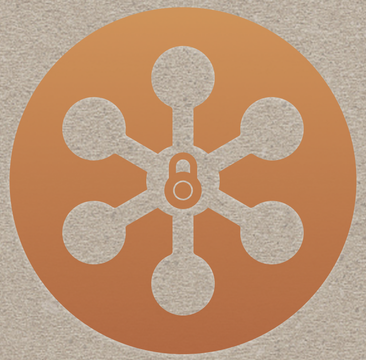
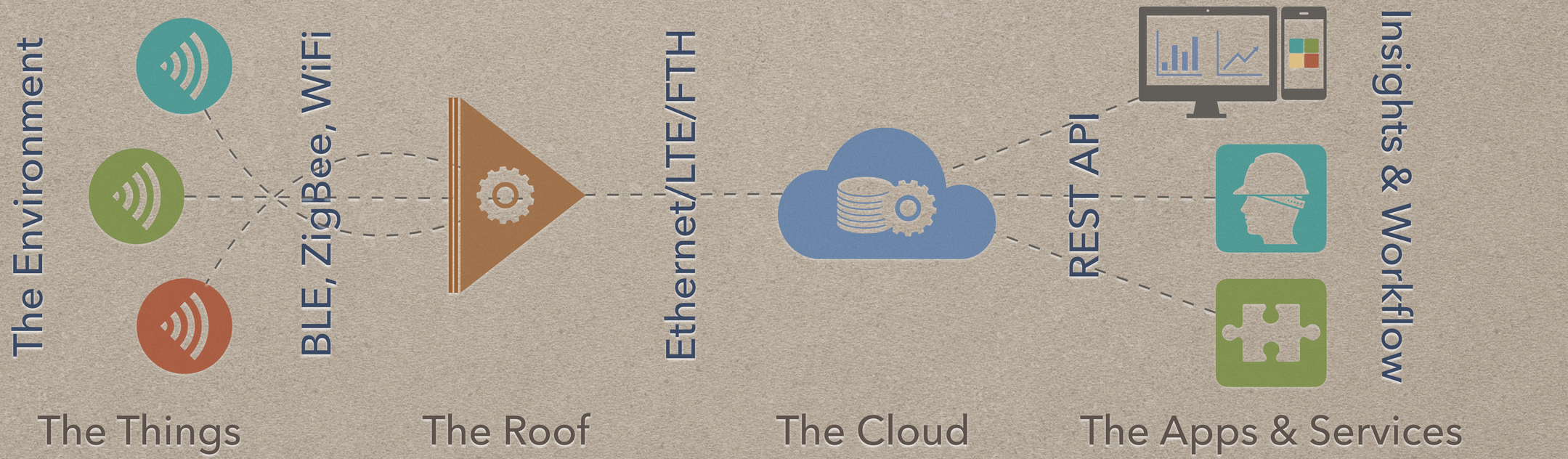


SECURING THE INTERNET OF THINGS

SYAM MADANAPALLI | AN EARLY IETFER FROM INDIA

THE INTERNET OF THINGS



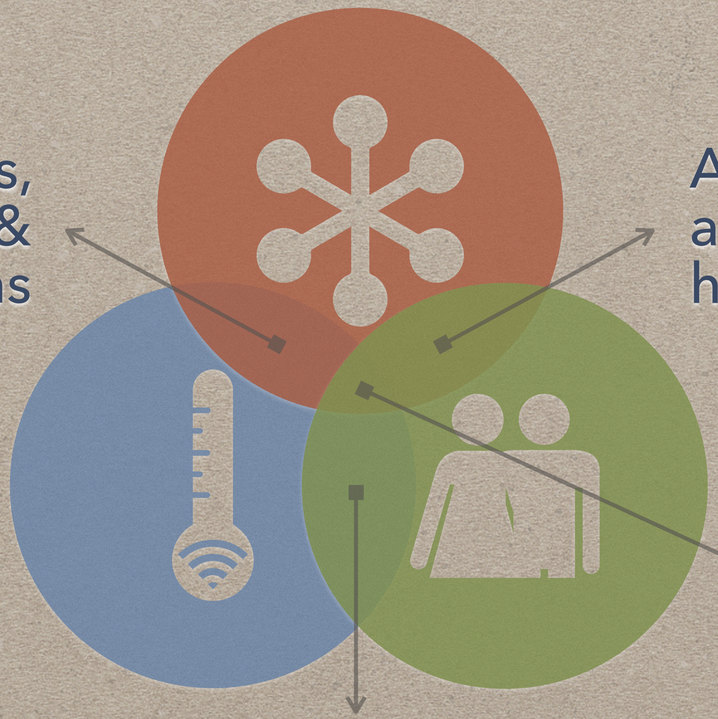
The State → The Context → Data & Analytics → Information & Actions

IOT SECURITY IS COMPLEX

Big Scale

Variety of devices, protocols, & applications

Applications & devices are personal, and involves humans & physical world



Constrained Devices

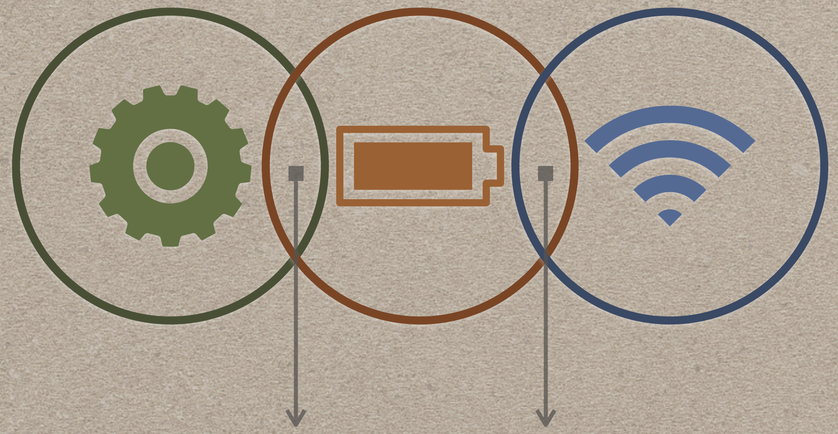
Tech Illiterates

Lack of UI & challenging to configure, prone to errors and easy to attack

Big Impact

Safety & economic risks, loss of privacy and business interruptions

THE CONSTRAINED DEVICES



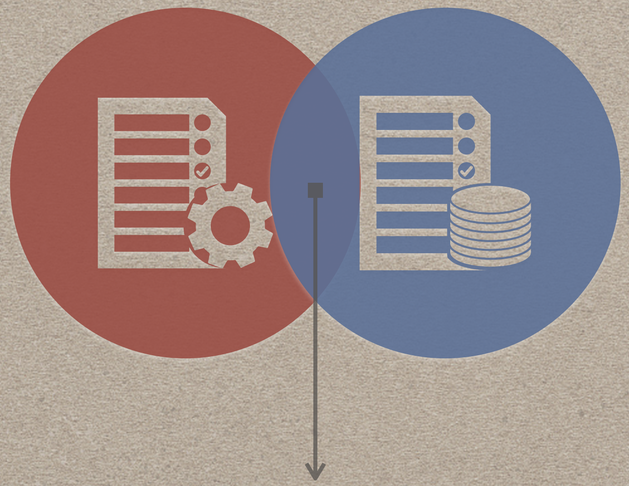
Cannot protect themselves.

Vulnerable to DoS attacks

- Limited Computing
- Limited Power
- Limited Bandwidth

Provide an indirection for computing resources.

THE END USERS ARE TECH ILLITERATES



Lack of knowledge, transparency and impact

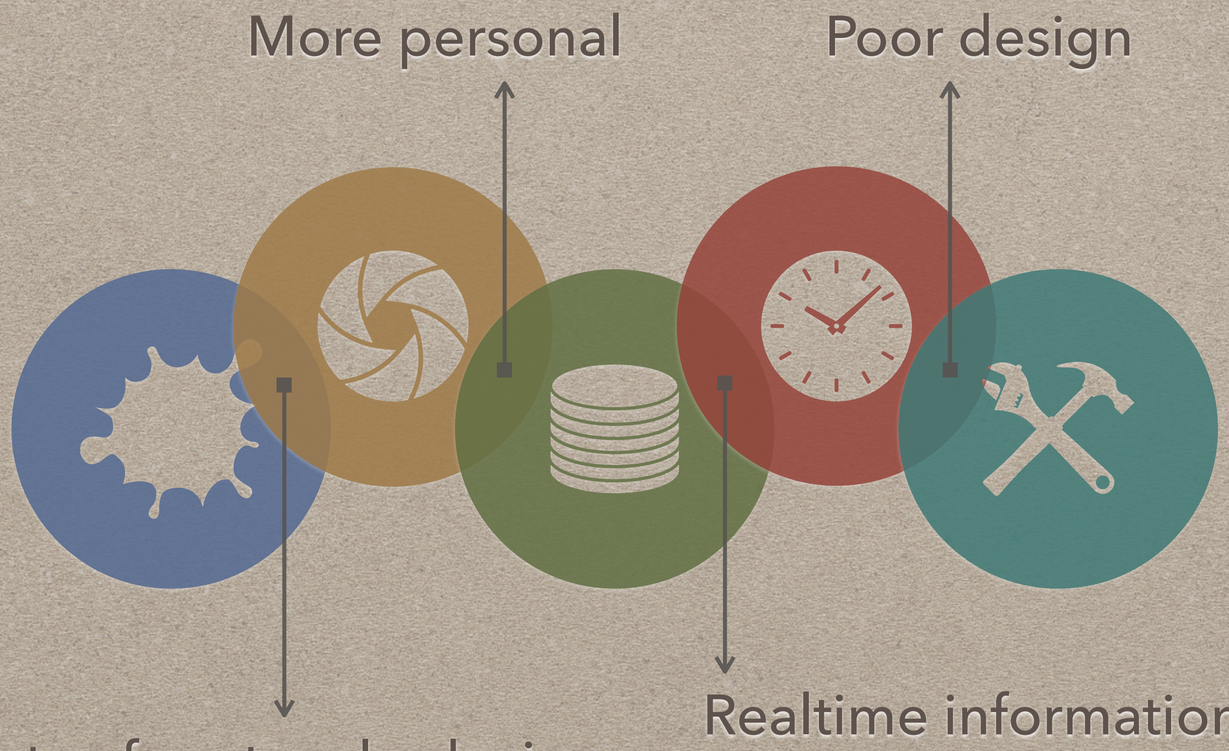
Loss of privacy, and safety & economic risks

Secure Provisioning

Privacy Management

Reduce the technology complexity and ease their role.

THE SCALE



- Bigger Attack Space
- Diversity
- Big Data
- Day-to-Day Usage
- Lack of Experience

Make them autonomous, decentralized & resilient.

THE BIG IMPACT

Business interruption,
Damage to reputation
& economic risks

Theft of Personal Data

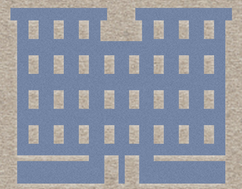
Safety Risks

Hijacking Physical Assets

Allow communication to IoT applications only from trusted sources!

WHO IS RESPONSIBLE FOR SECURITY?

Device Manufacturers



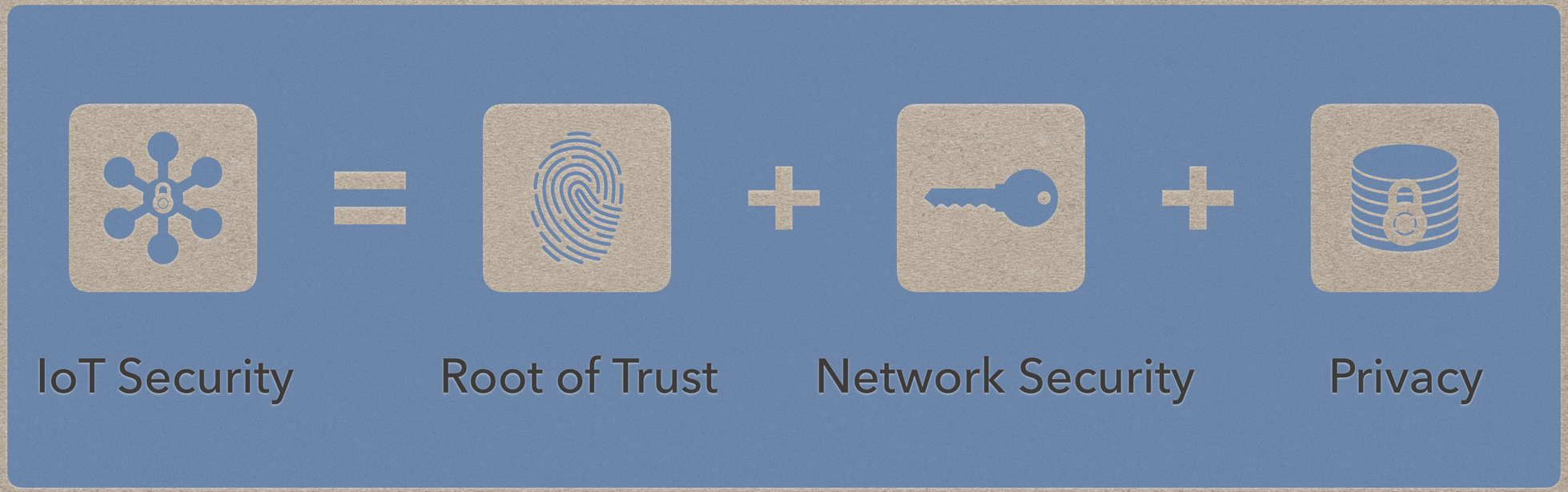
Software Vendors

Network Builders

Service Providers

Standards will bring the ecosystem together to build secure systems.

IOT SECURITY != CYBER SECURITY



Network Security = Secure Provisioning + Secure Key Management + Authentication & Authorization + Secure Communication

A NEW THINKING FOR IOT SECURITY

Indirection
Computing assistance

Autonomy
Function independently

Decentralized
Dispersed functions

Resilient
Ability to isolate & recover

Accountability
Ability to prosecute

A FEDERATED ARCHITECTURE

Self protection,
best practices

Homes

Enforcement by
the state law

Cities

Cooperation &
coalition

States

Global cooperation
& programs

The World

A learning from human evolution for distributed security architecture.

SECURING THE INTERNET OF THINGS

Uninternetting
Don't expose things over the Internet

Indirection
Move security computing one level up

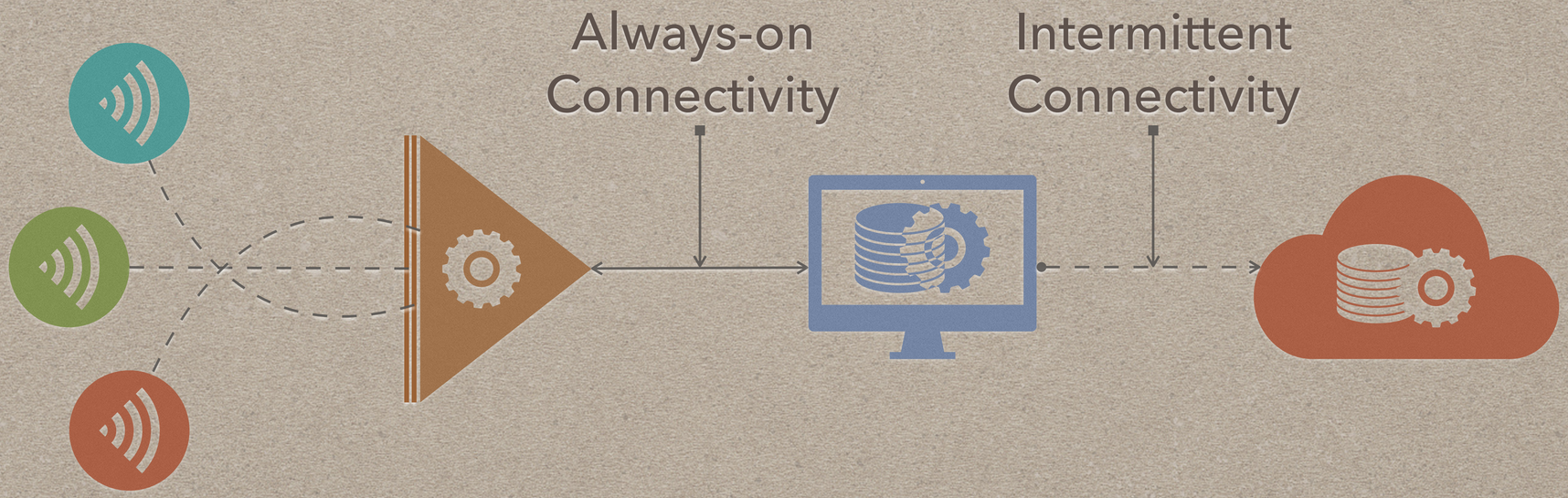
Security Gate
Allow only trusted sources

Security Fusion
Contextual analysis

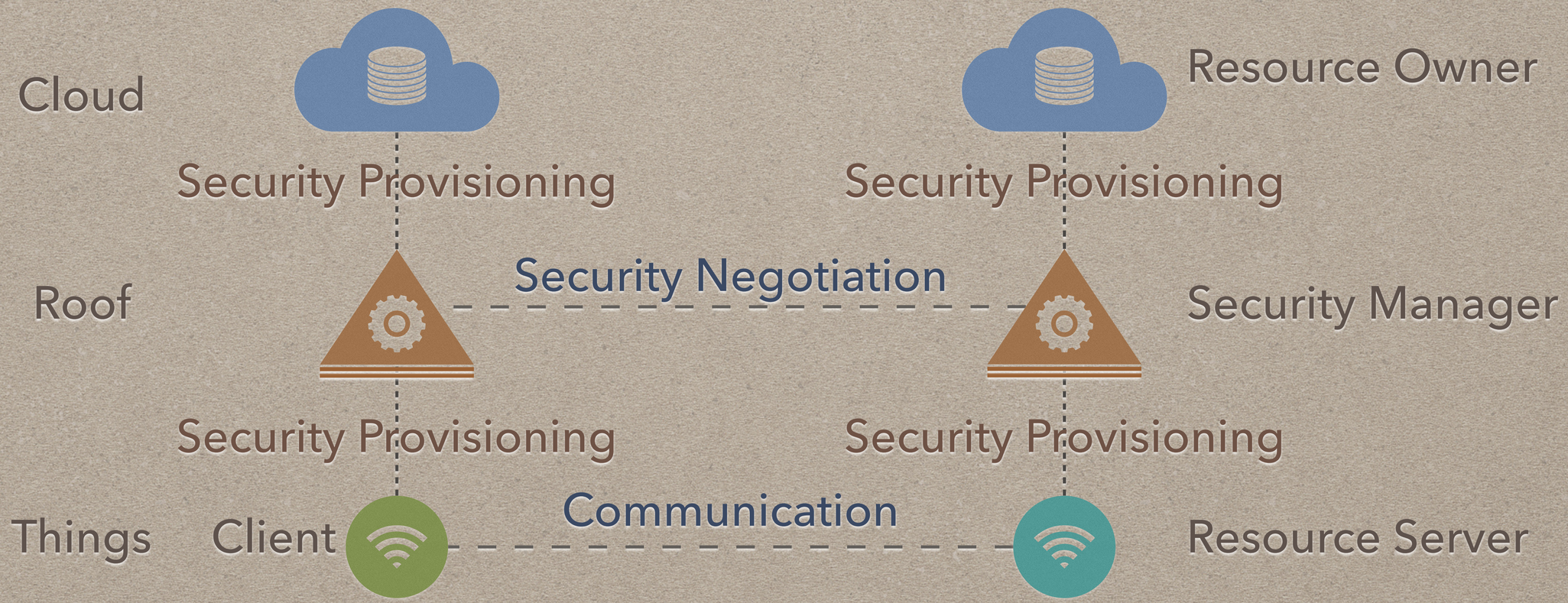
Multi Factor Authentication
Extra layers of security

A combination of these would help in building robust protection against the threats.

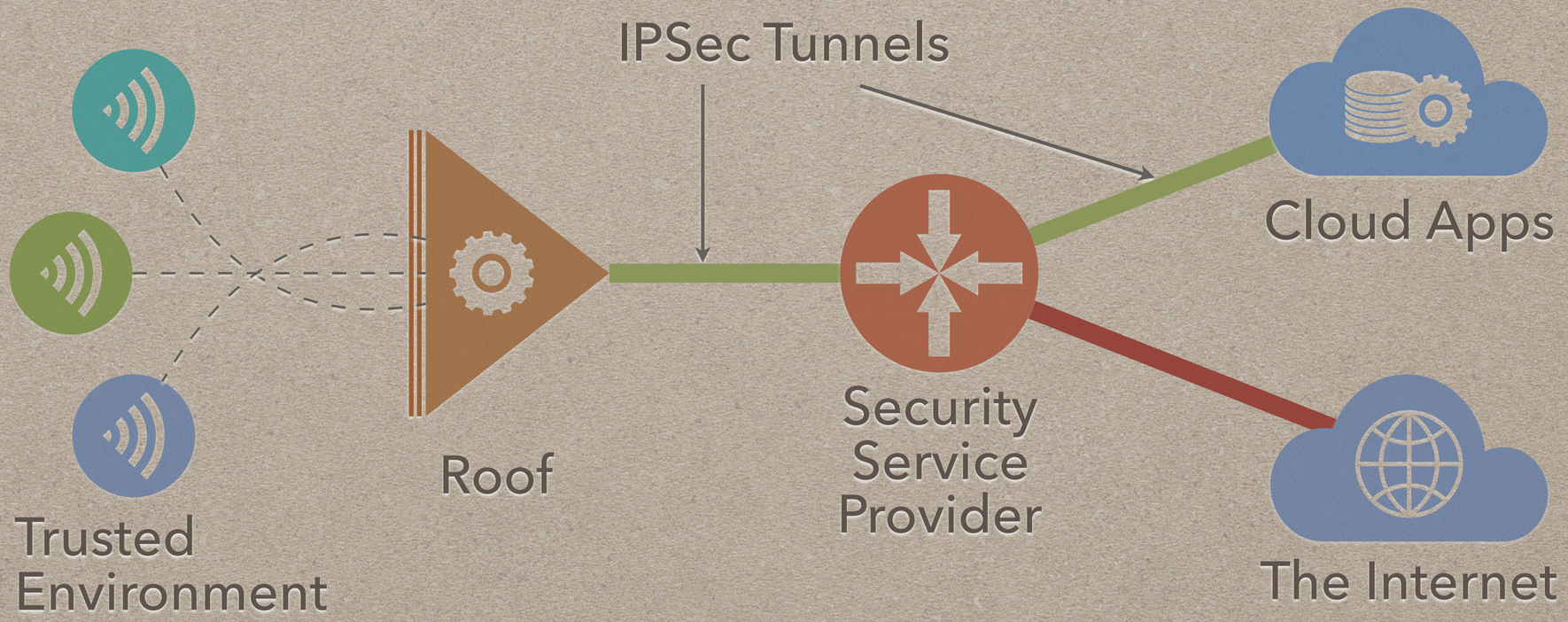
UN-INTERNETTING



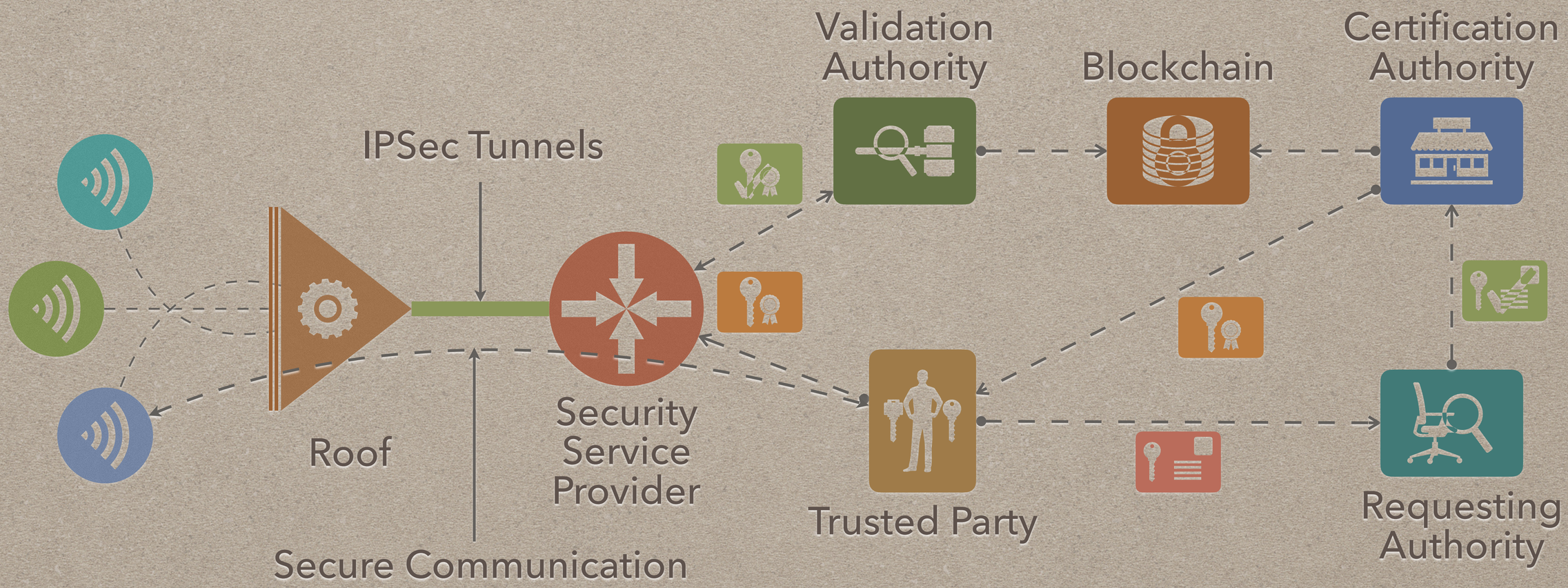
IOT SECURITY BY INDIRECTION



SECURITY GATE - SECURITY SERVICES

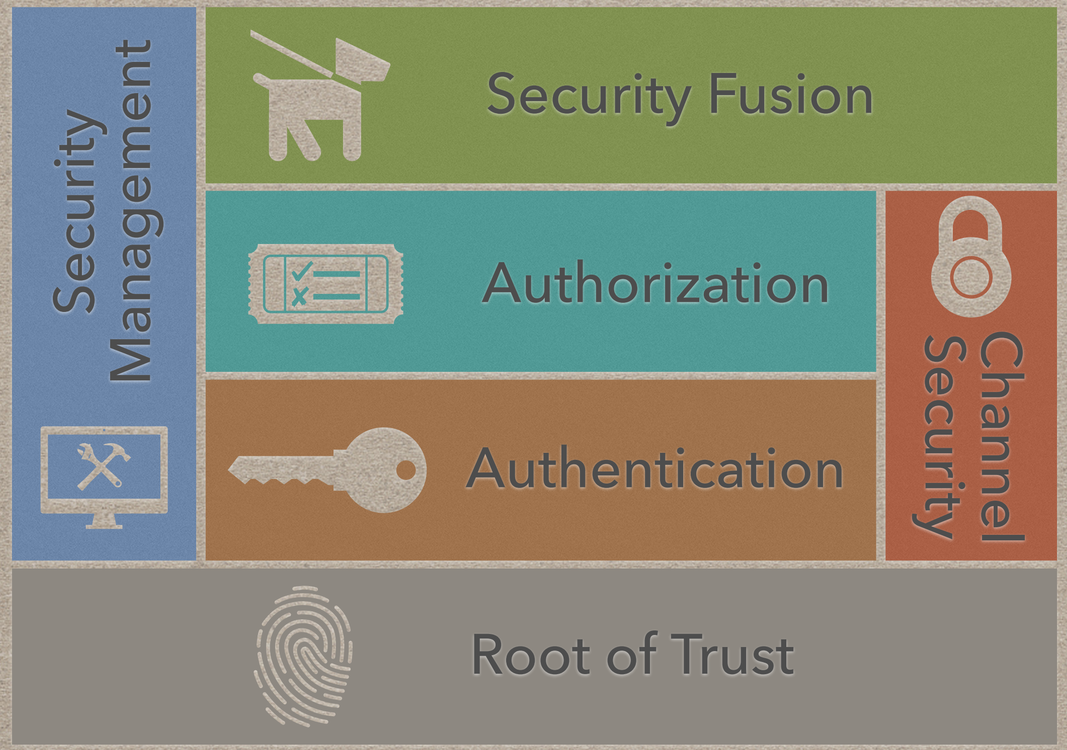


PKI FOR IDENTITY



PKI binds public keys with respective identities of entities.

SECURITY FUSION



Security Fusion

Security by design

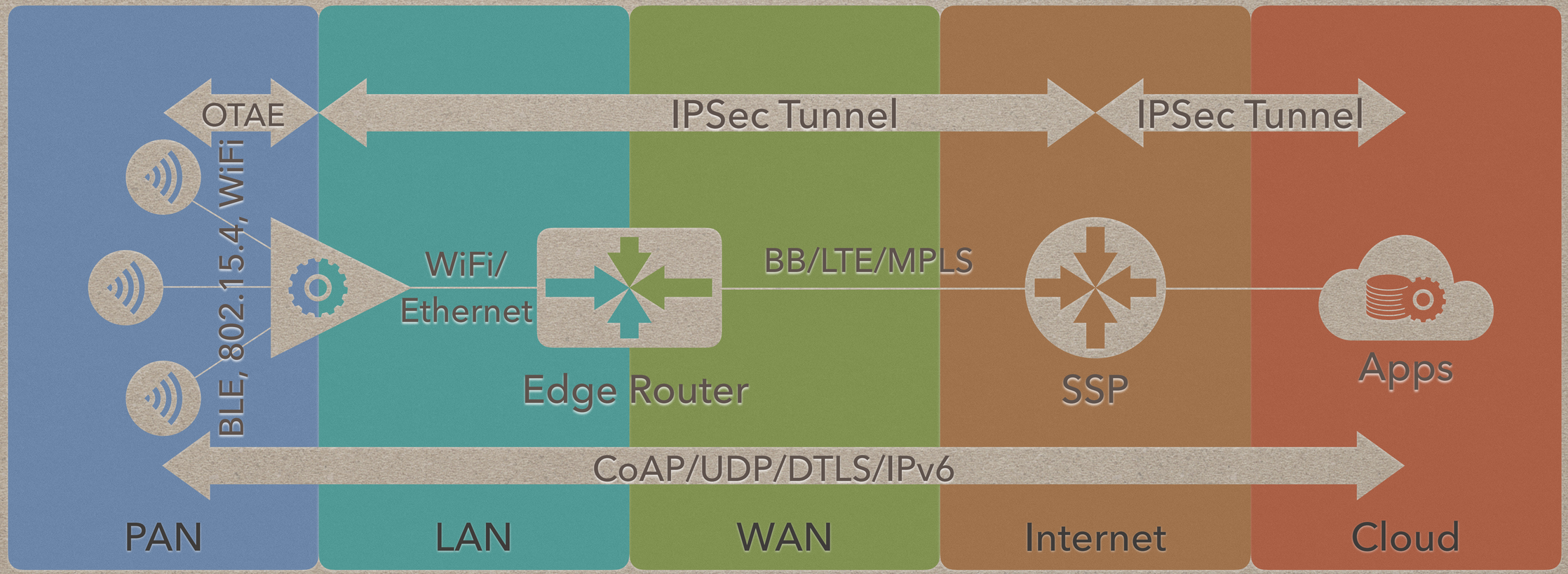
Contextual analysis

Multi factor authentication

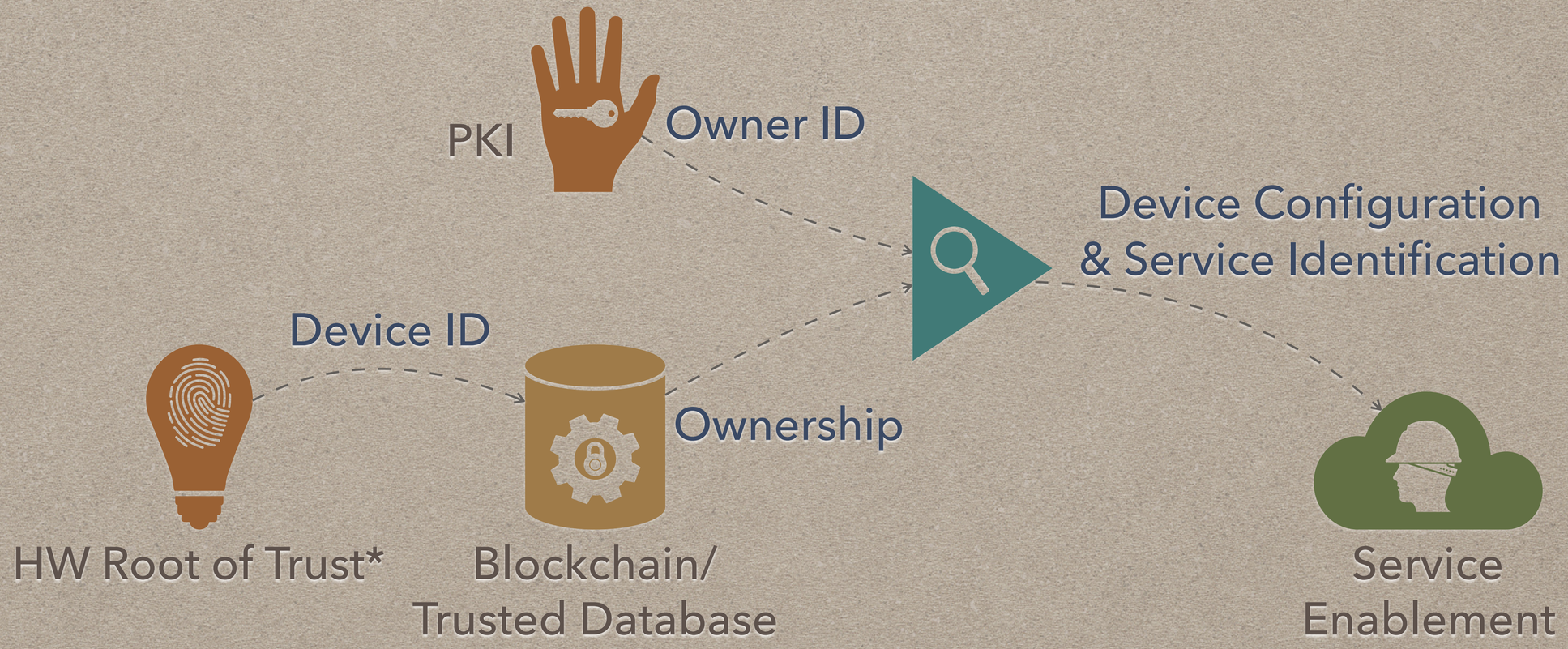
Prevent DoS attack on devices

Minimize device computing

SECURING THE NETWORK SEGMENTS



THE ROOT OF TRUST



CLASSES OF IOT DEVICES

	Class 0	Class 1	Class 2
RAM, ROM, IP	< 10KB, 100KB, No IP	~ 10KB, 100KB, CoAP	~ 50KB, 250KB, IPv6, HIP
Cryptography	Over the air	Symmetric cryptography	PKI based
Protection	One level up	Assisted at one level up	Self and services at one level up
Interface	IoT Services	Security Provisioning and Services	Security Services
Applications	Only for trusted environments	Battery powered under the Roof	Mains powered & standalone devices

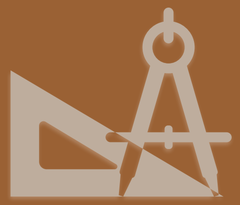
PRIVACY MANAGEMENT

Informed Decision Making

End-to-End Transparency

Weighing Privacy vs. Benefits

Contextual Awareness



Privacy by Design

Government Regulations

STRATEGIC PRINCIPLES FOR IOT SECURITY

1 Incorporate security at the design phase	2 Promote security updates and vulnerability management	3 Build on proven security practices
4 Prioritize security measures according to potential impact	5 Promote transparency across IoT	6 Connect carefully and deliberately

* *United States Department of Homeland Security, November 2016*

FUNCTIONAL ASPECTS OF IOT SECURITY

Channel Security - Protect the communication path

Root of Trust - Secure boot capabilities

Security Management - key management, policies, security updates

Security Fusion - Detect, block and report unauthorized access attempts

Cooperation - share information and learn best practices

Security Bootstrapping - Initial security configuration and procedures

Security Services - protect the resources and manage vulnerabilities

Data Protection - Protect the data at rest in the servers and equipment

Identify, Authentication and Authorization - Allow access only to authorized entities & accountability

These need to be supported for constrained devices in constrained environments.

SECURITY STANDARDS FROM IETF

IPsec — Suite of protocols for IP layer security

IKEv2 — The Internet Key Exchange

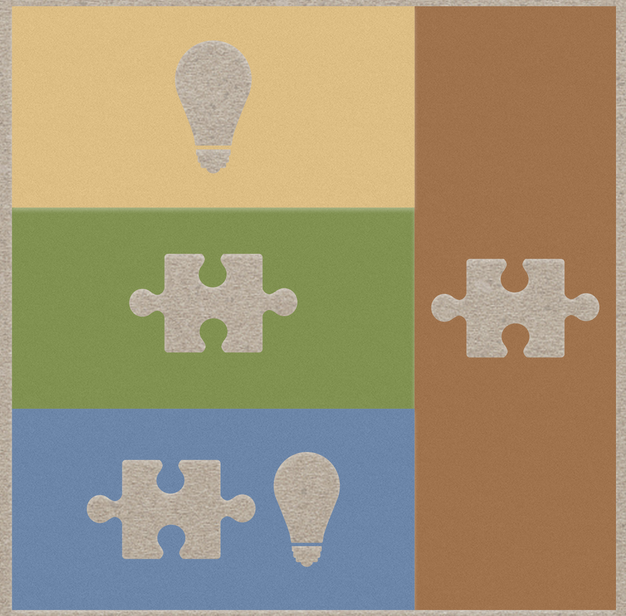
PKI — Public Key Infrastructure

ACE — Authentication and Authorization for Constrained Environments

DTLS — Datagram Transport Layer Security

Security protocols for protecting communication, and data at rest as well as to identify trusted sources.

THE NEED FOR AN IOT SECURITY STANDARD



Need to be a standard

Differentiator

Applications/Services

IoT Services

Devices

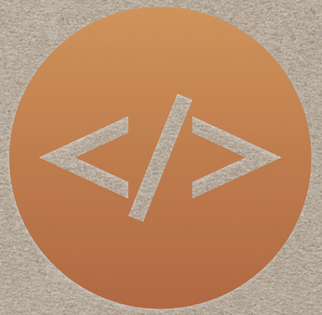
IoT Security

Scalable and trustworthy IoT applications require a security standard with a minimal set of protocols & Businesses should compete on application/Service level innovation!

WAY-FORWARD

Publish a gap analysis

Initiate a global effort for establishing security standards



Initiate a prototype implementation

IETF is best suited to do this gap analysis so that the appropriate SDO can take up filling the gaps and an open source reference prototype implementations.

THANK YOU!

SMADANAPALLI@GMAIL.COM | @SMPALLI

@Connections, a pre-IETF India Forum, November 8, 2017.