Public Safety Use Case for ACE
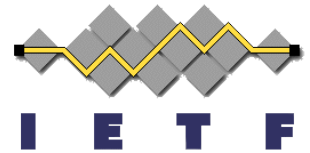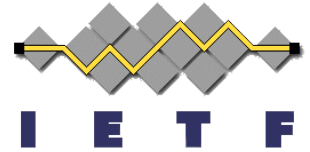
Akbar Rahman

IETF-93 (Prague), July 2015

https://tools.ietf.org/html/draft-rahman-ace-public-safety-use-case-00

Use Case (1/2)

- A Fire Department requires that as part of the building safety code, that the building have sensors that sense the level of smoke, heat, Etc., when a fire breaks out.

- These sensors report metrics which are then used by a back-end server to map safe areas and un-safe areas within a building and also possibly the structural integrity of the building before fire-fighters may enter it.
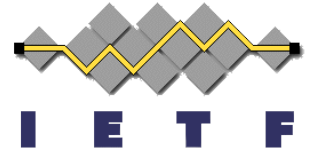
- Sensors may also be used to track where human/animal activity is within the building. This will allow people stuck within the building to be guided to safer areas and suggest possible actions that they make take (e.g. using a client application on their phones, or loudspeaker directions) in order to bring them to safety.

- In certain cases, other organizations such as the Police, Ambulance, and federal organizations are also involved and therefore the co-ordination of tasks between the various entities have to be carried out using efficient messaging and authorization mechanisms.

Authorization Problem Summary (1/2)
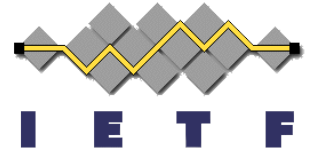
- R1. The principal wants to ensure that only authorized clients can read data from sensors and send commands to the actuators.

- R2. The principal wants to be able to grant access rights dynamically when needed. This may be triggered where the Principal may be human or machine (server/cloud system).

- R3. The principal wants to ensure the authenticity of the data originating from the sensors (authenticating the originator of data).

Authorization Problem Summary (2/3)
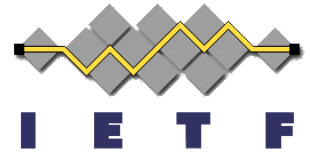
- R4. The principal wants to ensure the Integrity of the received data; also wants to verify the Integrity of the sensor since in the case of fire, the sensor may itself be damaged, therefore will have to rely on sensors from different rooms.

- R5. The principal wants to ensure that data sent to the actuators are Integrity protected.

- R6. The principal wants to ensure that extremely time-sensitive operations have to be carried out in a quick manner.
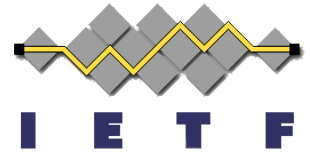
- R7. The principal wants to ensure the ability to prove that an entity (e.g. police or fire chief) that issued a message had indeed issued the message by using non-repudiation mechanisms.

- R8. The principal wants to ensure that all the messaging and data involved during a crisis is audit-able in a transparent manner (e.g. for accident post-mortem investigations)

Next Steps
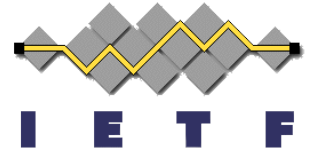
- Does this public safety use case make sense to be included in the WG Use Case draft?