3.0 Theoretical Simplified System with DIDO

Return to User Scenario: Identity

Figure 1 represents a theoretical PII Secure Smart Contract (PIISSC). At its core, the PII Smart Contract acts as a repository of other identifiers and PII. The PIISSC by design is usable locally as just a wallet for PII and Identifiers or it can be placed onto a DIDO (i.e., Blockchain, Distributed Ledger Technology (DLT), DAG, etc). When it is being used locally, all the interactions with the PIISSC are simply transforms, when it is placed onto the DIDO or updated on the DIDO, the interactions are Transactions. Regardless local or DIDO usage, the PIISSC provides a unique hash that identifies the current state of the PIISSC.

1. A local copy of the PIISSC is downloaded onto a local computing device
2. Personal Identifiable Information and information is added to the PIISSC locally. Each update made to the PIISSC is local and considered a transform. Examples of information stored in the PIISSC are:
    1. Passport numbers
    2. Passports images
    3. Fingerprint images
    4. Credit Card and Debit Card details
    5. Credit Card and Debit Card images
    6. Important Details from documents such as (visas, work permits, marriage certificates, birth certificates, etc.)
    7. Important Document images
3. An identifier for the PIISSC in its current state is available as hexadecimal text, Bar Code (Barcode), or Quick Response Code (QR Code). **Note:** every time new information is added to the PIISSC, the identifier changes.
4. Using Biometric Authentication between the external users and the PIISSC stored data (i.e., finger prints, voice, or facial recognition)
5. Asking pre-canned questions to the PIISSC using bar codes or QR Codes (i.e., Is the person over 18? Is the person a Citizen? Does the person have a work permit?, What is the person's Credit Card Number?)
6. Using free form text and voice to ask questions to the PIISSC
7. The questions are analyzed according to an ontology to reformulate the questions that can be analyzed by a rules engine
8. Providing a response. Either
    1. Trinary responses Yes/No/Unknown, True/False/Unknow
    2. Short answers such as unknown, passport number, credit card number, etc
9. Providing rules governing the PIISSC usage. For example:
    1. Only during this time period
    2. Expires after this date
    3. Only while in this geographic vicinity
    4. Only using this IP address
    5. Only in this geographic vicinity at this particular time
    6. Only before or after a particular event

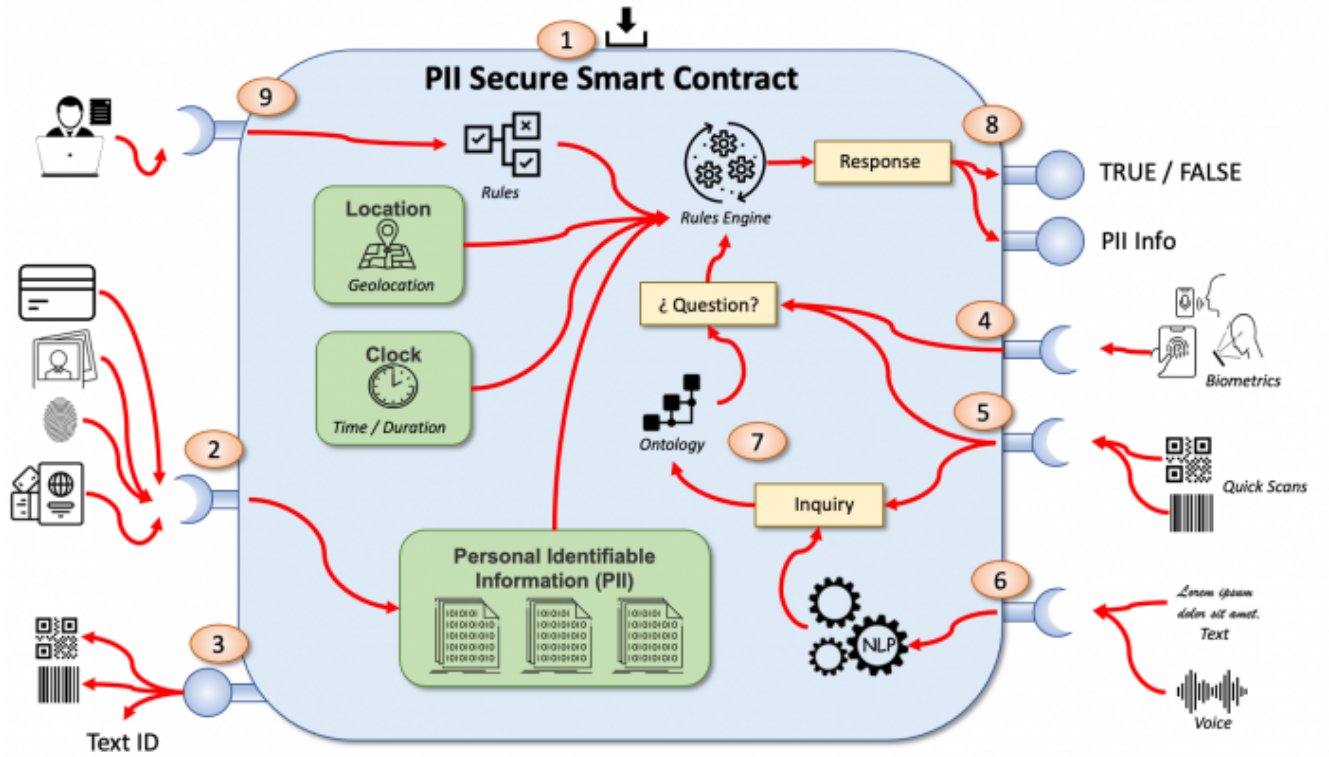
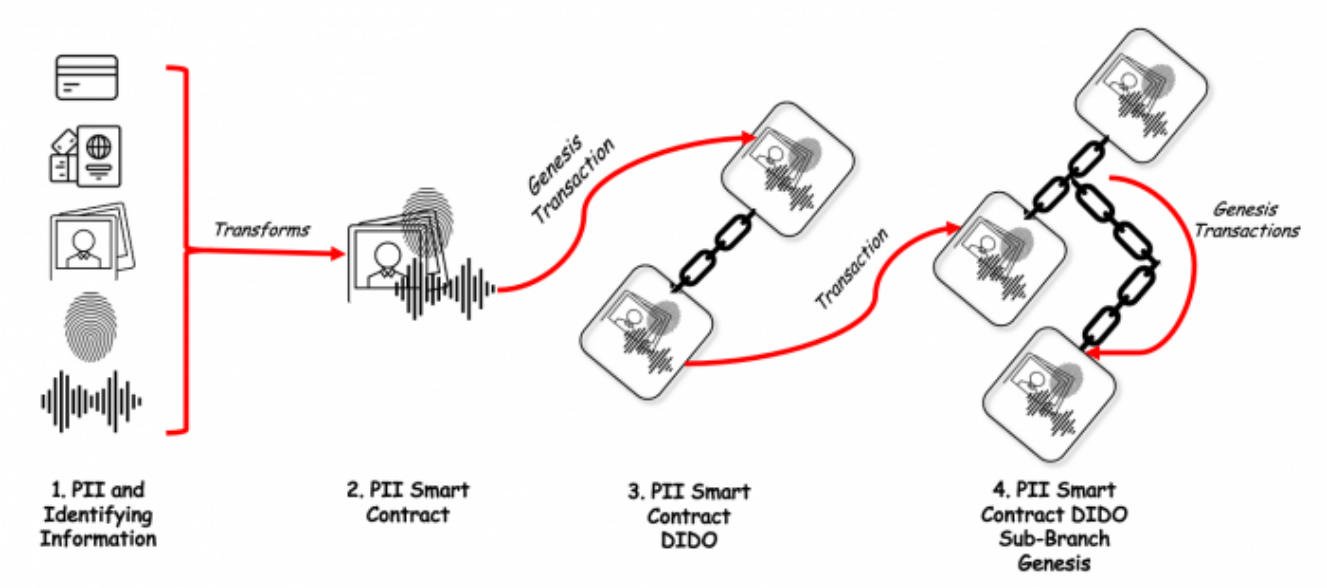


Figure 1: A theoretical PII Secure Smart Contract

Figure 2 represents some major activities surrounding the PII Secure Smart Contract (PIISSC).

1. The PIISSC is downloaded to a local computer
2. PII is collected and added to the downloaded copy of the PIISSC. These operations are transformations rather than transactions because the modifications to the PIISSC are only local and do not be propagated to other DIDO nodes
3. The local PIISSC is deployed onto the DIDO creating a genesis record for the Smart Contract. All subsequent modifications to the Smart Contract on the DIDO require a transaction
4. At some point, a sub-branch of the original Smart Contract records is created. This sub-branch may contain all of the information found in the original subcontract, or it may contain a subset of information. The subsetting does not include the full transaction log (journal) for the Smart Contract, only the current set, and an indicator back to the record where the branch occurred. At this point, the PIISSC has its own Identifier and its own lifecycle.



Discussion of Theoretical System

The following provides a detailed discussion of some of the issues associated with a Theoretical Simplified System Using DIDO scenario.

- 3.1 Activities
- 3.2 Issues