Contribution ID: **139** Type: **not specified**

A standardized approach to accessing identity information over decentralized connected device networks

As the concept of Internet of Things slowly moves from a futuristic idea to a pervasive reality, a number of novel challenges start appearing. The hardware and software ecosystem for IoT applications is today fragmented and highly unstandardized and several different architectures, protocols and hardware platforms are being proposed by technology providers. The idea of decentralized architectures based on protocols and technologies like block chains is emerging as a possible, intrinsically more secure, scalable and user-centric model for the implementation of tamper-resilient, distributed, transactions-based architectures for IoT applications.

At the same time, the use of personal data, today already pervasive in a variety of applications from user profiling for e-commerce applications, to social networking, or electronic medical records, will only increase with the increased use of wearable or connected devices collecting and transmitting biometric data like fitness bands, connected scales, blood pressure readers. The use of fingerprints, retinal scans or heart rate patterns are also used as authentication factors in an increasing number of devices for applications ranging from unlocking phones or computers to opening doors and starting cars.

Most of the identity management challenges in decentralized networks of sensors and connected devices are still unexplored and unresolved. Concerns must be legitimately expressed about ownership, use, storage, sharing, and the risk of abuse of personal identity and biometric data in such highly distributed scenarios. Work on defining a standard, open stack of technologies to implement decentralized architectures is being proposed as a way of starting the consolidation and standardization process in this domain. As part of this work, particular importance must be given to the specific aspect of standardizing the human-device interfaces when exchanging and using personal biometric information as a way of identifying and authorizing people and their access to devices and systems in decentralized, autonomous networks where such personal information is not and should not be centralized and stored in any specific place.

We propose to define, design, and implement a model, a reference architecture and a set of standard APIs to be used by sensors and connected devices to handle biometric identity information, with fine-grained user-defined permissions for use in autonomous, decentralized IoT scenarios.

Summary

Primary authors: DI MEGLIO, Alberto (CERN); MANCA, Marco (CERN)

Presenter: DI MEGLIO, Alberto (CERN)