DTLS In Constrained Environments (DICE)

We're a WG ☺

WG Chairs:

Dorothy Gellert dgellert@silverspringnet.com
Zach Shelby zach.shelby@arm.com

Security Area Advisor:

Stephen Farrell stephen.farrell@cs.tcd.ie

Mailing List: dtls-iot@ietf.org
To Subscribe: https://www.ietf.org/mailman/listinfo/dtls-iot

Note Well

This summary is only meant to point you in the right direction, and doesn't have all the nuances. The IETF's IPR Policy is set forth in BCP 79; please read it carefully.

The brief summary:

- **By participating with the IETF, you agree to follow IETF processes.**
- **If you are aware that a contribution of yours (something you write, say, or discuss in any IETF context) is covered by patents or patent applications, you need to disclose that fact.**
- **You understand that meetings might be recorded, broadcast, and publicly archived.**

For further information, talk to a chair, ask an Area Director, or review the following:

BCP 9 (on the Internet Standards Process)

BCP 25 (on the Working Group processes)

BCP 78 (on the IETF Trust)

BCP 79 (on Intellectual Property Rights in the IETF)

What are we here to do?

The scope of this WG is to define the following:

1. The first task of the working group is to define a DTLS profile that is suitable for Internet of Things applications and is reasonably implementable on many constrained devices.
2. The second task of the working group is to define how DTLS record layer can be used to transmit multicast messages securely.
3. The third task of the working group is to investigate practical issues around the DTLS handshake in constrained environments.

Goals and Milestones

Dec 2013 - WG document for DTLS for Constrained Environments profile

Dec 2013 - WG document for secure group communication for IoT

May 2014 - DTLS for IoT profile specification submitted to the IESG for publication as standards track

Jun 2014 - Secure group communication specification submitted to the IESG for publication as standards track

Agenda

- Administration [Chairs] 10 Minutes
- DTLS Profile [Zach Shelby, Klaus Hartke] 10 Minutes
  - Goal: Find WG participants
- Multicast draft [Sandeep Kumar] 20 Minutes
  - Goal: WG input and discussion on next steps
- DTLS practical issues [Klaus Hartke] 10 Minutes
  - Goal: Identify output needed from DICE
- Session Resumption [Rene Hummen] 10 Minutes
  - Goal: Information about ongoing related work
- DTLS Relay [Sandeep Kumar] 10 Minutes
  - Goal: Information about ongoing related work
- Next Steps [Chairs] 05 Minutes

DTLS Profiling for IoT

Zach Shelby, Klaus Hartke

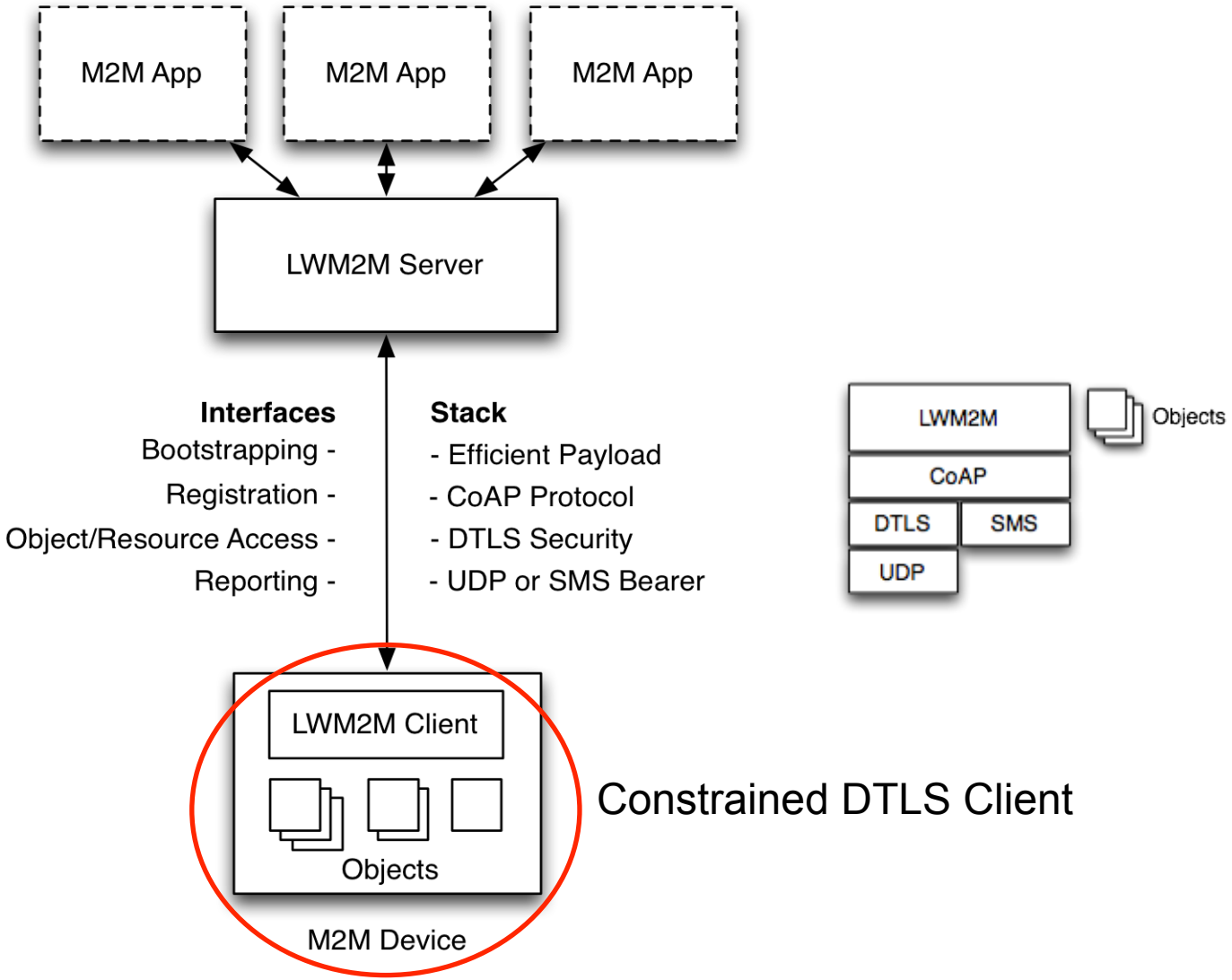
http://tools.ietf.org/html/draft-keoh-dtls-profile-iot-00
http://www.ietf.org/id/draft-keoh-lwig-dtls-iot-01.txt
http://www.ietf.org/id/draft-hartke-core-codtls-02.txt
http://www.ietf.org/id/draft-tschofenig-lwig-tls-minimal-03.txt

DICE, IETF-88 Vancouver

DTLS Profiling

- Our protocols are generic, often not tailored to specific deployment environments.
- With smart objects there are constraints about what features to implement with an impact for interoperability.
- Profiles of DTLS require information about the expected use case.

Simple Use Case – OMA Lightweight



Potential Profiling Examples

- Constrained node to implement DTLS Client only
- Limit to the security modes defined in CoAP
  - PSK, RPK, X.509
- Require mutual authentication
- Clarify needed protocols & extensions
  - Sub-set of Alert and ChangeCipherSuite
  - Determine if session resumption needed
- (Maintain cipher negotiation)