OBJECT SECURITY IN WEB OF THINGS

JOHN MATTSSON
GÖRAN SELANDER
GÖRAN AP ERIKSSON

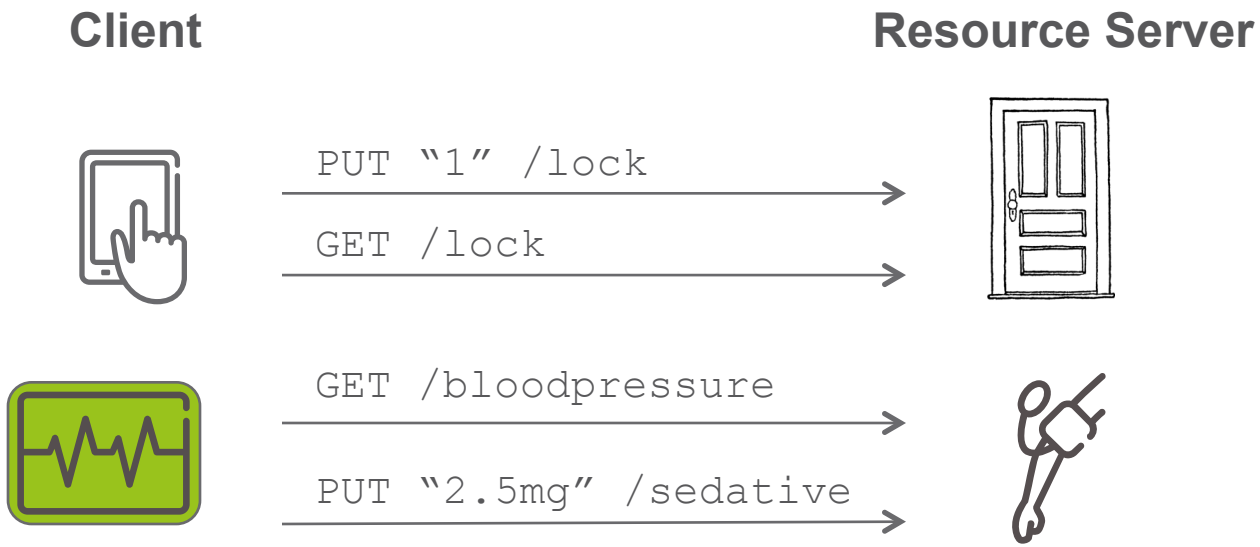
ERICSSON RESEARCH

EXECUTIVE SUMMARY

- Market potential for IoT is held back by fragmentation:
  - a plethora of communication technologies, focus on transport layer protocols
  - lack of a common approach to enabling services
- Web of Things brings new security and privacy challenges, trust models with many parties
- Flexible security solutions and standards required:
  - to protect sensitive data and user privacy
  - to distribute policies in a secure and standardized way.
  - cannot be solved in a satisfactory way with only transport layer security.
- Same privacy problems arise in the general web setting
  - processing and storage more and more moving into the cloud.

AUTHORIZATION

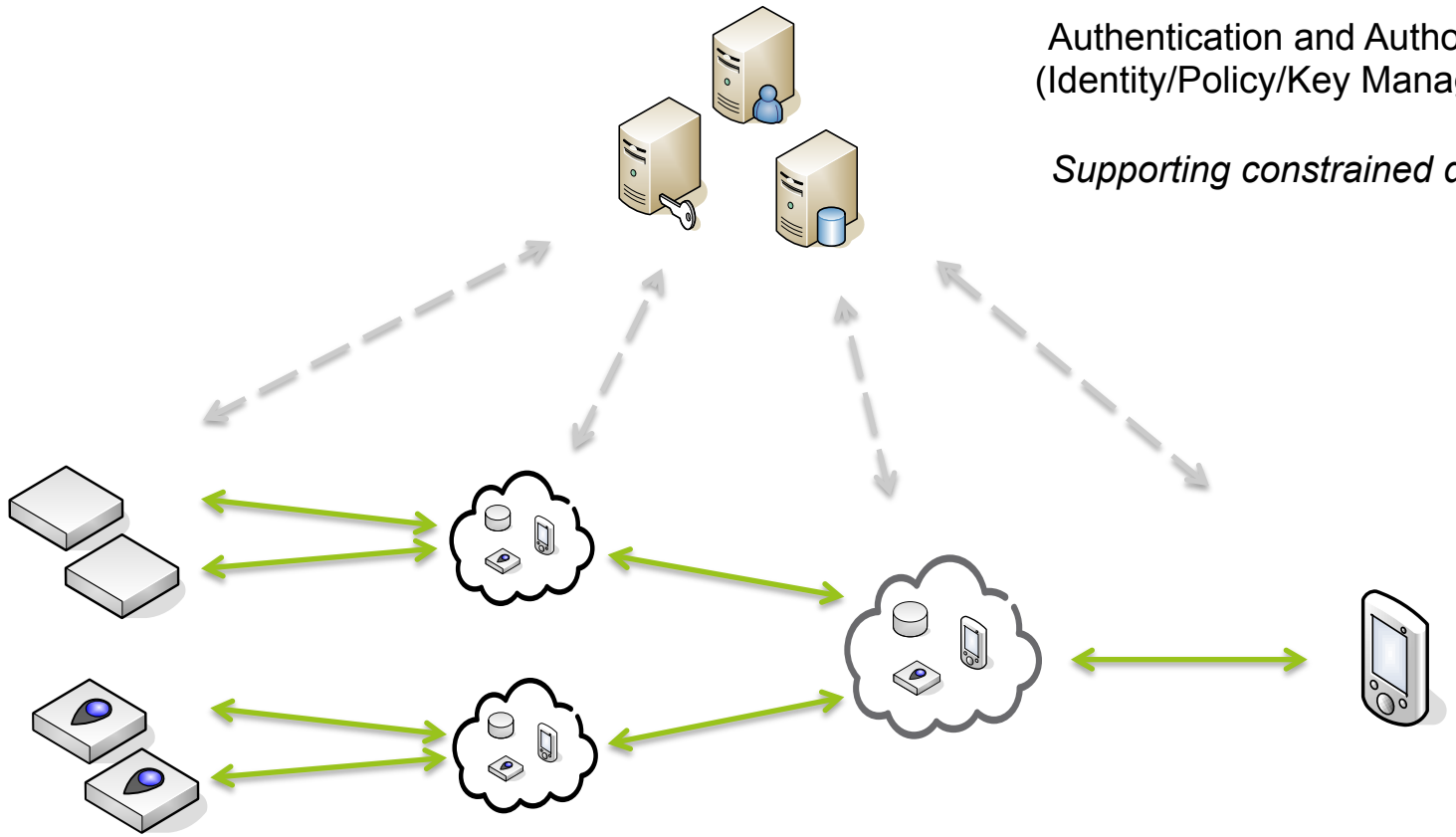
- Fundamental question: Who has the right to access what? Drives the security and privacy requirements – defines the solution.



- New IETF WG: Authorization in Constrained RESTful Environments (ACE)
- Problem: How to support explicit and dynamic authorization in networks of constrained devices from various vendors?

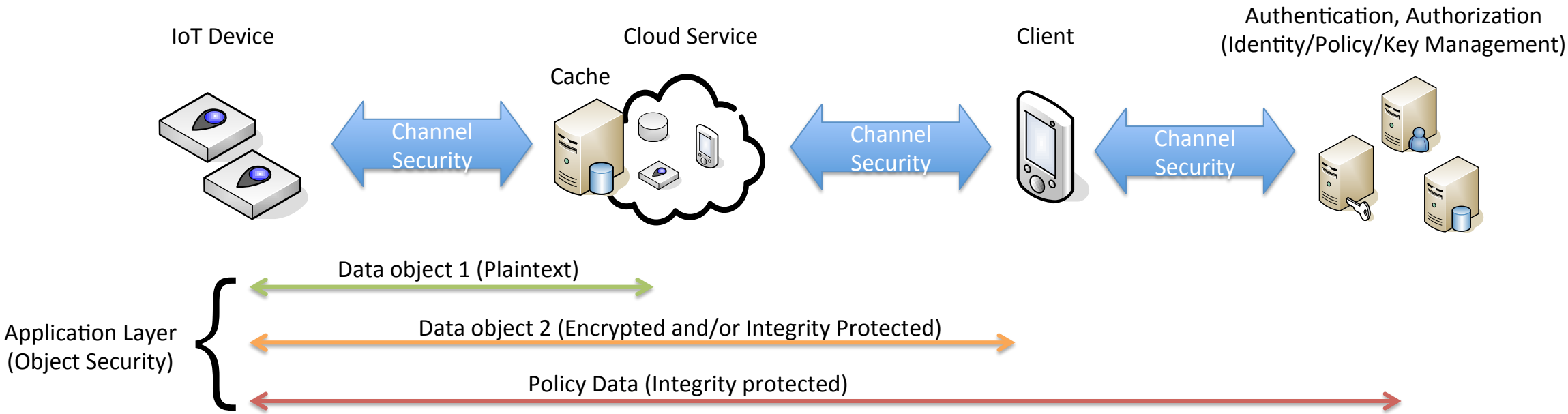
BASE ARCHITECTURE

- Sensors, Actuators (some constrained)
- Clients (may be browsers)
- A chain of Services (sensor and client)
- Servers (e.g. authorization)



OBJECT SECURITY

- Transport layer security is not sufficient, only supports fully trusted services.
- Object security protects sensitive information and policy data e2e, enables caching of protected data
- Hop-by-hop channel security includes services. Only needed data and metadata accessible to services
- Ensures control and security of information owners as well as end-user privacy



CONCLUSIONS

- Web of Things with services requires standardized flexible security solutions on the application layer
  - to protect sensitive data and user privacy
  - to distribute policies and authorization information
- Many pieces are available, some are in the making, some are missing
- W3C should secure handling of data and policies in the Web of Things:
  - Developing standards and best practices for object security, including:
    - Multiparty protocol for secure exchange of information objects, metadata, identities of the information objects and endpoints, key management, etc.
    - Browsers need APIs for key management, object encryption, decryption, manipulation etc.
  - Interoperable scalable formats for policies syntax, semantics.
    - Management of large sets of policy information
  - Access control in general, privacy more specifically

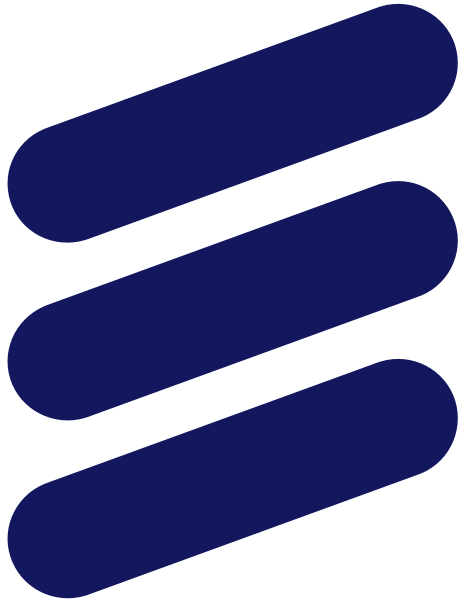
REFERENCES

IETF Authentication and Authorization for Constrained Environments (ACE)
https://datatracker.ietf.org/doc/charter-ietf-ace/
http://tools.ietf.org/html/draft-seitz-ace-usecases-00
http://tools.ietf.org/html/draft-seitz-ace-problem-description-00

IETF Javascript Object Signing and Encryption (JOSE)
https://datatracker.ietf.org/wg/jose/charter/

W3C Encrypted Media Extensions
http://www.w3.org/TR/encrypted-media/

W3C Subresource Integrity
http://www.w3.org/TR/SRI/



ERICSSON