IoT Identity and Access Management Subgroup Proposal

Ahmad Sghaier Omar and Bilal Saleh

Background:

The role of identity management in the Internet of Things (IoT) is expanding to address how to identify IoT devices, manage their interactions and the services they offer, and control access to sensitive data. This requires Identity and Access Management (IAM) to be capable of managing human-to-device, device-to-device, and/or device-to-service/system interactions. Additionally, in many cases IoT devices are connected intermittently and/or temporarily and during that period they are required to communicate with other devices, services and the infrastructure. Commencing the communication requires that devices authentication and authorization to be performed according to a well-governed identity management life cycle that can ensure unique and global identification mechanism.

Problem:

The vast majority of telecom device management platforms are centralized where an authority handles the interaction between its own devices and with other devices belonging to other authorities. Among other limitations this centralized management model introduces, it does not allow devices to communicate and exchange data in a secure peer-to-peer fashion. This limitation constitutes a foundational flaw that will hamper the massive anticipated IoT devices growth and adoption.

Solution:

The limitations of the centralized device management model can be addressed by a shared and decentralized solution based on DLT. DLT offers a secure and trusted peer-to-peer data exchange among IoT devices. Due to its inherent immutability and anonymity features, a DLT-based IoT device management solution can maintain historical records and can also protect the identities of devices and users.

Some key device management requirements for a peer-to-peer IoT network include

- Global IoT device registry
- Device identity life cycle process management
- Device Registration processes.
- Device ownership management, including ownership transfer
- Device life cycle management
- Device Identity portability

A DLT-based IoT IAM solution enables the assignment of a unique and global digital identity for each device. Such identity can be maintained throughout the device life cycle, including the management of device ownership and identity update. Additionally, it can maintain device identity life cycle through a set of smart contracts that handle business processes and rules execution [1].

A Blockchain-based IoT IAM implementation offers a number of logistical and financial benefits to ecosystem participants in any vertical, particularly the Telecommunication industry. These benefits stem from the basic DLT promise of increasing transparency, security, and reducing friction and complexity which in turn reduce costs.

Proposal:

We propose the creation of the IoT IAM subgroup under the Telecom SIG with the purpose of coming up with a Hyperledger-based IoT Identity and Access Management solution and develop a Proof of Concept (PoC). The goal is to demonstrate through a functioning PoC how DLT can be leveraged to manage IoT devices and to control access to them using smart contracts.

We also propose develop formal working relationships with the Hyperledger Indy group and the Telecom Management Forum (TMF). Working with TMF is critical for DLT adoption in the IoT space from an interoperability and integration with legacy OSS/BSS.

PoC Use Case:

The GSM Association (GSMA) manages the allocation of International Mobile Equipment Identity (IMEI) it issues to device manufacturers to ensure that no two devices have the same IMEI. The GSMA stores basic information associated with each IMEI, such as the manufacturer name and the device model identifier in the IMEI Database (IMEI DB).

The IMEI DB is a central database under the full control of the GSMA. It contains the IMEI numbers of millions of mobile phones and data cards that are in use across the GSM and LTE networks globally.

One of the drawbacks of the GSMA's centralized IMEI DB lies in its power of imposing high membership fees on its members which prohibit many small operators, particularly in developing countries, from joining and connecting their Equipment Identity Register (EIR) with the GSMA's Central Equipment Identity Register (CEIR). This problem not only shuns small operators from participating in the global smart phone supply chain, but also retailers who would like to sell to them.

Another drawback is the slow process for accessing and updating the IMEI DB which is strictly limited to the participating service providers. The process of reporting theft or stolen devices, for example, is a very tedious and slow due the lack of trust and transparency. It is very difficult for reporter of theft to prove his/her ownership of the device. Thus, reporting a stolen device takes days and weeks before the IMEI DB is updated and replicated across all operators' EIRs.

Among the estimated 1250 mobile operators worldwide, only 119 operators have joined the GSMA IMEIDB, according to GSMA website, by end of 2018 [3]. This represents approximately 10% of total number of operators participating in providing information and utilizing the GSMA IMEIDB to counteract a problem amounting to losses estimated at 45.3 billion EUR [4] and among the main reasons to the lack of adoption is the centralized approach used in managing IMEI DB.

We propose that the subgroup develops a decentralized IMEI registry along with a simple device lifecycle management based on Hyperledger Fabric and smart contracts. The decentralized IMEI DB solution will demonstrate the use of Decentralized Identity Identifiers and Verifiable Claims based on the DID W3C specification [5]. It will also utilize Hyperledger Indy for identity creation and claims verification. The verifiable claims will address cases such as proof of ownership, proof of valid authorities' certifications (e.g. FCC, CE, IC).

The solution will have at least two smart contracts. The first smart contract is a registrar that will handle manufacturers, operators, and third parties' registrations, with the possibility of implementing automatic TAC generation and allocation. The second smart contract will handle device identity CRUD operations, as well as ownership transfers.

References:

1- A. Sghaier Omar and O. Basir “"Identity Management in IoT Networks Using Blockchain and Smart Contracts." **https://doi.org/10.1109/Cybermatics_2018.2018.00187**

2- GSMA Membership Fees, [Online] Available: **https://www.gsma.com/membership/membership-fees/**

3- IMEI Showcase, Dec 2017, [Online] Available: **https://imeishowcase.gsma.com/en#!/imeiblacklist**

4- N. Wajsman and A. Burgos and C. Davies and M. Mani and S. Kumar, “The Economic Impact of Intellectual Property Rights (IPR) Infringement in Smartphone Sector,” Rep. European Union Intellectual Property office, Feb. 2017. **https://euipo.europa.eu/tunnel/ipinfringement/smartphonesectoren.pdf.**

5- DID Decentralized Identifiers v1.0 Core Data Model and Syntax, **https://www.w3.org/TR/2019/WD-did-core-20191107/**