M2Mi™

Machine-to-Machine Intelligence Corporation

Machine-to-Machine Security and Privacy: Challenges and Opportunities

Geoff Brown, CEO

geoff.brown@m2mi.com @M2MiCorp

M2Mi Overview

- M2Mi provides a SaaS M2M and IoT-to-Cloud Platform
- Founded: 2006 at NASA Research Park
  - Products in production on thousands of network and compute assets
- Intellectual property and patents
  - “Personal portal and secure information exchange” (US7376652, Patent 2003)
  - Global Trademark “M2M Intelligence®”
- Industry leadership
  - Founding OASIS MQTT member; Chair of security sub-committee
  - Member, Smart Grid Interoperability Panel

ORACLE
OASIS
CISC
intel
M2M
Machine-to-Machine Intelligence Corpo
IBM
SGIP
SMART GRID INTEROPERABILITY PANEL
ERIC
vodafone

- Gartner Cool Vendor 2014, Connected World Top 100
- Available for trial and purchase via the IBM Cloud Marketplace

Enterprises failing to secure M2M transactions

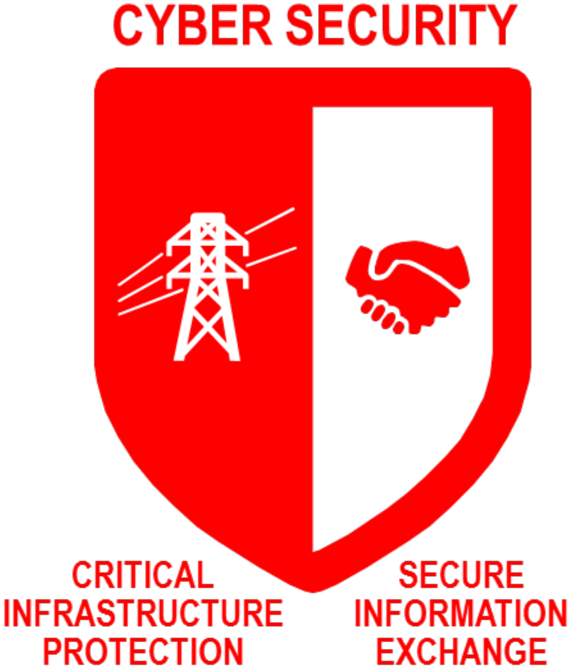
M2M security remains inadequate*

M2M security priority is high

- 96% of IT decision makers define data security of M2M transactions a priority this year
- Being compliant with regulations in the M2M environment is more important that efficiency gains

Security technology is not keeping up

- Does not solve issues of privacy, scale, trust, key management, nor do they provide dynamic policy-driven decisions to move data
- Does not address shift from IT and InfoSec to Operation technology (OT) security


CYBER SECURITY
CRITICAL INFRASTRUCTURE PROTECTION
SECURE INFORMATION EXCHANGE

sight, Feb 25, 2014. Enterprise Failing to Secure M2M Transactions

Security is stifling M2M and IoT potential

IDC reports security as #1 hurdle to adoption

Trust – untrusted networks, untrusted devices

Cost – large number of devices requires very low costs

Privacy – who owns the data and how to securely share

Performance – edge devices do not have cycles for security

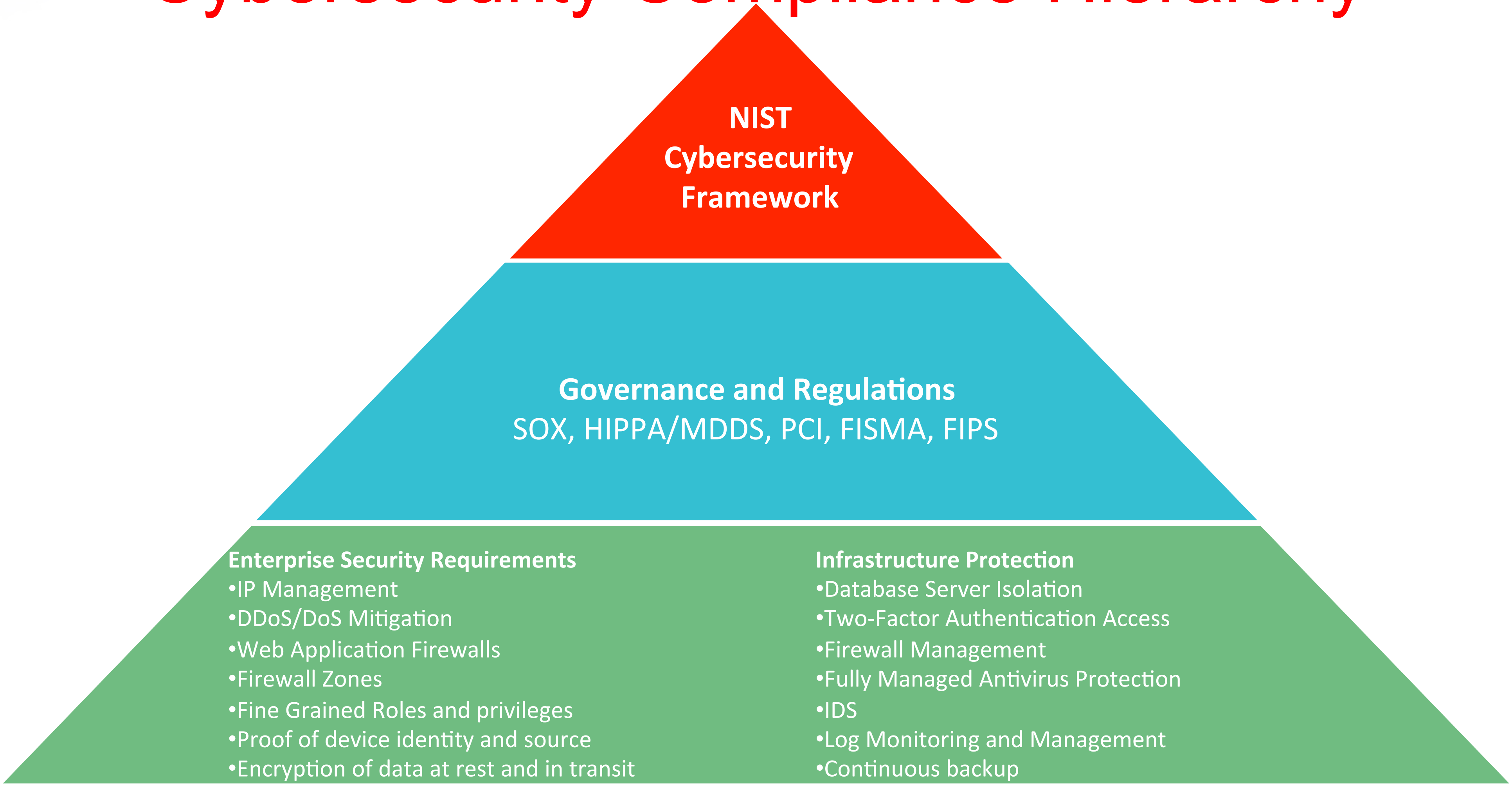
Dynamic – static policies cannot address changing environment

Interoperability – large number of diverse participants

Advanced Security and Privacy Considerations

- NIST Cyber Security Framework
- Emerging Crypto specifically for M2M and IoT (Simon & Speck)
- The “lockbox” security paradigm for Critical Infrastructure

Cybersecurity Compliance Hierarchy



NIST Cybersecurity Framework

Governance and Regulations
SOX, HIPPA/MDDS, PCI, FISMA, FIPS

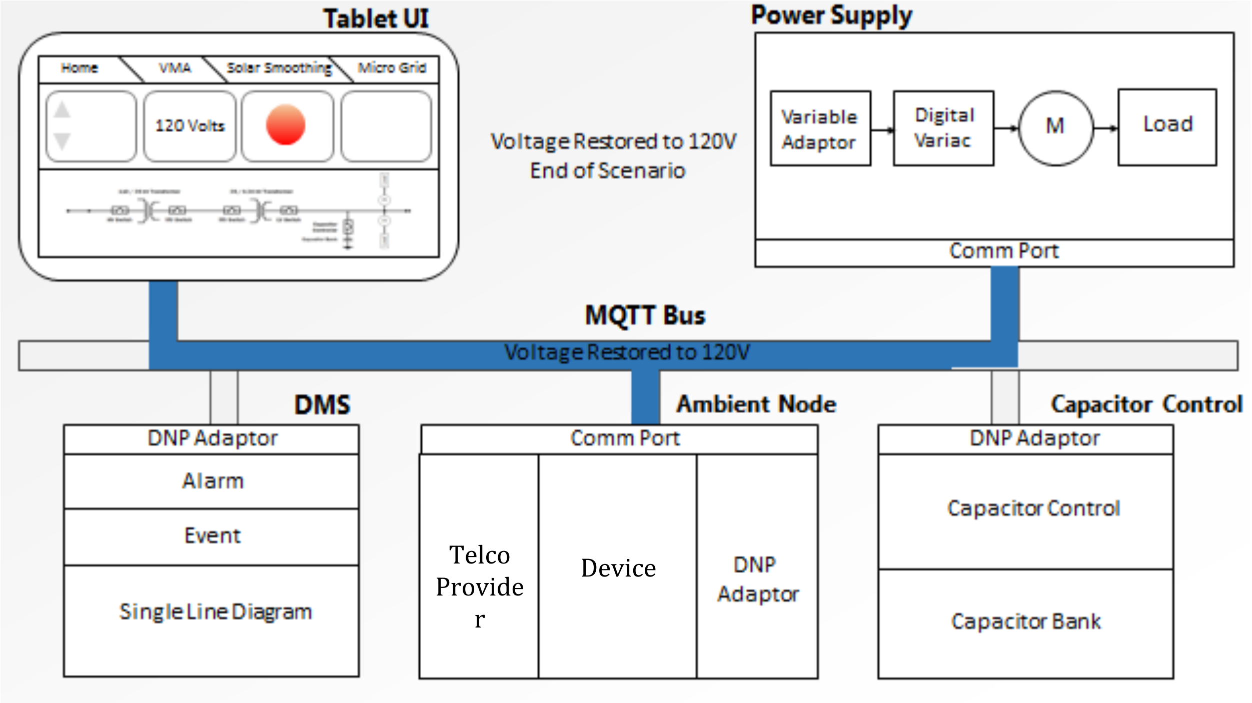
Enterprise Security Requirements

- IP Management
- DDoS/DoS Mitigation
- Web Application Firewalls
- Firewall Zones
- Fine Grained Roles and privileges
- Proof of device identity and source
- Encryption of data at rest and in transit

Infrastructure Protection

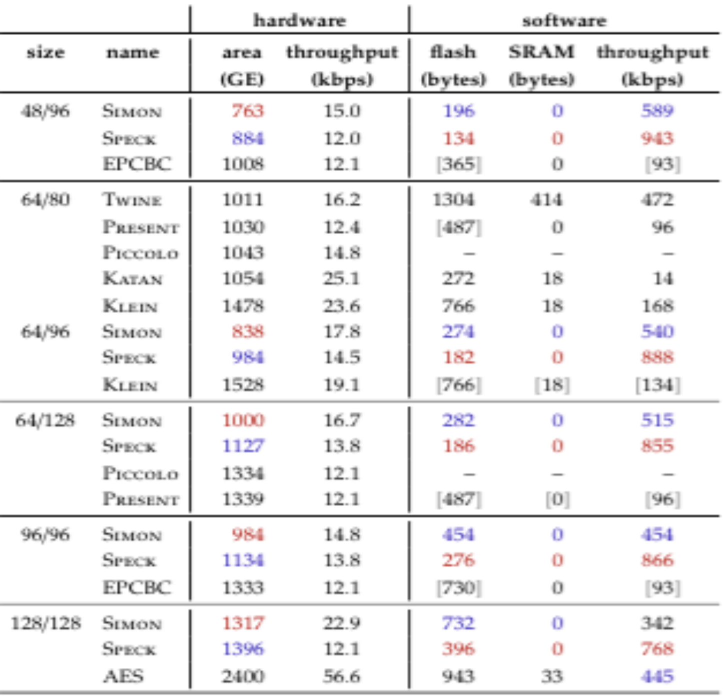
- Database Server Isolation
- Two-Factor Authentication Access
- Firewall Management
- Fully Managed Antivirus Protection
- IDS
- Log Monitoring and Management
- Continuous backup

Smart Grid – internal structure



Reference : https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=mqtt-security

Simon & Speck



		hardware		software		
size	name	area	throughput	flash	SRAM	throughput
		(GE)	(kbps)	(bytes)	(bytes)	(kbps)
48/96	Simon	763	15.0	196	0	589
	Speck	884	12.0	134	0	943
	EPCBC	1008	12.1	[365]	0	[93]
64/80	Twine	1011	16.2	1304	414	472
	Present	1030	12.4	[487]	0	96
	Piccolo	1043	14.8	–	–	–
	Katan	1054	25.1	272	18	14
	Klein	1478	23.6	766	18	168
64/96	Simon	838	17.8	274	0	540
	Speck	984	14.5	182	0	888
	Klein	1528	19.1	[766]	[18]	[134]
64/128	Simon	1000	16.7	282	0	515
	Speck	1127	13.8	186	0	855
	Piccolo	1334	12.1	–	–	–
	Present	1339	12.1	[487]	[0]	[96]
96/96	Simon	984	14.8	454	0	454
	Speck	1134	13.8	276	0	866
	EPCBC	1333	12.1	[730]	0	[93]
128/128	Simon	1317	22.9	732	0	342
	Speck	1396	12.1	396	0	768
	AES	2400	56.6	943	33	445

Table 1.1: Performance comparisons. Size is block size/key size; hardware refers to an ASIC implementation, and software to an implementation on an 8-bit microcontroller; clock speeds are 100 kHz (hardware) and 16 MHz (software). The best performance for a given size is indicated in red, the second best in blue. Numbers in brackets are our estimates; "–" means these values were unavailable at the time of writing.

- Lightweight Block Cypher for M2M and IoT from NSA

- Simon – Hardware implementation
- Speck – Software implementation

- Ideal for Crypto rotation

- Simon& Speck submitted and accepted by ISO Standards Body 29192-2 (6 month wait)

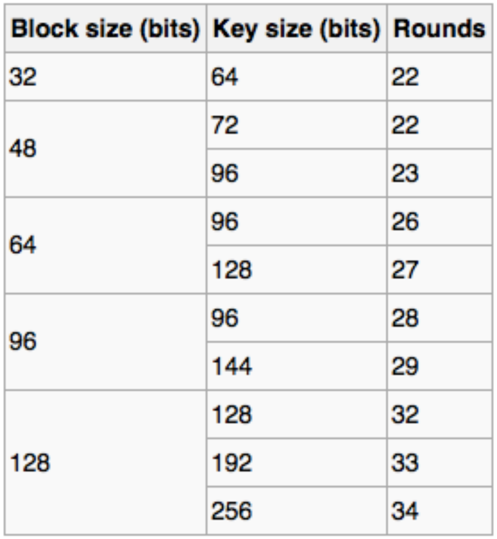
tp://en.wikipedia.org/wiki/Speck_(cipher)

Simon : http://en.wikipedia.org/wiki/Speck_(cipher)

Mi™

Corporation

Speck



Block size (bits)	Key size (bits)	Rounds
32	64	22
48	72	22
	96	23
64	96	26
	128	27
96	96	28
	144	29
128	128	32
	192	33
	256	34

Reference code of encryption of Speck variant with 128 bit block size and key

```
#include <stdint.h>

#define ROR(x, r) ((x >> r) | (x << (64 - r)))
#define ROL(x, r) ((x << r) | (x >> (64 - r)))
#define R(x, y, k) (x = ROR(x, 8), x += y, x ^= k, y = ROL(y, 3), y ^= x)

void encrypt(uint64_t *pt, uint64_t *ct, uint64_t *K)
{
  uint64_t i, B = K[1], A = K[0];
  ct[0] = pt[0]; ct[1] = pt[1];

  for(i = 0; i < 32; i++)
  {
    R(ct[1], ct[0], A);
    R(B, A, i);
  }
}
```

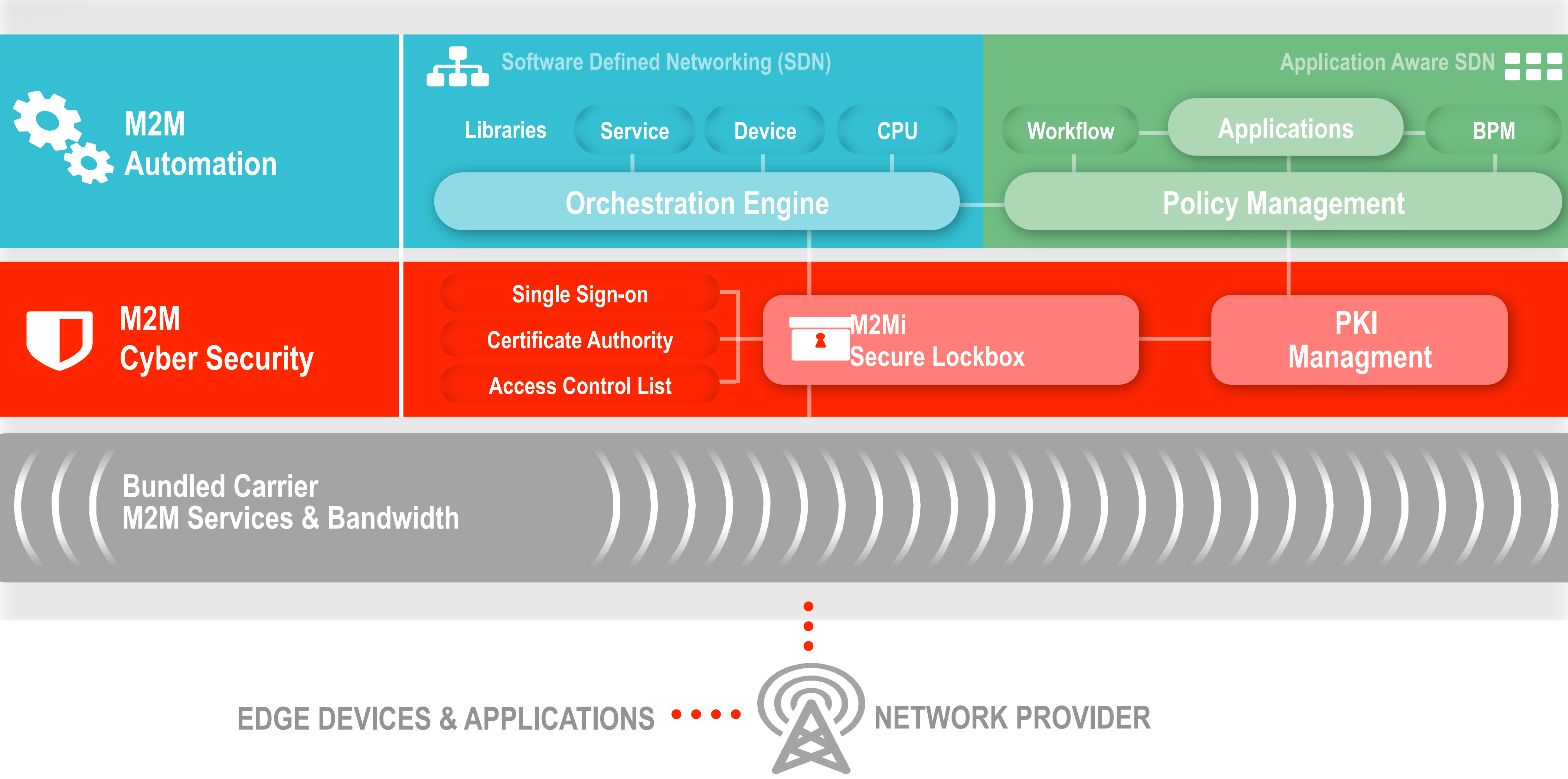
tp://en.wikipedia.org/wiki/Speck_(cipher)

Cryptanalysis Performance

PECK : Differential cryptanalysis can break 17 rounds of Speck128/128 with 2^{113} data,
^{2} bytes memory and time complexity of 2^{113}.
ectangle attack can break 18 rounds of Speck128/192,256 with $2^{121.9}$ data,
$^{25.9}$ bytes memory and time complexity of $2^{182.7}$.

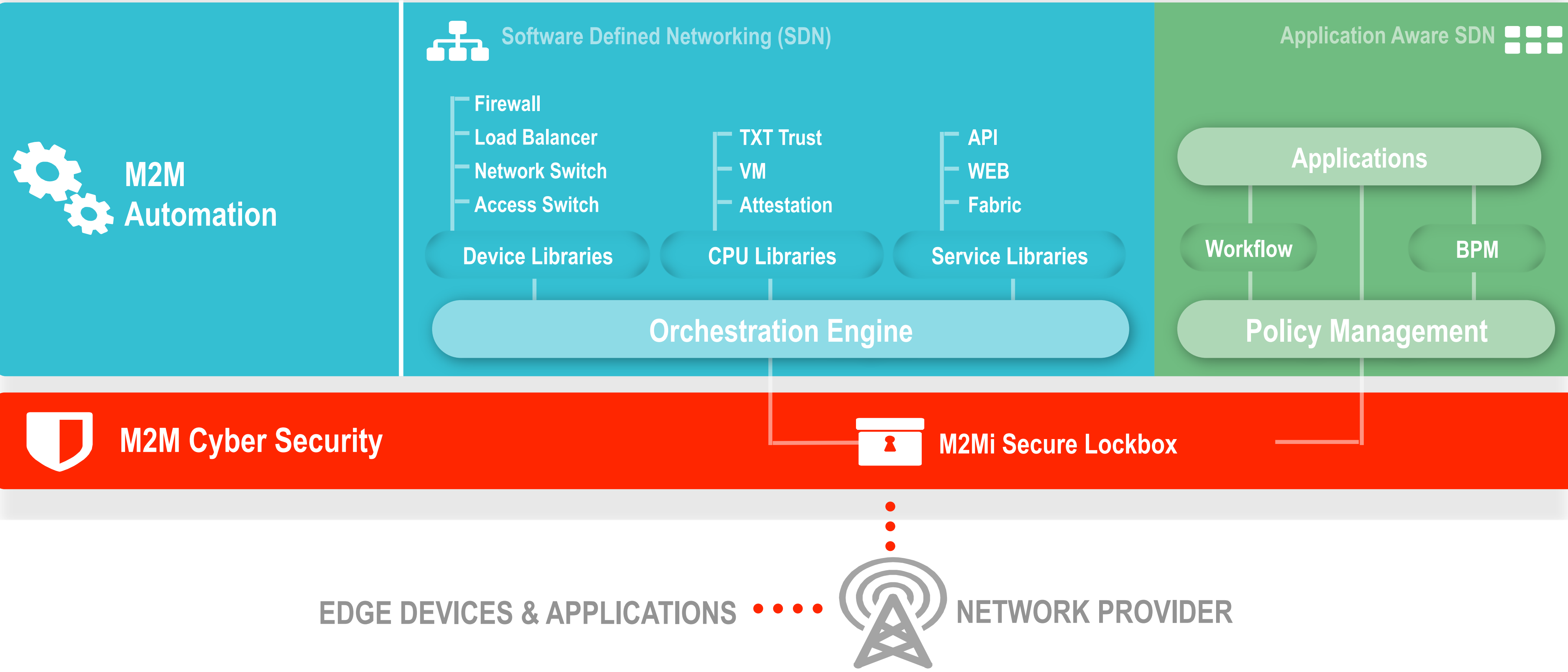
MON : Differential cryptanalysis can break 46 rounds of Simon128/128 with $2^{125.6}$ data,
$^{0.6}$ bytes memory and time complexity of $2^{125.7}$ with success rate of 0.632

M2Mi Logical Architectu



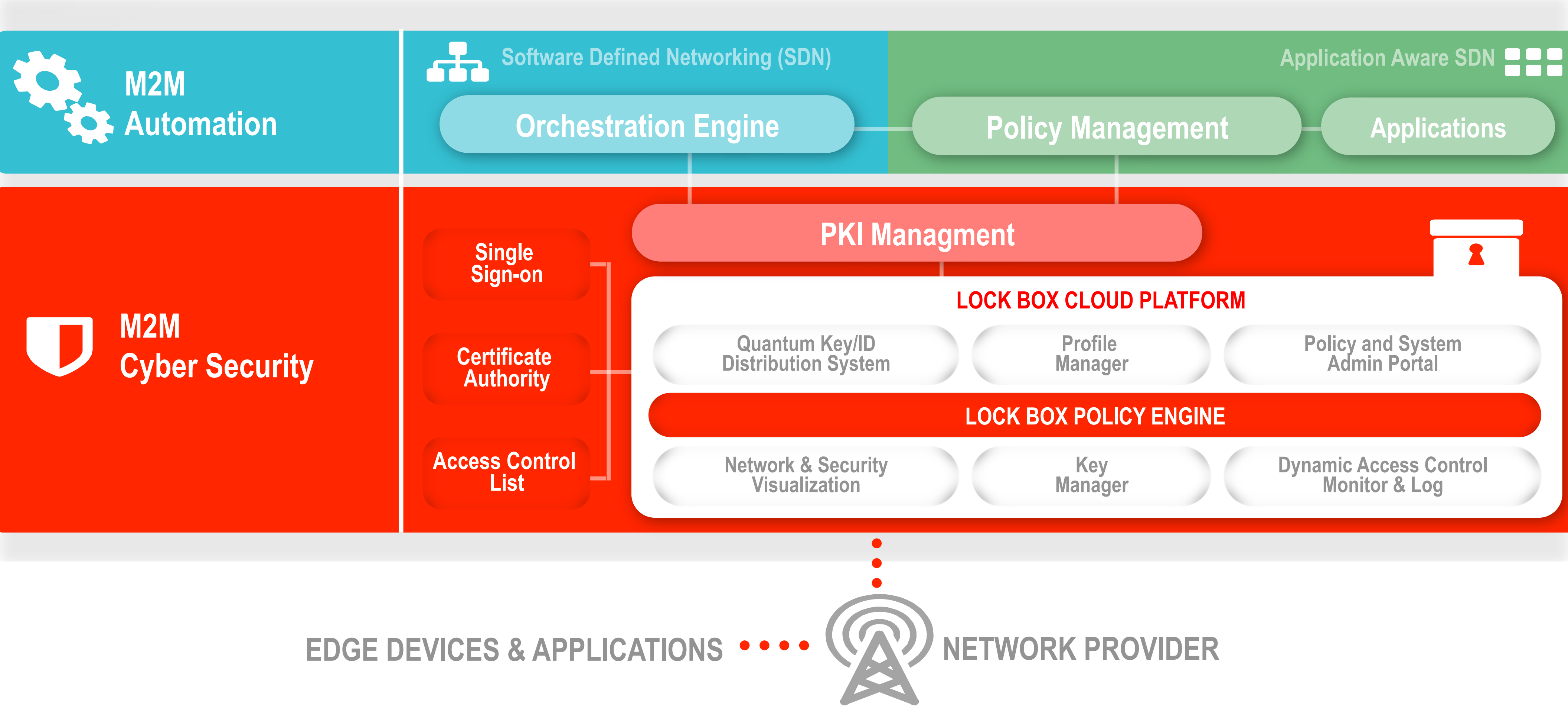
Mi™
Corporation

Data Center Viewpoi

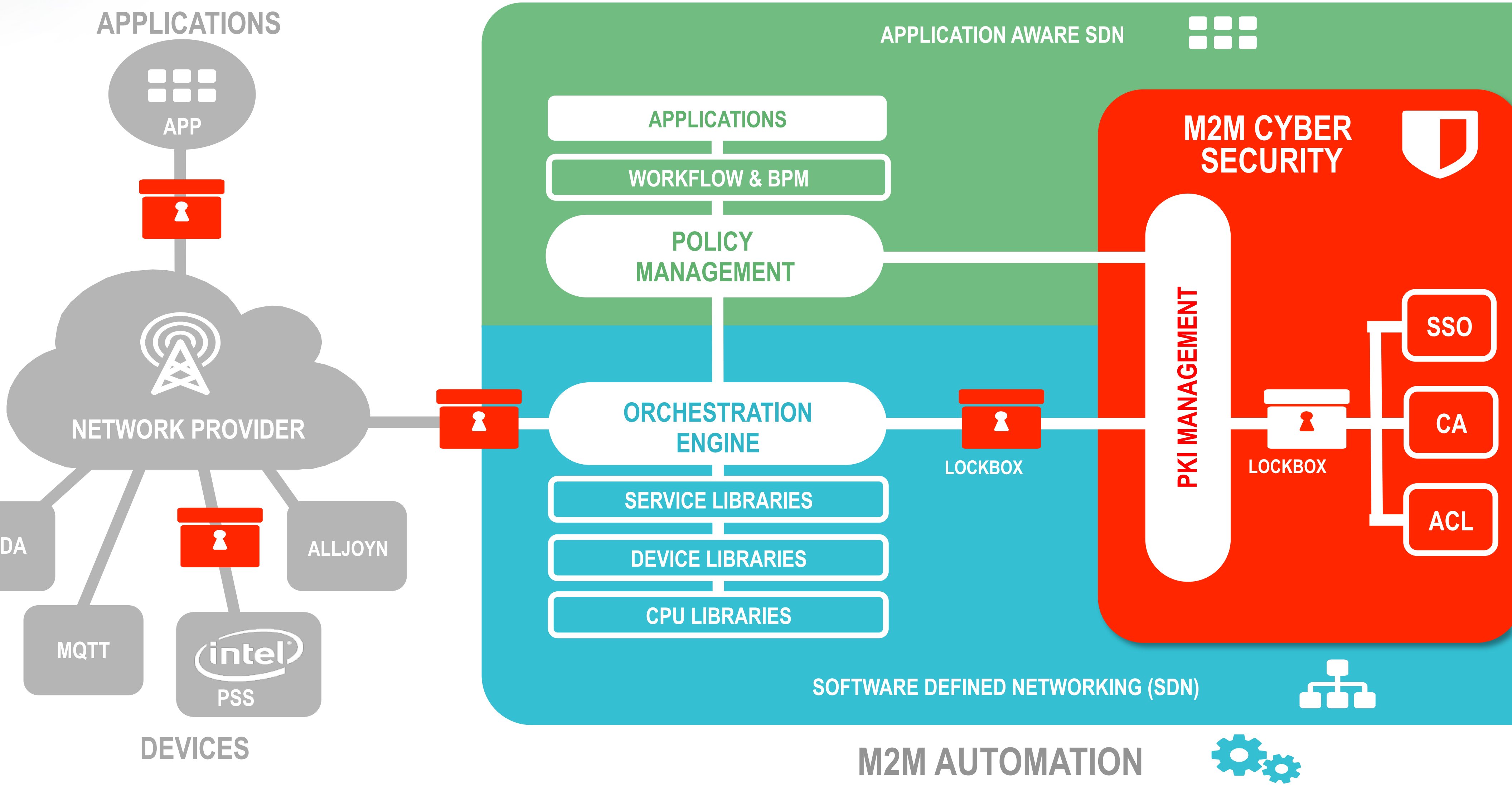


Mi™
Corporation

Security Viewpoi

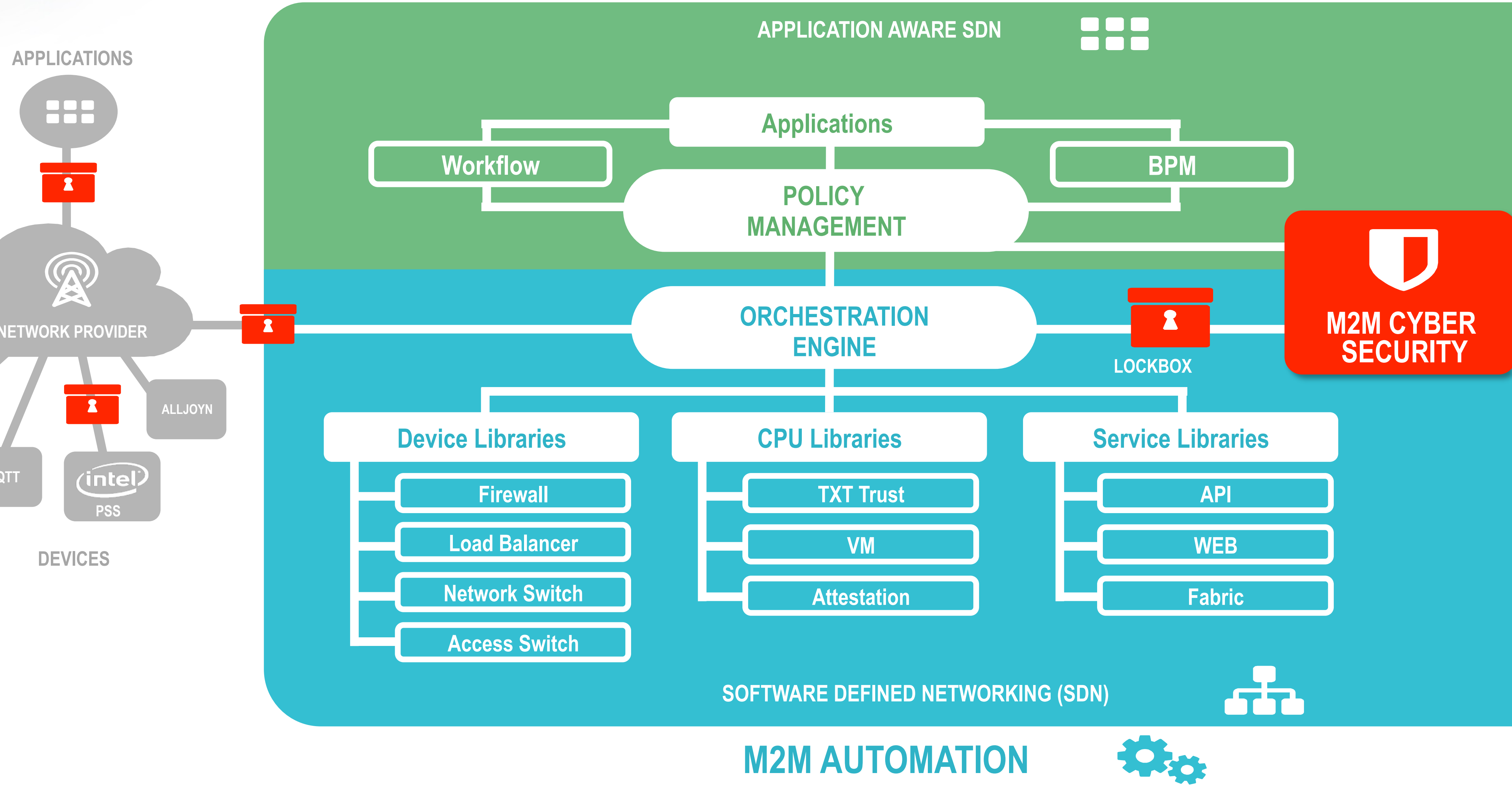


M2Mi Logical Architectu



Mi™
Corporation

Data Center Viewpo



APPLICATIONS

NETWORK PROVIDER

ALLJOYN

QTT

intel
PSS

DEVICES

APPLICATION AWARE SDN

Applications

Workflow

BPM

POLICY MANAGEMENT

ORCHESTRATION ENGINE

LOCKBOX

M2M CYBER SECURITY

Device Libraries

- Firewall
- Load Balancer
- Network Switch
- Access Switch

CPU Libraries

- TXT Trust
- VM
- Attestation

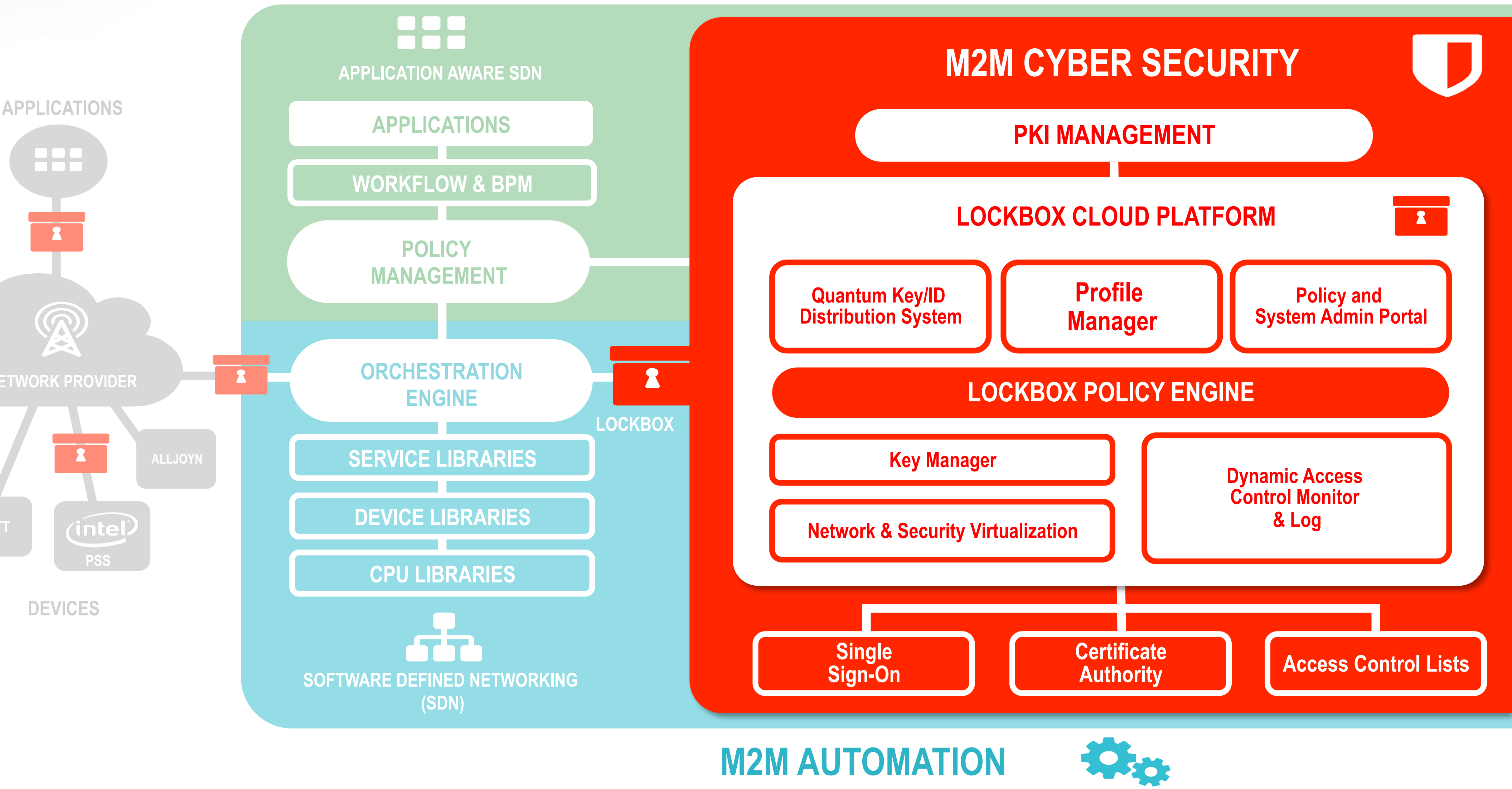
Service Libraries

- API
- WEB
- Fabric

SOFTWARE DEFINED NETWORKING (SDN)

M2M AUTOMATION

Security Viewpo



APPLICATIONS

ETWORK PROVIDER

ALLJOYN

T

intel
PSS

DEVICES

APPLICATION AWARE SDN

APPLICATIONS

WORKFLOW & BPM

POLICY MANAGEMENT

ORCHESTRATION ENGINE

SERVICE LIBRARIES

DEVICE LIBRARIES

CPU LIBRARIES

SOFTWARE DEFINED NETWORKING (SDN)

LOCKBOX

M2M CYBER SECURITY

PKI MANAGEMENT

LOCKBOX CLOUD PLATFORM

Quantum Key/ID Distribution System

Profile Manager

Policy and System Admin Portal

LOCKBOX POLICY ENGINE

Key Manager

Network & Security Virtualization

Dynamic Access Control Monitor & Log

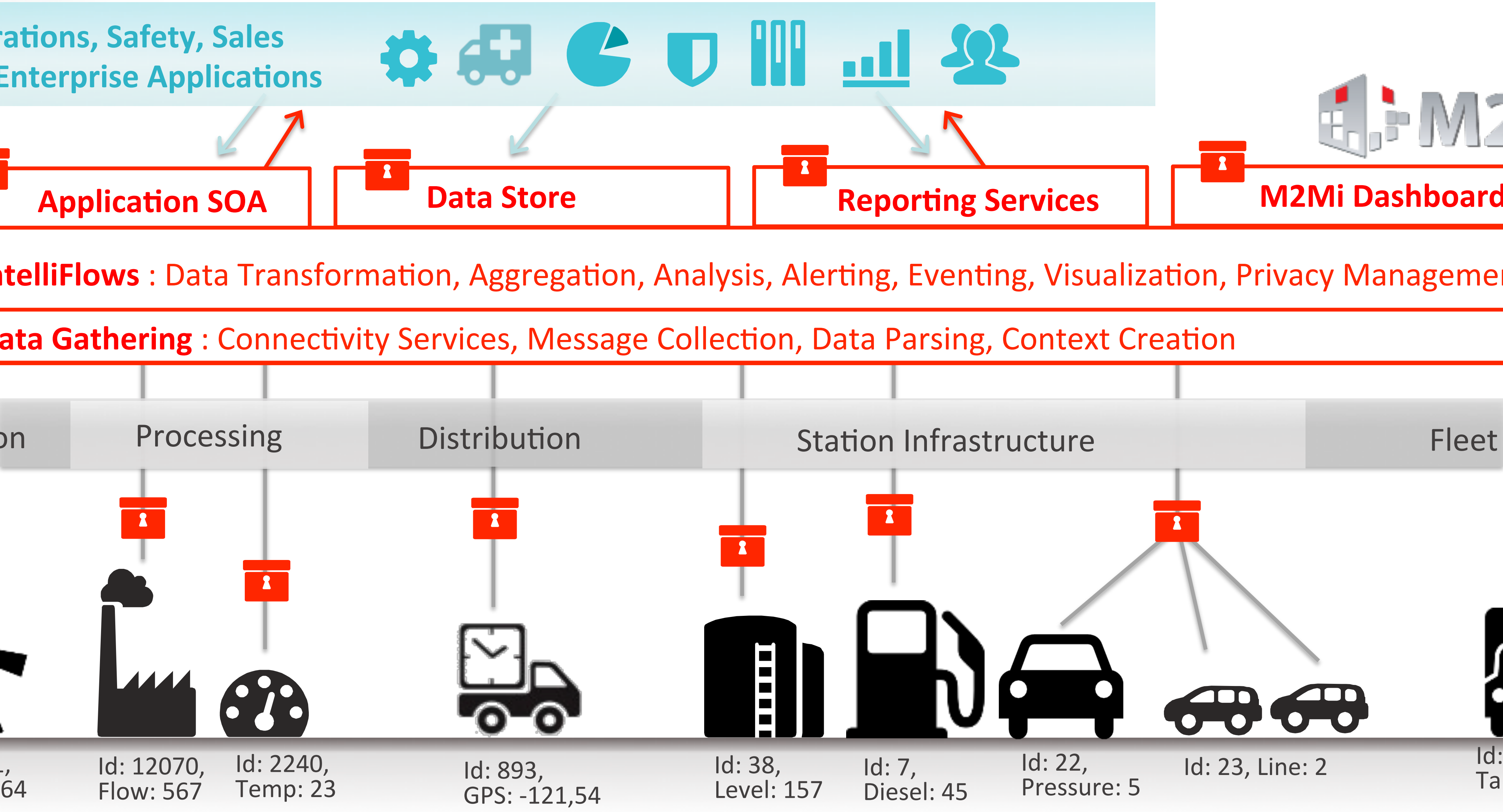
Single Sign-On

Certificate Authority

Access Control Lists

M2M AUTOMATION

Use case



rations, Safety, Sales
Enterprise Applications

Application SOA

Data Store

Reporting Services

M2Mi Dashboard

ntelliFlows : Data Transformation, Aggregation, Analysis, Alerting, Eventing, Visualization, Privacy Managemen

ata Gathering : Connectivity Services, Message Collection, Data Parsing, Context Creation

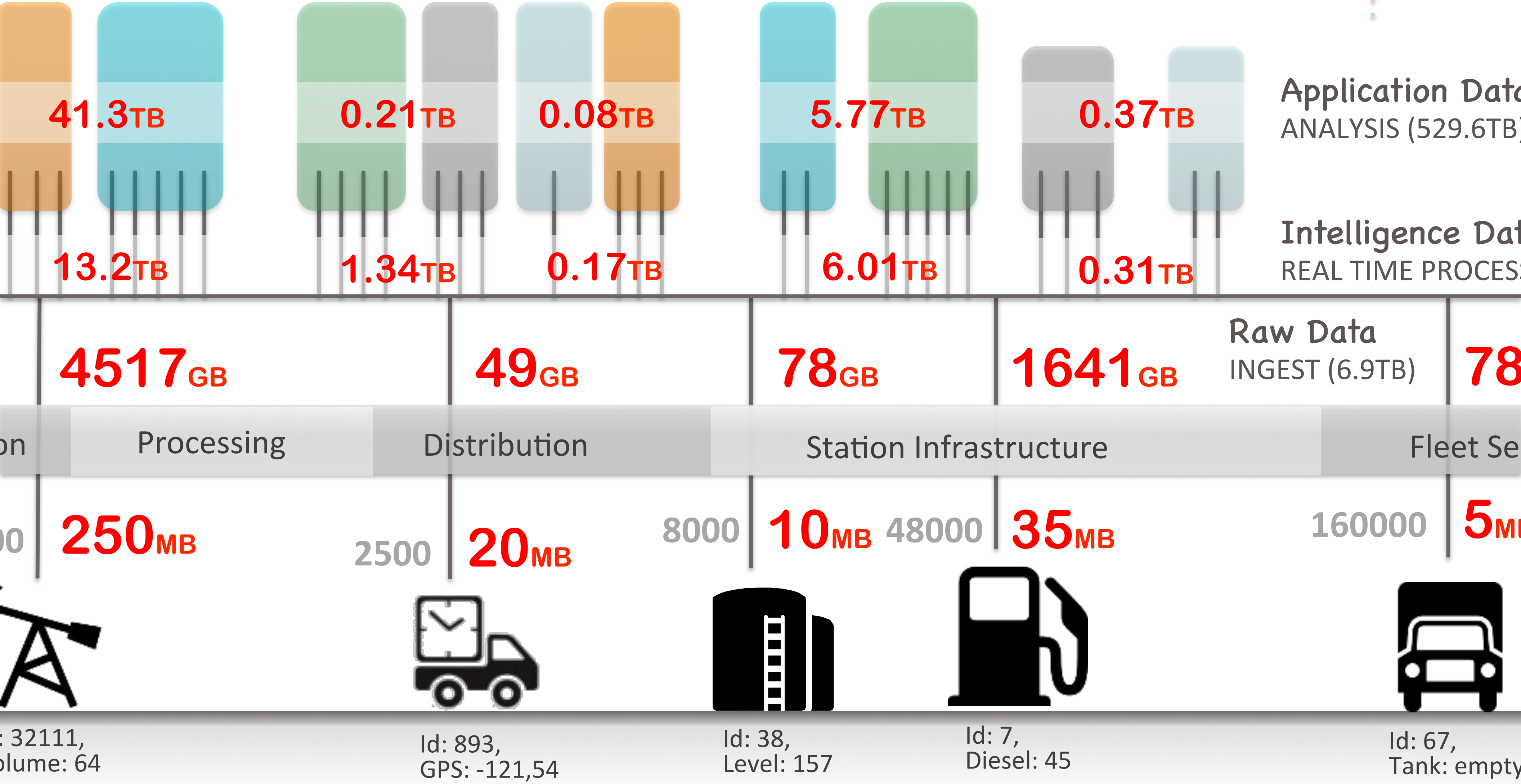
M2Mi : Where does all the data go?

230,311 MSGs/ sec

50 Av MS

237,000 devices

143 ME str



41.3TB

0.21TB

0.08TB

5.77TB

0.37TB

Application Data ANALYSIS (529.6TB

13.2TB

1.34TB

0.17TB

6.01TB

0.31TB

Intelligence Dat REAL TIME PROCES

4517GB

49GB

78GB

1641GB

Raw Data INGEST (6.9TB)

78

on

Processing

Distribution

Station Infrastructure

Fleet Se

00

250MB

2500

20MB

8000

10MB

48000

35MB

160000

5MI

: 32111, olume: 64

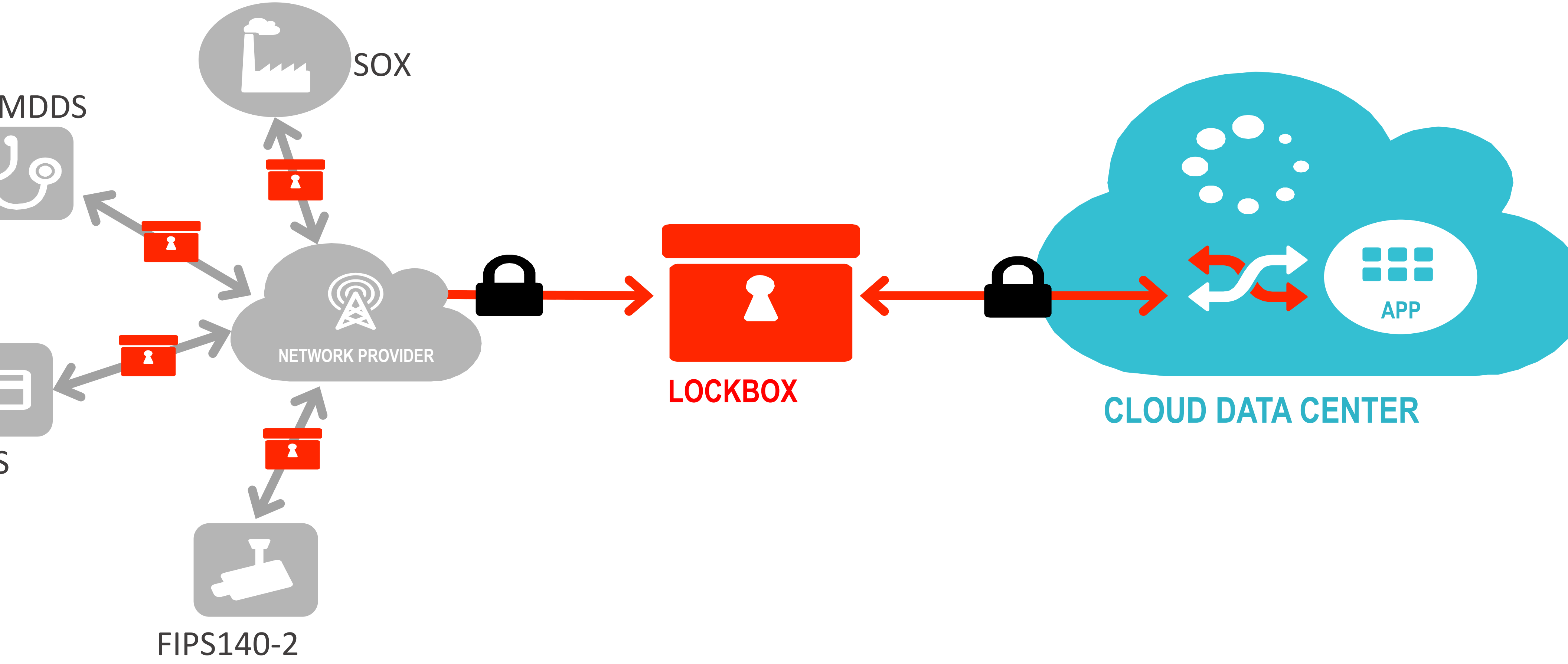
Id: 893, GPS: -121,54

Id: 38, Level: 157

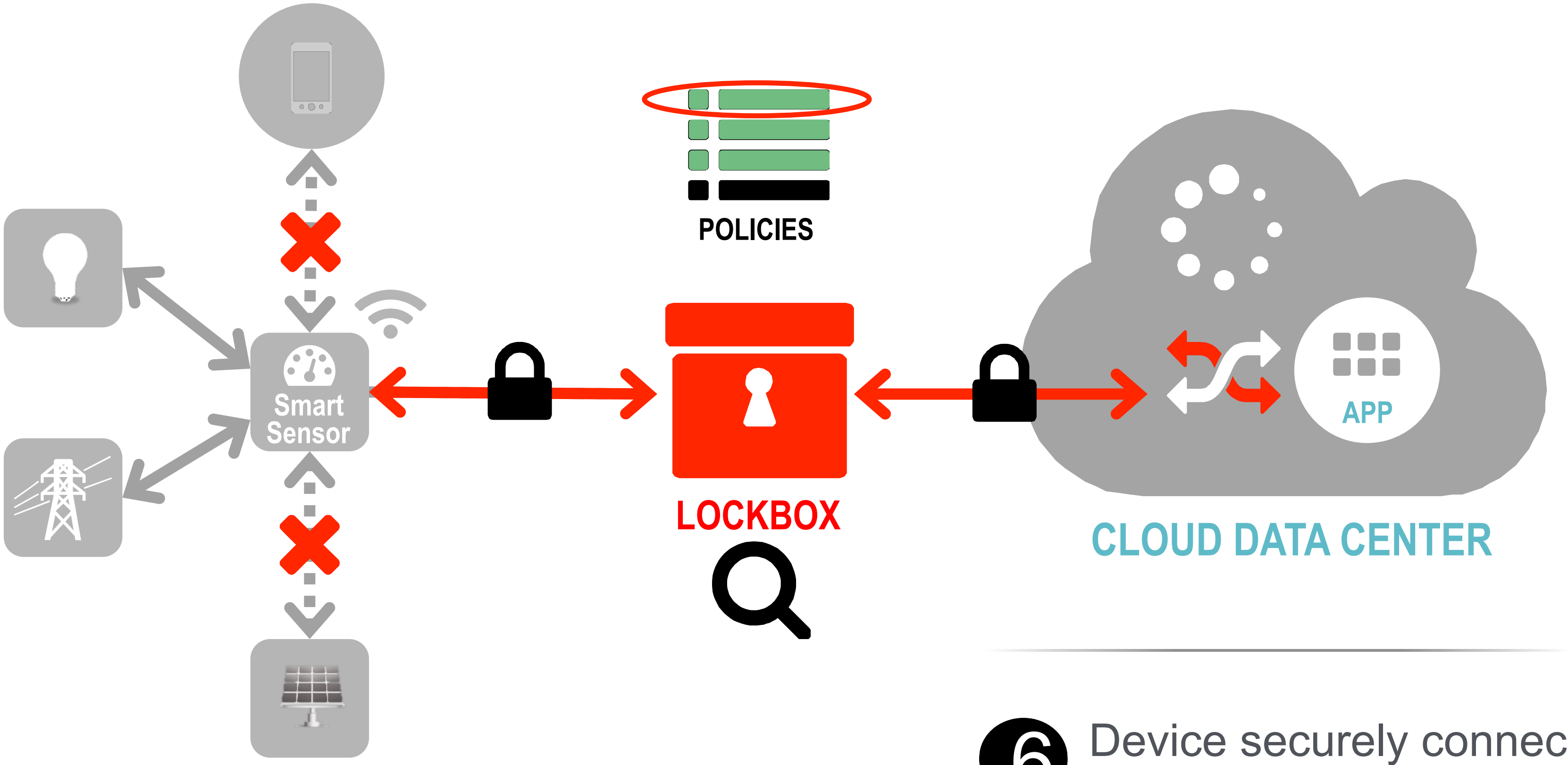
Id: 7, Diesel: 45

Id: 67, Tank: empty

Industry Specific M2M Compliant Network



Lockbox technology – use case scenario



❻ Device securely connects to cloud app, based on current policies, and shares information

Internet of Things

Smart Home Automotive Retail Health Care Smart Grid Critical Infrastructure Manufacturing

M2Mi™

Machine-to-Machine Intelligence Corporation

Questions