IOTA
ACCESS
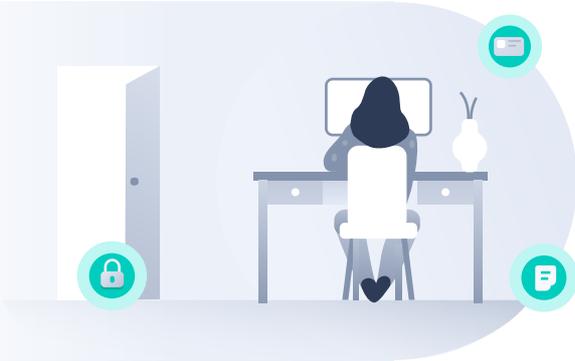
01

Alice runs her company in a building with smart locks. Alice writes a Policy where her employees are allowed to enter the building only under specific conditions (such as time, employee ID, clearance level).

02

Alice owns a vehicle that she wants to rent for Bob for 260 MIOTA. Bob is able to use this device after transferring 260 MIOTA to the Device's (or Alice's) Wallet.

CHALLENGE

How to remotely delegate access to physical devices and data streams in a **secure, fault tolerant** and **auditable** manner?

A highly flexible framework for access-control - natively integrated with **Distributed Ledger Technology** and **secure hardware** support is the best way to efficiently solve this problem.

IOTA Access

IOTA Access is a DLT-based open-source framework for building access control systems for IoT resources such as vehicles, wallets, smart locks and sensor data. With IOTA Access, you can build and embed applications inside your resources to:

- Grant and revoke access at any time
- Charge users for access
- Set access restrictions

ACCESS CLIENT

ACCESS SERVER

IPMI
Smart Vehicle
Smart Scooter
Data Streams
Smart Lock

Target Device

IOTA

Access Policies

IOTA Access encodes the logic for access control into **Policies**. Attributes are described in combination with binary operations that result in the **_(grant, deny, conflict, undefined)_** set of logical outcomes for access control of some target resource.

ACCESS POLICY UPDATE — Alice (Device Owner) → Access Policy → IOTA Permanode (Storage of the Tangle's entire history) → Target Device

Policies contain rules that define which actions a user may access.
Policies are objects with the following data structure:

- **Policy ID:** Signed hash of the Policy.
- **Policy Object ID:** Identifier of the target device.
- **Signature Object ID:** Identifier of the human/device who wants to control the target device.
- **Actions:** List of actions to be performed, with attributes, conditions and obligations.

Device Rental Scenario

Alice owns a Device that she wants to rent to Bob for 260 MIOTA. Bob will be able to use this device after transferring 260 MIOTA to the Device's (or Alice's) Wallet. Alice uses Access Mobile Client to create the Policy that delegates device access to renters. She stores the Policy on an IOTA Permanode. Bob uses Access Mobile Client to pay the rental fee and initiate Access Requests, while the outcome to his requests are stored on the Tangle.

ACCESS REQUEST

Bob (Permitted User) — Access Request + Tx Hash → Target Device — Access Decision → Bob (Permitted User)

Rental Fee

Verify Payment (Tx Hash)

Log Action

IOTA