...making excellence a habit.™

07 September 2021

BSI response to the Bank of England's discussion paper on New Forms of Digital Money

Introduction

1. BSI (the British Standards Institution) is making this response to the Bank of England, as the National Standards Body for the UK. BSI has a public function in support of the UK economy. We bring together experts from stakeholders (including government, industry and consumers) and facilitate the development of standards to give guidance based on best practice, to ensure a level of consistency and quality, and also to enable interoperability and re-use across organisations. All of which are core to the Bank's development of Digital Money.
2. BSI experts work collaboratively. Our committees and working groups have to accommodate a wide range of views, often strongly held, to reach a consensus or collective decisions on which standards can be built. The Digital Money discussion document has raised divergent views and we are already working to bring convergence. We offer our collaborative and consensus way of working to the Bank to support their development of UK's Digital Money.

About BSI

3. As the UK's National Standards Body, BSI operates in accordance with a Memorandum of Understanding with the UK Government. The MoU notes that standardization is a key factor in support of a number of government policies, including competitiveness, innovation, reduction of trade barriers, fair trading and protection of consumer interests, environmental protection and public procurement.
4. BSI represents the UK view on standards in Europe via the European Standards Organizations CEN and CENELEC and internationally via ISO and IEC. BSI is a member of ETSI (The European Telecommunications Standards Institute) and provides support to DCMS through their membership of ITU (The International Telecommunication Union).
5. BSI is responding to the question in this consultation with evidence provided by committee experts. BSI provides the infrastructure for over 13,000 experts, who are the voice of UK economic and social interests, to be influential in the international standards organisations. BSI's experts are from industry and government, and many of them, have extensive international experience at the strategic and tactical levels across the full spectrum of trust operations and risk mitigation. They include advisors to UK and other governments, the EU and international bodies such as UNHC, World Bank and Interpol. For more information on the committees that helped shape this response please see Annex I.
6. In addition to developing standards that aid interoperability, re-use and best practice, BSI committees provide a valuable vehicle for experts to work together, share knowledge and further understanding, nationally and internationally. This is invaluable when dealing with complex societal challenges, such as the National Digital Twin Programme[1], and this can be harnessed for Digital Money too.

[1] https://www.cdbb.cam.ac.uk/what-we-do/national-digital-twin-programme

Key messages

7. BSI Committees IST/12 - *Financial services*[2] and DLT/1 - *Blockchain and Distributed Ledger Technology*[3], with assistance from experts from IST/17 – *Machine Readable Identity Documents*[4] and IST/33 – *Information security, cybersecurity and privacy protection (including Identity)*[5], have collaborated to respond to this call for evidence. The committees would welcome further discussion with the Bank of England to help identify areas where standardization can support the strategy around new forms of digital money. For more information on the committee structure and remit please see Annex I.

8. The committees see a number of key areas where BSI and standardization can support the Bank of England in their approach to new forms of digital money:

    a. Cybersecurity

    b. Counter-fraud

    c. Identity management of persons, organisations and non-person entities

    d. Interoperability

    e. Privacy

    f. Data Quality

    g. Risk Management

    h. Financial Inclusion

    i. Governance of and co-regulation distributed systems

9. Within BSI's catalogue of national, European and International standards (the standards catalogue[6]) there are a significant number of underpinning standards that can help support the Bank of England's strategy going forward. These standards are designed to set out clear and unambiguous provisions and objectives. Each standard is kept current through a process of maintenance and review whereby it is updated, revised or withdrawn as necessary. BSI's standards evolve to meet market requirements or industry innovations. Where new standards are required, BSI is well placed to bring together UK stakeholders to create documents that are built on consensus and full open consultation. An initial list of potentially relevant standards is provided in Annex II. These standards have been selected based on the content of the Bank's discussion paper and additional assumptions made by BSI. These additional assumptions are provided in Annex III.

[2] https://standardsdevelopment.bsigroup.com/committees/50001771
[3] https://standardsdevelopment.bsigroup.com/committees/50270820
[4] https://standardsdevelopment.bsigroup.com/committees/50001773
[5] https://standardsdevelopment.bsigroup.com/committees/50001780
[6] BSI seek wherever possible to develop international standards first, maximizing the UK stakeholders' significant influence on market access conditions globally. European regional standards are developed where there are no international standards or where there are specific interests in the region that could not be addressed globally.International and European standards are adopted for the whole of the UK as British Standards, alongside a diminishing proportion of national-only standards that meet purely local needs.

Context

10. BSI stands ready to assist considerably on the best practice guidance and normative standards for the safe governance and operational use of digital technologies across public and private sectors, and internationally, upon which the evolution of digital money will depend. However, BSI is not able to comment on the monetary policy considerations in this discussion paper on New Forms of Digital Money.
11. The speed of change is high, and as a result terminology also evolves fast - from new terms, to existing terms capturing technologies not envisaged originally - as a result, it is important to be very specific in articulating what is in scope under the proposals and what is not. In particular, we define the following terms for the purpose of this response:
    a. **Digital Payments**: we mean any payment occurring via a digital infrastructure by means of an official currency, legally recognised by the Bank of England. This means that by digital payments in this document we are not addressing any cryptocurrency or similar thematic.
    b. **DLT / Blockchains:** by Distributed Ledger Technology (DLT), including blockchain technology, we mean a distributed storage system, built with the objective of creating trusted sources of information. They are structured to provide a transparent, traceable, immutable, reliable and auditable infrastructure to seamlessly and securely exchange cryptographic keys. The result is delivering a range of benefits for participants, offering faster, cheaper and safer alternatives to traditional systems and processes.
    c. **Data:** Data itself needs to be clearly defined, as generated from either the traditional sources and new data arising from digital platforms and distributed ledgers, but limited to those that can be traced and are from formally and legally recognised sources cryptographically protected, possibly in real time and offering a strong degree of granularity, which allows it to meet the widest possible set of requirements.
12. Collaborative reports by Sir Mark Walport (ex-CSA, Gov Office of Science)[7] and Lord Holmes[8] (and others) highlight the opportunities of DLT for national public good in the UK digital economy and society. They describe what needs to be done for short- and longer-term benefits while reducing risks and costs. The core message is that the beneficial use of technology for the UK's digital economy and society depends fundamentally on high quality data and trust underpinning a national collaborative approach. This dialogue is being repeated with international allies and industry partners in many developed countries.
13. Three core themes of this discussion paper are confidence, safety and financial inclusion. Confidence requires safety (it won't cause harm) and financial inclusion (it supports the whole of society in a single approach). The legal requirements for safety of the individual and public safety in the physical world are well defined, but less so in the digital world where increasing digitisation demands that this be addressed so that risks can be mitigated effectively. Legislation and standards are key to building the policies, procedures and mechanisms upon which safe collaboration depends.

Creating a safe system

14. Safety depends upon four pillars - cybersecurity, counter-fraud, high data quality and collaborative governance. All of these feature in any risk mitigation strategy, which normally

[7] https://www.gov.uk/government/publications/distributed-ledger-technology-blackett-review
[8] https://chrisholmes.co.uk/wp-content/uploads/2020/12/Distributed-Ledger-Technologies-for-Public-Good_leadership-collaboration-and-innovation.pdf

includes five stages - Identify (risk), Protect, Detect, Respond and Recover. Major incidents usually result from either a failure to identify a risk or to have a balanced approach to protection, detection and response. So it will be with the creation, operation and use of digital money; safe use of data at the transaction level both for payments (including tax) and credit provision. BSI and ISO are very active in all of these pillars.

15. Cybersecurity. Blockchain/DLT and the rise in distributed systems are creating new cybersecurity challenges, particularly as variations and hybrids of these technologies grow. Vulnerabilities in the cryptography, key management, programming languages and implementations are being addressed but at a high cost to cybercrime victims. More systematic and globally consistent use of such technology may help to support payments leveraging both the existing data from traditional sources and new data arising from digital platforms and distributed ledgers.
    a. ISO has conducted a Security Evaluation of Consensus Mechanisms study, which showed significant flaws in common existing solutions including security, performance and availability.
    b. For DLT/blockchains it is therefore paramount that adequate requirements and encryption mechanisms are set up to ensure that platforms built on such technologies can be properly trusted and that cybercrime is prevented.
    c. Common Policies, standards and assurance models for Confidentiality, Availability and Integrity (CAI) and Authentication, Authorisation and Accountability (AAA) will be required.
    d. Ensure alignment with the work being carried under the current 2021 G20, and the relevant G20 Leaders as well as B20 recommendations. Specifically, we note the importance of the current debate in the direction of considering cyber threats at the same critical level of the current biological pandemic. To this extent there is a need to reinforce resilience and sustainability of critical information infrastructure and data security against major cyber incidents. The need to define clear approaches to (1) prevent, (2) crisis management and (3) recovery, to protect digital access and both domestic and cross-border data flows, especially during and after major cyber incidents.

16. Counter-Fraud
    a. The distinction needs to be made between:
        i. Digital payments wherein one or both counterparties are anonymous, for transactions that fall below the threshold for which recipients of cash are required by law to submit identifying information for the counterparty.
            1. Because this is anonymous and below the threshold, digital and social inclusion is encouraged and the operating costs and friction are minimised, in the same manner as cash.
            2. Because digital cash is below the threshold, the financial and social risks are reduced.
            3. What policies, procedures and mechanisms should there to prevent aggregation or repeat payments, or other forms of abuse and cybercrime?
        ii. Digital payments wherein both counterparties use asset custodians, wherein financial regulations demand increasingly strong and pervasive AML and Know Your Customer/Know Your Business compliance.
            1. Because this is pseudonymous (someone knows the identity) or veronymous (the identity is declared), surveillance can undermine areas of digital and social inclusion.
            2. Most major stakeholders require high-assurance digital technologies and high quality data, particularly around KYC and KYB, to manage their risks, and this requirement is gradually flowing through the digital business economy. However, this practice also introduces social costs, particularly if individual persons are required to prove their identity before undertaking

ordinary activities, which can create a perception of unwarranted intrusion into private affairs, for which better privacy-preserving and context-sensitive techniques are required. When this perception is combined with evidence that those with the means to do so can avoid such monitoring, for example by using proxies or unregistered contracts, and people who are willing to break the law are able to steal and use the credentials of others, or to compel others by force to act at their behest, then law-abiding parts of society object because measures designed to keep them safe are instead open to abuse. Mitigating techniques and technologies are available but the collaborative organisational arrangements to make best use of them to deal with these detailed challenges need to be created.

b. Counter-fraud Collaborative Situational Awareness (CSA) complements Cyber CSA, and is particularly relevant when combating the insider threat in and across service operators, impersonation, and money laundering trails. Organisational transaction monitoring and finance intelligence units can benefit from the use of ZKP and SMPC to identify and defeat such threats.
c. Public authorities such as HMRC, FCA, PRA, MHRA, MOD increasingly require greater end-to-end traceability and provenance of products and confirmation of their associated payments, as well as customs tariffs and tax take. The development of Digital Money should be integrated with these if possible.

17. Privacy. Being able to demonstrate verifiable privacy by design in the general case, and the protection of personal information in other cases, is essential to public confidence. There is much misunderstanding about GDPR/DPA and privacy. In particular, data protection is no substitute for privacy by design[9].There are new technologies, notably Zero Knowledge Proofs and Secure Multi-Party Computation, that enable the validation of personal information without collecting or exchanging any personal data at all. Functional examples include:
    a. Proving that two parties hold the same data attribute or set of attributes or any other formatted data object such as an image or cryptographic primitive;
    b. User or device authentication either by validation of a shared secret or proving possession of a password;
    c. Validating claimed data against an authoritative source;
    d. Proving that a rule is satisfied sufficient for policy compliance;
    e. Proving that the results of a calculation or algorithm or Boolean/logical expression are compliant or the same between two or more organisations;
    f. Enable data protection for a link between an on-chain reference and off-chain PII, which can be removed to ensure Right to Erasure ("Right to be forgotten") and retain blockchain integrity.

18. High Quality Data. All of the above involves the need for high quality, trusted data, from authoritative sources that can be re-used with confidence by multiple parties to make important, sometimes vital, decisions quickly.

19. Governance.
    a. The purpose of governance is to manage all risks within a given scope, including opportunity risks. All the stakeholders in a digital community must be involved in a collaborative governance model. Omitting one group of stakeholders creates risks for the other stakeholders.
    b. The governance model should enable both proactive and reactive management of risks and issues, with a strong emphasis on collaborative situational awareness that includes all operational stakeholders right to the end-point.

[9] See H Nissenbaum. "Deregulating Collection: Must Privacy Give Way to Use Regulation?" May 2017. https://doi.org/10.2139/ssrn.3092282

c. To address matters related to organised crime and national security, a national intelligence and incident coordination centre must be fit for purpose and inclusive. UK financial regulators may not see this as their role, but many other nations' regulators have engaged in operational processes that allow them to regulate at digital speed. If not, then it is in the Bank's and national interest to ensure that such a collaborative centre is created with a mix of industry partners.

20. Many experts believe that DLT is an appropriate technology for the implementation of digital money. There are valid and sound justifications for this approach.[10] However:
    a. There are alternative designs, with other chosen trade-offs. China's CBDC (e-Yuan) is based on Zero Knowledge Proofs (ZKP) and not blockchain. Four pilots are near completion and 12 more are about to begin. China has imposed a national security blackout on the technical details, however two questions are being pursued amongst ISO experts: why has China chosen to use ZKP and how will blockchain CBDCs interoperate with China's ZKP?
    b. No country has yet approved legislation to address a company's legal responsibilities ("company law") for the use of distributed, (semi-) autonomous systems. Within Europe, Malta has come closest. The general consensus is that single jurisdictionality will be required and it is too early to shape an effective multi-jurisdictional approach. The Law Commission has been involved in these considerations and they could assist in aligning the evolution of legislation with the evolution of best practices and standards, to meet the overall Digital Money objectives. We imagine that a co-regulatory approach might be useful or necessary to ensure that a distributed system could be developed in such a manner that ensures public oversight of the system and accountability for its operators.

21. The Treasury has launched a consultation on potential requirements for the inclusion of personal information for the transferor and beneficiary for virtual asset transfers above £1,000. This consultation is consistent with the direction FATF is taking regarding Virtual Asset AML/CFT. We note that this restriction falls well below the maximum value for which cash can be accepted from an anonymous source by UK merchants. If such a policy were to be introduced, then UK persons would have less privacy when transferring digital cash compared to when transferring physical cash. It is important to note this in the context of the ever-diminishing access to physical cash and acceptance of cash by merchants in the UK[11][12].

22. Consideration should be given to how CBDC transactions might be differentiated from fiat transactions for operational and potential regulatory reasons. Should CBDC transactions fall within scope, there may be a requirement to clearly identify specific CBDC issuers and denominations via use of codes similar to currency values defined in ISO 4217. We specifically note that individual fungible tokens are mutually substitutable and therefore cannot be marked or distinguished from each other, e.g. via serial numbers or the equivalent.

Discussion paper questions

Q8. Do you agree with the Bank's view on protection and privacy? What would you regard as a minimum set of protections?

[10]See Section 3.1 of G Goodell, H Nakib, and P Tasca. "A Digital Currency Architecture for Privacy and Owner Custodianship." Future Internet 13(5), 130, May 2021. https://doi.org/10.3390/fi13050130
[11]Access to Cash Review, March 2019. https://www.accesstocash.org.uk/media/1087/final-report-final-web.pdf
[12]D Tisher, J Evans, K Cross, R Scott, and I Oxley. 'Where to Withdraw? Mapping access to cash across the UK.' University of Bristol, November 2020. http://www.bristol.ac.uk/media-library/sites/geography/pfrc/Where%20to%20withdraw%20-%20mapping%20access%20to%20cash%20across%20the%20UK.pdf

23. BSI supports the Bank's view of the importance of data protection and privacy, especially in the context of financial inclusion. BSI has been an active participant in the development of a series of international standards that provide accepted best practice on topics of relevance such as privacy information management. We specifically note the 2009 report delivered by the Constitution Committee of the House of Lords, which states "Mass surveillance has the potential to erode privacy. As privacy is an essential pre-requisite to the exercise of individual freedom, its erosion weakens the constitutional foundations on which democracy and good governance have traditionally been based in this country."[13]
24. Digital payment solutions promise to reduce the transaction costs and frictions associated with financial remittances, including retail payments involving ordinary consumers. So far, modern digital payment solutions broadly require custodial accounts with banks, in turn carrying the burden of registration and AML/KYC obligations for both ordinary persons and custodians. Such mechanisms are considered necessary to prevent asset custodians from using their privileged position to facilitate illicit activity, although they have also been demonstrated to inhibit financial inclusion[14].
25. From a Financial inclusion perspective, it is critical to minimise the "Regulatory burden" on firms, particularly looking at the impacts MSMEs, who face a proportionately higher cumulative regulatory and administrative burden relative to their resources. If jurisdictions recognize a more systematic and globally consistent use of digital technologies in their legislations and regulations, this will help to overcome some of the high administrative, compliance (e.g. AML and KYC requirements) and transaction costs, and hence raise inclusivity.
26. New digital technologies should be deployed with care to minimise the risks and maximise the benefits, particularly for the public good and the digital economy. We believe this means protecting and future-proofing a public payment option for ordinary retail transactions as the demand for digital payments grows.
27. BSI stands ready to work with the Bank of England to advance its financial inclusion goals by identifying and creating the necessary standards that enable all persons to conduct low-risk transactions via non-custodial wallets, without the need to establish or use custodial accounts.

Q10. What steps could be taken, and by whom, to help promote interoperability of new forms of digital money with other payment systems, and thereby foster a competitive environment?

28. BSI strongly supports the Bank's view that standards are an essential part of interoperability and that any infrastructure would need to consider technology and data standards so that information could be exchanged seamlessly between the different systems involved. We believe the provision of common technical standards for digital money are a necessary pre-requisite for facilitating the technical interoperability of new forms of digital money with other payment systems.
29. BSI, through its participation in ISO standards development work, as well as its own standards initiatives, provides expertise covering standards relevant to the successful implementation of digital money, and for delivering interoperability with other payments systems as needed. As mentioned above we have included for convenience a list of these standards in Annex II. We would like to take the opportunity to provide some further detail on some of these standards in the sections below.

[13]House of Lords. Constitution Committee – Second Report, Session 2008-2009. https://publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1802.htm

[14] GIABA (2018). Research and Documentation Report, 'Know Your Customer/ Customer Due Diligence Measures and Financial Inclusion in West Africa: An Assessment Report.' GIABA, Dakar, Senegal. https://www.giaba.org/media/f/1062_FInal%20KYC-CDD%20Assessment%20Report%20Published.pdf

30. BSI has been actively involved in defining an international standard, ISO 24165 Digital Token Identifier (DTI), to provide a technology-neutral mechanism for the unique and unambiguous identification of digital money. The DTI covers representation of digital money, including stable coins, as well as other digital tokens outside the scope of the Discussion Paper such as utility tokens, security tokens etc.
31. The DTI could enable technical interoperability in multiple ways, including (i) interoperability between payment systems for the same digital money; (ii) interoperability between different forms of digital money; and (ii) interoperability between digital money and fiat money (the latter being identified via its own international standard ISO 4217 Currency Code).
32. BSI experts have had a leading role in the international development of cybersecurity, identity and privacy standards, which provide the baseline for digital safety, trust and confidence, in an increasingly complex environment of consumer rights, legislation and risk mitigation. Digital money will need to leverage these standards in order to support the full spectrum of interoperability: legal interoperability; policy interoperability; data interoperability; technology interoperability; systems interoperability and governance interoperability (also known as federation).
33. In addition, there is an increasing requirement to link regulated non-financial assets to financial payments for reasons of provenance, traceability, efficiency and taxation, for which some authorities and global financial institutions are planning. It is reasonable to expect that some forms of digital money will similarly have to interoperate with these payment systems and support non-financial asset requirements.
34. Competition, particularly in the digital era, requires the maximum amount of re-use and commonality to drive down cost, such that competitive advantage is focused on the unique selling point (USP) or value-add. The greater the re-use and the focus of resources on the USP, the faster the USP can evolve and deploy to maintain competitive advantage. Consequently, digital money will become more integrated into the business process and the user experience, which will require it to support more dimensions of interoperability over time, raising the potential for "policy collisions" between policy domains. BSI's experts have international experience in developing standards to support and enable such increasing complexity, participating on all the relevant committees.
35. The proposed new EU eIDAS Regulation[15] includes a requirement for all member states to issue "digital wallets" to their citizens by 2025. This will create an expectation and a need across UK consumers and businesses in the same timeframe. International standards can play a key role in facilitating interoperability of digital wallets across jurisdictions.
36. BSI is responsible for the UK input into other key international financial services data standards. These include ISO 17442, the Legal Entity Identifier (LEI), which is now widely accepted as the standard for identification of a growing cross section of financial and other entities in regulatory reporting and beyond. The LEI could be used to identify recipients of payments using digital currency, for the purpose of facilitating tax reporting and regulatory compliance. The LEI could also help payers (including retail consumers) confirm that their money will be sent to the correct recipient, as they can with cash, via various mechanisms such as physical location, human verification, etc.
37. BSI also actively participates in the continued development of ISO 20022, which is well known to the Bank, and increasingly utilised in payments infrastructures, and for the delivery of regulatory reports. ISO 20022 provides a methodology for the creation of financial messages, and provides a semantic foundation for financial services. ISO 20022 could potentially have a key role in the interoperability of digital money with fiat currencies and payments systems. However, ISO 20022 was designed in the context of transactions among asset custodians and other financial

[15] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2021%3A281%3AFIN

intermediaries, and as currently constituted is unlikely to be sufficient to cover the anticipated use cases for CBDC. We anticipate that it must be adapted to meet new requirements, including but not limited to privacy by design for unidentified counterparties, before it can be applied to transactions involving non-custodial wallets.

38. BSI is also engaged in the development and maintenance of many other potentially relevant standards that could enhance interoperability. As mentioned earlier, Annex II provides the list of such standards that the committees have identified as being potentially relevant technologies that could underpin or support digital currency.

Conclusions

39. BSI welcomes the Bank's focus on the benefits to society from the introduction of new forms of digital money, whilst also considering how to mitigate any associated potential security and privacy challenges.
40. The standards overseen by BSI committees on financial services and digital ledger technologies can support the Bank's policy objectives by enabling interoperability, security and privacy for digital money, as well as by enhancing financial inclusion.
41. As the National Standards Body for the UK, BSI is uniquely placed to consider which national, European and international standards can best be utilised to further the Bank's objectives. The selection of appropriate standards can provide opportunities for the UK to establish a global leadership position in this space that promotes innovation across the UK financial services and technology industries and creates sustained competitive advantage to UK industry.
42. Conversely, the lack of appropriate standards may result in suboptimal outcomes, such as when determining the appropriate balance between security risks and social benefits of digital money.

Recommendations

43. BSI asks the Bank to review the considerations, suggestions and proposed clarifications outlined in this response. We would appreciate feedback on the items outlined, and we remain available to offer any further clarification or details the Bank may require (for example helping to update the ISO 20022 standard for payment messaging).
44. BSI urges the Bank to engage with its committees to identify how the standards overseen by BSI can support the Bank's work on new forms of digital money. The Bank is currently engaged with BSI Committee IST/12; we would encourage further engagement with other relevant committees to gain further insight on the areas of focus. We would also encourage strategic engagement to help enhance collaboration and identify areas where BSI can support the Bank further.

Annex I

BSI relevant standards committees

IST/12
IST/12 is the BSI Committee responsible for the UK input to the development and maintenance of financial services security, information exchange and reference data standards. As such IST/12 acts as the mirror committee for the International Organisation for Standardisation (ISO) Technical Committee 68 (TC 68). In this capacity IST/12 provides UK contributions to the development of all financial services standards falling within the remit of ISO TC68, as well as for the preparation, revision and amendment of any British Standards relating to financial services not covered by ISO.

Committee members include public authorities, payment processors, financial services institutions and trade associations, financial data vendors, financial technology companies and academic institutions.

DLT/1
Under the direction of the BSI Standards Policy Strategy Committee, DLT/1 is responsible for the UK input into ISO/TC 307 and CEN/CENELEC/JTC 19.

Members include public authorities, DLT trade associations, technology companies, academic institutions, innovation hubs, SMEs and start-ups.

IST/33
IST/33 is the UK mirror committee for ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection. It is largest committee in ISO and its standards have the greatest global usage. It covers:

- Security requirements capture methodology;
- Management of information and ICT security; in particular information security management systems, security processes, and security controls and services;
- Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information;
- Security management support documentation including terminology, guidelines as well as procedures for the registration of security components;
- Security aspects of identity management, biometrics and privacy;
- Conformance assessment, accreditation and auditing requirements in the area of information security management systems;
- Security evaluation criteria and methodology.

IST/17
IST/17 is the UK mirror committee for ISO/IEC JTC 1/SC 17 - Cards and security devices for personal identification. It covers:

- Identification and related documents,
- Cards,
- Security devices and tokens

and interface associated with their use in inter-industry applications and international interchange. This includes passports and driving licences, and their mobile equivalents.

Annex II

List of Potentially Relevant Standards

Standard	Description
ISO 4217 Currency	Currency Codes
ISO 13616 IBAN	Financial services — International bank account number
ISO 17442 LEI	Financial services — Legal entity identifier
ISO 20022 Message scheme	Financial services — Universal financial industry message scheme
ISO 20275 ELF	Financial services — Entity legal forms
ISO 22739 Vocabulary	Blockchain and distributed ledger technologies — Vocabulary
ISO 23257 Reference Architecture	Blockchain and distributed ledger technologies — Reference architecture
ISO TS 23526	Security aspects for digital currencies
ISO TS 23635	Blockchain and distributed ledger technologies — Guidelines for governance
ISO 24165 DTI	Digital Token Identifier
ISO TR 24332	Blockchain and Distributed Ledger Technology in relation to authoritative records, records systems, and records management
ISO 24366 NPI	Financial services – Natural Person Identifier
ISO/IEC 9798- 5:2009.	Information technology - Security techniques - Entity authentication -
Part 5:	Mechanisms using zero-knowledge techniques
ISO/IEC 29100:2011.	Information technology - Security techniques - Privacy framework
ISO/IEC 29191:2012.	Information technology — Security techniques — requirements for partially anonymous, partially unlinkable authentication
ISO/IEC 27002:2013	Information technology - Security techniques - Code of practice for information security controls
ISO/IEC 29115	Information technology - Security techniques – Entity Authentication Assurance Framework
ISO/IEC 29151:2017.	Information technology - Security techniques - Code of practice for personally identifiable information protection
ISO/IEC 29134:2017.	Information technology - Security techniques - Guidelines for privacy impact assessment
ISO/IEC 27018:2019.	Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
ISO/IEC 27551:2021.	Information technology - Security techniques - Attribute Based Unlinkable Entity Authentication

Annex III

This Annex captures the key assumptions made by BSI when determining the list of standards that may be relevant to the Bank's discussion paper.

The Payments Landscape

(1) The use of cash is declining in many countries around the world. Part of the reason is the relative efficiency of digital payment channels. The result is that the variable revenues of operating a cash infrastructure are falling below the fixed costs, and as a result, the maintenance of cash infrastructure is increasingly untenable.

(2) In the UK, facilities to deposit and withdraw cash have become less prevalent, debit cards and e-commerce (Internet) payments via custodial accounts are capturing a larger share of payments, and brick-and-mortar merchants and vendors are increasingly refusing to accept cash.

(3) The systematic replacement of cash by intermediated forms of payment via custodial accounts is harmful to consumers. In particular, cash affords its users the following benefits that modern retail payments do not:

a. Accessibility. Nearly everyone can use it. The user interface for cash is simple, it has built-in features for accessibility and security, and its users do not need special registration, contracts, bank accounts, network connectivity, or even electricity.

b. Non-Discrimination. Because the value of cash is intrinsic, everyone's money is as good as everyone else's. If one person gives cash to another, the amount of value that one party relinquishes is exactly equal to the amount of value that the other party gains. What cash can do is not specifically enabled or limited by the identity of its bearer.

c. Privacy. Users of cash have no reason to fear that their activities will be profiled on the basis of their transactions. Most cashless payment methods leave behind a data trail that can be used to construct a detailed history of an individual's habits, location, and circumstances.

d. Ownership. Cash is truly owned by its bearers. Users of cash know that their transactions will succeed without the risk that a third party might block them, in contrast to instruments that are ultimately under the control of third parties and for which their users have only limited rights.

(4) The systematic replacement of cash by intermediated forms of payment via custodial accounts undermines monetary sovereignty. Funds held as cash are the direct obligations of the central bank, whereas funds held in custodial accounts are the obligations of private-sector banks. Government deposit insurance obscures but does not eliminate the difference between these two forms of money from ordinary consumers. When consumers conduct transactions using the obligations of private-sector banks, the effectiveness of monetary policy is undermined, both because multinational banks can transparently shift the risk among currencies and because multinational banks can reduce their reliance upon the central bank of the country in which their account holders conduct transactions.

(5) Both cash and custodial accounts with banks allow consumers to conduct transactions using currencies other than the currency of the nation in which the transactions take place. But with custodial accounts, the choice to use foreign (or corporate) currencies can be frictionless.

Consumer Requirements

(6) Consumers have a right to conduct low-risk transactions with merchants, vendors, and other providers of retail goods and services, without revealing PII that can be used to associate themselves with the transaction. For the avoidance of doubt, PII includes any persistent identifier associated with the consumer as well as any reference to another transaction done by the consumer.

(7) The vast majority of transactions conducted by most consumers are low-risk.

(8) It is possible to regulate transactions without collecting PII of the consumer that can be used to associate a payer with a transaction. In particular, it is possible to collect information about the payee for compliance with tax and AML/KYC regulations, along with relevant information about the size, location, and nature of the transaction, while allowing the payer to be anonymous.

The Solution Space

(9) Anonymous accounts generally contravene AML/KYC recommendations and, because they implicitly link successive transactions done by a consumer to each other, are not actually private for most legitimate retail use.

(10) A wallet is an application to generate, manage, or use private and public keys. It can be implemented as a software or hardware module, and it can be used to store keys representing value. A non-custodial wallet is a wallet that is under the direct control of the consumer that owns the assets that it contains. A non-custodial wallet is not an account or quasi-account; it is not provided or administered by a third party.

(11) A consumer can have an arbitrary number of non-custodial wallets, and a non-custodial wallet does not forcibly contain any identifying information that can be used to link the assets it contains to the owner of the assets.

(12) A consumer can withdraw digital currency from a regulated money services business into a non-custodial wallet using privacy-enhancing technology, such as blind signatures or zero-knowledge proofs, to ensure that the assets contained in the non-custodial wallet are fungible and not distinguishable or recognisable by the regulated money services business or any other parties as having been associated with its owner or the transaction in which the digital currency was withdrawn.

(13) The transactions of a central bank digital currency system would be performed by regulated money services businesses.

(14) A central bank digital currency system would include a mechanism to ensure that its system operators do not equivocate. This mechanism could be a distributed ledger.

Annex IV

Background on BSI

BSI is the UK's National Standards Body, incorporated by Royal Charter and responsible independently for preparing British Standards and related publications and for coordinating the input of UK experts to European and international standards committees. BSI has nearly 120 years of experience in serving the interest of a wide range of stakeholders including government, business and society.

BSI represents the UK view on standards in Europe (via the European Standards Organizations CEN and CENELEC) and internationally (via ISO and IEC). BSI has a globally recognized reputation for independence, integrity and innovation ensuring standards are useful, relevant and authoritative.

BSI is responsible for maintaining the integrity of the national standards-making system not only for the benefit of UK industry and society but also to ensure that standards developed by UK experts meet international expectations of open consultation, stakeholder involvement and market relevance.

British Standards and UK implementations of CEN/CENELEC or ISO/IEC standards are documents defining good practice, established by consensus. Each standard is kept current through a process of maintenance and review whereby it is updated, revised or withdrawn as necessary.

Standards are designed to set out clear and unambiguous provisions and objectives. Although standards are voluntary and separate from legal and regulatory systems, they can be used to support or complement legislation.

Standards are developed when there is a defined market need through consultation with stakeholders and a rigorous development process. National committee members represent their communities in order to develop standards and related documents. They include representatives from a range of bodies, including government, business, consumers, academic institutions, social interests and regulators.

Further Information

BSI would be pleased to provide further information or to discuss the content of this submission. For further information please contact:

Sahar Danesh
Government Engagement Manager
British Standards Institution
Email: sahar.danesh@bsigroup.com
Tel: 020 8996 7388
Mob: 07876 478908