POSEIDON

RELATED TOP STORIES

Digital identity: Fighting cybersecurity threats

Over the past decade, there have been more than 2,550 healthcare data breaches. Digital identity verification is one key to fighting cybersecurity threats through replacing easily breakable usernames and passwords with other protections such as biometrics can thwart fraudsters.

see more

United Arab Emirates' Ministry of Health Launches Blockchain System

United Arab Emirates’ (UAE) Ministry of Health and Prevention (MoHAP) has launched a blockchain system for recording and sharing healthcare data.

It will also help improve data and information validation and consistency, which in turn provides a high level of transparency and trust in the healthcare services sector.

see more

GDPR: Europe Continues To Wrestle With The Long Arm Of American Law

The European Court of Justice ruled that “the right to be forgotten”, one of the core data privacy protections enshrined in the EU’s flagship General Data Protection Regulation (GDPR), only applies to search results inside the European bloc.

The potential conflicts between the CLOUD Act and the GDPR could leave European service providers facing a tricky dilemma, because it will now be difficult for European companies to comply with the CLOUD Act without breaching the GDPR.

see more

PoSeID-on BLOCKCHAIN SOLUTION

The heart of the PoSeID-on decentralized platform for user data privacy protection has been designed and developed over a Smart Contract driven Blockchain network. Known entities will maintain it, but it'll be open to every PoSeID-on platform user, so the data will be protected but transparent at the same time.

For security reasons, interaction restrictions have been added to permit the operation with the Blockchain using Smart Contracts. There are some strategies that allow to redirect the execution from one entry Smart Contract to different backend Smart Contracts, but mainly it will be done by giving governance operations to the entry Smart Contracts. The Data Subject grants or revokes the data requested by the Data Processor, whatever it is. A set of operations will be permitted to be done in blockchain with a decentralized execution view. This set of operations is the functionality face for the blockchain clients and thus the Data Subject and Data Processor operation entry point. These operations will include: Request Personal Identifying Information (PII) Permission; Grant PII Permission; Revoke PII Permission; Check PII Permission; and PII Access Notification.

According to the GDPR, Data Processors need each Data Subject permission to collect and manage his/her PII. A function will provide the appropriate mechanisms for a Data Processor to request that kind of permission. When a specific permission is requested for a specific Data Subject, the Data Processor needs to wait for that permission to be granted by the Data Subject. The operation timestamp will denote the starting time for the permission to take effect, and the permission will automatically stop having effect when the requested end time is reached. Therefore, this operation will be linked to one previous permission request. The Blockchain users (both Data Subjects and Data Processors) will be provided with their own, auto-generated, unique, private, recoverable and secure key set.

For this purpose, a full offchain-but-distributed managed system has been created. In order to comply with the highest security and privacy requirements, PoSeID-on Blockchain node managers must hold the related cryptographic content and their node keys. This design allows to have a single access point of information stored in a central repository. Therefore, the management of the nodes, and the management of the keys, will be carried out by the data processors (DP) themselves. Moreover, the Quorum design - the software used for the implementation of the ledger - allows the management of these keys for laboratory validation without relying in hardware. The scenario implies that:

- The keys cannot be stored in a Hardware Security Module (HSM).
- The keys must be known by at least one server.
- The keys that belong to a node must be stored in the node itself and execute the process of unlocking on demand.

On the other hand, the keys belonging to the users (Data Subjects or DS) will be protected by the BC API component.

The stored content will be secured through the standard model of Ethereum V3 KeyStore. Any external system that needs to be queried in order to get some information requires two things: a protocol of communication and a client to communicate with.

Technically speaking, PoSeID-on will adapt both communication protocol and client implementation to the platform requirements. This means that communication protocol will be JSON-RPC communication over HTTP connection. Thus, PoSeID-on clients will only need to be compliant with HTTP standard defined at Hypertext Transfer Protocol (RFC 2616) and encapsulate their messages as JSON-RPC following the standard. This behavior must remain the same, independently of the nature of the client interacting with the solution. This way, PoSeID-on allows different kind of device types – e.g. smartphones or browsers –to communicate using this standard for those situations in where a direct peer communication is required. The objective is to encapsulate the Blockchain complexity over a RESTful API where end users and clients will only need to be compatible with REST APIs, maximizing the targeted audience.

see more

Papaya and PoSeID-on Workshop on Privacy Challenges in Public and Private Organizations at the IFIP Summer School on Privacy and Identity Management

Recent advances in information technology such as the Internet of Things and/or the cloud computing paradigm enable public and private organisations to collect large amounts of data and use advanced techniques in order to infer valuable insights and improve their businesses. Unfortunately, these benefits come with a high cost in terms of privacy exposures given the high sensitivity of the data that are usually analysed/processed at powerful third-party servers. Given the ever-increasing of data breaches, the serious damage they cause, and the need for compliance to the European General Data Protection Regulation (GDPR), these organisations look for secure and privacy preserving data handling practices.

During the workshop the team presented an approach to the problem of user data protection and control, currently being developed in the scope of the PoSeID-on H2020 European project, the presented solution complies with EU's General Data Protection Regulation, and explores the use of Blockchain technology to provide data transactions protection and accountability, as well as full control of users over their own data.

The goal of this workshop was to identify and present the privacy challenges related to data collection/analysis by public and private organisations and to encompass research advances in the privacy enhancing technologies that will enable privacy preserving data management and GDPR compliance. Moreover, the workshop served as a discussion environment for those familiar with cryptographic tools and discuss possible concerns and risks when it comes to applying such tools in different areas, when data is critical and sensitive. We intended to understand and shed light on the mental models, trust factors, and the possible risks and concerns when it comes to data analysis on the encrypted data and how these discussions might be used to foster collaboration among potential privacy enhancing technology outputs of PoSeID-on and PAPAYA projects.

See more

InNorMadrid, Forum on Blockchain and Ciber-security

InNorMadrid, the Association for the Innovation Development of North Madrid organized on Oct 1st 2019 the Forum on Blockchain and Ciber-security, with the aim of promoting effective collaboration and technology transfer between industry and university. Participants from diverse organizations (large companies, SMEs, and universities) have presented the most recent advances in research and innovation in the areas of ciber-security and blockchain, oriented to multiple applications. Antonio M. Ortiz, from PNO Innovation presented the PoSeID-on Project as an example of collaboration among various institutions to foster innovation using Blockchain, remarking its application in the Data Protection field. The presentation of PoSeID-on raised the interest of the participants, not only from the technological point of view, but also from the commercial opportunities that represent the collaboration in research and innovation.

Funded by Horizon 2020
Framework Programme of the European Union