



Accompanying document to the Public Call

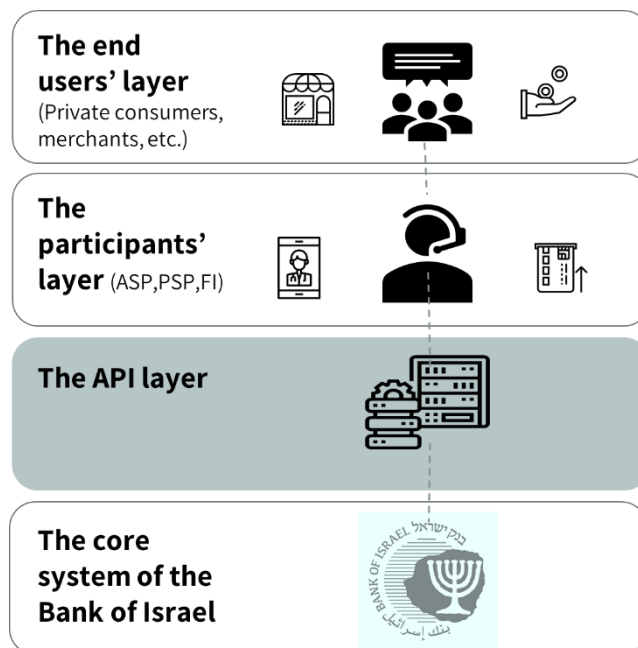
This document is being published together with the Public Call that appears on the [Digital Shekel Challenge website](#). Its objective is to provide complementary information regarding the Digital Shekel Challenge for potential contestants.

1. On what will the Challenge focus?

The Challenge will focus on the interface between the Digital Shekel core system, which is managed by the central bank, and the system's participants, which will be represented by the contestants in the Challenge.

The contestants will be required to use the API layer that will be made accessible by the Bank of Israel, and to implement its functionality on a use case that they will choose to propose in the Challenge. The Challenge will not involve "real" end users. Those will be modeled by the contestants themselves.

Figure 1 – The various components of the two-tier model and the focus in the Challenge





2. The participants' layer in the Digital Shekel system

The vision being formulated at the Bank of Israel with regard to the participants' layer in the two-tier model of the Digital Shekel system includes three types of entities, with each having different functionality in the system:

- 2.1. **Payment service providers** (DS-PSPs¹) – These entities will be responsible for creating the end users' technological approach to the Digital Shekel system², carrying out KYC procedures for their customers, providing and retrieving means of access to the system, customer service, and more. The payment providers will not develop balance-sheet financial exposure at any stage of providing Digital Shekel services, in accordance with the working assumption in the Digital Shekel project and reinforcement of the technological, business, and legal feasibility of this assumption in the "[Sela](#)" [project](#)". Connecting the end user with such an agent is necessary for the operation of the Digital Shekel system, in accordance with the two-tier model for the system.

Emphases and assumptions for this type of participant in the Challenge

- The DS-PSP will support the end user's on-boarding process to the system, and will model a user interface for the end user, based on which the end user will be able to offer all of the functionalities that are possible based on the API layer.
- For the sake of simplicity, the assumption in the Challenge is that every wallet is linked to one DS-PSP at any given time.³

¹ Digital Shekel Payment Service Provider.

² There may also be indirect payment providers that are not directly connected to the system, and which provide Digital Shekel services on the basis of connectivity to a payment provider that is connected to the system.

³ This is a simplified assumption for the trial, and does not reflect the Bank of Israel's vision with regard to the competitive and open ecosystem in the Digital Shekel system.



2.2. Institutions that manage current accounts (FIs⁴) – Financial institutions that manage current accounts that are not in digital shekels for the public (commercial banks, the Postal Bank, deposit and credit unions, financial asset services providers, and so forth) and that will need to enable conversion transactions for end users from the accounts that they manage or from cash to digital shekels and vice-versa.

Emphases and assumptions for this type of participant in the Challenge

- The Challenge does not deal with the full functionalities required from this type of participant, in accordance with the indirect distribution model for digital shekels that is apparent in the project.⁵ It focuses on the function to support funding or defunding of digital shekels.
- The existence of this type of participant is necessary in order to support funding or defunding options for end users as the basis for various use cases that will be proposed by the participants. Therefore, in order to ensure this functionality in the Challenge, the Challenge team will model a number of FIs that will be able to serve the DS-PSPs that the various contestants will establish to make funding or defunding transactions in the end users' wallets. However, insofar as a particular contestant chooses to act as an FI for its customers alongside its role as a DS-PSP, it will be able to do so.

2.3. Additional advanced service providers (ASPs) – These entities will be able to provide additional *optional* services to end users, such as: budget management, analysis services for merchants, fraud monitoring services, and so forth. In addition, they will be able to participate in the provision of advanced conditional payment services. For instance, they will be able to serve as a third

⁴ Funding Institutions.

⁵ For more information, please see Chapter 5 of the logical architecture documents for the Digital Shekel system. The Challenge assumes a starting point where the FIs hold a Digital Shekel balance on the bases of prior accounting in the RTGS between the FI or its representative in the RTGS and the Bank of Israel.



party responsible for sending the “trigger” for locking or releasing money in a conditional payment transaction.

Emphases and assumptions for this type of participant in the Challenge

- The assumption in the Challenge is that an ASP participant will be able to operate directly vis-à-vis the central bank’s core system (through the API layer) for end users connecting through it (while in reality, it may be decided that this access will be limited to access through the DS-PSP that serves the customer.
- ASP authorizations are limited to a small set of APIs relative to the DS-PSP (as will be detailed in the Appendix below). For instance, an ASP participant will not be able to initiate payment on behalf of the end user directly vis-à-vis the central bank.

The premise in the Digital Shekel project is that some of the entities that will participate in the Digital Shekel system will choose to operate in a single role in the system (for instance, only as a DS-PSP), and that others will choose to participate in more than one role (for instance, as both a DS-PSP and an FI).

For the purpose of the Challenge, each contestant that chooses to participate in the Challenge will have defined authorizations (as a default choice) to operate in the sandbox as two different DS-PSPs⁶ and as an ASP⁷ in order to examine the functionalities offered to this type of participant and its ability to support innovative use cases.

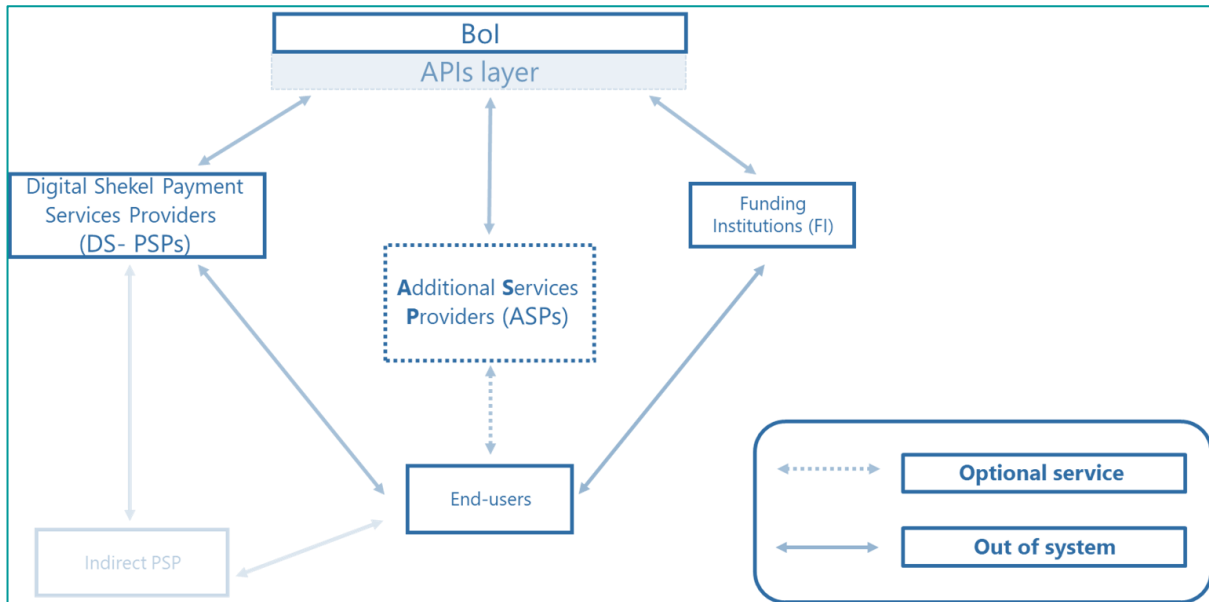
In addition, it will be possible for the contestant to obtain a wallet from an FI participant in order to support funding and defunding transactions by end users that receive DS-PSP service from it.

⁶ For the purpose of optimal modeling of the use cases that involve more than a DS-PSP, such as a synchronous transactions including a request to pay.

⁷ For the purpose of examining the functionalities proposed to this type of participant and its ability to support innovative use cases.



Figure 2 – Digital Shekel schematic



3. What design decisions and main assumptions should you know?

- 3.1. The Digital Shekel is issued by the central bank as a retail CBDC, and represents a direct central bank liability toward its users;
- 3.2. The Digital Shekel can be converted at a 1:1 ratio to a commercial bank liability or to cash;
- 3.3. The function of payment providers in the Digital Shekel system (DS-PSP) is not limited just to entities currently operating as banks or financial institutions;⁸
- 3.4. Transactions between Digital Shekel users are done in real time over the central bank system, without netting;
- 3.5. The central bank will not have access to details identifying end users in the system, or to broad information concerning the transaction;
- 3.6. As part of the Challenge, the system provided by the Bank of Israel will not provide the users' transaction history. Such histories will be managed by the contestant;
- 3.7. There will be no restrictions on Digital Shekel balances or transactions as part of the Challenge.

⁸ However, it is important to note that the Digital Shekel system participants will be subject to regulation and supervision that will be determined later on.



4. What are the APIs that will be made accessible by the central bank?

As part of the Challenge, the Bank of Israel will make the APIs accessible to contestants for various functionalities: to operate the wallet, allow the user to facilitate transactions to program advanced payment transactions and to connect an ASP to the Digital Shekel wallet.

5. Examples of API support in innovative use cases

Challenge contestants will be asked to technologically develop the solution for applying the innovative use cases that they will propose, while using the API layer that will be developed by the central bank. The use cases may offer solutions to existing or future problems in the market. The following are two examples of use cases based on the API layer. (The full list of the APIs appears in the Appendix below.)

- 5.1. Children's wallet, supervised by the parent: The option of connecting sub-wallets to the main wallet ("OpenSubWallet") may support the business need of children's wallets that are connected to a main wallet (such as that of a parent), enabling the parent to supervise the child's sub-wallet, and decide to freeze or temporarily disable the wallet's activity.
- 5.2. Delivery vs. Payment (DvP): A use case in which goods are ordered and payment is made, in whole or in part, only against the delivery of the package by a courier company. In such a case, we can assume that there are payment providers (or the payer and the beneficiary) involved, and the courier company provides services to the beneficiary and acts as an ASP in the Digital Shekel system. For this purpose, a **ThreePartyLock** would be instituted, and as soon as the package is actually delivered to its destination, the courier company will be able to exercise the **DrawDownLock**. As a result, the locked amount will be fully transferred to the beneficiary as long as all of the transaction conditions are fulfilled, or partially transferred if not all the conditions are fulfilled.



6. With what will the Challenge not deal?

As stated, the Challenge focuses on the technological functionality made accessible by the central bank, and its ability to support various use cases, with an emphasis on the more innovative among them. The Challenge will not focus on other issues, such as privacy⁹, CML/CFT, or offline payments.

7. Technological requirements

Contestants that are chosen from among the applicants to participate in the Challenge will receive a follow-on detailed technical document. In order to successfully compete in the Challenge, it is necessary that the contestant's team have the following technological abilities:

- 7.1. Development in languages that allow APIS and working with tools that allow this like Postman.
- 7.2. RESTFUL APIS: Understanding REST's principles and methodologies, including HTTP operations like Get, Post, Delete.
- 7.3. JSON / XML: Ability to work with common data transfer formats.
- 7.4. Recognition with recognized communications protocols in payment systems such as ISO20022.
- 7.5. Information Security: Understanding information security principles and asymmetrical encryption to protect data traffic.

⁹ The technological infrastructure in the project is specified to support a high level of privacy by design, for instance through the possibility of encrypting messages that will be transferred between participants over the central bank's infrastructure. However, the Challenge does not deal with other aspects related to privacy, such as the information structure at the central bank, anonymous transactions, and so forth.



Appendix - The list of APIs

Topic	SubTopic	API name	Description	Further explanation
Wallet	Wallet management	Open	Opening a main (private or business) Digital Shekel wallet in the Bank of Israel's core system	Onboarding of an end user to the system (by the DS-PSP) will include the creation of a wallet in the system for the end user
		OpenSubWallet	Opening a subwallet that is connected to the main wallet.	Enables, for instance, the allocation of a certain balance from the main Digital Shekel balance for a particular purpose: child's wallet, joint activity of spouses or partners, for a subsidiary



The Digital Shekel Challenge



Topic	SubTopic	API name	Description	Further explanation
				business unit, etc.
		Disable	Temporary disabling of wallet activity (main or sub) in the Digital Shekel system	Following the disablement, no activity will be possible in the wallet, and it will not be possible to make or receive payments.
		Freeze	Freezing of activity in the main or subwallet	Under the freeze, payment will still be possible to the frozen wallet, but not from it. For instance, in order to support main wallet's ability to supervise a subwallet (parent and child) or the ability to protect the



The Digital Shekel Challenge



Topic	SubTopic	API name	Description	Further explanation
				wallet where there is concern that the means of access has been lost or stolen.
		Enable	Cancellation of the temporary disabling or freezing of a main or subwallet	
		Close	Closing the main or subwallet in the central bank's core system	As opposed to Freeze or Disable, this action is not temporary. Once it is taken, if the end user wants to go back to using the digital shekel, he will have to undergo a new process.



The Digital Shekel Challenge



Topic	SubTopic	API name	Description	Further explanation
	Management of unique customer identifier	Alias	Creating a proxy for the user's Digital Shekel wallet	In the Challenge, the Alias will be a mobile phone number.
		DeleteAlias	Deleting the proxy from the user's wallet	
		LookUpAlias	A search for a wallet's information by a proxy.	When an end user wants to make a payment, he provides the beneficiary's alias to the DS-PSP. Through this API, the DS-PSP locates the beneficiary's wallet address.
	Defining FI	ConnectFI	Connecting the wallet to an FI. FIs are entities that manage	Connecting the wallet in the Challenge to an FI (which will be



The Digital Shekel Challenge



Topic	SubTopic	API name	Description	Further explanation
			current accounts for the public outside the Digital Shekel system, and enable their customers to convert money from their account to digital shekels (funding) and vice-versa (defunding)	modeled by the Challenge team or by the contestant) is necessary in order to support funding and defunding actions from the wallet.
		DisconnectFI	Disconnecting the wallet from the FI	For instance, if the end user changes his bank account, and wants to disconnect the wallet from the old bank account and then connect it to the new account.



The Digital Shekel Challenge



Topic	SubTopic	API name	Description	Further explanation
	Balances	Balance	Restore the balances of a particular wallet	
		AvailableBalance	Present the available balance for use in a particular wallet	The total balance minus the locked balance.
Transactions	Payment (Credit transfer)	Pay	Transfer a Digital Shekel from one wallet to another.	
		SplitPay	Split transfer – from one wallet to a number of different wallets.	
	Payment request	RequestToPay	Payment request by the beneficiary's wallet to payers' wallets.	



The Digital Shekel Challenge



Topic	SubTopic	API name	Description	Further explanation
		Authenticated RequestToPay	Enables the DS-PSP of the payment receiver to include a verification package with the request to pay such that the payer's DS-PSP will be able to confirm the request without contacting the end user.	For instance, for payment at a point of sale (pos) or a situation in which the payer provides the beneficiary with an account debit authorization (for instance to make periodic payments to infrastructure companies)
	Funding and defunding	Fund	Conversion of digital money that does not represent a central bank liability (for instance, a current account at a commercial bank or at an entity that manages a	This transaction is based on the transfer of digital shekels from an FI's wallet to an end user's wallet (against a debit to the end user's account vis-à-



The Digital Shekel Challenge



Topic	SubTopic	API name	Description	Further explanation
			<p>payment account for a customer) to a digital shekel, or conversion of cash to a digital shekel. The result of loading is that the balance in the end user's Digital Shekel wallet increases.</p>	<p>vis the FI— outside the Digital Shekel system).</p>
		Defund	<p>The reverse of a "Fund" transaction – conversion of a Digital Shekel to other digital money or to cash.</p>	<p>Accomplished by transferring digital shekels from the end user's wallet to the FI's wallet (against a credit to the end user's account vis-à-vis the FI— outside the</p>



The Digital Shekel Challenge



Topic	SubTopic	API name	Description	Further explanation
				Digital Shekel system).
Programmability	Defining locks (incl. locks limited to a certain timeframe in order to prevent permanent lock)	RequestToLock (TwoParty)	Locking a Digital Shekel amount in the payer's wallet based on a message sent from the potential beneficiary's PSP to the potential payer's PSP, and including the lock data.	In a "two party" lock, the trigger for applying or canceling the lock is sent by the beneficiary's PSP.
		ThreePartyLock	This functionality enables the involvement of a third party (who is not the PSP or either the payer or the beneficiary). For instance, an ASP that provides services to	In such a case, the trigger for applying or canceling the lock is sent by the third party. For instance, a courier company that can ascertain that the package has reached the



The Digital Shekel Challenge



Topic	SubTopic	API name	Description	Further explanation
			the beneficiary and initiates the lock vis-à-vis the payer's PSP.	beneficiary and activate the payment.
		HTLCLock	Initiation of a Digital Shekel lock based on an HTLC mechanism (Hash Time Lock Contract).	The trigger for applying the lock and completing the transaction between the parties is based on the use of a "secret" (as common in HTLC mechanism). This API can be used, for instance, to ensure payment in digital shekels against the transfer of a digital asset



The Digital Shekel Challenge



Topic	SubTopic	API name	Description	Further explanation
				on another network.
	Cancellation and continuation of locks	CancelLock	Cancellation of a Digital Shekel lock that was set in the past	For instance, if the parties decide to cancel the transaction for which the lock was put in place.
		DrawDownLock	Application of a two or three party lock and partial or full transfer of the locked amount to the beneficiary	Will be done by the participant who is responsible for confirming that the transaction conditions have been met and that the payment can be completed
		DrawDownHTLC	Application of the HTLC lock and transfer of the full locked	Through use of a "secret".



The Digital Shekel Challenge



Topic	SubTopic	API name	Description	Further explanation
			amount to the beneficiary	
	Information on locks	LockbyLockID	Obtaining information on a specific lock based on the LockID	For instance, in order to update the end user regarding the money that he has locked in a particular transaction
		LockbyPSP	Obtaining information on all existing locks in the wallets of customers of the requesting PSP	
		LockbyWallet	Obtaining information on all locks active in the wallet	For instance, in order to update the end user regarding all the money that he has locked in all of his pending transactions



The Digital Shekel Challenge



Topic	SubTopic	API name	Description	Further explanation
ASP connection to the digital shekel wallet		ConnectASP	Connecting an ASP to the wallet to provide other optional services to the end user	Potential services: budget management, analysis services for merchants, fraud monitoring services, innovative payment applications, etc.
		DisconnectASP	Disconnecting an ASP	

Also available for an ASP participant