously, the payee must be identified to the payer in order for them to authorise the payment. However, the payer must be able to remain anonymous to the payee. This will potentially require changes to eIDAS Qcert for ES as we understand there is currently a requirement to include the common name in the Qcert.

We believe under no circumstances should the CBDC transaction meta-data contain any information that would allow PSPs or others to track previous transactions of the counterparty. Our understanding is that this may be necessary in the UTXO model. We believe it is valid for this meta-data to be visible to the central bank, however it should be end-to-end encrypted by the respective CBDC app so that only the central bank can decrypt it.

We believe that no party to a transaction should be anonymous to the central bank. We also believe it would be inappropriate if any approach were to be adopted that would result in a reduction in transaction information being included within a payment. For example, the ISO PAIN.001 structure is very rich and has ample space to include detailed information about the nature and purpose of the payment. Any new CBDC technical structures should support the inclusion of this additional data which is beneficial to combat anti-money laundering and the financing of terrorism and tax evasion.

The central bank could use several instruments to manage the quantity of digital euro in circulation (such as quantity limits or tiered remuneration), ensuring that the transmission of monetary policy would not be affected by shifts of large amounts of commercial bank money to holdings of digital euro. What is your assessment of these and other alternatives from an economic perspective? (Tiered remuneration is when a central bank sets a certain remuneration on holding balances of digital euro up to a predefined amount and a lower remuneration for digital euro holding balances above that amount.) (213389)

Type: (T/text-long)

Neutral

What is the best way to ensure that tiered remuneration does not negatively affect the usability of a digital euro, including the possibility of using it offline? (213390)

Type: (T/text-long)

Neutral

If a digital euro were subject to holding balance limits, what would be the best way to allow incoming payments above that limit to be shifted automatically into the user's private money account (for example, a commercial bank account) without affecting the ease of making and receiving payments? (213391)

Type: (T/text-long)

Neutral

What would be the best way to integrate a digital euro into existing banking and payment solutions/products (e.g. online and mobile banking, merchant systems)? What potential challenges need to be considered in the design of the technology and standards for the digital euro? (213392)

Type: (T/text-long)

We believe that involving existing market led vehicles such as the Berlin Group NextGenPSD2 Access-To-Account APIs and also the EPC ad-hoc stakeholder group on MSCT would provide the best approach to integrating a digital euro into the existing payment landscape. Furthermore, we support the approach that any technical enhancements made to support CBDC be where possible made available to other payment instruments, such as SCT-Inst.

Financial, payment and technology professionals' perspective (15793)

What features should the digital euro have to facilitate cross-currency payments? (213393)

Type: (T/text-long)

In our opinion, where possible it would be ideal for common interoperability standards be established in the CBDC implementations of multiple central banks in support of enabling cross-border and cross-currency payments.

Should the use of the digital euro outside the euro area be limited and, if so, how? (213394)

Type: (T/text-long)

No

Which software and hardware solutions (e.g. mobile phones, computers, smartcards, wearables) could be adapted for a digital euro? (213396)

Type: (T/text-long)

We believe it is essential that all PSP end-user solutions include the following elements:
a) A private key (possession element) residing in a Qualified Signature/Seal Creation Device in order for the corresponding signatures to be deemed a QSEAL or QES.
b) The private key be activated by either biometrics (Inheritance) and/or a PIN (knowledge)
c) A display element to display as a minimum the amount and payee to the Payer. All display elements used by a payer's PSP must be audited as part of their wider SCA procedure.
We believe that software/hardware solutions such as mobile phones, computers and wearables could be adapted for a digital euro (both as PSU wallet apps and POS terminal apps). However, we don't believe it is appropriate for a PSP solution to be delivered only via a smartcard unless the PSP solution utilised an accompanying device to provide the display element.

What role can you or your organisation play in facilitating the appropriate design and uptake of a digital euro as an effective means of payment? (213397)

Type: (T/text-long)

We are a startup specialises in providing mobile apps for e-ID and Strong Customer Authentication (SCA). We have aligned our proposition closely to eIDAS and the related Advanced Electronic Signature (AdES) standards. We are contributors to a number of industry initiatives, including the Berlin Group NextGenPSD2 Advisory Group and the EUeID Working Group (2).

During much of 2020 we participated in the Berlin Group 'Signed Payment Request' working group. This focussed on the capture of Embedded SCA for all NextGenPSD2 payment and consent types. A key use case of this group covered initiation of instant payments (and the capture of SCA) at a physical Point of Sale (POS) and also online at the Point of Interaction (POI). An important POS requirement was for the person's (PSU's) smartphone to not require a network connection. For this we proposed the use of proximity communication technologies such as QR codes and BLE. Here is a link to our POS demo that was presented to the EPC MSCT multi-stakeholder group in December.

More recently, in the EUeID forum we have been involved in extensive discussions about the important synergies between eID and CBDC and also the alignment of Self-Sovereign Identity (SSI) concepts with eIDAS electronic signatures.

We would very much like the opportunity to be involved in a funded proof of concept through which the 'end user solution' interoperability standards required by CBDC (POS and P2P) could be explored further. We believe the approach outlined within the Berlin Group "Signed Payment Request" proposal provides an excellent starting point. I recommend it be extended as follows:
1) Adoption of SSI concepts to provide a separation between identity and attributes.
2) Extensions to support Offline/Offline instant payment scenarios. This would support transactions (including capture of SCA) where both POS and PSU smartphone (CBDC wallet app) offline.
3) Extensions to support CBDC including account based and UTXO approaches. Also extensions to support P2P transactions where both smartphones are offline.
The ultimate aim should be to provide general purpose eID/SCA approach for CBDC and bank money. This would encompass a range of financial transactions.