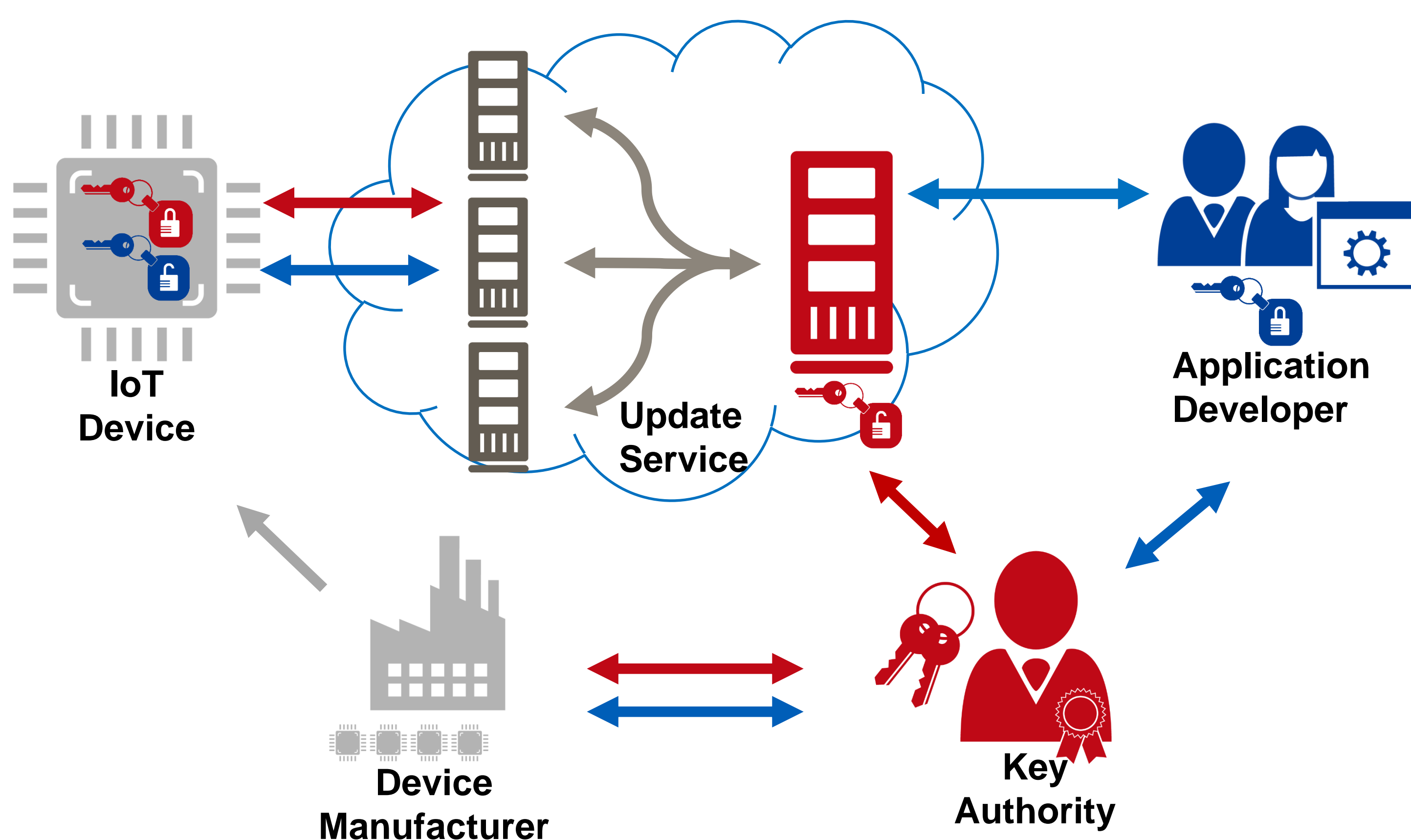


# How can **cloud computing** assist the management and **secure software update** of tiny IoT devices?

## Motivation

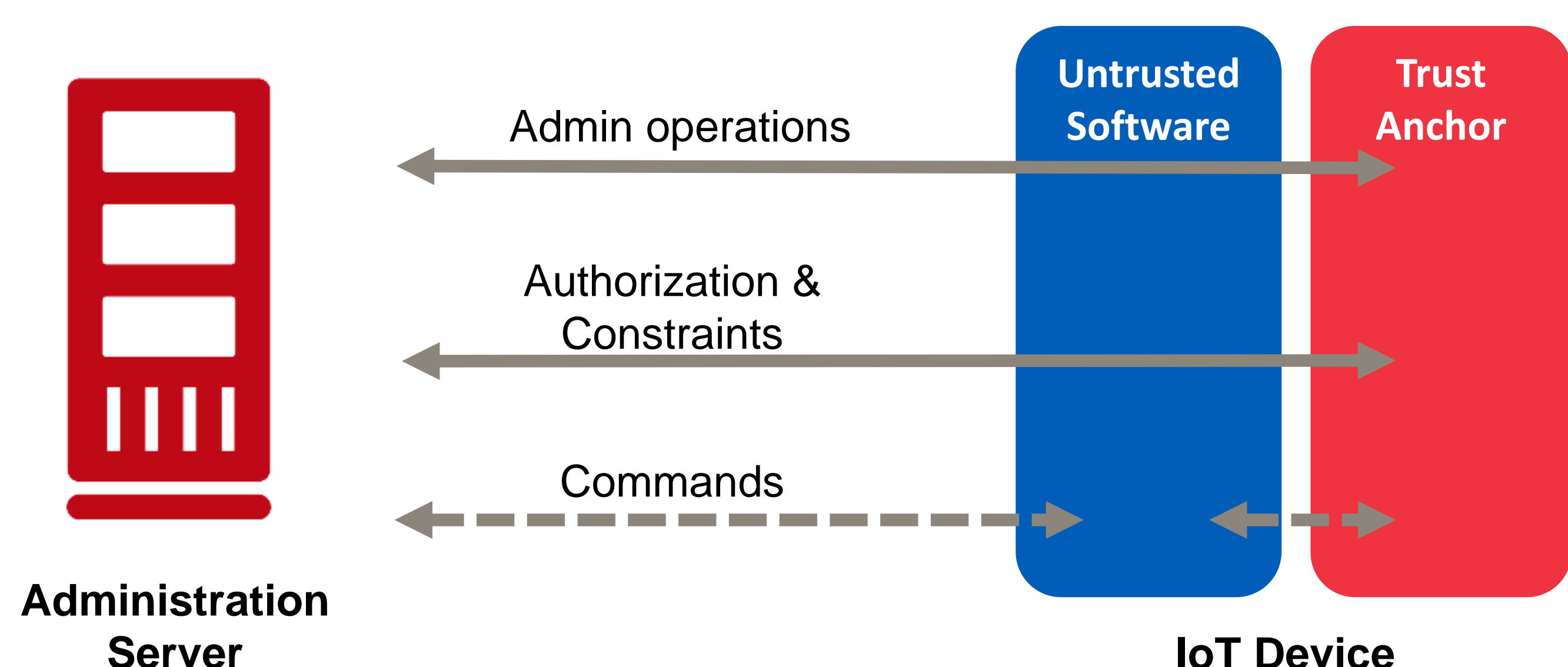
- **Resource-constrained** IoT devices used in **prolonged**, possibly **unattended** in the field
- Updates needed to **fix software flaws** and **enable new features**
- No established **open standards** for **over-the-air updates** in tiny IoT devices
  - State of the art: **Ad hoc proprietary solutions** or **lack of support** for in the field updates



Cloud-assisted management architecture

## Research directions

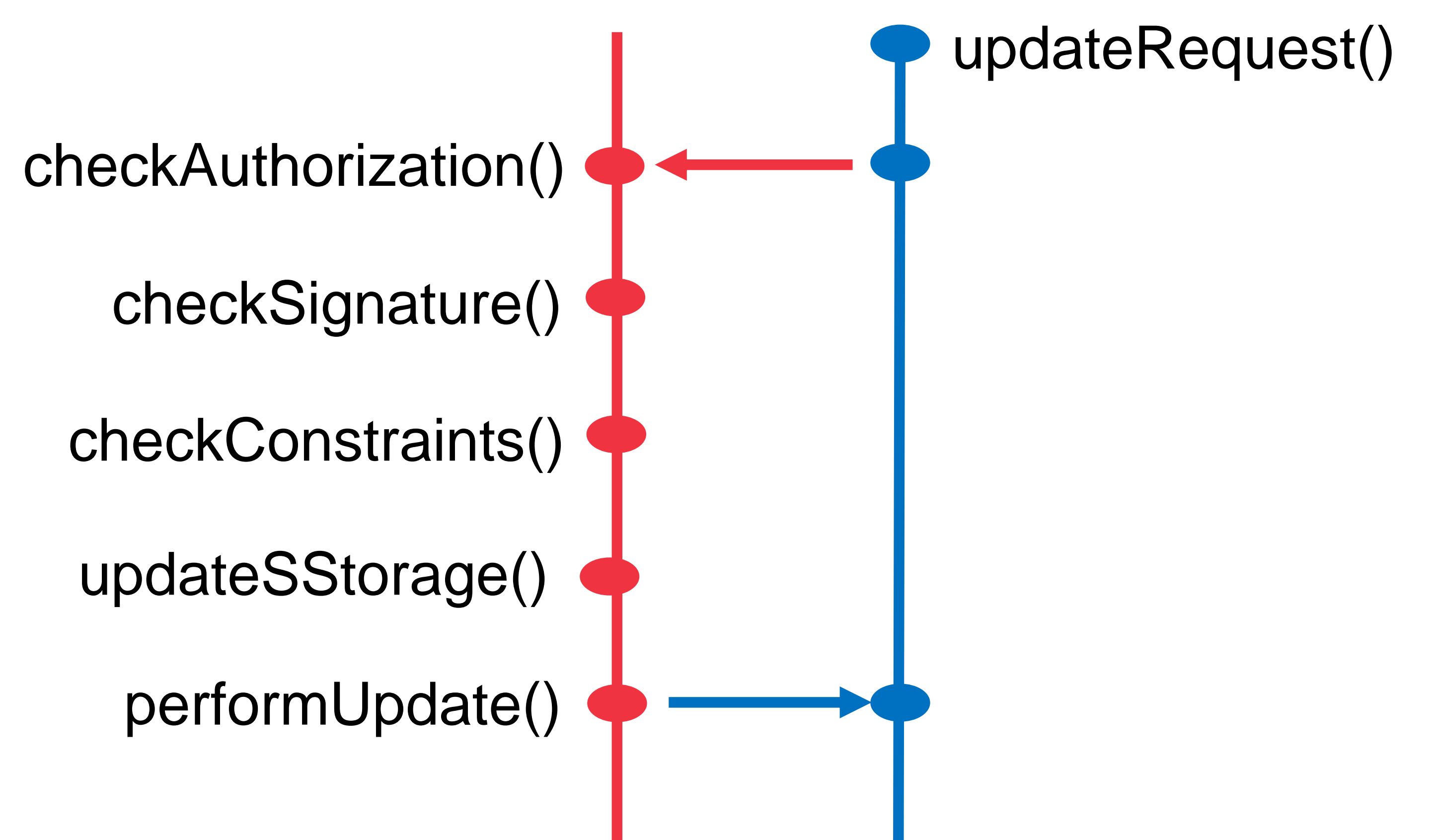
- Utilize **hardware-based trust anchors** in modern MCUs, e.g. **ARM TrustZone-M**
- Evaluate proposed **open standards**:
  - IETF **Open Trust Protocol** defines **PKI** and **web-centric messages** between devices and **Trusted Service Managers**
  - GlobalPlatform **TEE Management Framework** defines mechanisms for **Security Domains** and encapsulation of **authorized software** and **configuration**



GlobalPlatform TMF architecture overview

## Device concerns and requirements

- **Authenticity** and **integrity** of update
- **Immutable** device **identity**
- **Secure storage** for critical data
- **Security domains** with different **constraints** and **policies**
- **Rollback protection** of software and configuration
- **Robustness** and **operational impact**
- **Reachability** of devices with **intermittent connectivity**
- **Privacy** in **consumer devices**



Trust Anchor and Untrusted Software interaction

## Benefits from cloud-assistance

- **Pervasiveness** enables update deployment monitoring and device analytics
- **Scalability** of back-end functions to large-scale deployments
- **Elasticity** for scheduling **staged update** rollouts, e.g. security critical updates