

**Broadcom Foundation
Scholars Program at Tel Aviv University**

**The Need for a New Generation
of Authentication**

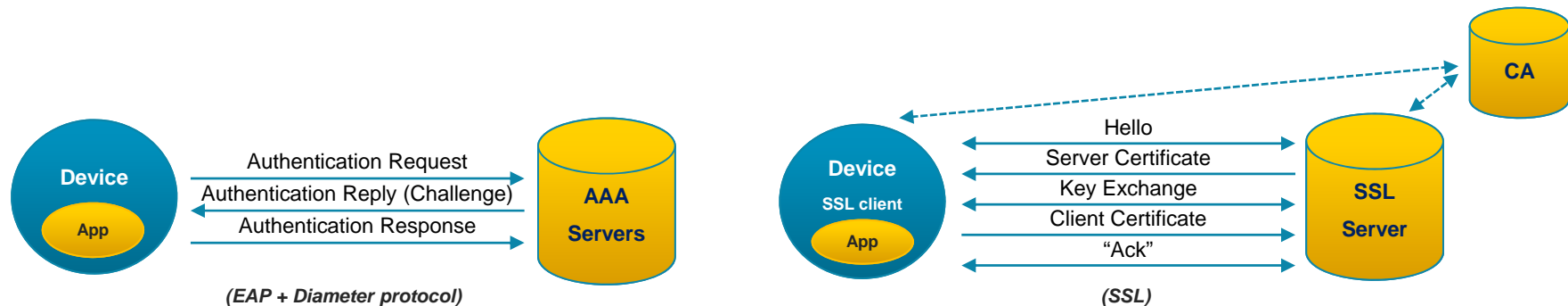


Philippe Klein, PhD
Associate Technical Director
Broadcom

22 Nov 2013

The Rational for Next Gen Authentication...

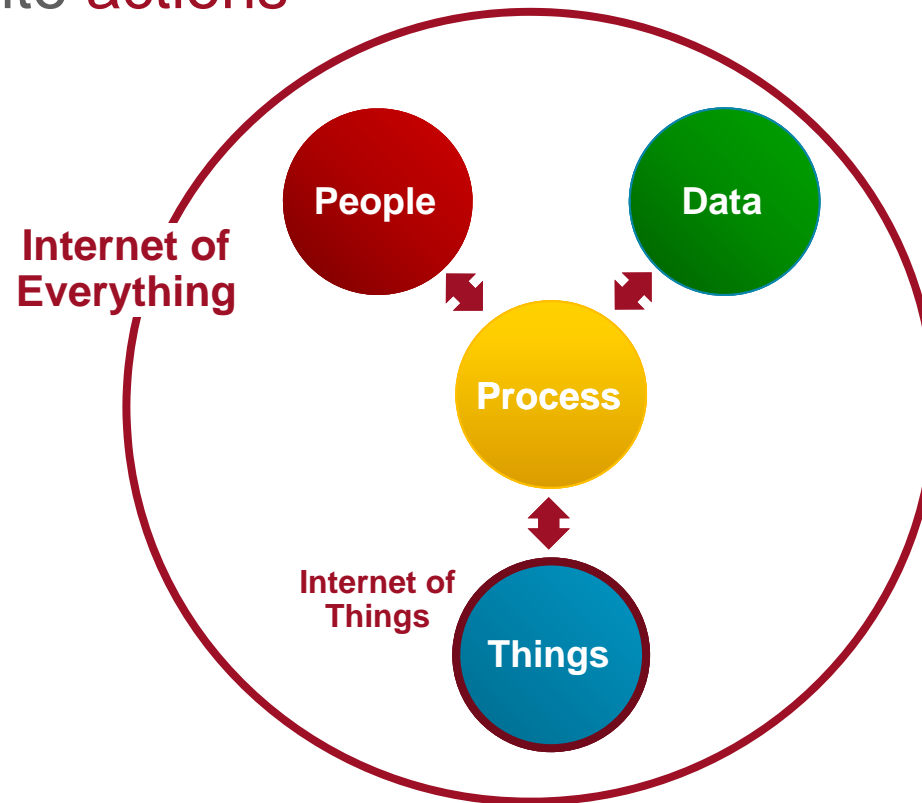
- In the current Authentication models authentication credentials are pre-configured on centralized servers:



- These models are inadequate for the Internet of Everything context in which any “thing” connects to any “thing”...
- ...and requires a shift of paradigm to address the new needs of authentication

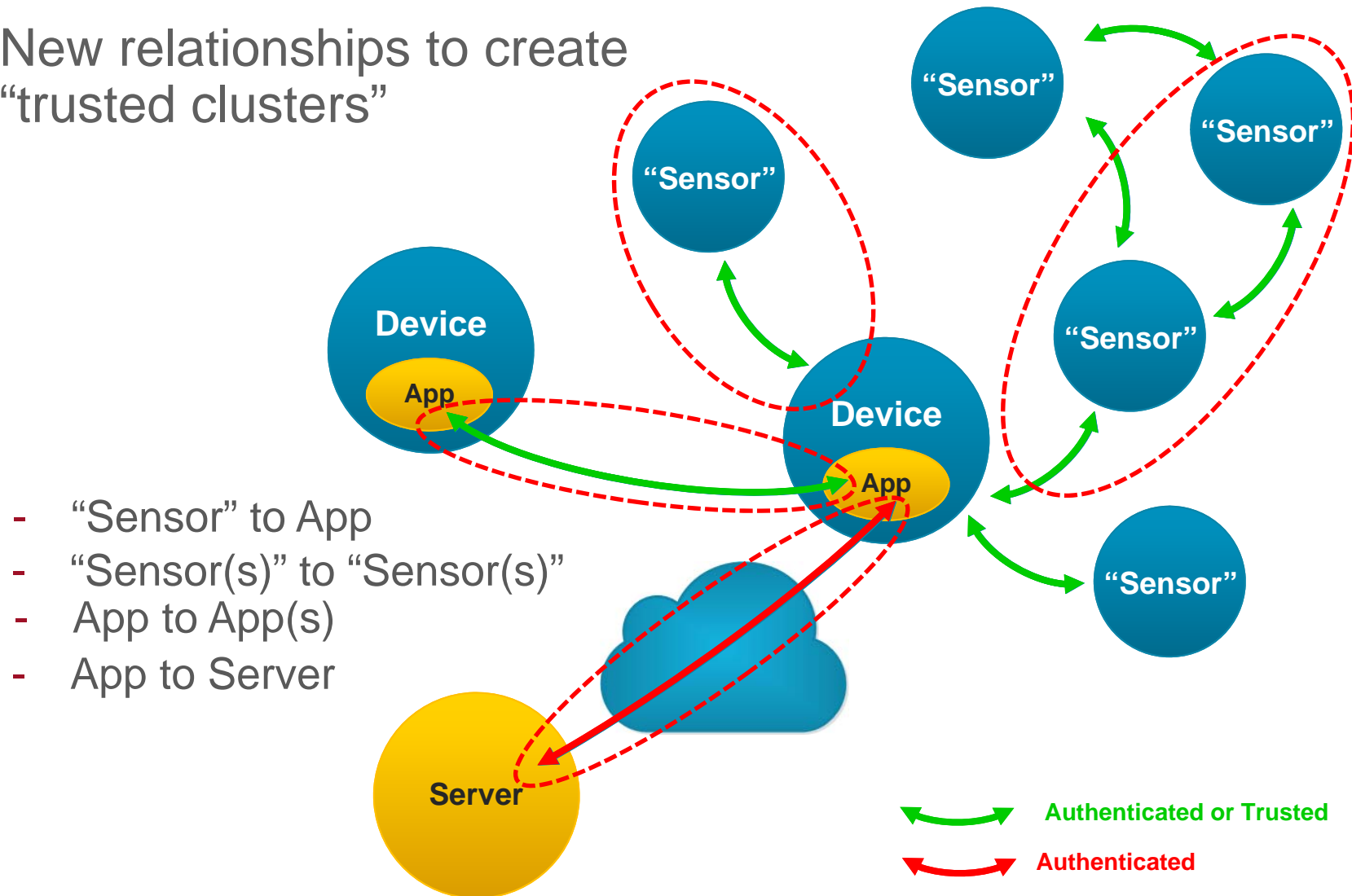
What is Internet of Everything (IoE) ?

- Built in top of Internet of Things (which connects “things”)
- IoE networks together **people, process, data and things**
- Turns information into **actions**



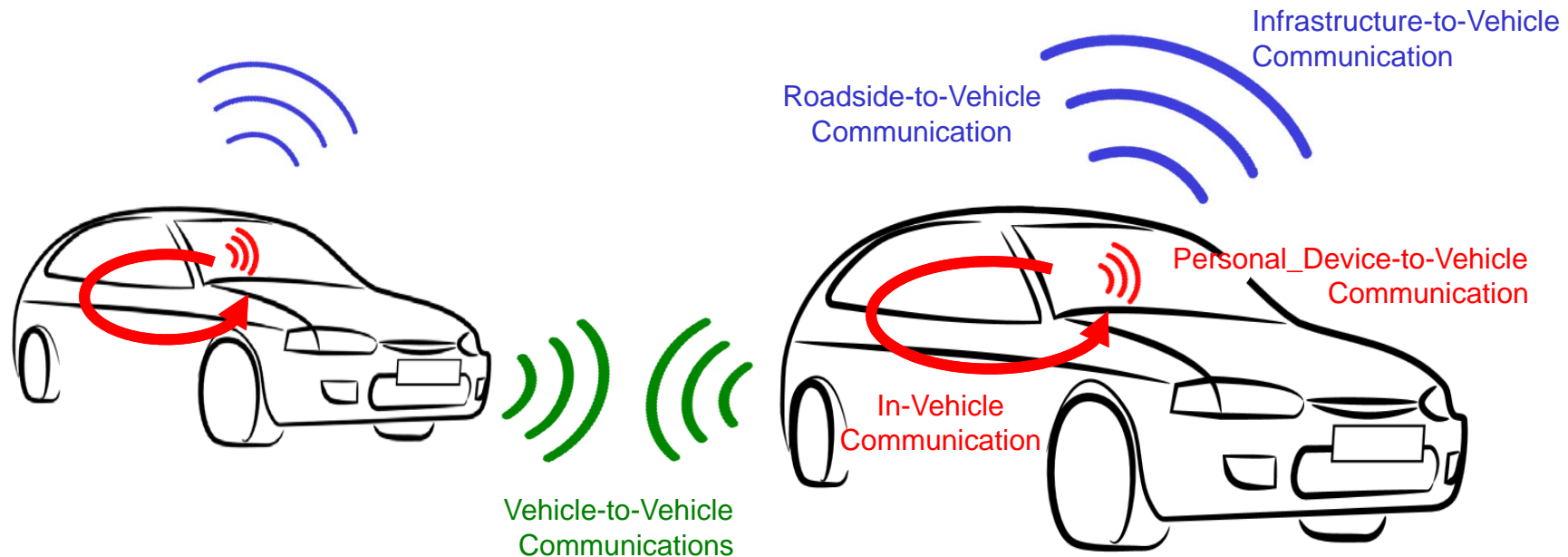
The New Authentication Context

- New relationships to create “trusted clusters”



Hot Topic” Example... Tomorrow’s Automotive Environment

- Connected cars will feature multiple dynamic networks (**that include mission critical networked functions...**)



The Need for Standardization



- Identity is the foundation for assigning access and privileges
 - Requires:
 - identity standards & standardized naming model
 - standard for identity assignment, renaming & removal
 - standard for trust establishment & revocation
- Security must not be a design afterthought
 - Innovative device designers are **not** necessarily security experts...
 - Innovation must bake **security in the design**
 - at the **hardware** level
 - thru **standardized framesets** specifying normative entities
 - Certifications

The Next Gen Authentication Requirements



- Must be **agile** and **dynamic**
(to adapt to context changes)
- Must be performed along the **whole** life time of the application
(and not at initialization stage only...)
- Must be able to identify persons, **devices**, **connections** and **data**
(device functionality, connection type, where and who created the data...)
- Must allow **correlation**
(such location correlation, time correlation,...)

The Next Gen Authentication Requirements



- Must be **multi-dimensional**
 - to support multi-factor parameters
 - to support multi-modal devices
 - to support multiple apps on the same device
 - to allow **multiple levels** of authentication **within** an application
(*e-commerce app, conditional access to content,
or for example, a sensor used for both fitness and e-health apps...*)

Multi-Factor Authentication

Knowledge

Something you know
(personal info, password, PIN,..)

Ownership

Something you have
(personal device)

Connectivity

Something you trust
(access, network, data integrity,..)



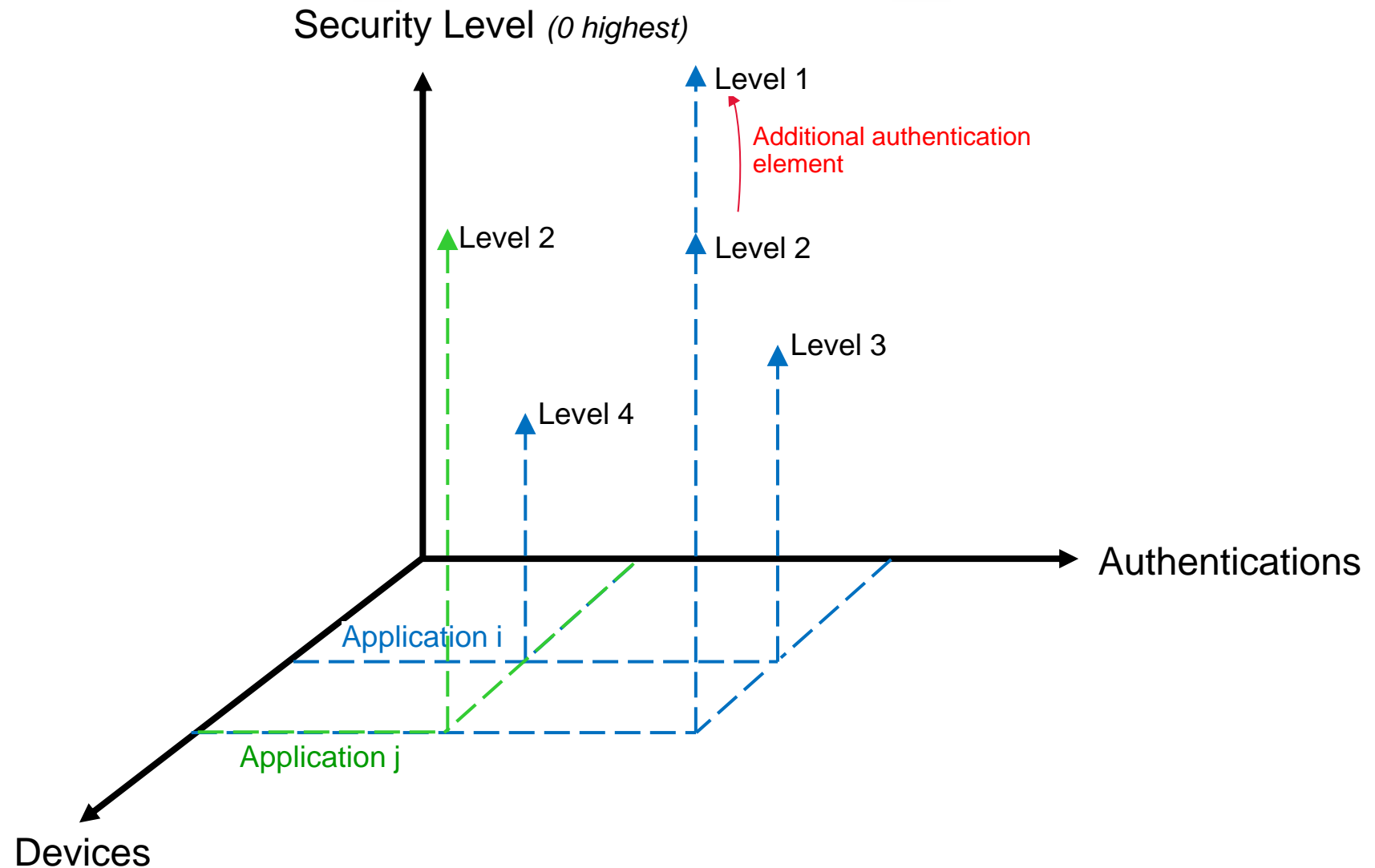
Geography

Somewhere you are/or are not
(context, location correlation)

Physiology

Something you are
(physical characteristics, biometrics)

Multi-Dimensional Authentication



Thank You



(philippe@broadcom.com)