# Thing-to-Thing proposed Research Group + W3C IG WoT

Thing-to-Thing pRG (T2TRG) + W3C IG WoT joint meeting

Summary meeting

Praha, CZ, 2015-07-18..-19+20

Prof. Dr.-Ing. Carsten Bormann

*TZI – Universität Bremen*

# Note Well

- You may be recorded
- The IPR guidelines of the IETF apply:
  see **http://irtf.org/ipr** for details.

# Administrivia (I)

- Pink Sheet
- Note-Takers
- Off-site (Jabber, Hangout?)
  - **xmpp:t2trg@jabber.ietf.org?join**
  - **https://plus.google.com/hangouts/_/_____**
- Mailing List: **t2trg@irtf.org** — subscribe at: **https://www.ietf.org/mailman/listinfo/t2trg**
- Repo: **https://github.com/t2trg/2015-ietf93**

# Agenda

- 15:20–15:50 Introduction
- 15:50–16:20 Updates from Consortia etc.
  - Georgios Karagiannis: AIOTI
  - Dave Thaler: Notes about the Alljoyn security model
- 16:20–17:00 Report from W3C/T2TRG meeting
  - Overview; working with CoRE, ACE
- 17:00–17:20 Way forward

# Agenda

- 15:20–15:50 Introduction
- 15:50–16:20 Updates from Consortia etc.
  - Georgios Karagiannis: AIOTI
  - Dave Thaler: Notes about the Alljoyn security model
- 16:20–17:00 Report from W3C/T2TRG meeting
  - Overview; working with CoRE, ACE
- 17:00–17:20 Way forward

# Poll

Who has been at a
T2TRG meeting?

# IETF: Constrained Node Network Cluster

| | | |
|---|---|---|
| INT | LWIG | Guidance |
| INT | 6Lo | IP-over-foo |
| INT | 6TiSCH | IP over TSCH |
| RTG | ROLL | Routing (RPL) |
| APP | CoRE | REST (CoAP) + Ops |
| SEC | DICE | Improving DTLS |
| SEC | ACE | Constrained AA |
| SEC | COSE | Object Security |

*) WG Charter in review

# IoT directorate

- Informal gathering of IoT experts working in and watching this space (run by INT AD)
- **good** to keep information flowing
- not that useful to
  - get work done
  - draw in wider expertise

# IRTF: Internet Research Task Force (sister of IETF)

- IRTF complements IETF with longer-term **Research Groups**
- Thing-to-Thing Research Group (T2TRG)
- Investigate open research issues in:
  - turning a true "Internet of Things" into reality,
  - an Internet where low-resource nodes ("Things", "Constrained Nodes") can communicate among themselves and with the wider Internet, in order to partake in permissionless innovation.

# Thing-to-Thing Research Group (T2TRG)

- Focus: issues that touch opportunities for standardization in the IETF
  - start at the adaptation layer connecting devices to IP, and
  - end at the application layer with architectures and APIs for communicating and making data and management functions (including security functions) available.

# W3C IG WoT

- W3C: The people who make the Web work
- IG: Interest Group
- WoT: Web of Things

# Why a Research Group now?

- First wave of IoT standards completed by the IETF
- IoT Consortia now forming to build infrastructure and industry agreements around those

➔ New requirements for research:
based on actual usage of the standards now available

# Areas of Interest

(to be discussed in formal chartering)

- Understanding and managing the motivation for single-purpose silos and gateways; facilitating a move towards small pieces loosely joined (hence “thing-to-thing”); scaling the number of applications in a single network
- Deployment considerations; scaling considerations; cost of ownership
- Management and Operation of Things
- Lifecycle aspects (including, but not limited to, security considerations)
- Cooperation with W3C, e.g. on data formats and semantics

# Areas of Interest (more explorative)

- Operating Things that have multiple masters/ stakeholders (including understanding role definitions of devices, owners, operators etc.)
- Exploring the duality of state- and event-based approaches
- Aspects of distribution (cf. “fog computing”); reliability and scalability considerations
- Containerization and other forms of mobile code

# Other objectives

- Definition of “Benchmark” or Reference Environments:
  - to enable regular plugfests, and
  - as a basis for repeatable, comparable research.
- Description of practical, real world, cross domain applications of connected Things
- Taxonomy, technology survey and best practice documents
- Fostering collaboration with industry fora and other organizations on networking of things

# Name, organization

- “Thing-to-Thing” is a homage to “end-to-end” RG
  - Not meant to exclude device-to-cloud models
- Open membership
  - emulate DTNRG or ICNRG as a model

# Relationship to IETF WGs

- These objectives will be achieved making use of a close involvement between the IETF community and the T2TRG.

- For the IETF, some RG documents may simplify the generation of (or even serve as) use case documents or other informational references.

- Close contact will be maintained with the IETF's IoT-related WGs and its IoT directorate.

# Relationship to IAB

- IAB workshops can be very successful in breaking ground
- 2011: Smart Object Workshop (Prague). RFC 6574
  - Also seminal for RFC 7228
- 2012: Smart Object Security (Paris). RFC 7397
  - Not an official IAB workshop
- Expect good cooperation with further IAB activities

# Agenda

- 15:20–15:50 Introduction
- 15:50–16:20 Updates from Consortia etc.
  - Georgios Karagiannis: AIOTI
  - Dave Thaler: Notes about the Alljoyn security model
- 16:20–17:00 Report from W3C/T2TRG meeting
  - Overview; working with CoRE, ACE
- 17:00–17:20 Way forward

# Alliance for Internet of Things Innovation (AIOTI)

**Georgios Karagiannis**

*Huawei Technologies*

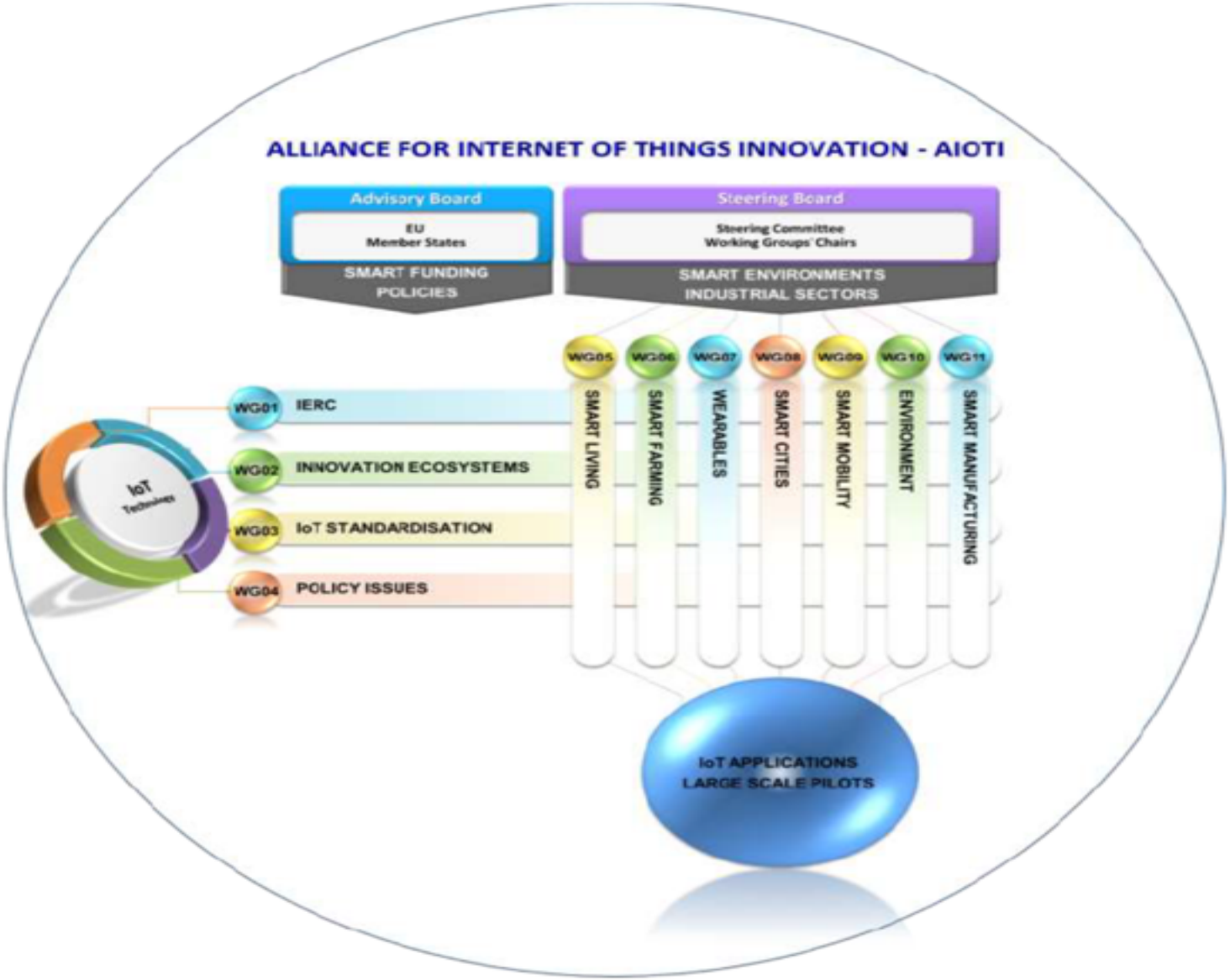
# IoT requires a Digital Single Market

- ***Eliminating barriers to operate across borders (e.g. roaming for connected cars)***
- ***Economics of scale and scope to lower costs, increase efficiency and enhance innovation***
- ***Inter-operability and common standards***
- ***Strive for globally-wide IoT innovation eco-systems***
- ***Strive for a common legal framework (trust, copyright, security, privacy, liabilities, ethics, etc.)***

# AIOTI Mission


- *Alliance launched by European Commission on 25 March 2015*
  - *http://www.aioti.eu/*
- *Place for action, a body oriented towards fast and concrete results, and whose members effectively contribute to planned works and activities*
- *Mission:*
  - *Building an IoT innovation ecosystem across the value chain /across silos*
  - *Put IoT on the map and link it to other EU and national initiatives*
  - *Prepare Large Scale Pilots for 2016*
  - *Advancing IoT convergence across verticals for standardisation/ interoperability*
  - *Discuss with industry to provide guidance for IoT in the DSM*

# AIOTI Structure



# Possible cooperation between AIOTI and IRTF T2TRG

- *AIOTI WG1 IERC: IoT European Research Cluster*
  - *Bringing together projects companies, organizations, people and knowledge at European level with the aim of defining a common vision of IoT technology and addressing European Research challenges*
    - *Research challenges identified by AIOTI WG1 can be used as input for the T2TRG research*
    - *T2TRG documents can serve as recommendations for the IoT research done in the context of AIOTI WG1*
- *AIOTI WG3 IoT Standardisation*
  - *Mapping of existing IoT standards and gap analysis, as well as defining strategies and use cases to develop (semantic) interoperability*
  - *T2TRG can cooperate with AIOTI WG3 on:*
    - *identifying gaps in existing Internet based IoT standards and proposing solutions on how they can be addressed*
    - *defining strategies and use cases to develop (semantic) interoperability*

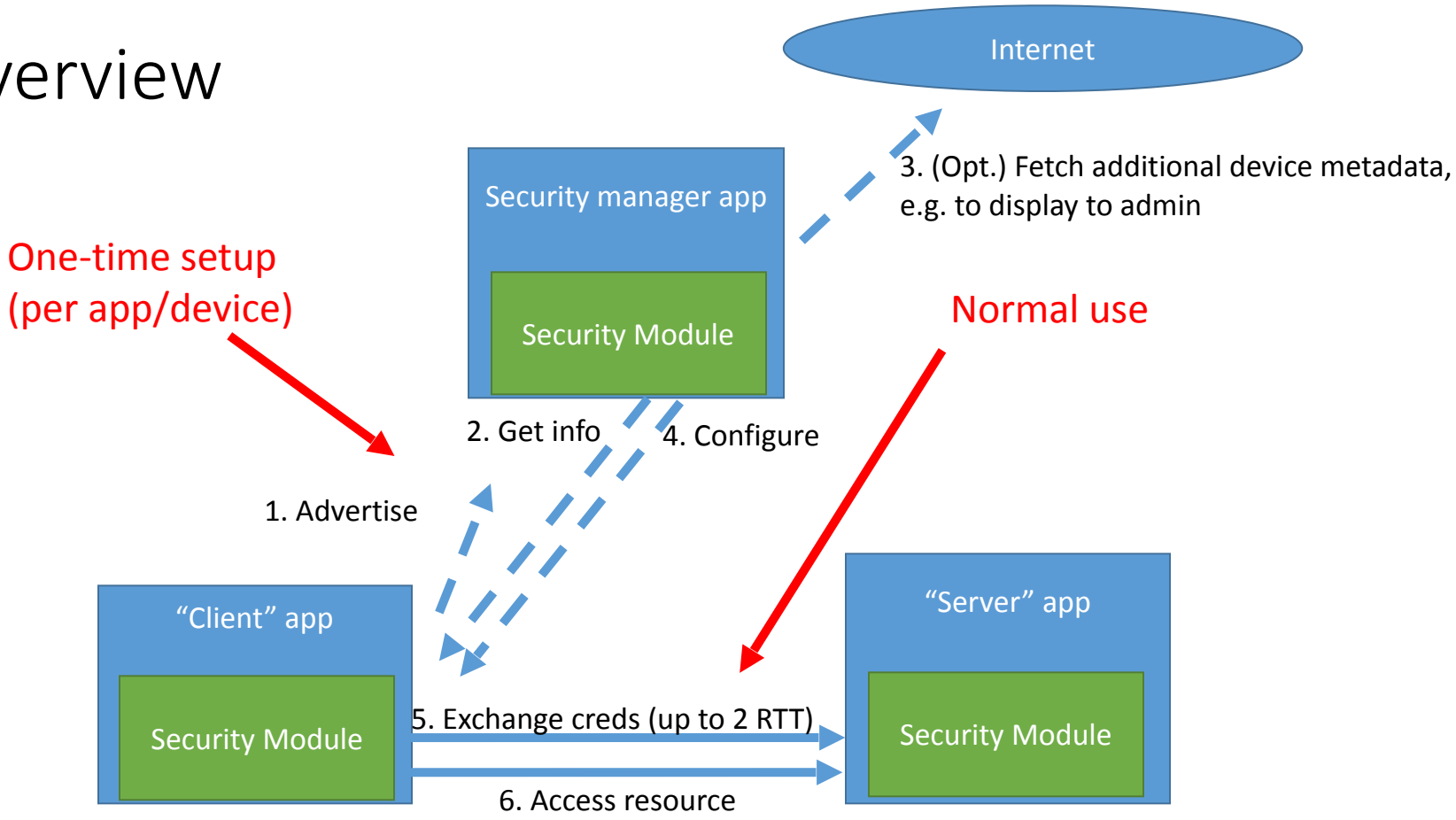
*Thank you*

# AllJoyn Security Model

https://allseenalliance.org/developers/learn/core/security2_0/hld

Dave Thaler <dthaler@microsoft.com>

# Overview


Internet
Security manager app
Security Module
3. (Opt.) Fetch additional device metadata, e.g. to display to admin
One-time setup (per app/device)
Normal use
2. Get info
4. Configure
1. Advertise
"Client" app
Security Module
"Server" app
Security Module
5. Exchange creds (up to 2 RTT)
6. Access resource

# Security principals

- Identity (“identity cert”)
  - An identity is actually a cert chain
  - Every application/device has its own identity
  - Root is the identity/group that runs/owns it
  - Delegation is permitted if one’s identity cert allows it
- Security group (“membership cert”)
  - Membership in a security group is also a cert chain with a membership cert as a leaf
  - Can get a membership cert chain from a different root from your identity
  - Every application/device also has membership certs for 0 or more security groups
  - Delegation is permitted if one’s membership cert allows it
- Certificate revocation *permitted* via CRL checking but no hard dependency on availability

# Examples

- Users:
  - Dad (self-signed)
  - Mom (self-signed)
  - Son (signed by Mom)
- Devices:
  - TV: admin = Dad
  - DCR: admin = HomeAdmin
  - Son's tablet: admin = Son
- Mom's Security groups:
  - HomeAdmins: { Dad, Mom }
  - LivingRoomDevices: { TV, DVR }

# Authentication

- An app has a set of trusted roots
- Identity is trusted if a locally trusted root appears anywhere in a peer's (identity or membership) certificate chain
- Identity cert chains exchanged at start of connection (usually mutual auth)
- Also provides membership certs that chain up to a cert in peer's identity cert chain
- Another option is the "real estate agent" scenario where your membership cert can be pre-provisioned in peer app/device and yours

# Authorization

- AllJoyn has both an **ACL** model and a **capabilities** model
  - *Both* checks must succeed for a call to succeed
- ACLs are on your resources and control what *peers* are allowed to do
- Capabilities are what *you* are allowed to do (enforced by peer)
  - Capabilities help protect against compromised apps/devices

# ACLs

- ACL (“policy”) are private between the app/device and its admin(s)
- Resources can be ACL’ed to a set of any of:
  - All (anonymous)
  - Any authenticated
  - Any authenticated that chains up to a given certificate authority
  - A specific security group
  - A specific identity (public key)
- ACL entries have separate flags for read vs write
- Optionally can also ACL who you will send outgoing calls to

# Capabilities, similar to “app manifest”

- Each application has a list of what resource paths (“interfaces”), but not resource instances, it can possibly access and expose
  - AllJoyn uses a hierarchical resource naming scheme that includes DNS names for uniqueness, similar to an XML namespace
- Authorized set of capabilities get signed by same entity as your identity cert (referred to as a “security manager”)
- When app is claimed, security manager gets this, and authorizes it for all or some (possibly empty) subset of these as part of giving it identity & membership certs
- Capabilities presented along with one’s certs when making a connection

# Bootstrapping

1. New app/device advertises itself as unclaimed
   - Could be passive advertisement (e.g., QR code)
   - Most common new device example is where device is a temporary WiFi SoftAP with a special SSID convention (or potentially IE's, etc. in future)
2. Security Manager app sees it, and queries its potential capabilities
   - Usually uses some sort of PSK/PIN scheme at this point, but could be anything
3. (Opt.) Get trusted textual descriptions etc. to assist human in acknowledging granting of capabilities
4. Security Manager configures app/device:
   - "Onboarding" = configuring L2 network credentials (e.g., WiFi keys) if needed
   - "Claiming" = configuring
     - 1 or more trusted root[1] certs
     - Identity cert chain
     - 0 or more membership cert chains
     - Signed capabilities
     - ACLs

[1]Manufacturer functionality such as app/firmware update might also use a manufacturer cert to verify code, but usually considered separate from rest of functionality

# Agenda

- 15:20–15:50 Introduction
- 15:50–16:20 Updates from Consortia etc.
  - Georgios Karagiannis: AIOTI
  - Dave Thaler: Notes about the Alljoyn security model
- 16:20–17:00 Report from W3C/T2TRG meeting
  - Overview; working with CoRE, ACE
- 17:00–17:20 Way forward

# This meeting

- Worked together with W3C IG WoT:
  - (A) “REST as we know it” ➔ “Beyond REST”
  - (B) Security and Lifecycle aspects in constrained nodes
- Focused on **common discussion**
- RG administrative things moved forward to next time

# Busy IETF weekend

- Fri/Sat: 6TiSCH/plugtest; Sun: 6TiSCH/**Hackathon**
- Sat/Sun: **Hackathon** (Chez Louis Room)
- Other RG meetings (Sun: ICNRG), ACM TPC, …
- Sun afternoon: IETF tutorials, …

https://github.com/t2trg/2015-ietf93/blob/master/agenda.md

# Agenda

Sat

- 10:00–13:00 Overview, Talks
- 13:00–18:00 Breakouts (A/B), start with Lunch

Hackathon invasions

Insert dinner here

Sun

- 09:00–10:00 Wrapup Breakouts
- 10:00–11:00 Talks
- 11:00–13:00 Breakouts (i/ii)
- 14:00–16:00 Wrapup, outlook, planning

Mon

- 15:20–17:20 Summary meeting (+ consortia)

# Results?

https://github.com/t2trg/2015-ietf93

# Near-term milestones

- Collect a small number of non-trivial, realistic **scenarios**
- Map technology to these scenarios; **evaluate**, benchmark, find gaps
- Document findings, best practices in **cookbooks**
- Run **plugReSTs** so researchers can test their approaches in the context of the scenarios

Evaluation Framework

# Direct exchange with IETF WGs

- 8 WGs in IoT Cluster
- Likely initial candidates:
  - CoRE
  - ACE

# 2010-03-09: CoRE

- “Constrained Restful Environments”
  - CoAP ➔ RFC 7252 (~~2013~~2014)
    - in processing: Observe, Block
  - Experimentals: RFC 7390 group communications
  - Discovery (»Link-Format«) ➔ RFC 6690

# The **Co**nstrained **A**pplication **P**rotocol

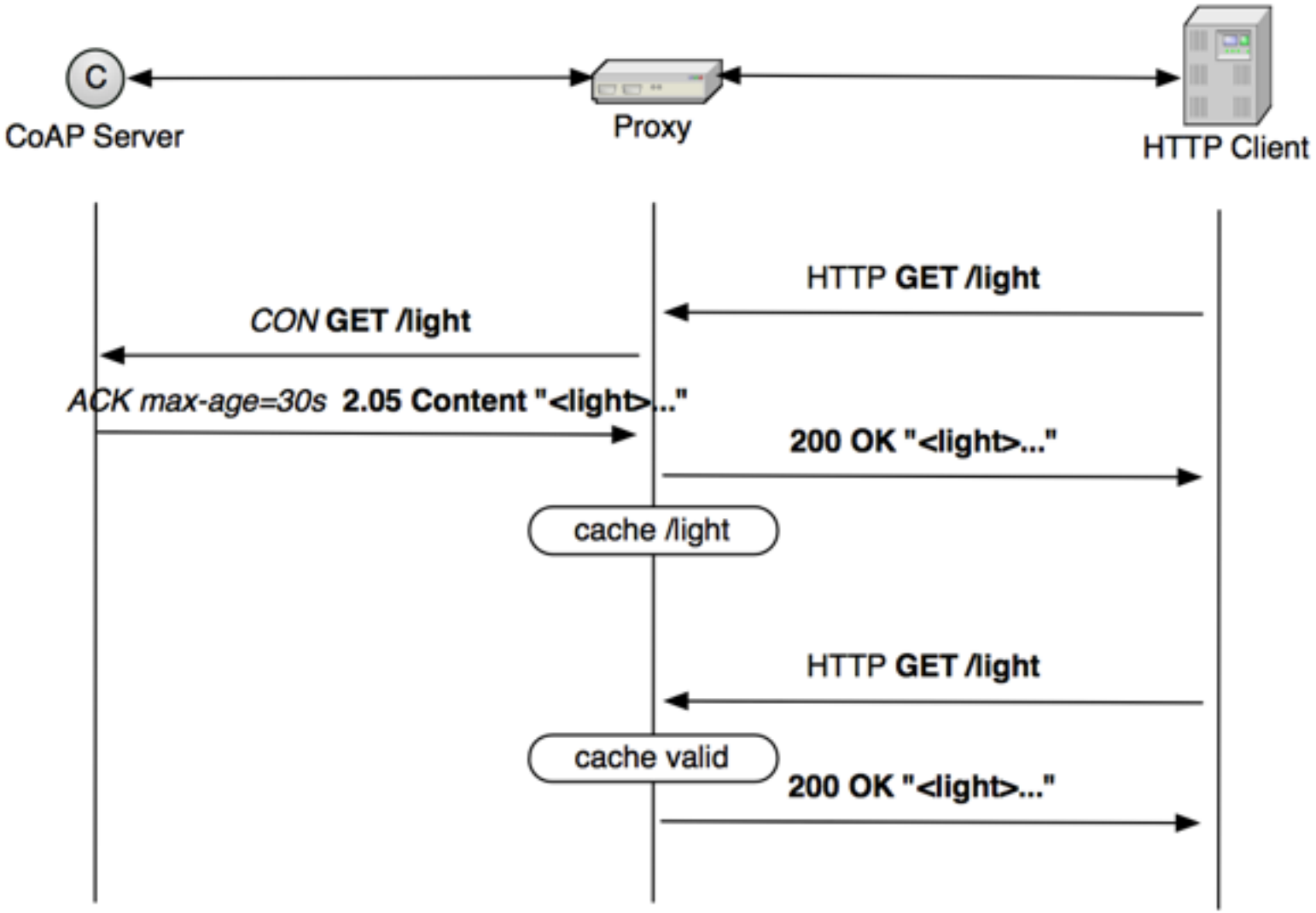
# CoAP

- implements HTTP's **REST** model
  - GET, PUT, DELETE, POST; media type model
- while avoiding most of the complexities of HTTP

- **Simple** protocol, datagram only (UDP, DTLS)
- 4-byte header, compact yet simple options encoding

- adds "observe", a lean notification architecture

# Proxying and caching




Source: 6lowpan.net

# REST

REST

Representational State Transfer

# How to use REST in IoT?

- Ignore it, build a SOAP on top
- Use it half-heartedly and reap some of the benefits
- Use it right
  - But does it really work well in the IoT?

RESEARCH

# What **is** the right way?

- Need to examine **non-trivial scenarios**
- Collect **authoritative** material
- Assemble a **cookbook** with design patterns
- **Yardsticks**? (cf. »Richardson Maturity Model«)

# CoRE work that might benefit

- COMI:
  Modeling collections; “Beyond URIs”
- Pubsub:
  event-state duality; subscription control resources
- Resource directory, CoRE interfaces:
  Resource structure (URIs may change, no implicit relation between parent and child resources, made explicit with link relations)
- SenML:
  A template for media type descriptions

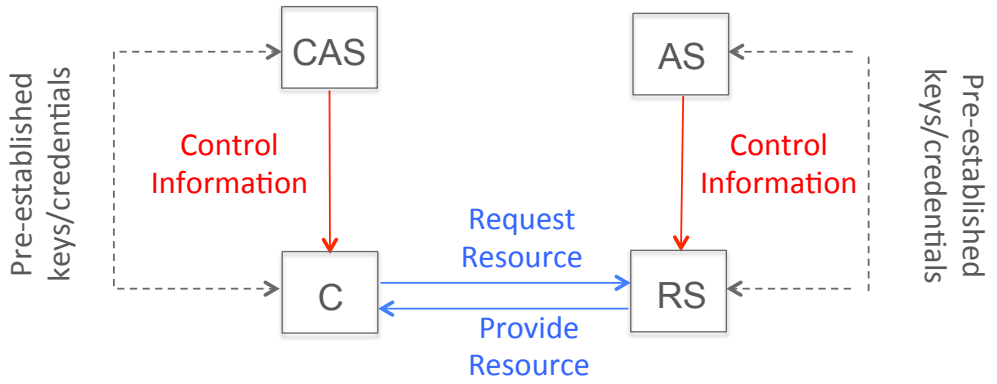
# Authentication and Authorization for Constrained Environments (ACE)

- WG formed on 2014-06-16
- Goals
  - Fine-grained **authorization** on constrained clients and servers
  - Focus on REST-based architectures
- Objectives
  - Look at existing technologies
  - Identify what is needed to support constrained devices
  - Focus on CoAP and DTLS in the beginning
- Tasks
  - Produce use cases and requirements
  - Identify authentication and authorization mechanisms suitable for resource access in constrained environments.

# ACE Architecture and Information Flows

Legend:

- Black boxes represent functions
  - Functions may be combined in one node
- Information flows in solid lines
  - Resource access (based on CoAP)
  - Control information (authorization information, keys, etc.)
  - Information flow may pass intermediary nodes




Information flows may be protected with session-based security (DTLS) or data object based security (COSE)

Source: draft-gerdes-ace-actors



Slide by Göran Selander
slides-93-cose-6.pdf

# T2TRG ↔ ACE

- Look at overall system security, at a full scenario level:
  - specific use cases from W3C IG WoT, ACE, and T2TRG
  - existing testbeds and installations
  - privacy aspects
  - evolvability
    - ownership transfer, "{bring,steal,sell} your own thermostat”
    - resilience to crypto disasters
- Use scenarios to evaluate solution proposals as discussed in the ACE WG; identify gaps

# Agenda

- 15:20–15:50 Introduction
- 15:50–16:20 Updates from Consortia etc.
  - Georgios Karagiannis: AIOTI
  - Dave Thaler: Notes about the Alljoyn security model
- 16:20–17:00 Report from W3C/T2TRG meeting
  - Overview; working with CoRE, ACE
- 17:00–17:20 Way forward

# Moving forward to an RG

- Need to work on charter
    - Working draft at https://datatracker.ietf.org/rg/t2trg/charter/
- Need to find 2–3 chairs
    - Good anchoring in research community
    - Regionally diverse
- We'll not rush this — but need to start soon

# Next T2TRG meeting

- Another opportunity to work with W3C IG WoT
  - next WoT F2F W44 (Oct 26..30) @ Sapporo
  - IETF94 W45 (Nov 1..6) @ Yokohama

# Where after Japan?

- SIGCOMM 2016?
- IEEE P2413?
- _____ (fill in)

# Backup

# T2TRG Summary

Cooperation with CoRE

# Constrained RESTful Environments (CoRE)

- Basic protocol (CoAP) almost done
  - RFC 7252
  - draft-ietf-core-observe
  - draft-ietf-core-block
- A few supportive elements
  - RFC 6690 (CoRE Link Format)
  - draft-ietf-core-resource-directory → standard interface for discovery
  - draft-ietf-core-http-mapping → transparent mapping between HTTP and CoAP
  - draft-vanderstok-core-comi → interface for network management
- Authentication and Authorization in Constrained Environments (ACE)

# Building Applications

- draft-ietf-core-interfaces

  Collection of useful mechanisms
  (e.g., control observe relations, “bindings” between resources)

- draft-koster-core-coap-pubsub

  Implementing publish/subscribe with CoAP
  (producers, brokers with standard interface, subscribers)

- draft-hartke-core-apps

  Template for describing hypertext-driven applications
  (URI schemes, media types, link relations, well-known locations)

# Issues

- Current practices mix paradigms
  - Typed resources vs HATEOAS
  - Subscriptions vs state transfer
  - “REST-as-we-use-it” (getting on the same page)

- Breakout “WoT TF APIs and Protocols / T2T Beyond REST”
  - Orchestration of Web Things
  - Use cases, requirements and modeling of subscriptions
  - Modeling of Web Thing as Typed Resources

# REST for the Internet of Things

- Collect accessible “authoritative” material on RESTful design
  - TL;DR–effect
  - explain, don't preach
  - Roy Fielding's thesis and blog posts (less accessible)
  - Book references
  - Review other blog posts and convert to drafts?
- Define REST compliance levels? (see also Richardson Maturity Model)
  - Help for development contracts

# Current Action Items

- Assemble a cookbook with design patterns
  - Provide an “executive summary”
  - Focus on properties and implications (benefits, drawbacks)
  - Define terminology
  - Explain benefits in context of concrete use cases
- Develop evaluation framework
  - Look into Internet Media Types for the IoT
  - Look into link relations / form classes for the IoT
  - Which REST constraints impact which (benefitial) properties
    - Interoperability
    - Change
    - …