



Enterprise IoT WG

Topics

- WG Background and Perspective
- Motivational Document
- Enterprise IoT Lifecycle Management Checklist
 - Checklist
 - Examples
- Next steps
- Deferred opportunities – IETF progress on management
- Participate!

WG Background and Perspective

- Started as a fusion effort by Internet2 CINO, T&I and ITANA, a national group of IT architects in 2016
- Perspective is enterprise-centric – what can the institution do to leverage and manage IoT, whether the things are organizational or consumer owned.
- Perspective is constructionist, realistic goals
- Bi-weekly calls, active notes and document curation
- Two immediate activities
 - Motivational Document – intent is to get campus leadership attention via relevant use cases
 - Enterprise IoT Lifecycle Management Checklist
 - Some samples

Motivational Document and Risk Examples

- Intended for C-level leadership
- Presents both the opportunities and the risks associated with IoT on campus
 - Opportunities for research, institutional efficiencies, even improved student outcomes
 - Risks are financial, reputational, operational, and legion
- Has a set of examples to be inserted into the briefing doc, depending on institutional profile
 - Medical school, Engineering, Facilities, etc.
- Provides a list of lessons learned:
 - Pay attention
 - Understand that horses have left the barn
 - Look for gaps in responsibilities, lack of authority, etc.
 - New needs for data stewardship
 - A lifecycle approach is useful
- https://docs.google.com/document/d/1Gn_ULiRu5DgkZS5N98aUXvJ876Ty7wIWzsLDdkl_EXM/edit

Enterprise IoT Lifecycle Management Checklist

- An evolving set of questions to help direct the acquisition, deployment, and continuing management of IoT
- Intended to be useful across all types of institutional acquisitions, including research, health safety and security, operational, etc.
- Lifecycle phases include:
 - Discovery, Planning, Acquisition, Deployment, Maintenance and Decommissioning
 - Topics include network requirements, power requirements, security needs, privacy issues, data processing, etc.
- Intended to illuminate gaps, build connections, etc.
 - RACI analysis may be useful
- https://docs.google.com/document/d/15m6oMwQGBv1SNeVBO2SncpBNi9ZAd6w_JmYJw0QPeNo/edit

Three sample lifecycle checklists

- An emergency management system making extensive use of campus sensors, end-user devices, alarm and notification systems, etc.
- An acquisition of a IoT research system by an academic department
- An innovative student outcomes initiative that connects student schedules to sensors attached to preferred exercise devices in the Recreation Center, identifying exercise opportunities in real time
- https://docs.google.com/document/d/1C-M2Kq9E1E9K27UJTXPX2cVUNfnr4_DqTrML4F7PVvg/edit

Deferred opportunities

- Fingerprinting devices
- Integrated IAM and IoT
 - Several basic ingredients are being formulated by IETF
- Virtual segmentation and the elastic network perimeter
- Tracking IoT cybersecurity legislation

IETF activities – CORE and CoAP

- <https://www.internetsociety.org/blog/2017/11/rough-guide-ietf-100-internet-things/>
- CORE WG – CONstrained Restful Environments –
 - <https://tools.ietf.org/wg/core/>
 - Key output is CoAP – Constrained Application Protocol
 - <https://tools.ietf.org/html/rfc7252> and <http://coap.technology/>
 - specialized web transfer protocol for use with constrained nodes and constrained (e.g., low-power, lossy) networks. The protocol is designed for machine-to-machine (M2M) applications such as smart energy and building automation.
 - CoAP provides a request/response interaction model between application endpoints, supports built-in discovery of services and resources, and includes key concepts of the Web such as URIs and Internet media types. CoAP is designed to easily interface with HTTP for integration with the Web while meeting specialized requirements such as multicast support, very low overhead and simplicity for constrained environments.
 - See <http://coap.technology/impls.html> for implementations

IETF - ACE

- Authentication and Authorization for Constrained Environments
 - A framework for specific profiles and implementations
- Use cases at <https://tools.ietf.org/html/rfc7744>
- Intent is to transport OAuth tokens across CoAP to devices
- Draft Architecture at <https://tools.ietf.org/html/draft-ietf-ace-actors-06>
- " This means that the complexity of authenticated authorization can often be moved back and forth between these two aspects."

ACE Architecture

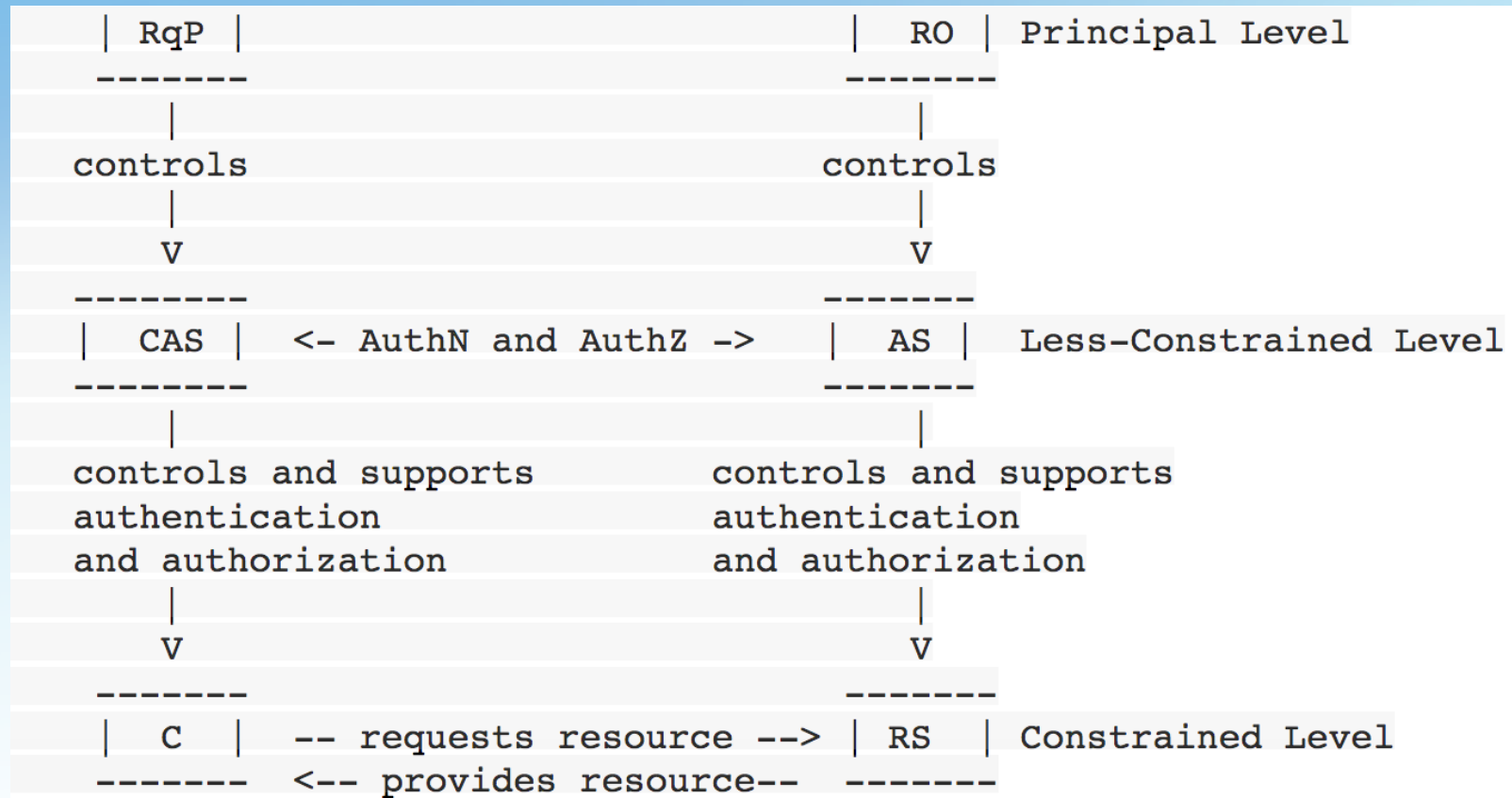


Figure 3: Overall architecture

Resources

- Enterprise-IoT WG Home for call agenda, notes, pointers to docs
 - <https://docs.google.com/document/d/100mjiAu9k3Al6JEUhO-w1JEKx3pjuXnMq7sEWXLCYhk/edit?pli=1>
- Motivational Briefing Doc
 - https://docs.google.com/document/d/1Gn_ULiRu5DgkZS5N98aUXvJ876Ty7wIWzsLDdki_EXM/edit
- Use cases for motivational doc
 - https://docs.google.com/document/d/1FVKpeFXLWGZRokZst86E6cUPHghqr7sejRw_RT2sfwA/edit
- Enterprise Lifecycle IoT Management checklist
 - https://docs.google.com/document/d/15m6oMwQGBv1SNeVBO2SncpBNi9ZAd6w_JmYJw0QPeno/edit
- Sample checklist responses
 - https://docs.google.com/document/d/1C-M2Kq9E1E9K27UJTXPX2cVUNfnr4_DqTrML4F7PVvg/edit