When IoT devices work in cooperation with each other, a system operator must shut out any malicious devices. We developed a framework that gives a certificate for IoT devices to work cooperatively. We constructed a cargo delivery demo system that can supply and invalidate certificates easily and safely. It prevents spoofing and unpermitted actions of IoT devices.

Features

- Enables safe control of validation/invalidation of certificates among IoT devices.
- Identity (ID)-based encryption*1 and pairing*2 encryption enable system operators to easily manage permitted IoT devices or usage time.
- When one IoT device verifies another IoT device, there is no need for server access or authentication. Thus, authentication between IoT devices can be done offline without the devices having to access the server.

Application Scenarios

- Home delivery services, with optimization of cargo delivery*3 by auto-collection and delivery with drones.
- Rental car services, with efficient car-sharing using cars*4 and electric engine keys.

---

*1 ID-based encryption: a kind of public key encryption that uses IDs
*2 Pairing: mapping from two points on elliptic curve to a finite field
*3 Number of cargo deliveries: about 3.745 billion (according to a survey by MLIT in 2015)
*4 Number of rental cars: about 597 thousand (according to a survey by MLIT in 2014)