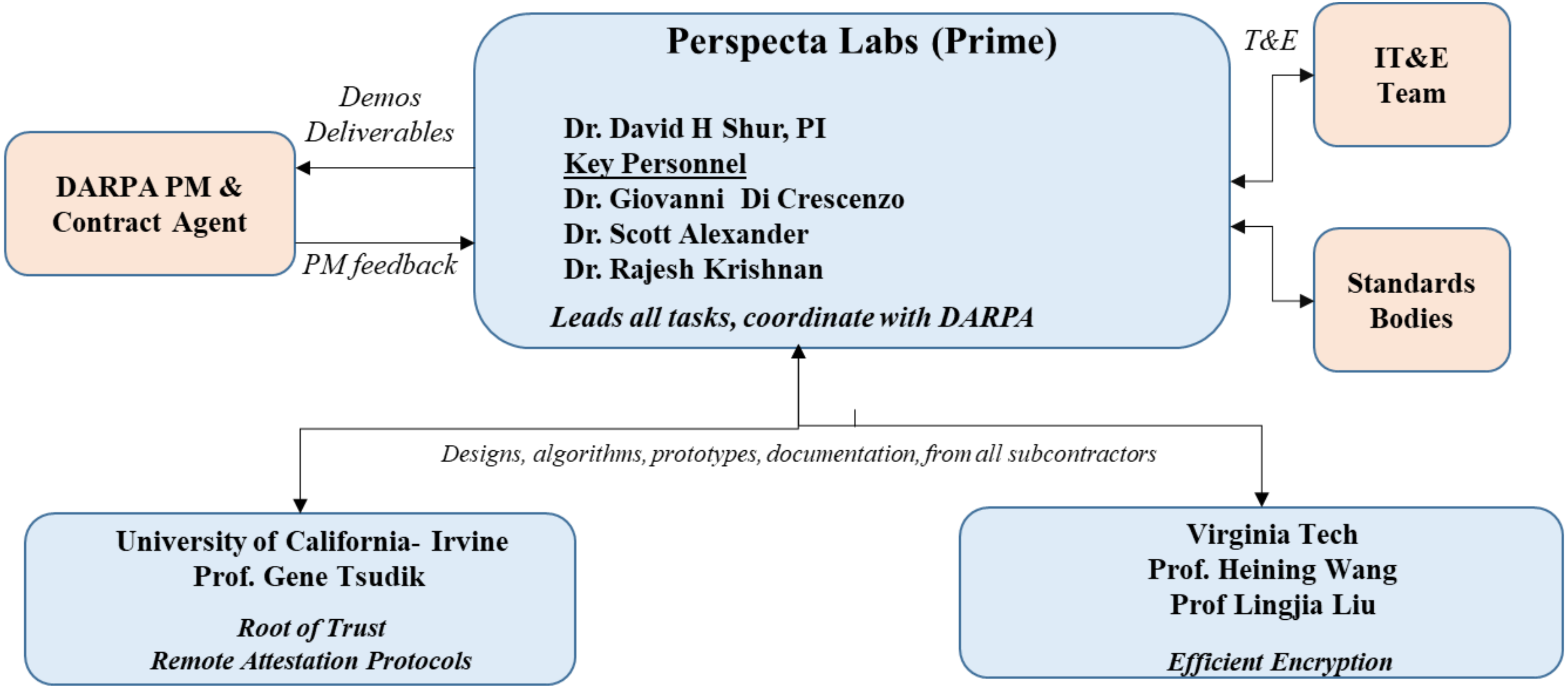
# OPS 5G –TA2

## SEcure DIstributed IoT ManagemENT for 5G (SEDIMENT)

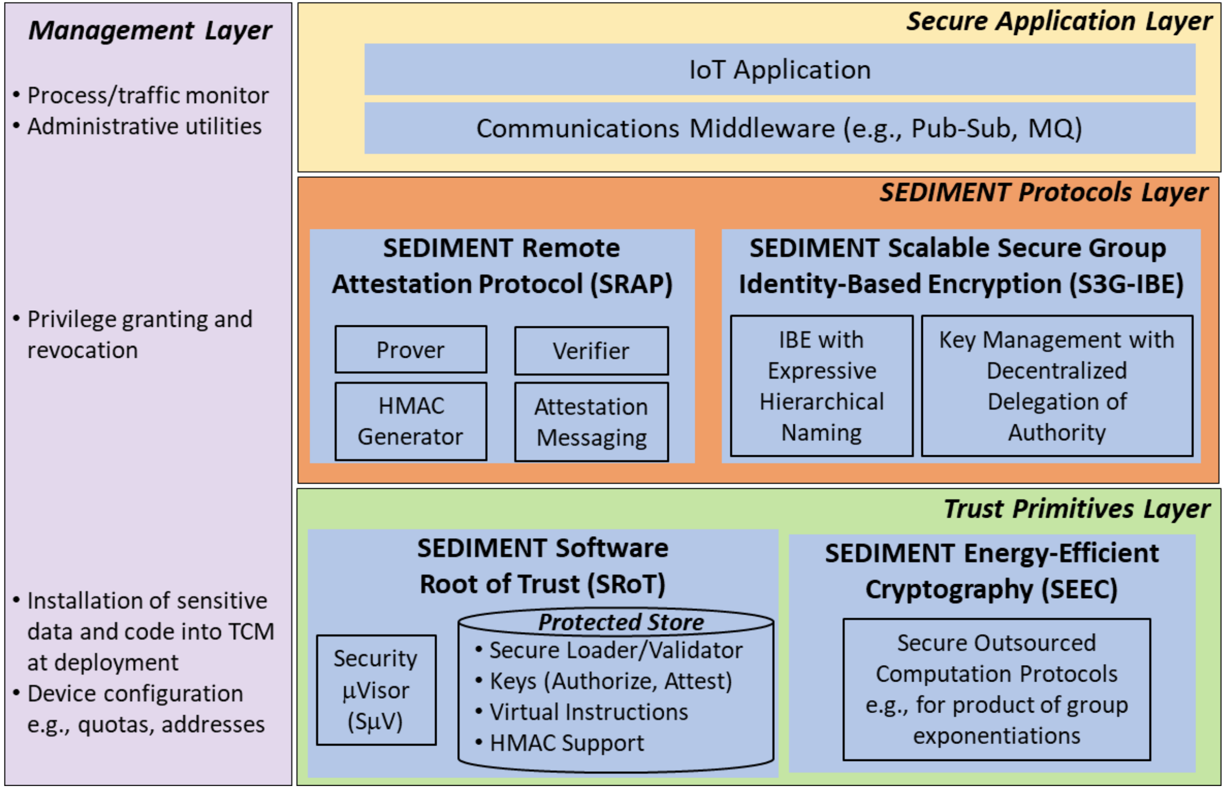
Presenter: David Shur (PI)

The views, opinions, and/or findings expressed are those of the author(s) and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.
This research was developed with funding from the Defense Advanced Research Projects Agency (DARPA).

# SEDIMENT Team and Management Structure



# SEDIMENT Overview

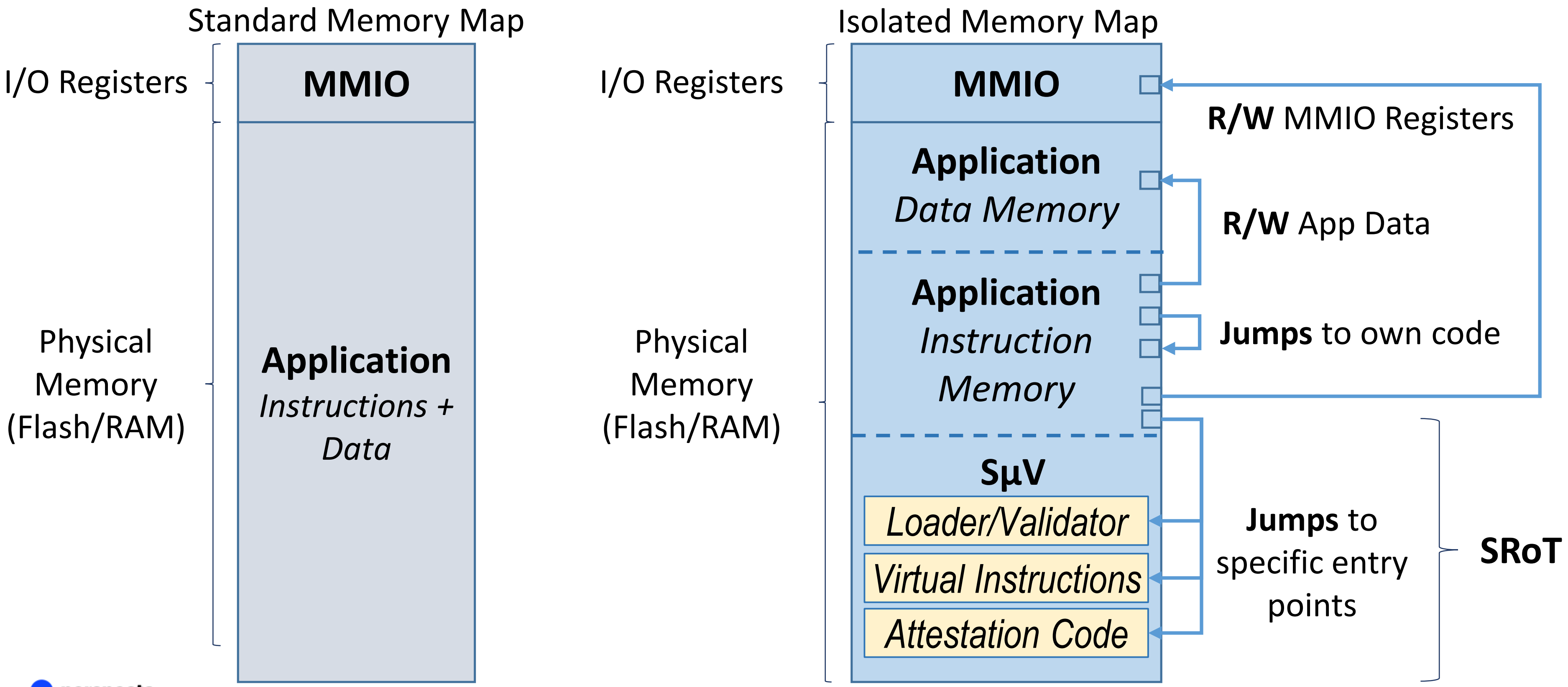



- SRoT establishes a **minimalist software root of trust**, able to easily operate within significantly resource constrained IETF class 1 IoT devices
- SRAP provides **remote attestation** for resource constrained IoT devices with guaranteed security properties
- S3G-IBE provides **specialized power efficient cryptography techniques** targeted to the most power, memory and computation constrained IoT devices.
- SEEC extends **state-of-the-art cryptographic mechanisms via secure outsourced computation**

perspecta LABS

# Software Root of Trust

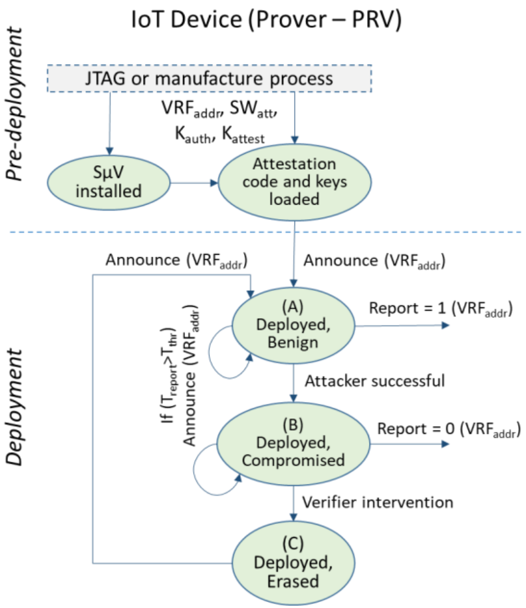
A protected store for holding sensitive keys for authorization and attestation, a secure loader and validator for binaries, libraries, enabling trust bootstrap

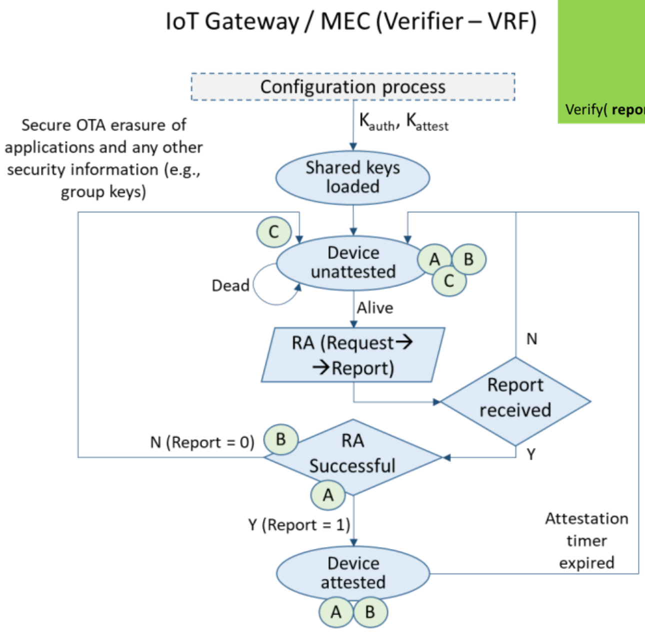


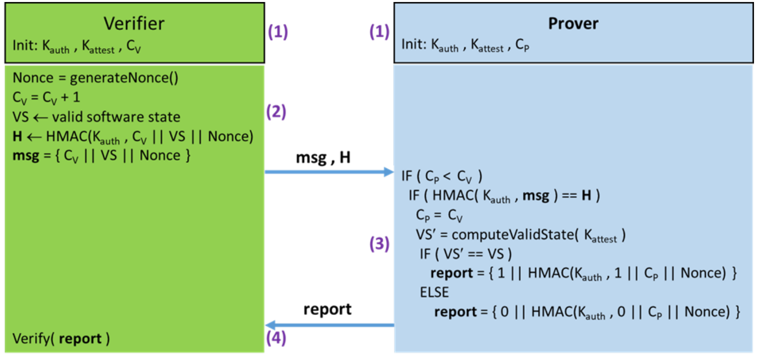

perspecta LABS

# Remote Attestation

Verifies an IOT devices software integrity without reliance on hardware



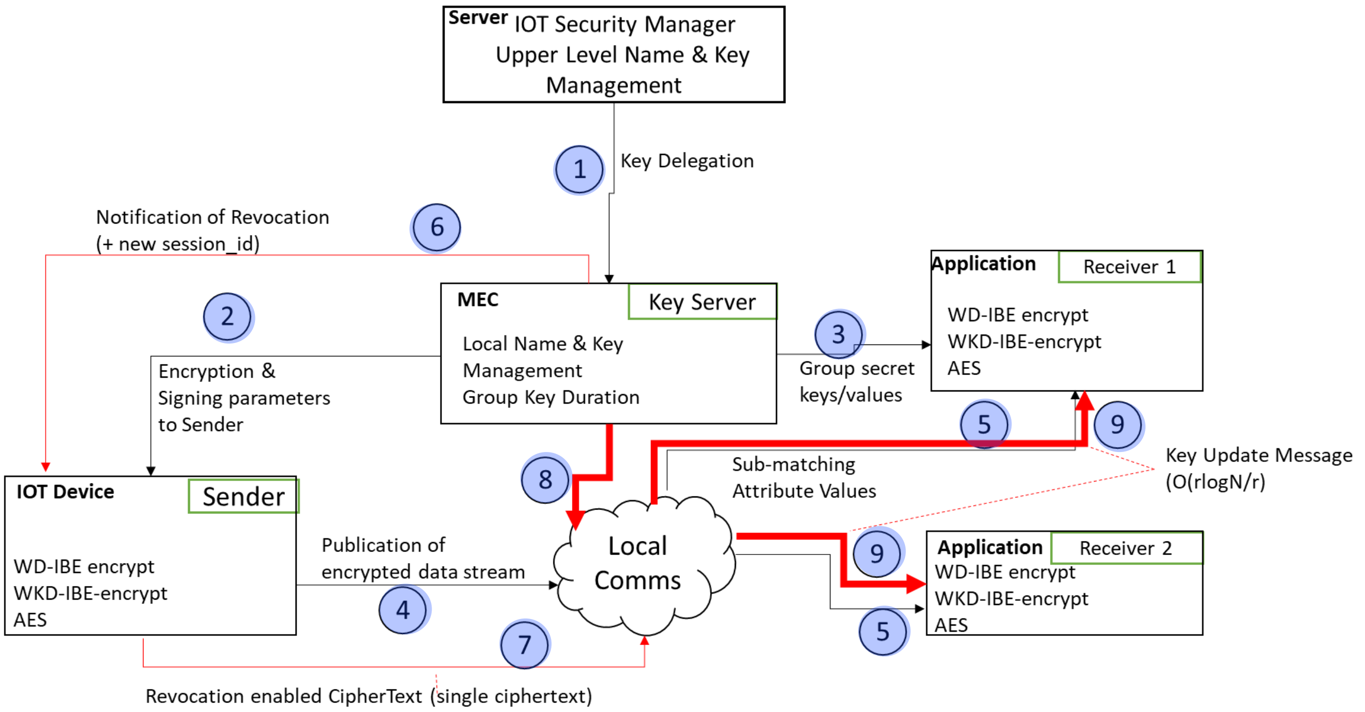




SEDIMENT Remote Attestation Protocol (SRAP)

perspecta LABS

# Scalable Secure Group Identity-Based Encryption

Supports encrypted communications across a broad spectrum of IoT devices with widely disparate SWaP

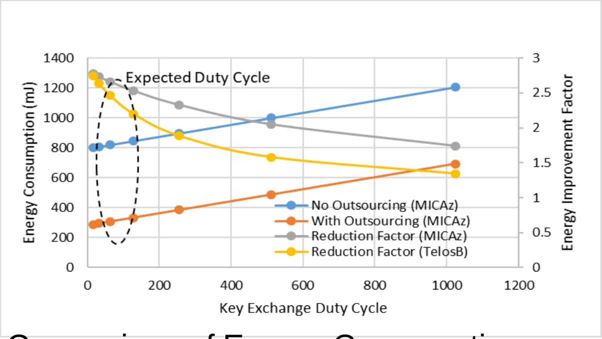



WD-IBE = Identity-based encryption with wildcard-based decryption
WKD-IBE = identity-based encryption with wildcard key derivation
AES = Advanced Encryption Standard

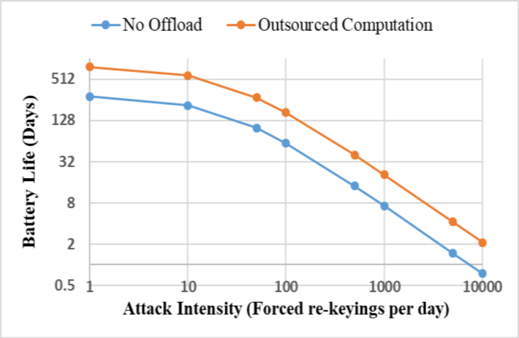
perspecta LABS

# Secure Outsourced Computation

Exploit Multi-access edge computing to improve efficiency of security protocols in long term emplacements




Comparison of Energy Consumption with and without Outsourcing




Battery Life under Energy Depletion Attack

**Outsourced computation protocol for product of exponentiations in a group**

***Client Precomputation***: Given group G with m generators, for i = 1,2,…,m and j = (0,1), choose random u[ij] ∈ G, compute v[j] = $\prod_i g_i^{u[ij]}$, and store (u[1j],u[2j],…,u[mj],v[j]), j=0,1

***Client Problem Instance***: Efficiently calculate F(x[1],x[2],…,x[m]) = $\prod_i g_i^{x[i]}$

**Client C**

Randomly choose λ-bit b
for i in 1,2,…,m:
  z0[i] = x[i] + u[i0]
  z1[i] = b*x[i] + u[i1]

if w0,w1 ∈ G:
  y = w[0]/v[0]
  if w[1]/v[1] == $y^b$:
    return y
return failure

(z0[1],…,z0[m]),
(z1[1],…,z1[m]) →

← w[0],w[1]

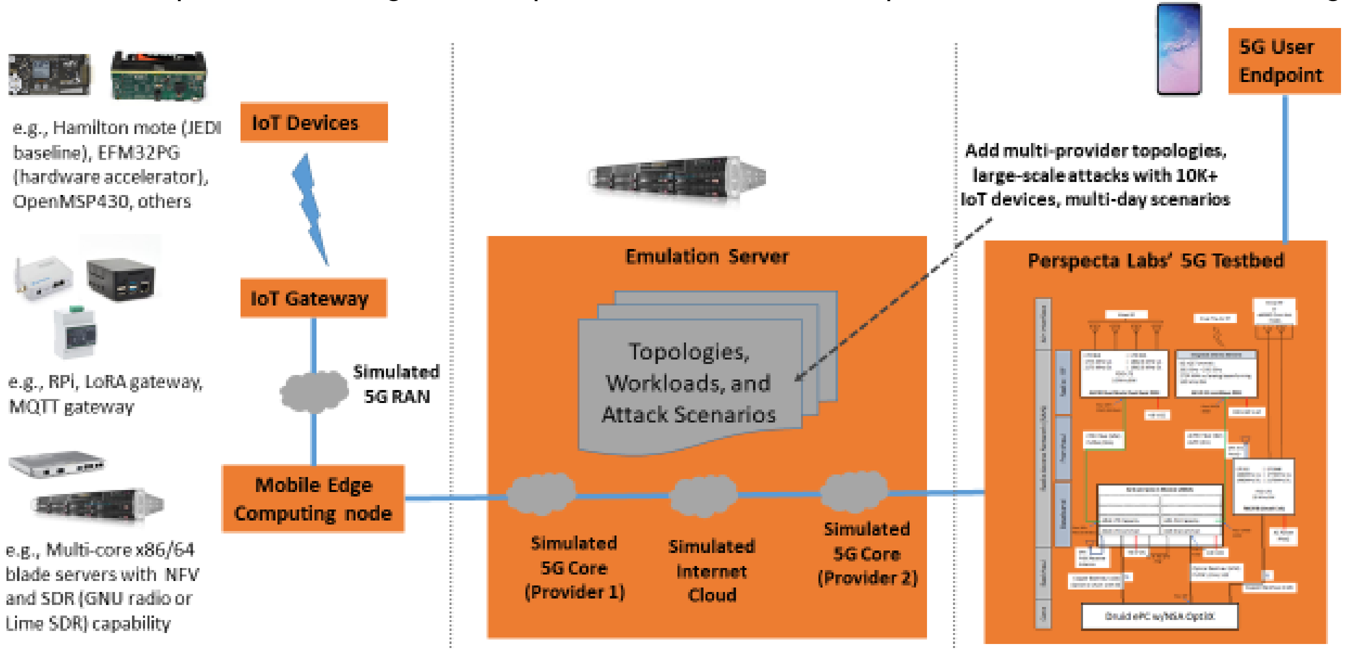
**Server S**

w[0] = $\prod_i g_i^{z0[i]}$
w[1] = $\prod_i g_i^{z1[i]}$

perspecta LABS

# Testbed & Evaluation

Measurements and quantitative insights to help refine architecture and protocols, workloads and testing




**Phase 1: Evaluate Efficient Cryptography on 5G IoT devices**

**Phase 2: Evaluate resilience to penetration attacks**

**Phase 3: Evaluate attacks at scale over a realistic 5G setup**

Compute 256-bit encrypt and sign in < 10 sec using < 70% battery

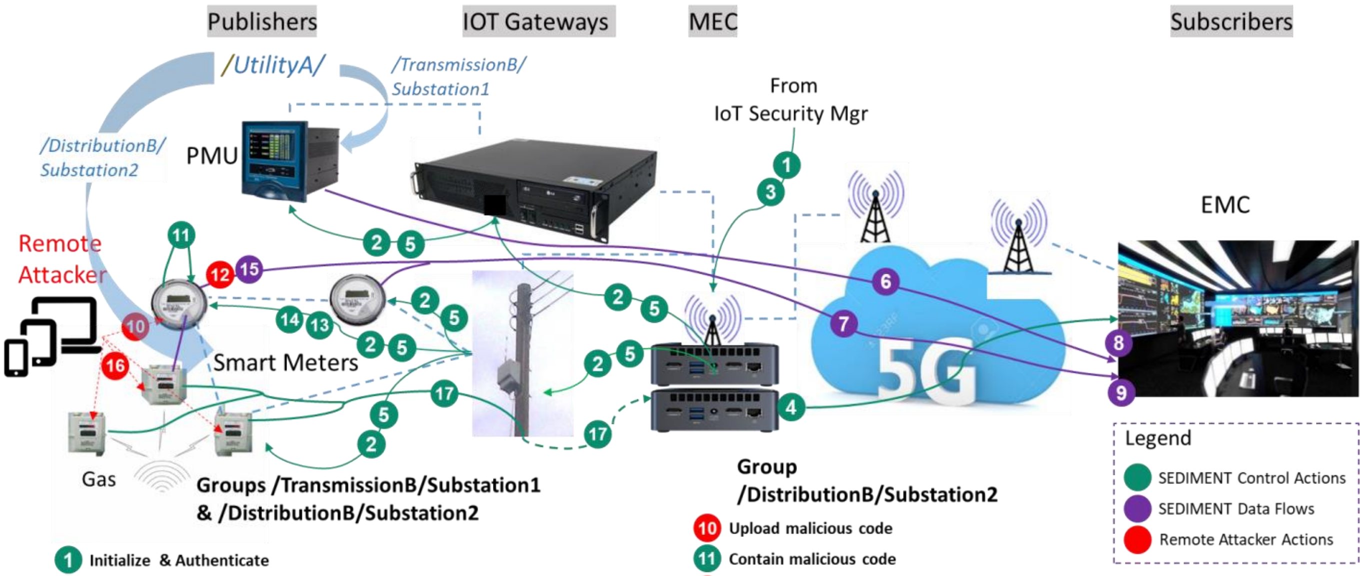
Resist ITE penetration test of many-to-many IoT for 4 hours using < 50% battery

Resist ITE penetration test of 10K IoT + UE for 2 days using < 25% battery

perspecta LABS

# SEDIMENT Information Flows Example

IoT infrastructure for monitoring and controlling Smart Grid assets from an Energy Management Center (EMC)



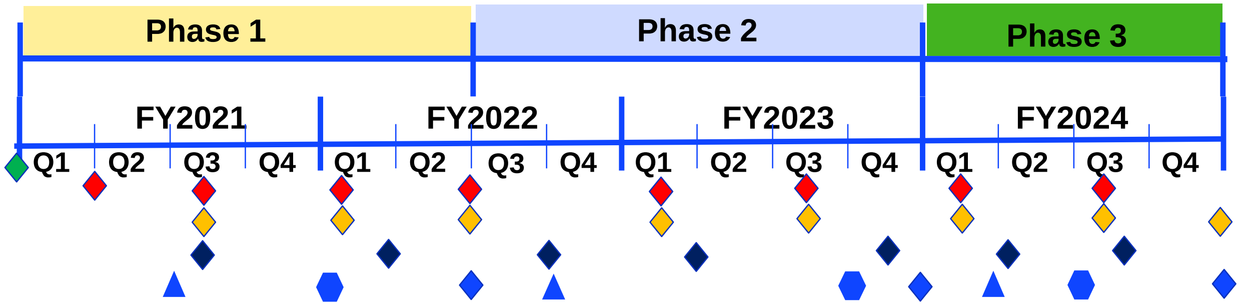

1 Initialize & Authenticate
2 Authenticate & attest in a proxy/delegated setting
3 Delegate group keys (two subscriber groups)
4 Send group secret keys/values (two subscriber groups)
5 Send encryption and signing parameters
6 7 Send encrypted data streams
8 9 Match attribute value and decrypt data streams

10 Upload malicious code
11 Contain malicious code
12 Disrupt encrypted data stream
13 Identify compromised devices via reattestation
14 Restore device (secure erasure, firmware and group keys update) & reattest
15 Restore full encrypted data stream
16 Launch energy depletion DDoS attack
17 Outsource computation to prolong device lifetime under DDoS attack

Explore Transition in 5G Applications in Energy Sector and Other Domains

perspecta LABS

# Schedule




**Establish efficient cryptography mechanisms**
- Software Root of Trust
- Scalable Security Architecture
- Group and Key Management
- Testbed & Internal Integration

**Enhance cryptography & evaluate resistance to attacks**
- Attestation protocols
- Pub/Sub and Resource based Encryption
- Distributed Cryptographic functions
- Test methodologies and implementation

**Scale up and Transition**
- **Harden components**
- **Operational support**
- **Standardization**

- **Kickoff**
- **PI Meetings/Summits**
- **Performer Demonstrations**
- **Evaluations**
- **T&E Platform defined**
- **T&E Platform assumed accessible**
- **T&E Integrated System Demonstrations**

perspecta LABS

# Summary

- Perspecta Labs has teamed with the University of California, Irvine, and Virginia Tech, to develop SEDIMENT: SEcure DIstributed IoT ManagemENT for 5G
- Assumes a zero trust architecture without reliance on additional hardware.
- Focuses on IoT devices, operating across the entire scale of devices on a 5G network, with special emphasis on resource-constrained endpoints.
- Leverages the concept of decoupled senders and receivers to scale up many-to-many communications security from the JEDI research effort, and enhances its key revocation mechanisms to improve the battery lifetime of the IoT devices
- Takes advantage of Multi-access Edge Computing (MEC) resources available to reduce the remote attestation, cryptographic computation and energy burden on the IoT devices.
- Testbed with phased plan to (i) establish and test efficient cryptography, (ii) evaluate resilience to penetration attacks, (iii) evaluate attacks at scale.