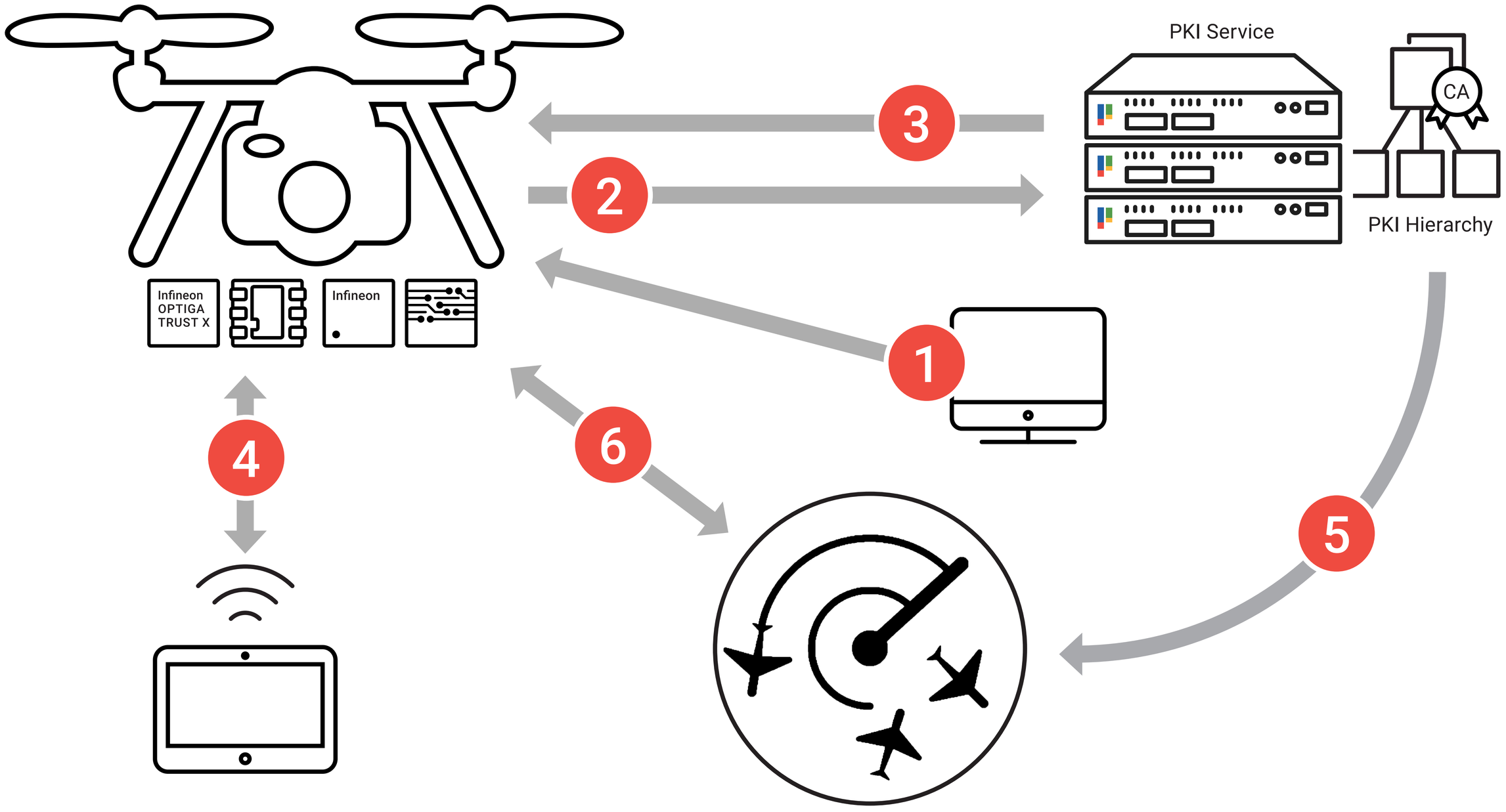
Multicopter Safety via Security
PKI in Action



Working Scenario:

1.
Initialization: Login and trigger certificate issuing. Key generation and signature creation is happening inside the secured hardware.

2.
Send certificate signing request to the PKI service.

3.
Send certificate(s) back to multicopter and store certificate(s).

4.
Activate credentials to allow multicopter flight.

5.
Flight control is part of the PKI hierarchy.

6.
Flight control could shutdown multicopter in case of non compliance, revocation, etc.

Motivation:

- Major incidents occur more often and the number of disruption reports continue to grow due to multicopters misuse and deliberate attacks.
- Targeted sites include airports: Frankfurt, Berlin, Gatwick, and Heathrow, for example.
- New reported incidents include: Oil pipeline cyberattack in the US, used as Improvised Explosive Devices (IEDs).

Threats:

- Manipulation of multicopter control software to disable no-flight zone, controlled airspace, etc.
- Misuse and deliberate attacks by anonymous users.
- Removal of controlled access from official bodies.

Solution(s):

Secure, anti-tamper solutions to enable embedded application security combined with remote accreditation and revocation. This enables market leading defenses used by government agencies and authorities to oversee controlled flight zones, owner ID, geo-fencing and geo-tracing.

- Flight control via secure certificate-based authorization.
- Simultaneous authorization and revocation from official bodies.
- Certificates and credentials are stored in secured hardware and eco systems via:
  - *OPTIGA™ Trust X* for core security, trusted user and cloud connectivity.
  - *NC1023* (eSIM) for secure 5G embedded connectivity with active control and beacon enablement.