Digital Identity Isn't Only For People

Robots will need passports because they will need to have authorisation to access resources. Would you believe it?

see more

12 of the biggest enterprise blockchain players of 2020

The enterprise blockchain space in 2020 looks a lot different from previous years, demonstrating the continuation and a drive to mature and advance.

see more

Spain, Italy setting new standard for GDPR enforcement

It is probably fair to say much of the enforcement focus regarding the General Data Protection Regulation (GDPR) has been on those regulators that have historically talked tough about preserving privacy—namely, data protection authorities (DPAs) in Germany, Belgium, France, and the United Kingdom.

see more

Testing and validation

The Poseidon platform is going to be released in few weeks. Before that, an accurate and thorough set of tests is being carried on by Poseidon partners, with the aim of:

- testing and validating each of the PoSeID-on components;
- verifying the correct integration of all software components and algorithms of the integrated PoSeID-on framework and customization.

For each test some requirements are established with the logic that each requirement has to be covered at least once from the tests and each test can cover more than one requirement.
Testing Modules

About the Personal Data Analyser, tests have the aim of:

- Communication with other PoSelD-on platform modules: The objective of this test is to ensure that communication with other modules and shared DB is functional.
- Ensure that metadata is extracted from documents when documents are sent for analysis.
- Ensure that contents are extracted and parsed from documents when documents are sent for analysis.
- Ensure that content being analysed is identified and classified with named entities associated with the pii types supported by the platform.
- Ensure that privacy risk analysis considers all the inputs and generates privacy warnings when privacy risk thresholds are triggered.

About the Risk Management Module, tests have the aim of:

- Verify if the RMM is able to subscribe into the message broker and forward the messages to the speed layer.
- Verify if the batch processor component of the RMM is capable of performing the machine learning pipeline in order to detect and evaluate risks.
- Verify if the stream processor of the RMM is capable of processing logs messages in near real-time, storing parsed messages and forwarding risk events to the service layer.
- Verify if the service layer of the RMM is capable of forwarding the warning messages with respect to the risk events and also updating the reputation of each data processor.
- Verify if the RMM is able to store the risk events into the Cassandra DB repository.

In order to test all the main aspects related to the blockchain, tests have been performed in order to:

- Ensure that only blockchain nodes keep track and store Poseidon permissions stored data.
- Blockchain API can effectively create private transactions when requested by Blockchain API clients.
- Verify that Quorum ledger successfully replicates transaction information along network peers.
- Verify the Account Manager works as expected providing logical or physical access control to ledger data and avoiding undesired accesses.
- Verify the system architecture design in where end-users rely on trusted Poseidon Data Processors services to make the interactions.
- Verify that designed smart contract for Poseidon permission management is used to validate business logic when the Poseidon platform Blockchain API receives a new call, allowing the execution of different operations: Request PII Permission, Grant or Revoke PII Permission, etc.
**Integrated and Functional tests**

The integrated tests are related to the integration of the different components of the platform, e.g. software components and algorithms, while functional tests have the aim of verifying the correct behavior of whole system.

As an example of this kind of test, in the following we will focus on some of those performed on the blockchain API, that represent the heart of Poseidon Platform.

The Blockchain API is the middleware in charge of connecting the Data Processor API with the Blockchain nodes. The Data Subjects - the end users of PoSeID-on - are given a Blockchain wallet managed by the Blockchain API. That wallet provides them with an infinite set of addresses and private keys that grant a secure interaction with Blockchain. The operations allowed by the Smart Contract, and therefore by the Blockchain API, are authorizing Data Processors to get information about permissions given to other Data Processors, fetching their permission related information and revoking their grants on selected permissions.

The main objective of the tests is to summarize the behavior and functions composed by the Blockchain API and the underlying smart contract considering the privacy considerations of the Burnable Pseudo Identities interaction design. Tests has as specific aim to:

- get the list of granted permissions by given Data Subject. In order to do so, a sequential call to Get permissions filtered by status flag will be executed
- verify grant access to Data Processor for given Data Subject and permission.
- verify access revocation to DP for given DS and permission.
- verify that Data Processors can successfully request access permissions to Data Subjects.
- verify that Data Processors can effectively check their permission status (granted or revoked by their data subjects) in order to comply with data regulations.

The functional tests performed on Blockchain API, indeed, are aimed to:

- validate that the blockchain will only manage permissions and not data.
- validate that, given that data are stored on cloud, the PoSeID-on platform will be able to guarantee the Right to be forgotten through data synchronization. Each time a user requests the deletion of his data from the platform or revokes the access permission to a specific Third party, the process will be automatic and managed only by the platform itself because every update validated by the blockchain and done on databases on cloud will be synchronized on local caches instanced within Third parties’ infrastructures.
- Blockchain ledger ensures data accesses: The objective of the test is to validate that, in order to implement the Right to be forgotten, we will concentrate on data access permissions, held inside the blockchain. Once access permission to Third Parties is revoked by the user, Third Parties are no longer allowed to use this data and are legally accountable if they ever use them. *We will guarantee the Right to be forgotten, making sure that Third Parties that use data outside the correct period of permissions are legally accountable. As agreed, Third Parties will be informed and warned of the risks they would incur if they were ever to use data after permission is revoked.*
- validate that, whenever users update/modify their personal information from the Privacy Enhancing Dashboard, Third Parties automatically receive these modifications as a consequence of data synchronization with the cloud. Every update validated by the blockchain and done on databases on cloud will be synchronized on local caches instanced within Third Parties infrastructures.
If you want to unsubscribe, please reply to this email with "unsubscribe"