Bank of Israel
May 2025

The Digital Shekel

Technological Consultations Series

Table of Contents

Introduction

The Bank of Israel published its Preliminary Design for the Digital Shekel System[1] on March 3, 2025, (the “Preliminary Design”) a multi-purpose Central Bank Digital Currency (CBDC) system that will address both the retail needs of end users such as households and businesses, as well as the wholesale needs of financial entities. The design is technologically agnostic.

The Bank of Israel is now seeking consultation from technology experts, academics, and potential vendors ("Respondents") regarding methods to achieve the capabilities of the Digital Shekel System. While the Bank has not made a decision whether it would or would not issue a CBDC in the future, the purpose of this process is to deepen the Bank’s knowledge regarding the technological feasibility of the design and the technologies that are expected to be available to implement key components of the design.

For that purpose, the Bank is publishing a series of six technological consultation (TC) topics regarding the following components of the Digital Shekel System:

TC1: Backend Layer[2]

TC2: Secure Transaction Messages and Communication

TC3: Offline Capabilities

TC4: Payment Authorization - Secure Containers & Cryptographic Key Management

TC5: Alias Management System

TC6: Fraud Monitoring System

As depicted in **diagram 1**, these components comprise a single digital shekel system and therefore must allow integration and interoperability.

Respondents should be familiar with the Preliminary Design and are encouraged to suggest innovative technological solutions to the overall design and requirements. We emphasize that the

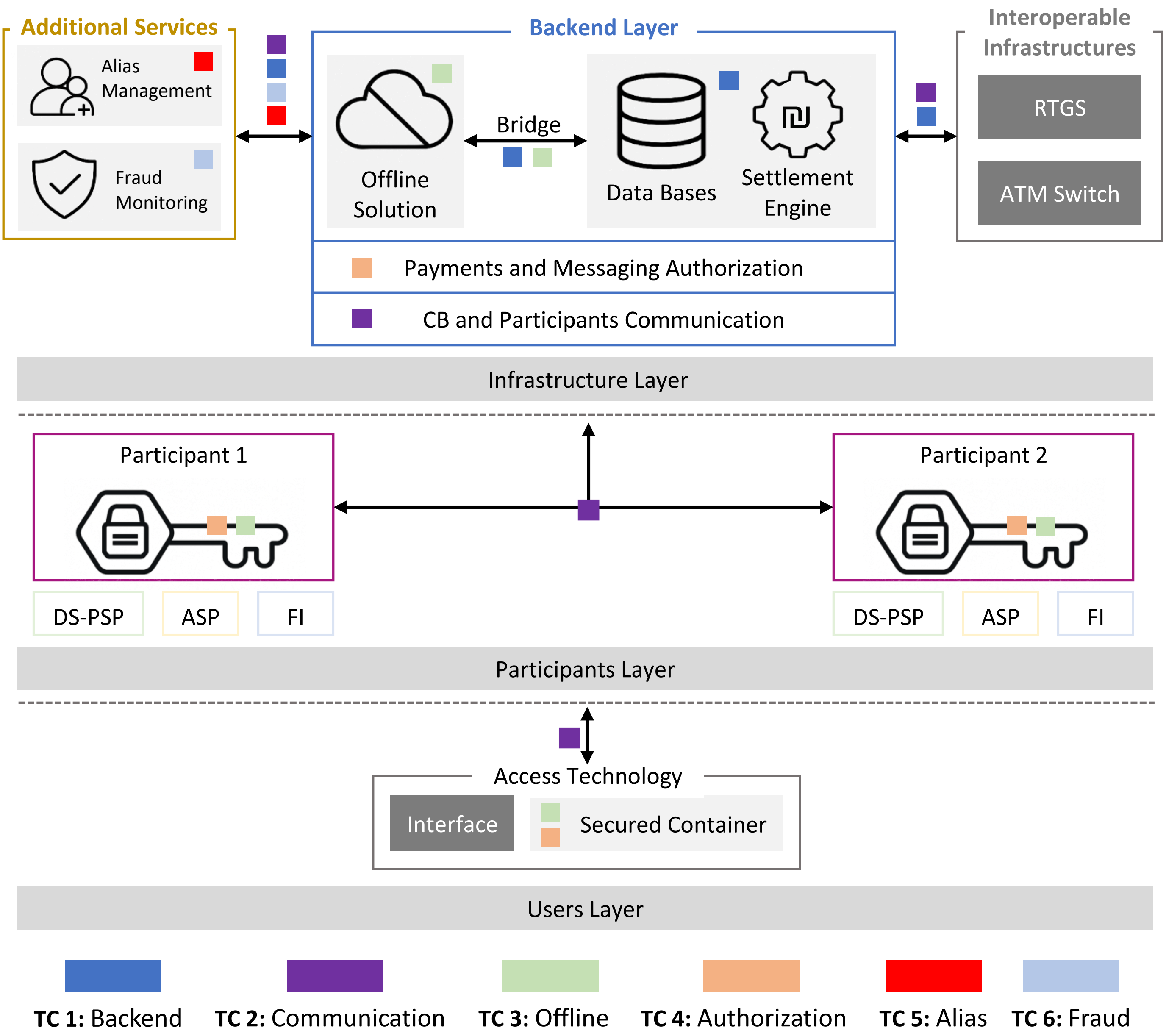
[1] “Preliminary Design for the Digital Shekel System”, available at: https://www.boi.org.il/media/54dpz1ew/initialPreliminary-design-for-the-digital-shekel-system.pdf (English). Also available in Hebrew. All page references to the Preliminary Design along this document are to the English version.

[2] Capitalised terms represent terms that are defined in the Preliminary Design.

Bank of Israel has not made any decisions regarding how best to technically implement the Digital Shekel System.[3]

Similarly, desired functionality may be addressed at different layers of the technology stack and we welcome discussion as to the appropriate layer where a given capability should reside. We welcome all responses that are consistent with the logical design and considerations contained in the Preliminary Design.

Diagram 1 - Components in scope for each Technological Consultation



[3] The use of terminology such as "balances," "databases," "wallets," or "tokens" should be construed broadly rather than suggesting certain technological implementations. CBDC and the Digital Shekel System may be based on any technology, and specifically are not limited to Distributed Ledger Technology (DLT).

For any or all of the six TCs, Respondents are invited to explain how the proposed technology or solution enables or allows the desired functionality, and to the extent possible, what requirements or challenges the proposed technology or solution attempts to solve. Additionally, where feasible, Respondents are invited to provide an estimate (or range) of the cost of implementation of suggested technology for an economy the size of Israel, taking into consideration setup costs as well as ongoing operating costs.[4] Other technological features such as flexibility to changes and upgrades, scalability as the user base increases and more use cases are introduced, should be addressed. Responses should include any constraints and assumptions that the technology solution they raise relies upon – e.g., if the solution only applies to Distributed Ledger Technologies, or any other restrictions.

To provide further information regarding the process and answer questions, the Bank of Israel will host a webinar (in English) on May 21, 2025 at 16:00-17:15 Israel time (9:00-10:15 EST, 15:00-16:15 CET). Interested parties can register to participate in the webinar through the following registration link.

This consultation process is a critical step in assessing the potential for a future Digital Shekel, and supporting an informed future decision regarding the issuance of a digital shekel.

The Bank of Israel looks forward to collaborating with potential vendors and experts to explore innovative solutions for the Digital Shekel System.

[4] See elaboration in section "General Description of the Suggested Solution" and footnote 5 below.

How to Respond to the Consultations

Responses should be submitted no later than June 30, 2025, in Word or PDF format, by email to digitalshekeltc@boi.org.il. Responses are to be submitted in English.

The consultations are addressing technology experts, academics, and potential vendors regarding methods to achieve the capabilities of the Digital Shekel System. Respondents are welcome to respond to one or more of the consultations; The Bank is expecting that some experts or vendors may have knowledge or solutions in only one or even in only some aspects of one consultation topic, whereas others may be offering full-fledged solutions covering all components of a potential CBDC system, and therefore relating to several or even all consultation topics. However, if responding to more than one consultation, each response should be submitted in a separate Word or PDF document, which may be sent in one or more email messages.

Each response should be structured as follows:

1. Consultation number and title (e.g. – TC1: Backend Layer)

2. Information regarding respondent:

    a. For Individual or Academic Respondents:

    - Individual's name and contact information (i.e. email address);
    - CV or description of experience and qualifications on CBDC-related projects, payments, or other relevant topics;
    - Academic affiliation (if applicable).

    b. For Company Respondents:

    - Company name, address, and website;
    - Representative's name and contact information (i.e. email address);
    - Brief background and description of the company;
    - Description of relevant experience;

3. General Description of the Suggested Solution:

    - **Executive summary** that provides the most important points the Respondent desires to make (**up to two pages**);

- **Detailed description of the proposed solution**, components, or capabilities, including justification or explanation as to the rationale behind the design or configuration of the proposed solution, components, or capabilities with regards to the consultation topic (**up to ten pages**). Please indicate whether the response includes trade secrets or commercial secrets.
- Where feasible, provide an estimate (or range) of the cost of implementation of suggested technology for an economy the size of Israel, taking into consideration setup costs as well as ongoing operating cost[5] (**up to one page**).
- Any further relevant information can be submitted in annexes.

What to Expect

All response submissions will be reviewed by the project team within several weeks after the submission deadline (June 30, 2025).

The Bank may, in its sole discretion, contact all or some of the Respondents for follow-up discussions regarding their responses or with a request to clarify or to complete information, to make a presentation or a demonstration, or to receive any information that it considers vital in order to further understand that response.

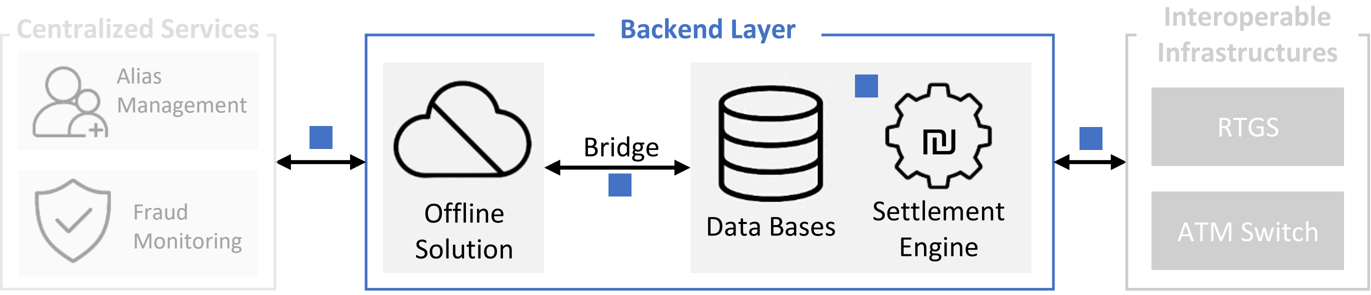
Analysis of the responses and follow up discussions is expected to be concluded by the end of 2025 or earlier. The Bank of Israel will not publically disclose information submitted to it by individual respondents or the content of individual responses. The Bank may publish aggregate analysis of the consultation responses but it does not commit to doing so. In later stages, the Bank may also, at its sole discretion, carry out Proof of Concepts (PoC) with some of the respondents.

[5] Please note that the cost estimation is solely for obtaining a preliminary understanding and to support an overall cost-benefit analysis of the digital shekel, and will not, under any circumstances, constitute a binding offer.

Disclaimers

1. This Technological Consultation is not a form of public tender or other binding process, and it does not incorporate any obligation whatsoever for the Bank to continue or to act in any purchase process.
2. Submission of a response to the Technological Consultation or any other additional information as described above, in itself will not prohibit the Respondents to submit responses to any RFI, RFP, or other tender if and when the Bank of Israel would publish in the future. In addition, it will not create a conflict of interest for that matter.
3. The framework of this Technological Consultation is not, in any form, creating a contract or any other legal relationship between the Bank and any of the Respondents. The Bank's right, in its sole discretion, to contact the Respondents as described above, will not create any type of obligation on the part of the Bank toward any of the Respondents.
4. The Respondents to this Public Consultation will bear all the expenses involved in preparing the response and will not be eligible for any reimbursement or compensation for these expenses.
5. The Bank has the right to accept a response even if it does not fulfill certain formal or technical requirements, if it decides, in its sole discretion, that there are specific reasons to justify this.
6. The Bank reserves the right, at any time, to make changes or corrections to this Technological Consultation, whether on its own initiative or as a result of a request of any third party. The changes or corrections to the Technological Consultation will be made public on the Bank’s website. It is the responsibility of the Respondents to check the Bank’s website from time to time to ascertain if changes have been made to the Technological Consultation and to modify their response to the changes, if there are any.

Technological Consultation 1 – Backend Layer



At its core, the System Operator[6] operates the Backend Layer[7] that ultimately authorizes and records changes to balances in the end users' digital shekel wallets.[8] The System Operator provides the technical means for the System Manager[9] to fulfil its role of ensuring the proper management of the system, including supervising the various Participants'[10] activities concerning the scheme rules, resolving disputes between participants, and other responsibilities.

The Backend Layer primarily consists of[11]:

1) a main/primary database that includes only the minimal information required to fulfil the technical roles of the System Operator namely:
   a. settling payment transactions;

[6] **System Operator -** The entity that operates the technological infrastructure according to the scheme rules and the terms of engagement with the system manager. The system operator will be the central technological entity with which most technological engagements of the various entities will be conducted. The Bank of Israel, or an entity appointed by it, is expected to fulfil this role.

[7] **Backend Layer –** The system components required by the system operator to perform its functions in the digital shekel system, including the necessary and/or derived databases from these actions (including the main database containing the balances in all end-user wallets). In particular, the backend will include the "settlement engine" - the component that enables the transfer of digital shekels as a result of a payment between two wallets - and the main database.

[8] A **wallet** is defined as a compartment in the digital shekel database where balances of digital shekels (and only digital shekels) are recorded.

[9] **System Manager -** The entity that defines the scheme rules and is responsible for the proper management of the system, including supervising the various participants in their activities concerning the scheme rules, resolving disputes between participants, etc. The Bank of Israel is expected to fulfil this role.

[10] A **Participant** is an organization that plays a role in the digital shekel system and is bound by the system's scheme rules. They have a direct relationship with the System Manager and System Operator. So far, the following types of participants have been defined for the digital shekel system: Digital Shekel Payment Service Provider (DS-PSP or PSP), Funding Institution (FI), and Additional Services Provider (ASP).

[11] Preliminary Design, pg. 101, section 6.1.

   b. enforcing or enabling the enforcement of policies (i.e., holding limits[12] or interest payments[13], and other policies that may differ based on certain characteristics of the transaction, the Participants, or other metadata);
   c. generating operational and statistical data (consistent with privacy principles).

2) a settlement engine which does not store information but instead acts in a stateless method to update and use the main/primary database, as well as other databases such as the participant database and the transaction database, and;
3) Integration into other components of the system and interoperability with external systems[14].

High Level Design Considerations

As discussed in the Preliminary Design, the Backend Layer should address the following items:

- Privacy – The System Operator operating the Backend Layer should not be able to identify the end-users or obtain any other personally identifiable information ("PII")[15].
- Additional data management for: [16]
  - Proper functioning of the system;
  - Perform statistical analysis of the adoption and use of the digital shekel;
  - Support conflict resolution between Participants;
  - Analyze policy measures and their impact on system activity (e.g., the application of interest, changing holding limits, etc.);
  - If desired in the future, for the System Operator to charge fees from PSPs, Fis, and ASPs according to transaction type.[17]
- Aggregated Transaction Database[18]
  - Allow comprehensive analysis of the characteristics of system activity;
  - Importantly, this should not allow the linking of transactions to wallets or end-users.

[12] Preliminary Design, pgs. 124-127, section 7.6.
[13] Preliminary Design, pgs. 128-131, section 7.7.
[14] Preliminary Design, pgs. 75-88, section 5.1.
[15] Preliminary Design, pg. 112, section 7.1.
[16] Preliminary Design, pg. 102, section 6.1.
[17] The System Operator retains the option to charge various fees from FIs, PSPs, and ASPs. Preliminary Design, pg. 116.
[18] Preliminary Design, pgs. 102-103, section 6.1.

- Participant Database[19]
    - Unique identifier, name and type of Participant, and any relevant data regarding the Participant.
- Interoperability with the existing domestic RTGS system[20];
- Interoperability with "Offline Digital Shekel Issuance Engine" and "Central Offline Wallet" functions;[21]
- Interoperability with cash-related systems for the conversion of cash to digital shekels[22];
- Equal Provision of Service – The Backend Layer should enable and ensure that end users of different PSPs enjoy the same performance standards regardless of which PSP they use[23].

Component - Primary Database

- secure payment transaction settlement solution;
- the enforcement of policies[24], including holding limits on a per end-user basis[25], enabling interest payments, etc.;

Component - Settlement Engine[26]

- the enforcement and management of rules and policies to decide whether and how to update the balances of wallets;
- immediacy and finality of payments;
- conditional payments that are based on external events or third-party approvals (including locking, unlocking, scheduled, batch, etc., using technologies like HTLC, oracles, or third-party decision-makers)[27];

[19] Preliminary Design, pg. 103, section 6.1.
[20] Preliminary Design, pg. 103, Figure 4.
[21] Preliminary Design, pg. 97, section 5.3.
[22] Preliminary Design, pgs. 65-67, section 4.3.2.
[23] Preliminary Design, pgs. 109-110, section 6.3.
[24] The enforcement of policies may reside at the Primary Database component and/or the Settlement Engine component.
[25] We recognize that the capability of enforcing policies, including holding limits, on a per end-user basis where end-users could have multiple wallets may be at odds with the strong privacy considerations outlined in the Preliminary Design and we encourage respondents to address these challenges.
[26] Preliminary Design, pg. 101, section 6.1.
[27] Preliminary Design, pgs. 88-89, section 5.2.

Integration, Interoperability, or Compatibility

- fraud monitoring system;
- alias management system[28];
- domestic RTGS;
- domestic ATM switch;[29]

Additional Scope

- coordination and use of one or more wallets per unique identifier, with each wallet able to be interacted with by one or more PSPs[30]
- conflict resolution mechanisms between Participants (e.g., sufficient audit information);[31]
- both very high transaction throughput and low latency with both micropayments and large payment amounts;
- ensuring need-to-know-only access to information and addressing privacy[32] considerations throughout the system, including the prevention of access to personally identifiable data by the System Operator and System Manager;
- supporting differing privacy requirements depending on the user type (i.e., an individual versus a PSP);
- the generation and collection of operational and statistical data regarding the system, while balancing privacy considerations;
- access for both citizens and non-citizens, with varying onboarding information available[33];
- supporting both asynchronous and synchronous payments, supporting payment universality by allowing payments to and from any access technology to another access technology[34];

[28] The Preliminary Design indicates a desire for separation-of-duties whenever possible to reduce centralization of data that could otherwise unmask the identities or transactions of end-users. The Alias Management component operated by a different operator than the Primary Database is one such example whereby the Alias Management component generates a unique identifier that is then used by the Primary Database. Preliminary Design, pg. 57, section 4.1.

[29] Funding a Digital Shekel wallet with cash while preserving privacy is a unique use case that requires coordination between multiple entities, and is further described in section 4.3.2, pg. 65, of the Preliminary Design.

[30] Preliminary Design, pgs. 57-58, section 4.1.

[31] Preliminary Design, pg. 102, section 6.1.

[32] Preliminary Design, pgs. 112-113, section 7.1.

[33] Preliminary Design, pg. 56, section 3.4.3.

[34] Preliminary Design, pgs. 59-61, section 4.2.

- supporting 24/7/365 operation with minimal disruption and high availability;
- having minimal single-transaction, worst-case latency for finality and settlement of no more than a few seconds[35];
- supporting waterfall and reverse waterfall operations;[36]
- supporting or use a common messaging format such as ISO 20022;[37]
- supporting horizontal and vertical scaling; [38]
- supporting a distributed deployment for resiliency.

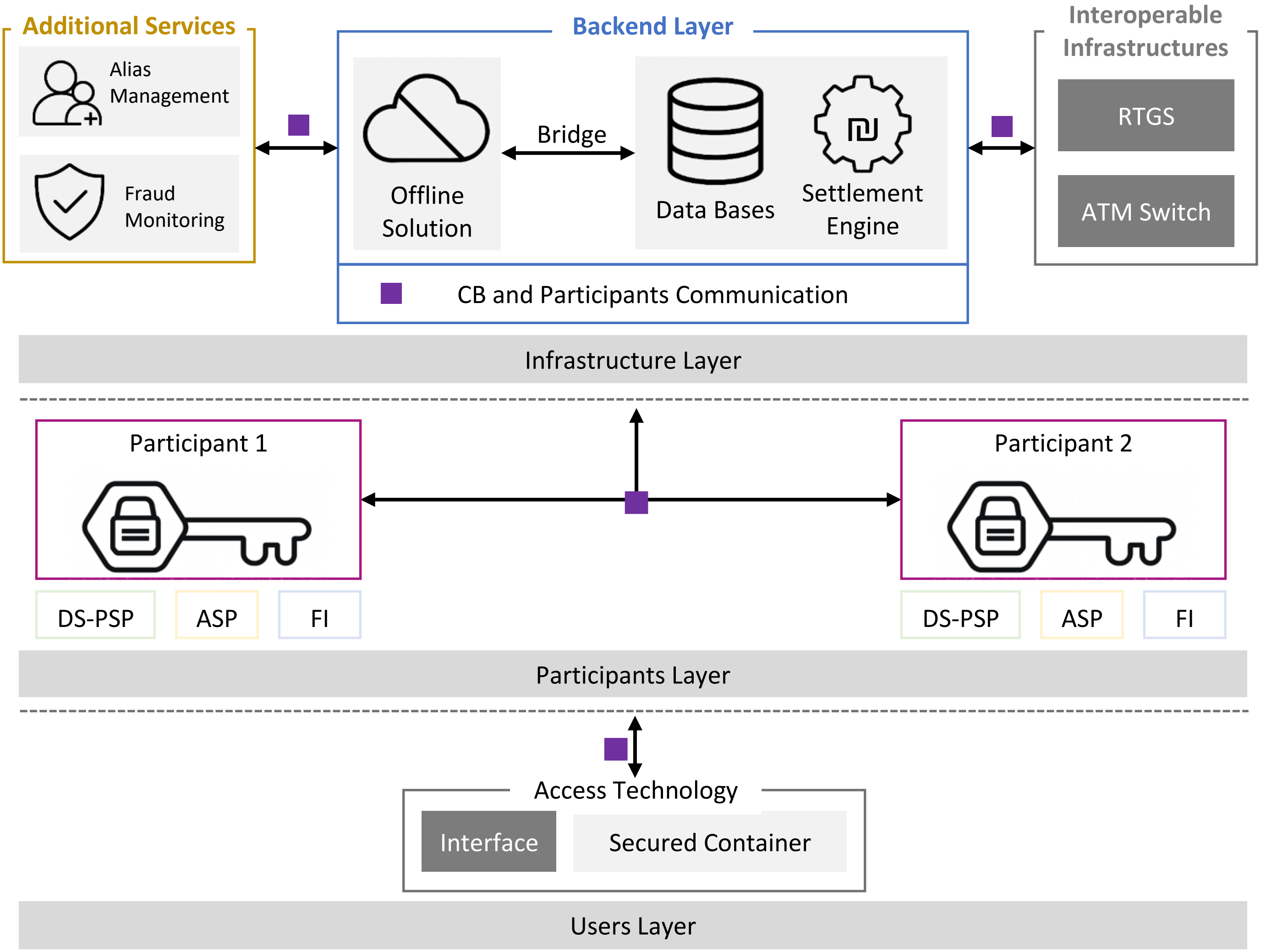
[35] Preliminary Design, pg. 110, section 6.3.

[36] *See* Preliminary Design, section 4.3.1, pg. 63, for a description of the "waterfall" and "reverse waterfall" workflow.

[37] Preliminary Design, pg. 106, section 6.2.

[38] Preliminary Design, pgs. 110-111, section 6.3.

Technological Consultation 2 – Secure Transaction Messages and Communication



This technological consultation seeks respondents to address the communication, messages, and information between two sets of entities:[39] between Participants and the operators of centralized services in the ecosystem (i.e., the Backend Layer's settlement engine[40], the Alias Management

[39] As described in section 6.2 of the Preliminary Design. Specifically, an example of the anticipated message flow is contained in on pg. 105.

[40] "**Settlement Engine**" - the component that enables the transfer of digital shekels as a result of a payment between two wallets - and the main database.

System[41], and the Fraud Monitoring System[42]), and between Participants[43] (PSPs, FIs, and ASPs) themselves. The scope includes the protocol, standards, networking, and other all technical aspects required to communicate necessary information for the system to operate with high levels of privacy, compliance, performance, scalability and reliability.

The scope also includes the technical structure of the payment message[44] (and related messages/payloads), the method of transmission between entities (i.e., hub-and-spoke through potentially the Backend Layer, peer-to-peer, and other communication models), and the information each entity in the sequence of transmission, relaying or communication will have the ability to access. For clarity, except for data required by the Backend Layer, this TC does not necessarily cover the payment messages or communication between Participants and end-users such as for traditionally retail transactions (e.g., point-of-sale terminals or mobile banking applications);[45] PSPs may adopt different mechanisms for interacting with their end-user customers.

Secure transaction messages and communications, separate from payment settlement, are required to support significant use cases including conditional payments that may use time-based business logic, user and usage-based business logic, and external conditioned based logic (i.e., two- or three-party locks, or hash-time lock contracts (HTLC)).[46] Other innovative use cases may include the sharing of transaction-related data like invoices, receipts, or asset settlement data.

High Level Design Considerations

While the specifics of certain aspects of communication messages may be determined technically based on the Backend Layer[47], this TC addresses additional topics related to a payment transaction

[41] Preliminary Design, pgs. 36-37, section 3.2.1.
[42] Preliminary Design, pg. 37-38, section 3.2.2.
[43] A "**Participant**" is an organization that plays a role in the digital shekel system and is bound by the system's scheme rules. They have a direct relationship with the System Manager and System Operator. So far, the following types of participants have been defined for the digital shekel system: Digital Shekel Payment Service Provider (DS-PSP or PSP), Funding Institution (FI), and Additional Services Provider (ASP).
[44] For example: JSON, XML, or other structures for the transmission of data.
[45] To support a wide range of use cases and encourage innovation, the message structure should support extensibility.
[46] Preliminary Design, pgs. 91-92, section 5.2.1.3.
[47] As an example, the Preliminary Design anticipates that a request to the settlement engine to perform a transaction from a wallet should be authorized by the private key held solely by the end user. *See* Preliminary Design, pg. 69, section 4.4. That means that the Backend Layer may define the data and the data's format

on the Digital Shekel System. It seeks to understand how information that may be transmitted may be communicated on a need-to-know basis while allowing the participants to perform their responsibilities within the system.

Components[48]

- API & message architecture
- Authentication and authorization (of messages and additional data)
- Security, availability & resilience

Additional scope

- Definition of the structure of the payment messages (and other messages)
- Mandatory and optional data support, for example:
  - Basic identifying details about the wallets or end-users involved in the payment transaction and the Participants involved in it;
  - Support necessary data for compliance (i.e. AML / Travel Rule[49])
  - Inclusion of additional details such as broader identifying information about the users and participants, and additional information that may be required for different types of transactions (e.g., the payee's ID number in the case of salary payments, the participant's wallet details for cross-fee payments, etc.)
  - Optional information items
- The method of transmission between Participants and to/from the Backend Layer
- The information the communication chain exposes to each entity – logical and physical separation of data (i.e., layers of encryption or peer-to-peer transmission)
- Compatibility with international standards like ISO 20022 (or others)
- Maximum flexibility with support for differing access rights to data, i.e., certain information to be shared with the Fraud Prevention System[50] without being read or exposed to other systems or entities;
- Hub-and-spoke, point-to-point and other communication models;
- Resilient routing protocols and methods;

required for authorization, but that data will need to be reliably and securely transmitted from the end-user, through the PSP, to the System Operator.

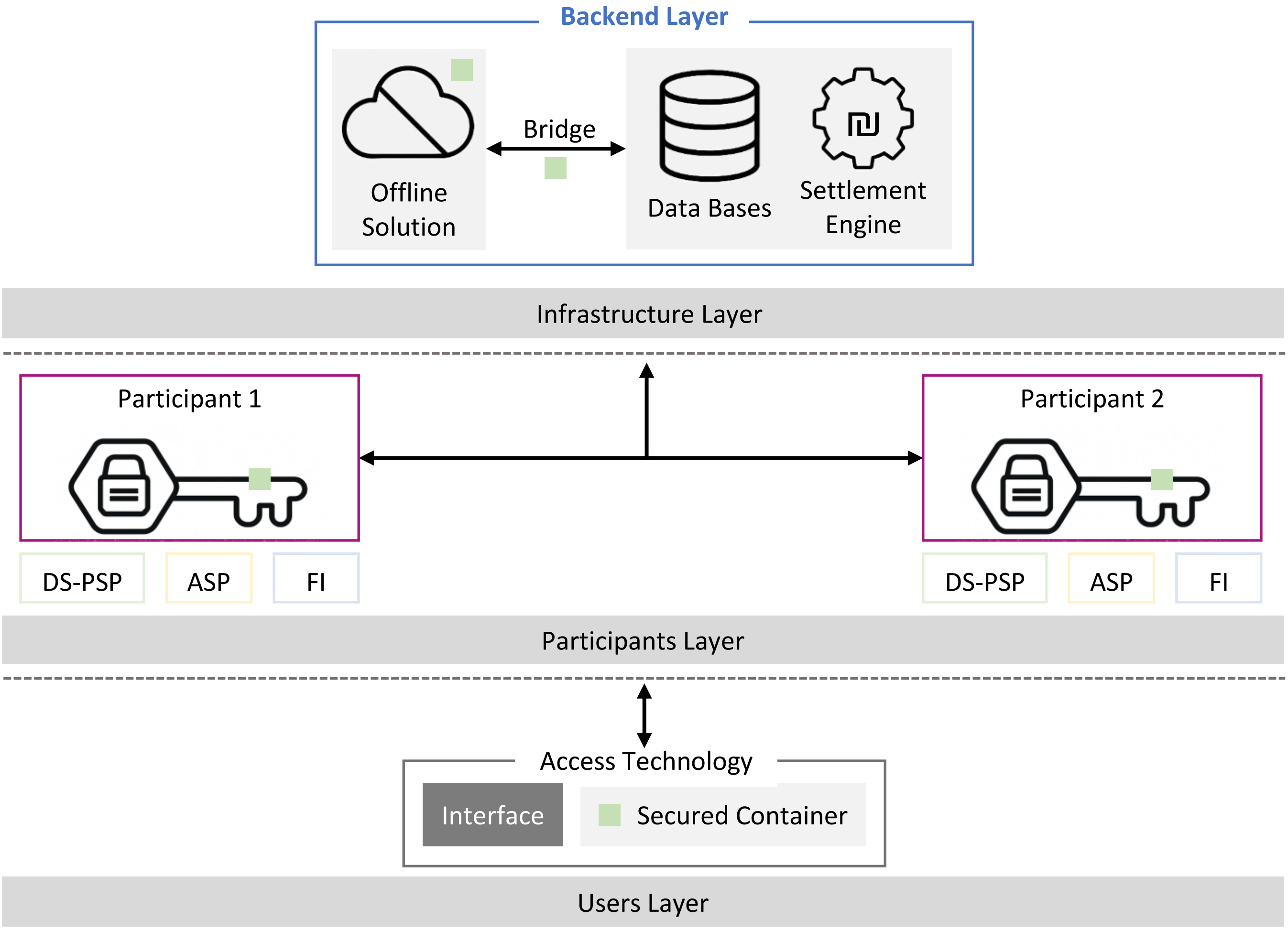
[48] Preliminary Design, pgs. 105-108, section 6.2.

[49] Preliminary Design, pgs. 119-121; section 7.4.

[50] Preliminary Design, pg. 38, section 3.2.2.

- Support for <u>both</u> high volume (i.e., micropayments) and/or high value (i.e., wholesale payments) transactions;
- How to support additional use cases that require authentication/authorization at the communication layer (not the payment settlement), such as exchanging payment related data like electronic invoices, data necessary for payment locking/unlocking/HTLC, etc.

Technological Consultation 3 – Offline Capabilities



This technological consultation is limited to technologies supporting payments without communication with end-users'[51] PSPs and without communication with the Backend Layer,[52] otherwise known as offline payments. Offline payments are innovative, technically complex, and significantly different than existing payment technologies due to unique security considerations.

[51] **End Users -** Anyone who can hold a balance and perform payment transactions with the digital shekel: individuals and organisations (businesses, non-profits, government offices, etc.). Participants in the system may also hold a wallet(s) and act as end users. An end user is the owner of the digital shekels in their wallet.

[52] **Backend Layer –** The system components required by the system operator to perform its functions in the digital shekel system, including the necessary and/or derived databases from these actions (including the main database containing the balances in all end-user wallets). In particular, the backend will include the "settlement engine" - the component that enables the transfer of digital shekels as a result of a payment between two wallets - and the main database.

The technology that supports offline payments is a subset of the anticipated Access Technologies that include a secure container and usually a user interface.[53] Two types of offline payment hardware are anticipated: [54]

- Active communication – hardware includes a power source that allows communication between devices (e.g., a smart phone with Bluetooth or NFC);
- Passive communication – hardware does not include a power source or the ability for independent communication (e.g., a smart card with a cryptographic chip);

On the Backend Layer, the Preliminary Design anticipates that the Backend Layer will account for the representation of the total holdings in offline digital shekel wallets.[55] The corresponding offline balances will be stored in the secure containers[56] of the access technology of end-users such as smart-phones, smart cards, and other devices.

High Level Design Considerations

- Provisioned by PSPs for end-users, but the System Operator[57] will set standards for offline technology
- Support online to/from offline funding and defunding operations for an end-user; support offline to offline payments from end-user to end-user[58]
- Support for preventing, detecting, and remedying unauthorized or disallowed offline transactions;[59]
- Support dispute resolution (e.g., non-repudiation of transactions)

[53] Access Technologies include: 1. Smart phones; 2. Smart cards, limited-functionality phones, or other dedicated devices; 3. Point of Sale (POS), and; 4. Cloud-based interface (cloud API). Offline payments will be supported on only some of these technologies. Preliminary Design, pgs. 59-60, section 4.2.

[54] Preliminary Design, pg. 99, section 5.3.

[55] *Id.*

[56] **Secure container** is responsible for 1) secure storage of sensitive information such as private keys, and 2) initiating transactions securely. See Figure 7, Preliminary Design, pg. 61, section 4.2. It may operate on the same device as the user interface, in the cloud, or in a hybrid manner.

[57] **System Operator -** The entity that operates the technological infrastructure according to the scheme rules and the terms of engagement with the system manager. The system operator will be the central technological entity with which most technological engagements of the various entities will be conducted. The Bank of Israel, or an entity appointed by it, is expected to fulfil this role.

[58] Preliminary Design, pgs. 97-98, section 5.3.

[59] Preliminary Design, pg. 96, section 5.3.

- The lifecycle of rules and limits including methods of detection and enforcement regarding offline transactions (i.e., holding limits,[60] transaction number and volume limits, freezing, time-based limits, user-type limits, synchronization requirements, etc.);[61]
- Storage limitations and constraints;
- Both system-wide and PSP configured rules, policies, and restrictions;
- Supporting anonymous and non-anonymous offline payments, with the technology recognizing the difference between the two types;[62]
- The synchronization of information regarding offline transactions;[63]
- Interoperability with systems to withdraw and deposit offline Digital Shekels to and from cash through ATMs;[64]
- Innovative offline use cases (e.g. machine to machine payments, micropayments. large value payments, etc.).
- Third-party fee tracking and collection.

[60] Preliminary Design, pgs. 124-127, section 7.6.

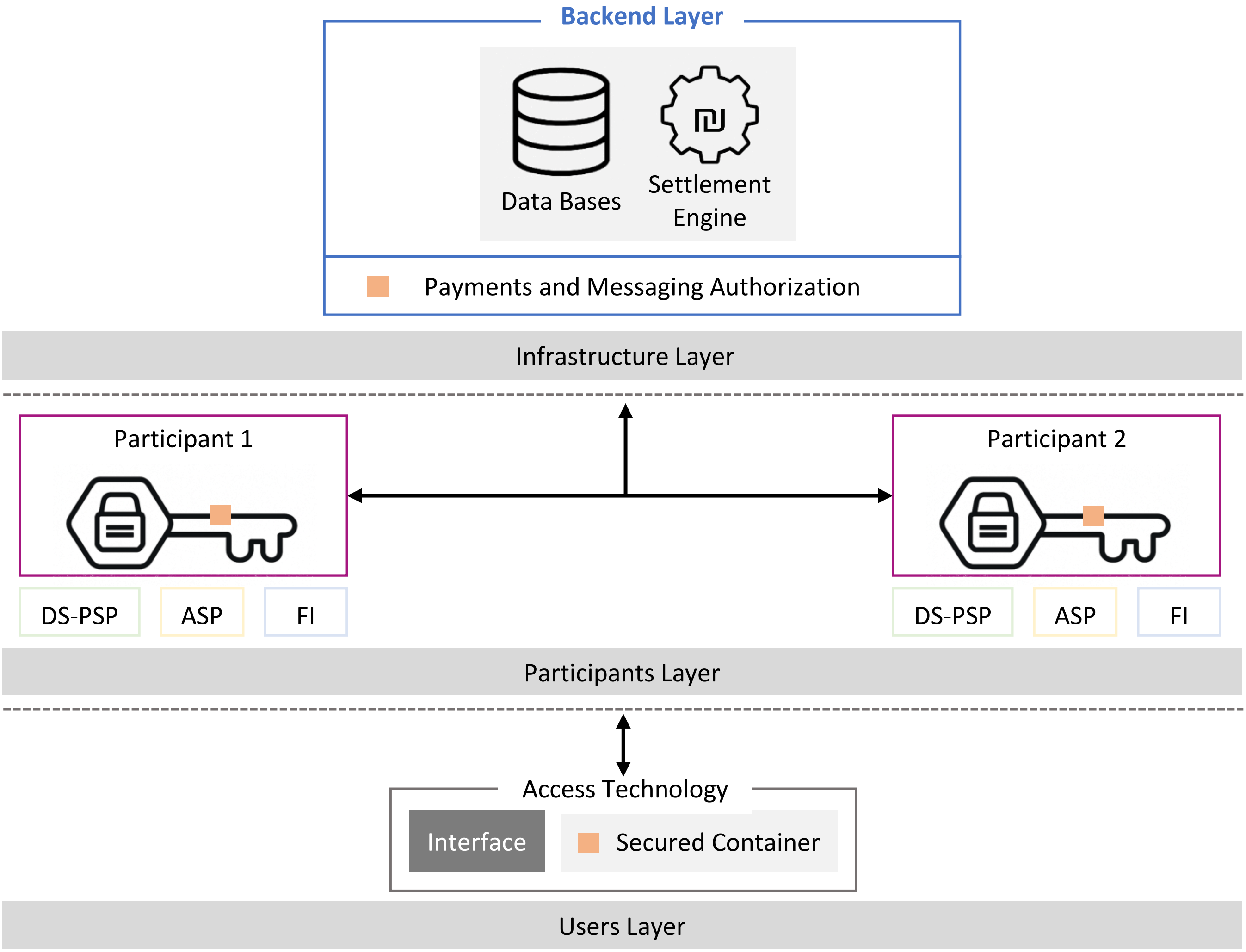
[61] Preliminary Design, pgs. 93-94, section 5.2.2.

[62] Preliminary Design, pgs. 97-99; Section 5.3.

[63] Respondents should address the benefits and trade-offs associated with storing transaction related data on offline devices that may (or must) eventually connect online. Aggregate data may provide monitoring capabilities to a similar level as transactions on the online system, even if such analysis must be performed post-factum. *See* Preliminary Design, pg. 98, section 5.3.

[64] The workflow for ATM funding/defunding is in Preliminary Design, pg. 65, section 4.3.2.

Technological Consultation 4 – Payment Authorization - Secure Containers & Cryptographic Key Management



This technological consultation seeks information regarding the primary methods to authorize payments at the Backend Layer[65] of the Digital Shekel system, namely through the use of cryptographic public-private keypairs and cryptographic digital signatures in secure containers.[66] Secure Containers enable the secure lifecycle of cryptographic keys that allow transactions to be

[65] **Backend Layer –** The system components required by the system operator to perform its functions in the digital shekel system, including the necessary and/or derived databases from these actions (including the main database containing the balances in all end-user wallets). In particular, the backend will include the "settlement engine" - the component that enables the transfer of digital shekels as a result of a payment between two wallets - and the main database.

[66] Preliminary Design, pg. 68-69, section 4.4.

performed from the end user's wallet on the Backend Layer, including: a key's generation, registration, storage, distribution and installation, use, rotation, backup, recovery, revocation, suspension, and destruction. Secure Containers along with a user interface comprise the Access Technology.[67] This technological consultation primarily focuses on online payments, as offline payments have additional considerations that should be responded to separately in Technological Consultation 3.

While the Preliminary Design anticipates that PSPs will provide the Access Technology[68] to end-users, the Bank of Israel desires to be informed regarding the existence of best-available technology, processes, and techniques that should be used within the Digital Shekel system so as to set standards[69] and inform decision making on other capabilities and components of the system like the Backend Layer.

Three types of Secure Containers are anticipated:[70]

1. On an edge device with a user interface (online or offline) – i.e., a smart phone, smart card;
2. External to the device with a user interface – i.e., Secure Container in the cloud;
3. A hybrid approach – i.e., Secure Container in the cloud, approval on smart phone; multi-party computation (MPC), key splitting, and other multi-step authentication.

Therefore, information is sought to address the wide variety of ways Secure Containers may be implemented, including addressing the following items:

- Cryptographic key lifecycle management[71] & Secure Container design;
- Authentication & authorization;
- Secure hardware & device-level protection;
- Preferable cryptographic algorithms (i.e., ECDSA, EDDSA, and quantum-resistant algorithms) and trade-offs

[67] Preliminary Design, pg. 59, section 4.2.
[68] **Access Technology –** The hardware and/or software that allows end users to perform payments and manage their digital shekel balances. An access technology includes a secure container and usually also a user interface.
[69] Preliminary Design, pg. 60, section 4.2
[70] Preliminary Design, pgs. 59-61, section 4.2.
[71] Hardware managing cryptographic keys should address or enable secure processes for all items of the key's lifecycle including a key's generation, registration, storage, distribution and installation, use, rotation, backup, recovery, revocation, suspension, and destruction.

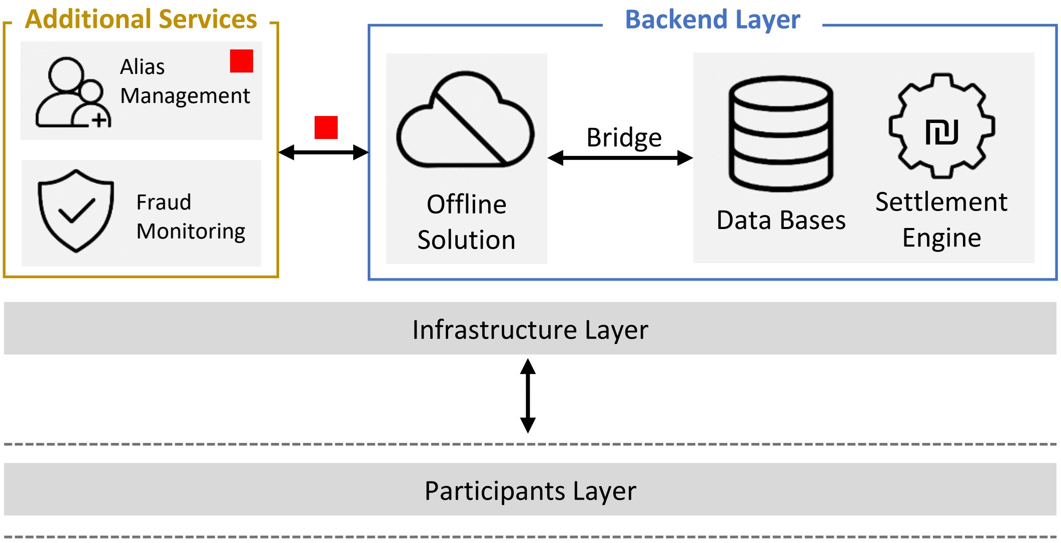
- Privacy-preserving technologies;[72]
- Compliance & interoperability standards.[73]

High Level Design Considerations

- To the extent possible, the Secure Container should be technologically agnostic to the Backend Layer;
- Support for asynchronous payments, without any interaction between the payer and payee's access technology;
- Support for synchronous payments which require positive user interaction by the payer or both the payee and payer;
- Compatibility with existing hardware (smart phones, PoS terminals);
- Ensuring that a PSP cannot initiate a payment without explicit authorization from the end user. This feature will be enforced not only by the system's rules but also technically.[74]
- Compliance with international hardware security standards.

[72] Preliminary Design, pg. 113-114, section 7.1.
[73] Preliminary Design, pg. 75-81, section 5.1.
[74] A technical solution will be provided for special situations where a transaction needs to be performed without the end user's authorization – for example, to enforce judicial orders such as inheritance or seizure orders

Technological Consultation 5 – Alias Management System



The success of the digital shekel will depend on the ability of end-users[75] to make payments in a simple and accessible way. To facilitate this, end-users should be able to send and receive digital shekels using an alias[76] (such as a phone number or email address) without needing to know the details of the other end-user's Payment Service Provider (PSP) or wallet details.[77] This service will allow end-users, through system participants[78], to use an alias-based, wallet-lookup service that provides the minimal amount of information required to initiate a digital shekel transaction to the relevant participants.

[75] **End Users -** Anyone who can hold a balance and perform payment transactions with the digital shekel: individuals and organizations (businesses, non-profits, government offices, etc.). Participants in the system may also hold a wallet(s) and act as end users. An end user is the owner of the digital shekels in their wallet.
[76] **Alias –** An easy-to-remember or retrieve nickname, such as a name, phone number, or email address of the end user linked to their wallet. The alias allows payments between end users without needing to specify the identifier, which may be a complex sequence of letters and numbers.
[77] **Digital Shekel Wallet –** A compartment in the digital shekel database where balances of digital shekels (and only digital shekels) are recorded. The wallet is used to perform funding, defunding, and payment transactions in the digital shekel system. There cannot be a negative balance in the wallet. The wallet is linked to the user's unique identifier, and the user's access to the wallet will be through a payment service provider. A user can hold multiple digital shekel wallets linked to their unique identifier. They can link a wallet or multiple wallets to multiple payment service providers or link multiple wallets to a single payment service provider.
[78] PSPs, ASPs and FIs

The Alias Management System may also allow segregation of duties in the Digital Shekel ecosystem. The Preliminary Design anticipates that the Alias Management System[79] will not be operated by the System Operator[80] operating the Backend Layer, thereby supporting the need to mitigating the ability to unmask end-users or wallets through transaction data. The Alias Management System would also be responsible for creating a unique identifier for an end-user that is then used by the System Operator in the Backend Layer.[81]

Therefore, information is sought to address the wide variety of ways an alias management system may be implemented, including addressing the following items:

- Identity & onboarding models;[82]
- Privacy considerations;[83]
- Cross system interoperability.[84]

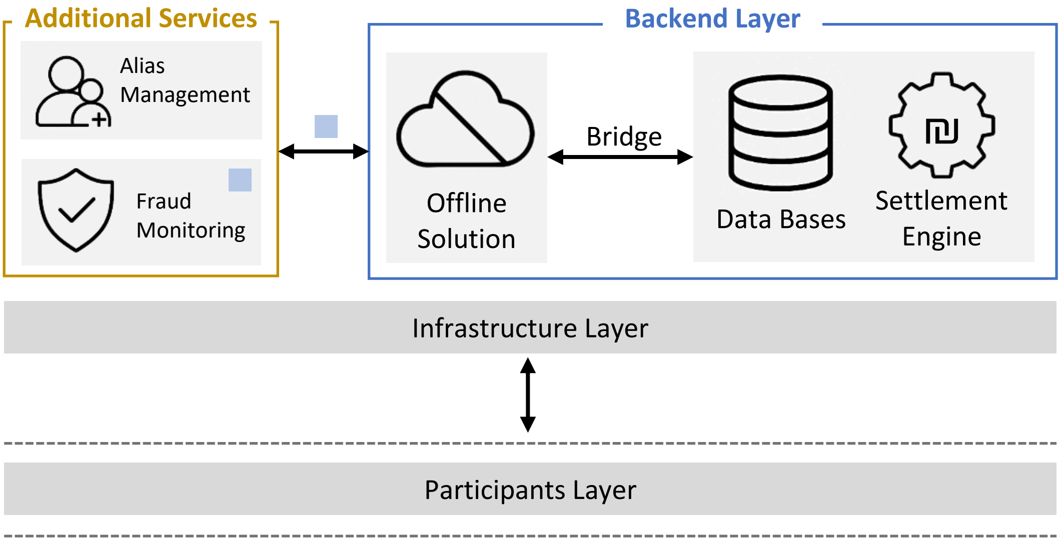
High Level Design Considerations

- Supporting a convenient user experience by use of Aliases while taking into consideration the tradeoff between user experience and privacy, specifically the requirement that no PII and payment patterns are available to any central entity.[85]
- Coordination and use of one or more wallets per unique identifier, with each wallet able to be interacted with by one or more PSPs. However, the data mapping must enable the enforcement of rules and policies on a per end-user level while addressing privacy considerations;[86]
- End users (through system participants) should be able to send a message or digital shekels to another end user using only the recipient's alias;[87]

[79] Preliminary Design, pgs. 36-37, section 3.2.1.
[80] **System Operator -** The entity that operates the technological infrastructure according to the scheme rules and the terms of engagement with the system manager. The system operator will be the central technological entity with which most technological engagements of the various entities will be conducted. The Bank of Israel, or an entity appointed by it, is expected to fulfil this role.
[81] Preliminary Design, pg. 57, section 4.1.
[82] Preliminary Design, pg. 41, section 3.3.1.
[83] Preliminary Design, pgs. 112-115, section 7.1.
[84] Preliminary Design, pgs. 75-81, section 5.1.
[85] Preliminary Design, pgs. 112-115, section 7.1.
[86] See fn. 28 regarding the tension between privacy considerations and the ability to enforce policies and rules.
[87] Preliminary Design, pgs. 36-37, section 3.2.1.

- The default wallet referred to by an alias should be able to be updated and managed by an end user without interruption to receiving payments;
- Alias registration, verification, and lifecycle management;
- Alias lookup service;
- Integration with additional system services and components;
- Interoperability with existing banking and payment infrastructures;
- User experience and accessibility considerations.

Technological Consultation 6 – Fraud Monitoring System



In order to assist PSPs, the Digital Shekel System will have a central fraud monitoring system to identify and prevent the misuse of the system. The Preliminary Design anticipates that PSPs remain exclusively liable for fraudulent transactions,[88] and this centralized system will help inform PSP decision making.

Being mindful of privacy considerations, the Fraud Monitoring System[89] will analyze a wide variety of data (to the extent such information is available and necessary) such as activity patterns, transaction history, geographical characteristics, wallet age, the 'network' of wallets interacting with the paying wallet, and more. Advanced techniques such as artificial intelligence and machine learning technologies can be used to identify anomalous behavior patterns and provide information that may be helpful for PSPs to measure risk.

Therefore, information is sought to address the variety of ways this Fraud Monitoring may be implemented, including addressing the following items:

- Real-time monitoring capabilities;
- AI/ML-based fraud detection;[90]

[88] PSPs will be responsible for preventing fraud and compensating customers in case of fraud, according to the rules in the Payment Services Law. However, offline and anonymous payments will not be eligible for consumer protection. *See* Preliminary Design, pgs. 11-12.
[89] Preliminary Design, pg. 37-38, section 3.2.2.
[90] Preliminary Design, pgs. 119-121, section 7.4.

- Rules engine & adaptive learning;
- Privacy, compliance & data ethics.

High Level Design Considerations

- Calculation and communication of a risk information at the request of a PSP
- Need-to-know based data minimization principles (e.g., the System Operator should not have access to the information of the fraud monitoring system)[91];
- Continuous 24/7/365 operation with minimal disruption and high availability;[92]
- Processing time should be minimized to ensure PSPs may make decisions so that transactions may fully finalize in no more than a few seconds (or may be suspended for further analysis by the PSP);[93]
- Post-transaction fraud analysis based on a complete picture of activity across all payment service providers in the Digital Shekel System and generation of statistics on misuse risks.

[91] The system should analyze a wide range of data (but in any case, not personally identifiable information (PII) of DS users), such as activity patterns, transaction history, geographical characteristics, wallet age, the “network” of wallets interacting with the paying wallet. Not all of this information may be available, depending on the technology choices of the Backend Layer. *See* Preliminary Design, pg. 38, section 3.2.2.

[92] Preliminary Design, pg. 110, section 6.3.

[93] Preliminary Design, pgs. 72-74, section 4.5.