Deep Dive into the Technological Consultation

Vincent Mele, Consultant

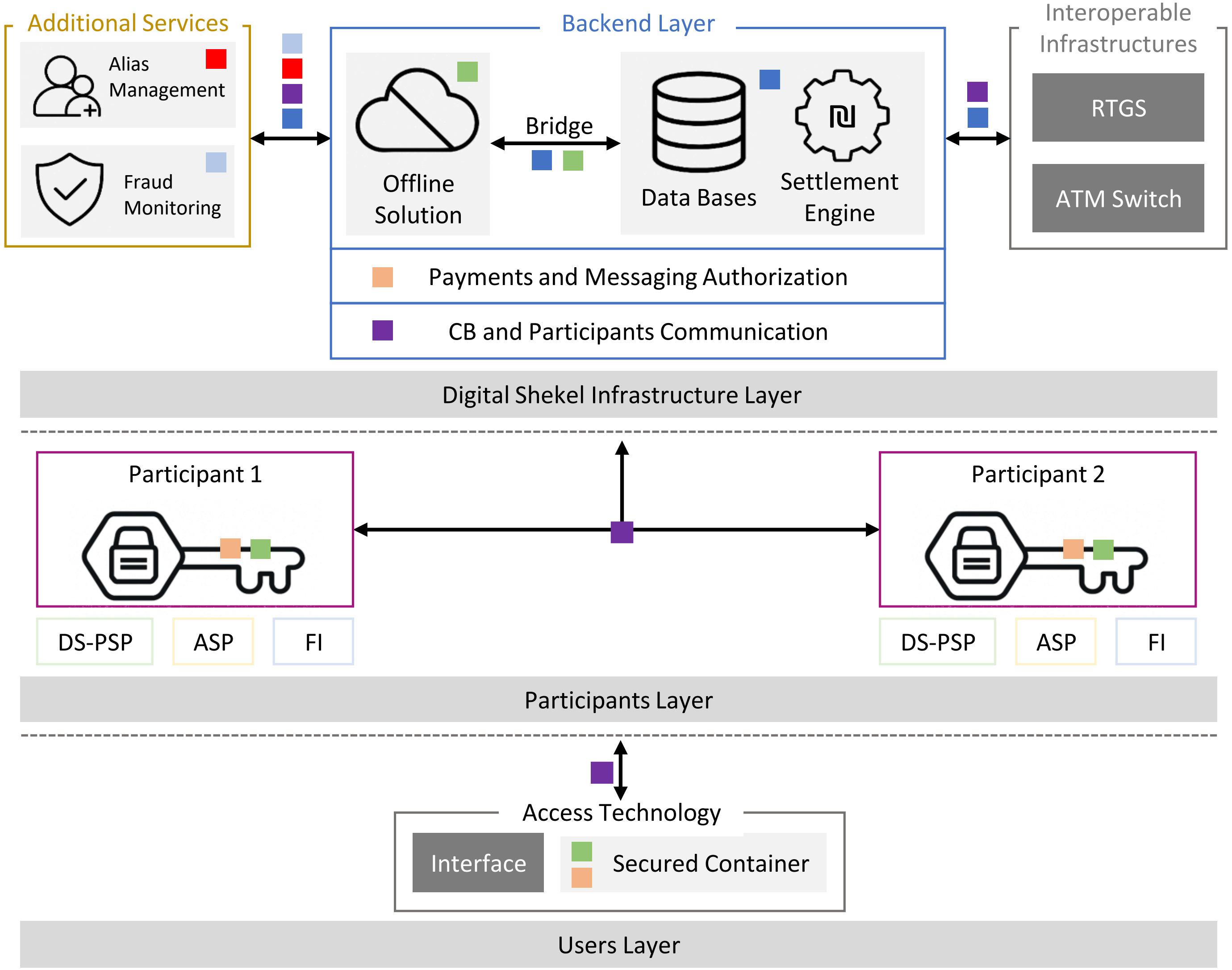
Today’s Focus

The Technological Consultations

- Context to the TC requests
- BoI is exploring all technological options:
  - DLT, non-DLT; centralized, distributed, etc.
  - There is likely no ‘one size fits all’ solution
  - When responding to TCs, please justify *the reasoning of technological choices*
- Send questions to the Q/A!

Context of the TCs

- 🟦 TC 1: Backend
- 🟪 TC 2: Communication
- 🟩 TC 3: Offline
- 🟧 TC 4: Authorisation / Key Mgmt.
- 🟥 TC 5: Alias
- 🟦 TC 6: Fraud



TC1 – Backend Layer

Purpose

1. Authorize and record changes to balances in end users' wallets (in the database)
   - Use and store the minimum amount of information necessary

2. Settlement Engine - stateless

Important Considerations

Privacy

Data Management

Aggregated Transaction Database

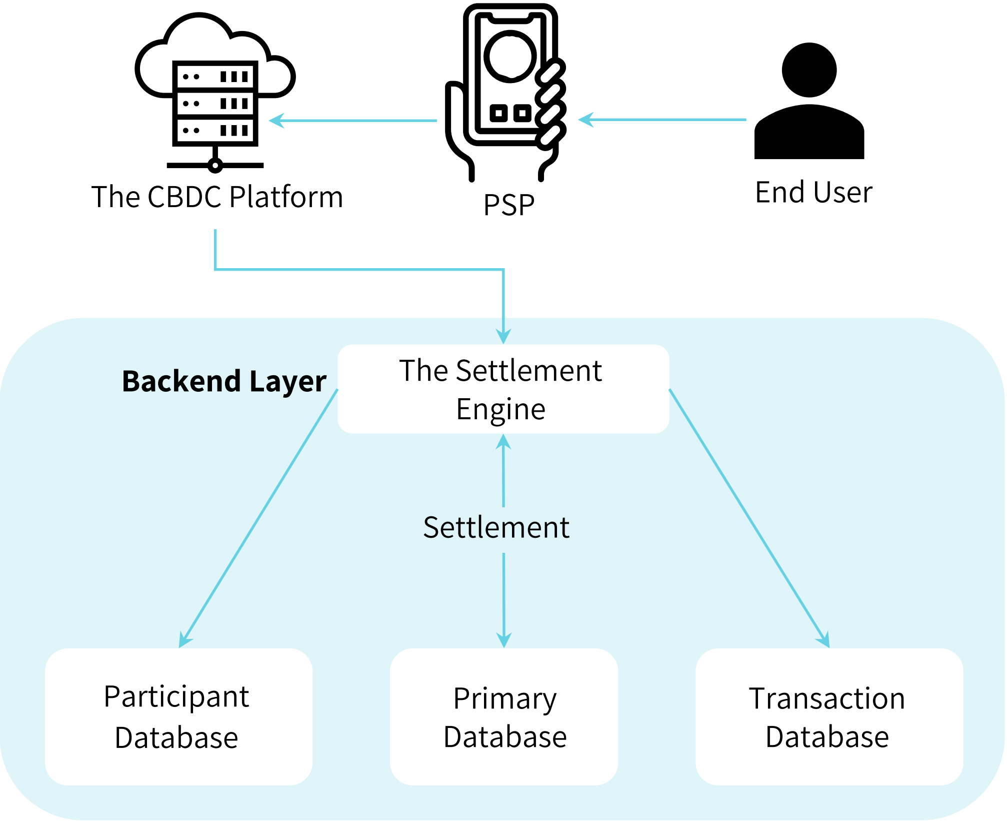
Participant Database

Interoperability

Functionality

- Holding Limits
- Interest Payments
- Other policies
- Statistical and Operational Data

A Close Look at the Backend Layer



All technologies considered: DLT or non-DLT

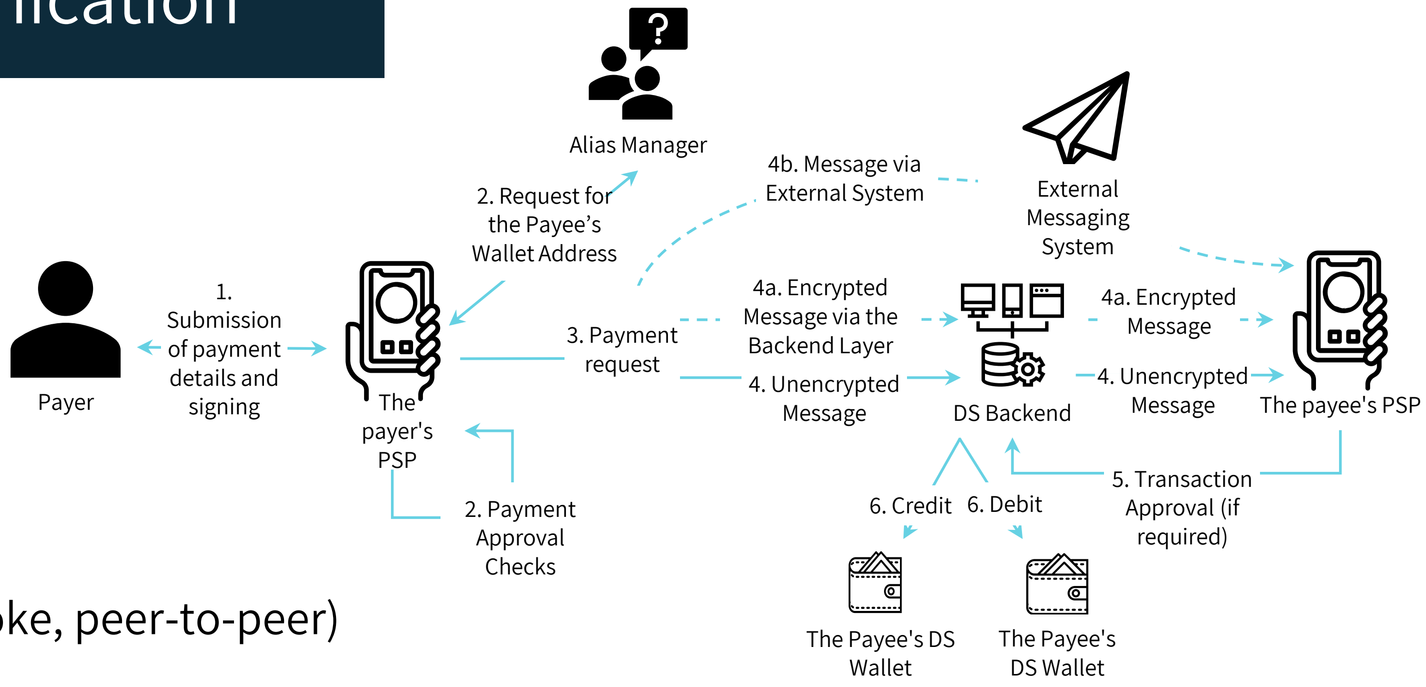
TC2 – Secure Transaction Messages and Communication

Primarily communication between:

- Participants and Infrastructure Layers (shown to the right)
- Participants to/from Participants

Some Considerations for response:

- Structure
- Method of transmission (e.g., hub and spoke, peer-to-peer)
- Need-to-know basis



Alias Manager

Payer

1. Submission of payment details and signing

The payer's PSP

2. Request for the Payee's Wallet Address

2. Payment Approval Checks

3. Payment request

4b. Message via External System

External Messaging System

4a. Encrypted Message via the Backend Layer

4. Unencrypted Message

DS Backend

4a. Encrypted Message

4. Unencrypted Message

The payee's PSP

5. Transaction Approval (if required)

6. Credit

6. Debit

The Payee's DS Wallet

The Payee's DS Wallet

Important:

Users should be authorizing payments via **private keys** (*See* TC4 – Secured Containers)

This means that the *payment* authorisation (which occurs in the Main Database the Backend Layer) may differ than the *message* authorisation (which occurs between Participants and the Infrastructure Layer or between participants themselves)

TC3 – Offline Capabilities

Offline functionality is subset of Access Technologies

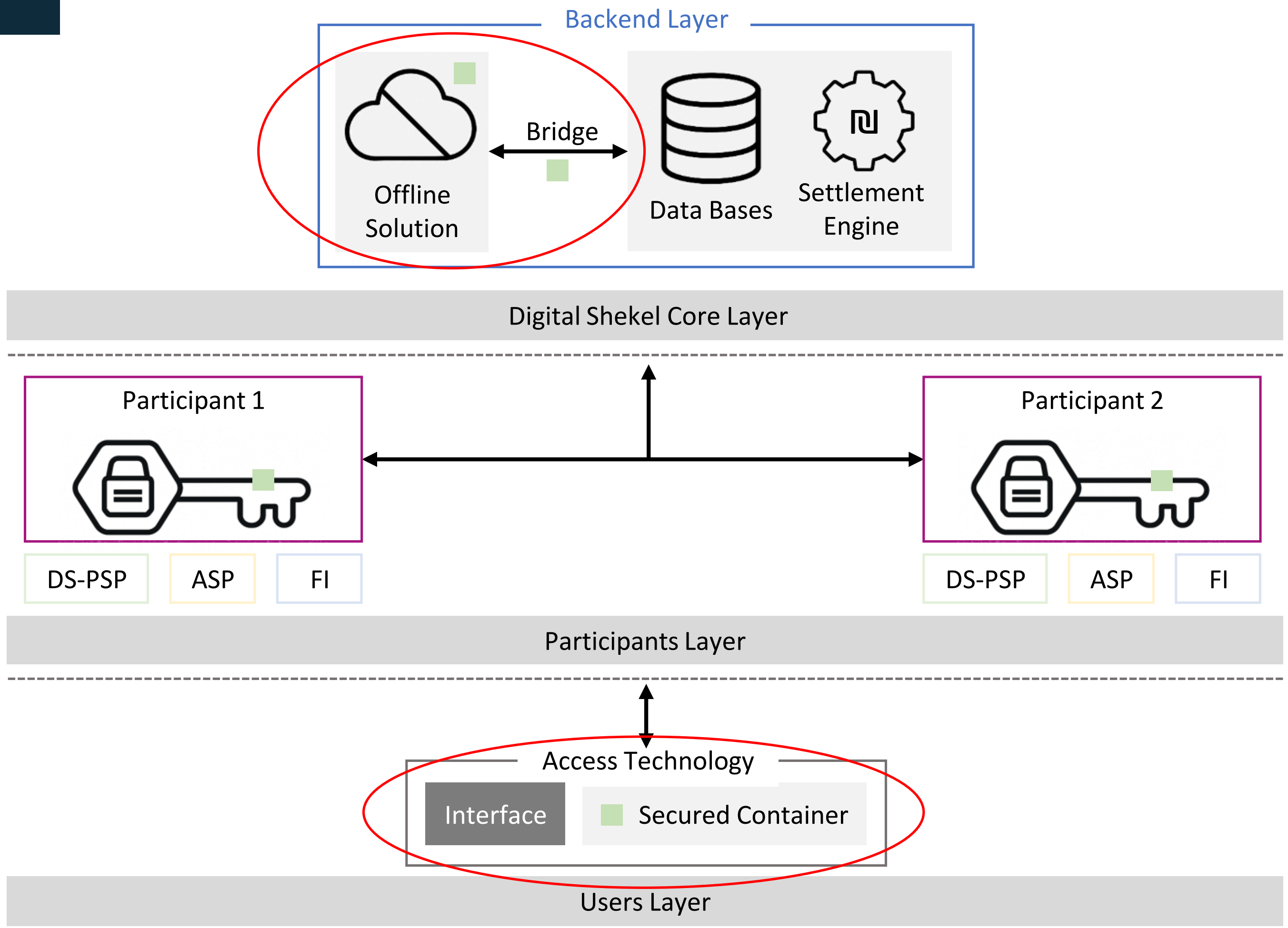
Finality and Settlement must be possible offline (without deferral)

Three types of Offline Payments:

- Fully Offline – (but challenges exist)
- **Intermittently Offline – primary focus**
- Staged Offline

Important considerations:

- Privacy – anonymous and non-anonymous
- Lifecycle of rules and lists
- Eventual synchronisation
- Dispute Resolution support
- Interoperability – incl. micropayments



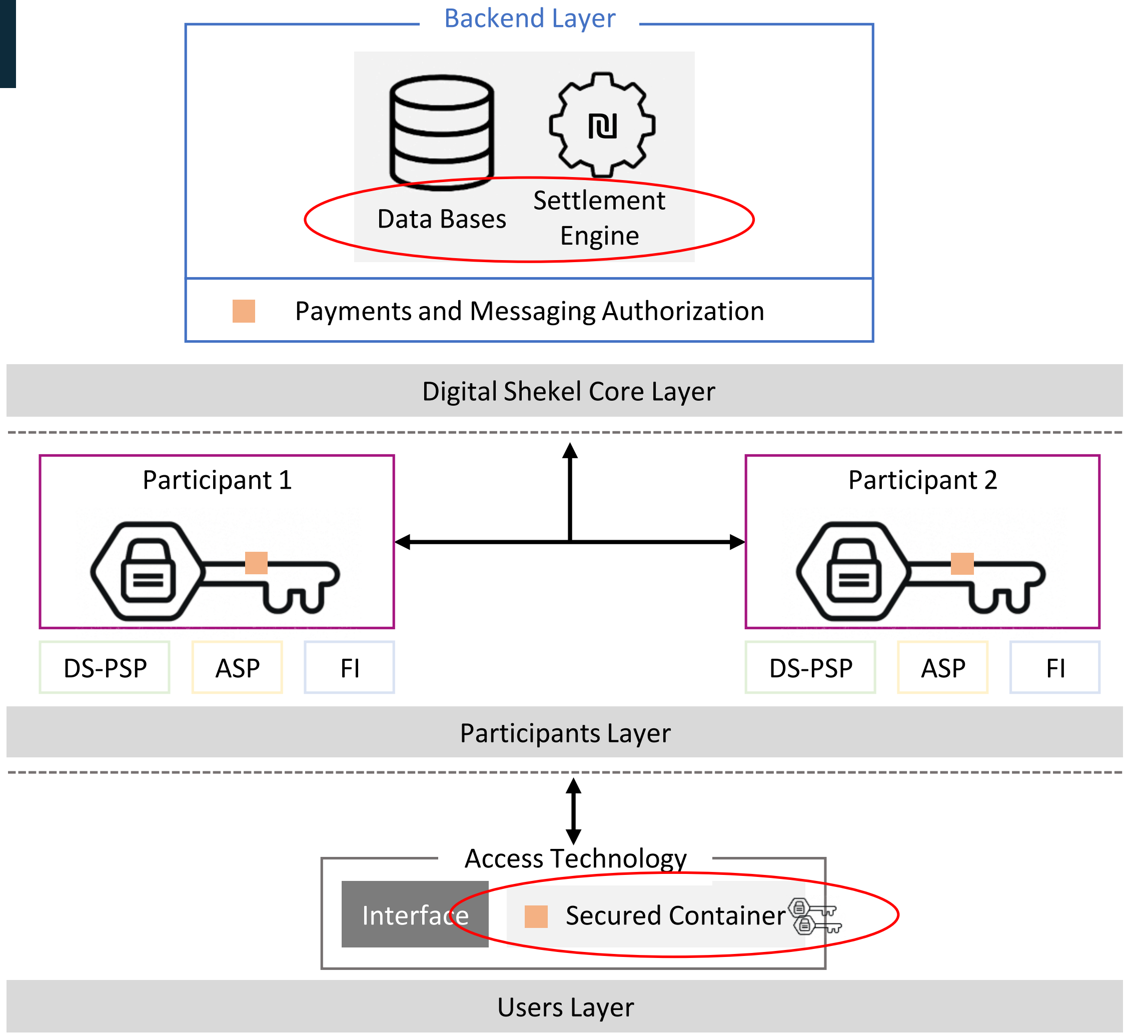
TC4 – Secure Containers & Cryptographic Key Management

Purpose

- **Authorization** of actions at the Backend Layer
  - Payments, balance queries, instructions
- Address *entire* key management lifecycle
  - Generation, registration, storage, distribution and installation, use, rotation, backup, recovery, revocation, suspension, and destruction

Technologically agnostic to Backend Layer

  - Smart phones, limited-functionality phones, smart cards, PoS, cloud-based APIs
- Asynchronous and Synchronous Payments

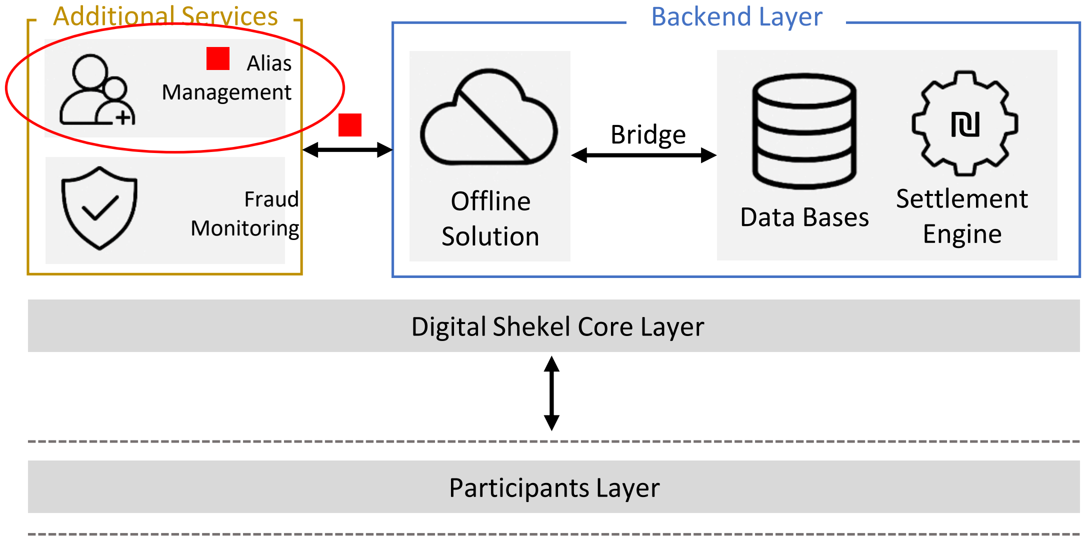


TC5 – Alias Management System

Purpose

- Enhance convenient user experience
- Perform important operational role
- Ensure privacy and segregation of duties

End-users can use wallet lookup service through PSPs in order to send payments only based on the recipient's alias. e.g., a DS payment to a mobile phone number

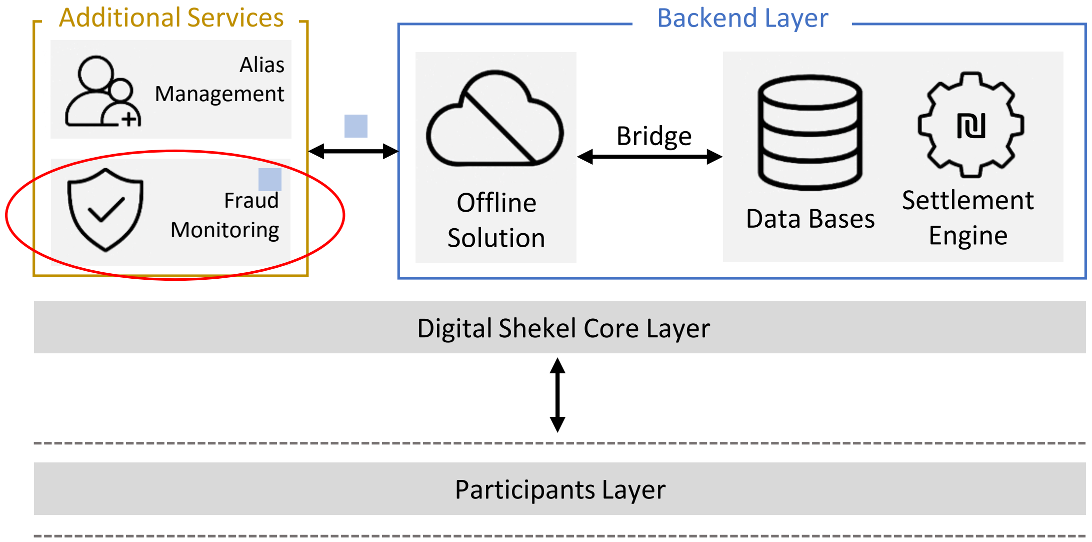


TC6 – Fraud Monitoring System

- Importance of the system's reputation and trust
- Assist PSPs in decision making

- How to create effective information for fraud monitoring without access PII and compromising privacy (what data *needs* to be available, when, and to whom)

- Privacy considerations
- Data availability (DLT v. non-DLT, etc.)



Conclusion

Remember: The Digital Shekel System is one system with interlinked components

For Responses:

- Be as detailed and as technical as possible – e.g., if you are a vendor, why did you make certain design decisions?
- Seeking guidance on individual components or sub-components, algorithms, methods
- Include non-functional considerations like security, performance, resilience
- Feasibility regarding costs and maturity
- Looking for innovation:
    - What is the cutting-edge of research and how would it be part of a larger Digital Shekel System?