DCash 2.0 - Central Bank Digital Currency
Request for Vendor Information

The Request for Vendor Information ("the RFVI") herein is issued by the Eastern Caribbean Central Bank ("the ECCB" or "the Bank") and seeks input to shape the discovery process for a Central Bank Digital Currency ("CBDC") technology solution for a commercially-deployed retail CBDC. Upon completion of review of responses to the RFVI the ECCB will issue a Request for Proposal.

In particular, the ECCB is seeking input from parties which have developed a retail CBDC solution or core components of such a solution which is deployment-ready.

Specifically, the target audience for the RFVI herein is:

- Vendors which may have offerings to enable core retail CBDC processes as outlined herein.
- Vendors which may have offerings which can integrate with a core retail CBDC to provide necessary third-party functions (some of which are outlined herein)

The ECCB is interested in a retail payment solution which performs core CBDC ledger functions and supports integration via secure API layer, allowing for third-party systems to integrate within the solution. Among the third-party systems which may ultimately be integrated with the core system includes (but are not limited to):

- Wallet Services Providers / Payment Services Providers.
- Core Banking systems.
- Advanced Payment Use Case providers.
- Identity Management and alias providers.
- Advance business intelligence and reporting providers.
- Offline payments

The objective of the RFVI is to obtain a description of your retail CBDC solution and/or ancillary third-party system, in relation to the areas highlighted. Diagrams can be included where appropriate to provide a better understanding of your offering.

Upon evaluation of responses Vendors may be invited to further participate in subsequent RFP exercise.

Submission Guidance

1. Interested individuals and organisations are invited to submit comments electronically in PDF format to email address dcash_admin@eccb-centralbank.org on or before 4:00 p.m. AST on 22nd January 2024. Electronic submissions received after the deadline may not be incorporated or taken into consideration.

2. Responses to the RFVI should include < RFVI Response: ECCB Central Bank Digital Currency > in the subject line of the email. Mailed paper submissions will not be accepted.

3. Response to this RFVI is voluntary. Each responding entity (individual or organisation) is requested to submit only one response, in English.

4. Responses may address one or more topics, as desired, from the enumerated list provided in this RFVI, noting the corresponding number of the topic(s) to which the response pertains.

5. Responses should include the name of the person(s) or organisation(s) submitting the comment, as well as the respondent type (e.g., developer, technology service provider, other).

6. Comments referencing materials that are not widely published should include copies or electronic links of the referenced materials.

7. No business proprietary information, copyrighted information, or personally identifiable information (aside from that requested above) should be submitted in response to this RFVI. Information gathered in the course of the RFVI may form part of public discussion.

8. Responses to this notice are not offers and cannot be accepted by the ECCB as forming a binding contract. Respondents are solely responsible for all expenses associated with response preparation.

9. All requests for further information should be directed to the ECCB at DCash_admin@eccb-centralbank.org and should include < RFVI Further Information Request: ECCB Central Bank Digital Currency > in the subject line of the email. Requests for further information should be submitted no later than on or before 4:00 pm AST 8th January 2024.

About the ECCB

The Eastern Caribbean Central Bank ("ECCB" or the "Bank") is the Monetary Authority for a group of eight island economies of the Eastern Caribbean Currency Union (ECCU), namely, Anguilla, Antigua and Barbuda, Dominica, Grenada, Montserrat, Saint Christopher (St Kitts) and Nevis, Saint Lucia, and Saint Vincent and the Grenadines. The Headquarters is located in St Kitts. Agency Offices are established on each of the other seven (7) member countries.

The primary objectives of the ECCB are:

- Regulate the availability of money and credit;
- Promote and maintain monetary stability;
- Promote credit and exchange conditions and a sound financial structure conducive to the balanced growth and development of the Participating Governments; and
- Actively promote through means consistent with its other objectives the economic development of the territories of the Participating Governments.

To undertake its functions, the ECCB issues currency, maintains foreign exchange reserves, provides account services, provides payment and settlement services and provides lender of last resort facilities to eligible parties. Additionally, the ECCB regulates and supervises commercial banks in the ECCU. These services are provided to participating member governments and the Eastern Caribbean Currency Union (ECCU) commercial banks.

The ECCB piloted a retail CBDC system which has been operational since March 2021 ("the current system"). The ECCB continues to operate the current system which enables the following processes and functions:

- Core ledger retail CBDC functions, i.e. internal processes (creation, destruction) external facing processes (issuance, redemption)
- Financial Institution external interaction with CBDC (web app)
- End User Interface with CBDC (retail and commercial mobile wallet)

The current system enables access to necessary third-party systems to facilitate various key business processes including:

- KYC
- AML/CFT
- Multi Factor Authentication
- Business Intelligence and Reporting
- Performance Management

As part of the pilot constraints the current system was not integrated with any other system including RTGS and financial institution's core banking systems.

Information Requested

Please provide information on either how your system may itself provide the specific functionality or support/facilitate the same through integration with third-party providers. If your system does not provide or support a specific functionality, please provide rationale explain.

Section I: General

The system you are describing should support at the most basic level the core retail CBDC processes of creation, issuance, redemption, and destruction.

1. What are the options for your solution's underlying ledger technology and infrastructure to support the CBDC?
2. Please describe how each unique CBDC elemental unit / balance / value, is recorded / tracked or within your solution.
3. How is your solution deployed into a client environment? (onsite / cloud / hybrid)?
4. If in the cloud, which cloud platforms does your solution support?
5. Please describe the distribution model(s) supported by your solution. (Distribution models may include CBDC issuance to various intermediaries prior to the end-user distribution phase. The Central Bank should remain the sole issuer of the CBDC.)
6. Please describe your solution's application architecture and system data model.
7. Please list third-party software necessary to provide the full retail CBDC functionality of your solution.
8. Please provide insights into your use of open-source software / licensed software required for your core retail CBDC system to run.
9. Please describe how your solution allows for the secure creation, issuance, redemption, and destruction of CBDC.
   - What controls are in place to ensure the creation process is sufficiently insulated from the subsequent issuance into the payment network?
   - Does your system support custom authorization for minting and issuance of CBDC?
10. Please illustrate payment flow orchestration supported by your solution.
11. Please describe how your solution lends itself towards the accounting of the CBDC throughout its lifecycle, including transfer to intermediaries.

Section II: Use Cases

1. Please describe how your system may support/facilitate the following payment use cases:
   - Person to person.
   - Consumer to Business ('brick and mortar' or e-commerce)
   - Business initiated - pay another business or pay individuals e.g., salaries).
   - Payments, to the Government e.g., taxes, and by the Government e.g., grants and disbursements.

2. Please describe how your system may support/facilitate more advanced payment use cases:
   - Recurring payments or 'subscription-like' payments.
   - Refunds or counter-transactions.
   - Bulk/batch payments.
   - Programmable payments.
   - Machine-initiated –automated payments, initiated by device and/or software based on predefined conditions.
   - Other use cases e.g., micro-payments, loyalty points, one-click checkout etc.

Section III: Account Lifecycle

1. Please describe how your solution may support/facilitate customer account lifecycle management, considering areas such as:
   - Onboarding and satisfying KYC requirements.
   - Utilisation of external identity management services.
   - Use of unique identifiers and aliases.
   - Treatment of suspicious activity from accounts.
   - Deprovisioning of customers.

2. Please describe how your solution may support/facilitate AML/CFT processes, considering areas such as:
   - Sanction screening.
   - Real time monitoring.
   - Alerting.
   - Enforcement of limits.
   - Reporting of suspicious activity.

3. Please describe how your solution may support/facilitate the creation of different account types for users based on various criteria considering areas such as:
   - Users' risk rating.
   - Identity proof provided.
   - Relationship with existing accounts (e.g., sub accounts).

Section IV: Integration

1. What APIs are supported by your solution?

2. Please describe how your solution delivers, and/or facilitates other providers to deliver:
   a. Necessary identity management functions including KYC and AML/CFT.
   b. End-user interfaces on a range of devices/form factors such as, but not limited to; mobile applications, payment cards, smart devices etc. (please describe for both consumer and merchant end-users).
   c. Integration with existing payment systems, such as Automated Clearing House (ACH), card processing network (switch) and access channels, such as POS network.
   d. Integration with wholesale payment systems, for example, Real Time Gross Settlement Systems (RTGS).
   e. Integration with financial institutions' core banking systems, Payments Services Providers applications, Government treasury functions, other key intermediaries.
   f. Integration with existing merchant e-commerce platforms.
   g. Programmability features.

3. Please describe how your solution may facilitate cross border payments.
   a. Please describe any interoperability standards with traditional payments systems to which your solution adheres.
   b. Please describe any interoperability standards with CBDC systems to which your solution adheres.

Please describe how your solution may facilitate foreign currency transactions.

Section V: Operations Management

1. Please describe what may be the roles and responsibilities required to operate and maintain the system; include an access control matrix if available.
2. How would your development and quality assurance processes be run to address software bugs, new feature releases and system updates?
3. How frequent are new releases?
4. How do you envisage interacting with the Bank to accommodate any necessary change management procedures?
5. How do you envision interacting with the Bank in a service assurance relationship to ensure optimal operation of the system?

Section VI: Monitoring and Performance

1. What are your solution's capabilities towards operational performance monitoring?
2. What performance metrics does your solution meet in relation to transaction processing and population size?
3. Describe your solution's capability towards high availability and load balancing.
   a. Describe how scaling will occur and whether automatic.
   b. Describe your solution's capability towards backup, recoverability, and business continuity management.
   c. How does your solution extend itself to integrate with Network Operations Centre services?
   d. How does your solution extend itself to integrate with Security Operations Centre services?

Section VII: Business Intelligence and Reporting

1. Describe your solution's capabilities to support business intelligence and reporting, inherently or via third-party vendors.
2. How does your solution lend itself to meet internal/external auditing and reporting requirements?

Section VIII: Offline CBDC

1. Describe your solution's capabilities to facilitate offline transactions either out-of-the-box or via third-party vendors.
2. Please highlight risk mitigations to counter the security risk posed by operating an offline CBDC.
3. Describe your solution's approach to security for offline payments including aspects such as, but not limited to, addressing consecutive transactions, extended duration offline, and other concerns.

Section IX: Security

1. Describe your system's protection against double spending, counterfeiting and other fraudulent activities.
2. Describe any other fraud detection capabilities of your system.
3. Describe your approach to protecting user data?
    a. How does your system limit sharing of sensitive information amongst various parties/ stakeholders in the system?
4. Describe the authentication mechanisms supported by the system?
    a. What specific measures are in place to support multi-factor authentication?
5. What compliance frameworks, such as ISO or NIST, does the system adhere to as designed and implemented?
6. Describe your solution's approach to cryptography covering areas such as,
    a. Encryption Algorithms
    b. Hash functions
    c. Key derivation mechanisms.
    d. Cryptography agility.
    e. Quantum computer resistance.
7. Describe your solution's approach to encryption key management including:
    a. Key rotation and password changes
    b. Wallet key custody.
    c. Recovery should users lose access to their CBDC wallet.
8. Describe the history and ongoing approach to security audits and penetration testing on your solution.
9. Describe the processes involved in revocation of access of solution providers?
10. Describe offboarding process for various entities including key intermediaries such as Financial Institutions, wallet/payment service providers?

Section X: Anonymity and Privacy

1. How are retail users and merchants identified within the solution and by each other?
2. Please describe if aliases may be allowed and how it may be accomplished?
3. What data protection and privacy legislation does the solution comply with?
    a. Are the privacy settings within the system configurable?
    b. Which jurisdiction/s have the solution been deployed and tested in? If none, what regulatory regime/s were considered in the design of the solution.
4. How does the system ensure that the Central Bank does not have direct access to payment transactions information and Personally Identifiable Information ("PII")?
    a. Given this constraint, how does the solution ensure necessary information can be made available to authorities under specific circumstances (e.g., investigations, legal requirement)?
5. Please describe the system's capability to support anonymous transactions (where the user's identity is not known to any participant in the solution) up to a predefined limit?
6. Which entities within the system would have access to retail financial transaction data?
    a. How are sender and recipient privacy protected?
7. Are account balances and transaction details only known to the user?
    a. If, yes how are these data protected. Please explain in relation to various stakeholders including, but not limited to, transaction counterparty, financial institutions, payment services providers, merchants, the Bank.