VIBE Cyber

Trust Nothing. Authenticate Everything.

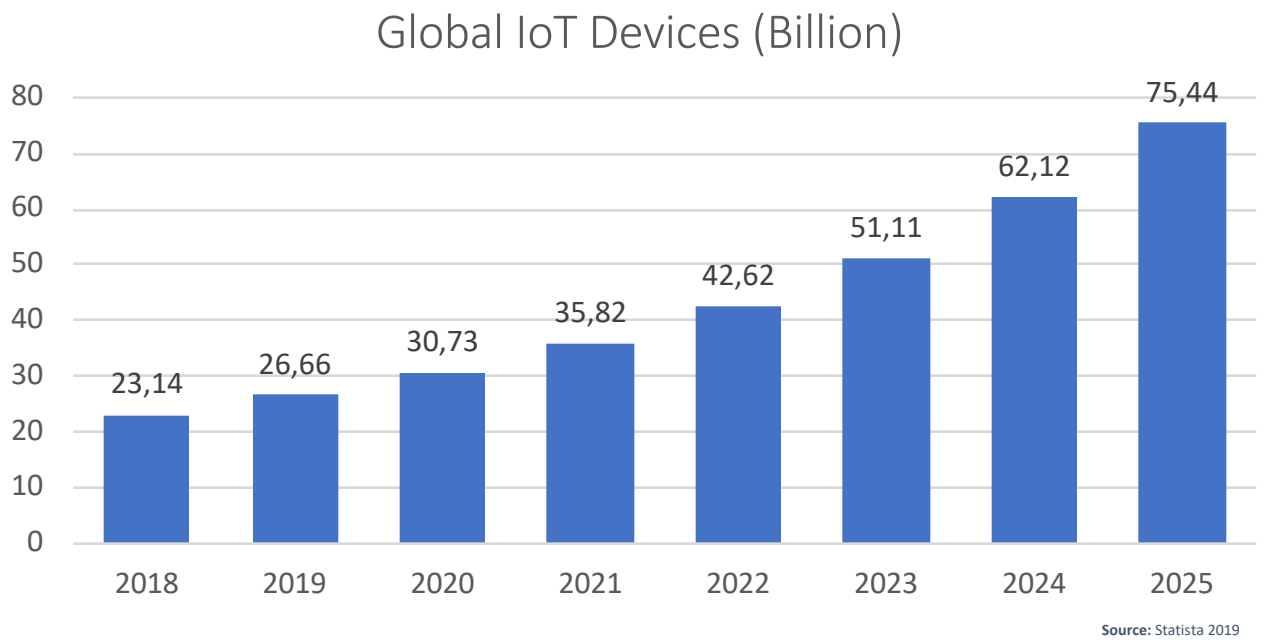
Challenged by IoT Security?

How a modern, certificate-less cryptosystem has solved the IoT security dilemma

Hisham Lamei
VIBE Cybersecurity International LLC
IoTSF 2019 : 26 November 2019 – London

Setting the Stage for IoT

VIBE Cyber
Trust Nothing. Authenticate Everything.



Deployed IoT devices projected to be 75.44 billion by 2025.

The IoT Opportunity

VIBE Cyber
Trust Nothing. Authenticate Everything.

IoT represents a tremendous opportunity to enhance our lives in virtually every industry

- Transportation (V2X) and Logistics
- Building Management
- Energy Supply and Distribution
- Water Management
- Healthcare
- Agriculture
- Financial Services
- Smart Home
- Wearables

To fully leverage the IoT opportunity, however, ironclad security of connected "things," and associated trust in IoT-generated data is paramount.

State of IoT Security

VIBE Cyber
Trust Nothing. Authenticate Everything.

IoT Manufacturers have effectively ignored security

- 80% of deployed IoT devices are not secure
  (Source: Ponemon Institute)
- 50% of US companies that use IoT devices have had a security breach
- average cost of security breach for $5m company is $650k
  (Source: Altman, Valandrie and Company)

The IoT security challenge is not only about protecting future IoT devices and related networks, platforms and applications from being compromised by cyber attacks. It involves eliminating the security risk inherent in the tens of millions of devices that are already deployed.

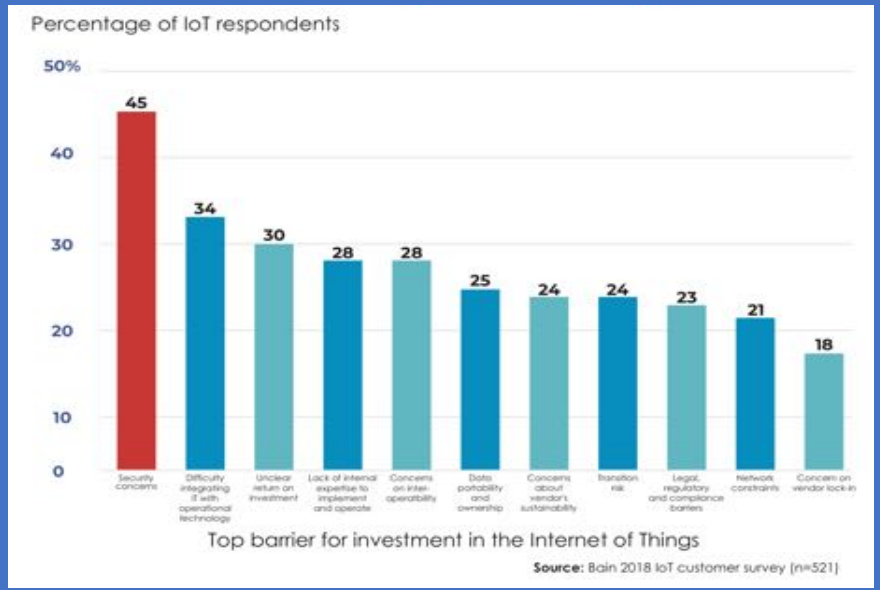
Security – The Critical IoT Barrier

VIBE Cyber
Trust Nothing. Authenticate Everything.

Deploying security correctly is no easy task as it requires skills and expertise that many companies lack. This leads to security being ignored at the product or service design stage, or bolted-on as an afterthought at the end of the design cycle.

The Situation is Dire. The list of serious cybercrimes includes documented attacks on connected cars, power grids, water systems, nuclear facilities, and the critical infrastructure supporting hospitals and airport security systems.

Security is the Leading Barrier to IoT Adoption



Another IoT Adoption Barrier - Scalability

VIBE Cyber
Trust Nothing. Authenticate Everything.

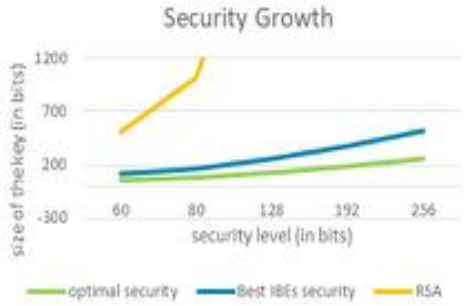
Scalability according to the NIST definition is "capabilities that can be elastically provisioned and released to scale rapidly outward and inward, commensurate with demand."

In the Cybersecurity Industry, scalability means the ability to

- Seamlessly deploy and manage the rapid growth of devices within a given application, and to do so economically, while adapting to operational requirements

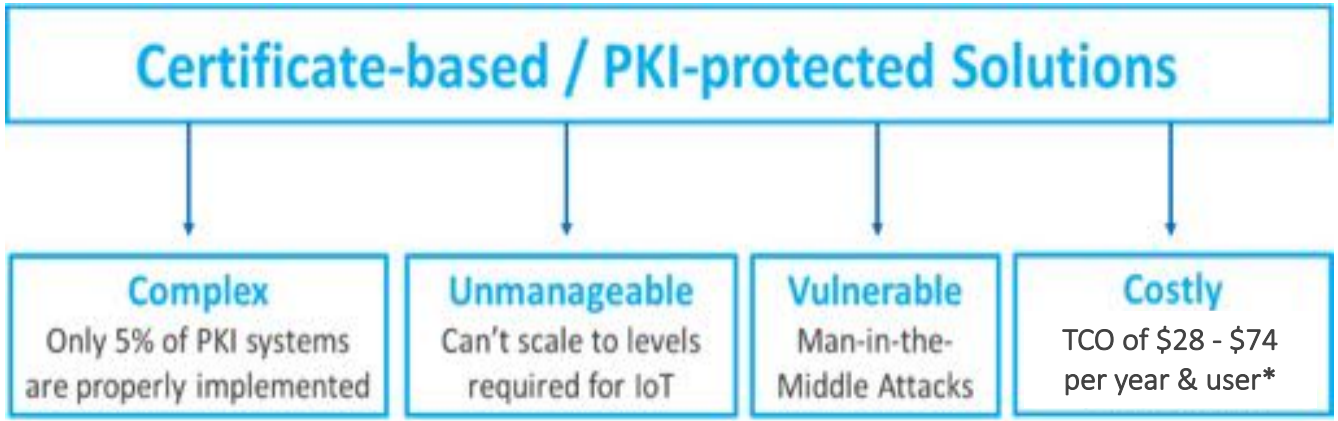
Scalability requires

- Efficiency in terms of data size, and signing length
- Sustainable efficiency, easily adaptable to inevitable future changes in security requirements



The Current Approach to Securing IoT …

VIBE Cyber
Trust Nothing. Authenticate Everything.



(*Source: Swift 2012; DigiCert 2019)

… has created a very serious, increasingly dangerous situation when it comes to securing Critical Infrastructure.

The Critical Infrastructure Cybersecurity Dilemma

VIBE Cyber
Trust Nothing. Authenticate Everything.

- UK Critical Infrastructure is under relentless and continual attack, and the “bad guys” are winning.
- 90% of IT Cybersecurity specialists report successful attacks, and 50% of these caused major disruption that led to critical systems downtime
  (source: Ponemon Institute)
- In many cases, organization don’t even know what is connected to the Internet, and what can be accessed by hackers (source: BBC News, 2019)

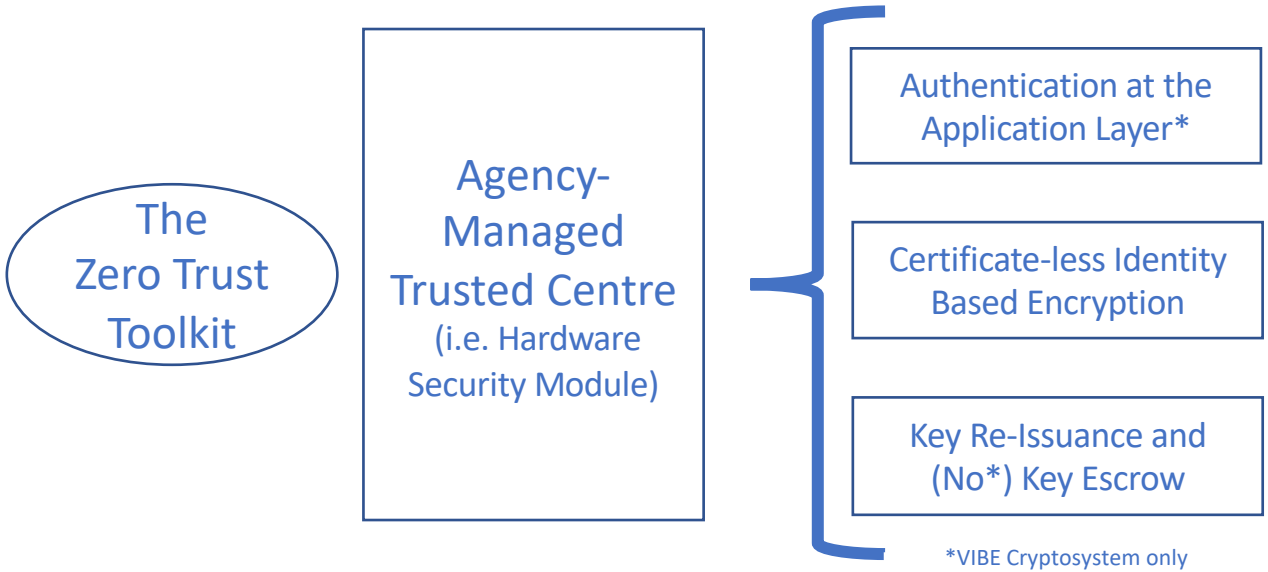
A UK parliamentary committee said late last year that it’s “impossible to protect critical infrastructure from cyber attacks.”

WE RESPECTFULLY DISAGREE

The “Zero Trust” Approach

VIBE Cyber
Trust Nothing. Authenticate Everything.

- Zero Trust is a holistic approach to network security, that is not associated with any one product or solution



“Zero Trust” – applied to IoT

VIBE Cyber
Trust Nothing. Authenticate Everything.

- The Zero Trust network security concept is based on a strict identity-verification process.
- The framework dictates that only authenticated and authorized users and devices can access applications and data, protecting those applications and users from advanced threats on the Internet.

Every “thing,” be it a device, gateway or sensor that is part of critical infrastructure, and every person who accesses it must be REGISTERED and AUTHENTICATED in an Agency-controlled Trusted Centre.

The Zero Trust “Offline” Advantage

VIBE Cyber
Trust Nothing. Authenticate Everything.

Once all devices are registered in the Trusted Centre (TC), the Public Key issuing component (e.g. HSM) can be taken offline, completely eliminating the threat of TC cyberattacks.

All communication among authenticated, registered TC users is peer-to-peer (or TC to TC)

The HSM can be easily returned to online status to accommodate adds and changes.

The Enabling Driver for “Zero Trust”

VIBE Cyber
Trust Nothing. Authenticate Everything.

Identity Based Encryption (IBE)

- Paper by Adi Shamir in 1984 developed the concept of IBE
- First commercial scheme by Boneh & Franklin in 2001
- Since then, IBE has spawned 651 academic research papers, and is a regular topic at the 4 major global Cryptographic Conferences
- IBE is used as primitive in most of public key cryptography schemes (Oblivious Transfer, Designated Verifier Signature, Multi Party Computation,…)

IBE has been recently adopted in the UK

Since 2018, the UK Government is using a variant of the pairing-based scheme (SAKKE) in UK emergency services

Identity Based Encryption and IoT

VIBE Cyber
Trust Nothing. Authenticate Everything.

In its niche market – key management for encrypted email – IBE is an effective crypto scheme. It was not designed for IoT, however, and as such has four inherent weaknesses.

- **IBE cannot viably validate the sender of a message**
  - effectively impossible and highly impractical with the initial IBE schema, given the very high computational requirements and related prohibitive communication costs.
- **IBE is susceptible to Man-in-the-Middle attacks on the Public Parameters**
  - when the public parameters are changed, a common occurrence in a dynamic IBE environment, there is no way of verifying that they haven't been altered, placing the entire IBE system at risk.
- **IBE always imposes Key Escrow**
  - effectively enabling the regeneration of created Private Keys.
- **IBE requires either Master Key or basic Identity change on rekeying/re-issuance of a Private Key**
  - effectively inefficient and highly impractical and in some uses cases even unacceptable

VIBE – Modern IBE Designed for IoT

VIBE Cyber
Trust Nothing. Authenticate Everything.

VIBE (Verifiable Identity Based Encryption) applies recent academic research which yields much greater efficiency in the computation of pairings over elliptic curves than IBE, creating a more secure, very practical public key scheme – ideally suited for IoT.

VIBE Verifies the Sender of a Message
Guarantees messages are decrypted by intended recipient

VIBE Ensures Secure Deployment
Ensures a mechanism to deploy and rekey to already populated nodes

VIBE Eliminates the Need to Protect the Public Parameters
Eliminating risk of MiTM attacks

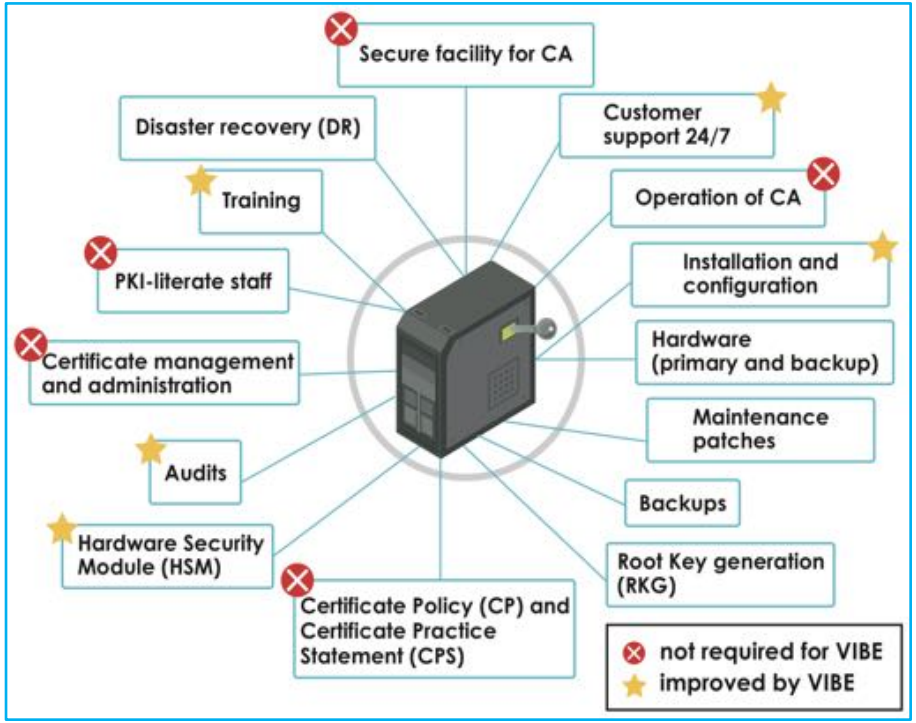
VIBE Eliminates Key-Escrow
Eliminating risk of Privacy Infringements

VIBE Total Cost of Ownership

VIBE Cyber
Trust Nothing. Authenticate Everything.

Compared to PKI, VIBE's reduced communications and infrastructure costs, and ongoing operational improvements yield:

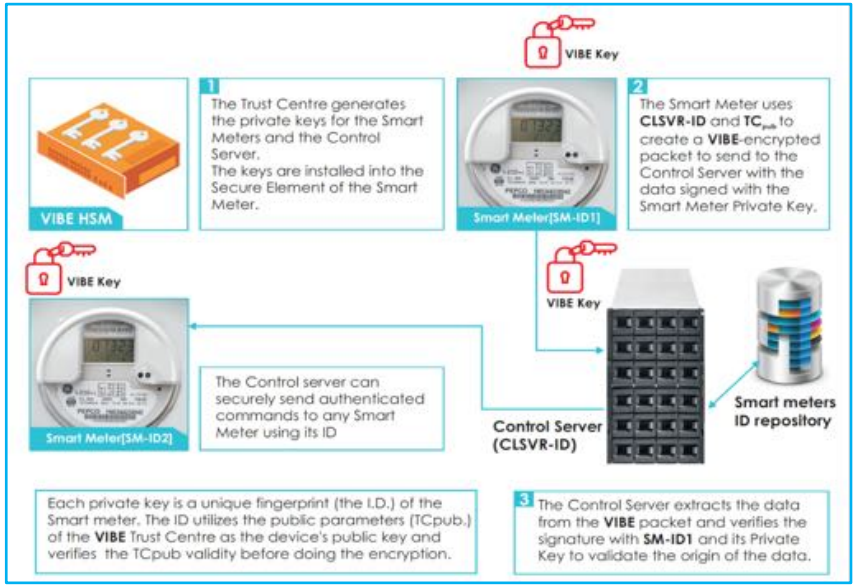
- ✓ 60% savings for one-time expenditures
- ✓ 40% savings on recurring expenses
- ✓ 30% savings on personnel costs



VIBE Use Case – Building Automation

VIBE Cyber
Trust Nothing. Authenticate Everything.

Building Automation Systems (BAS) today rely mainly on PKI, and often fail to establish the safety and privacy framework required for such mission-critical systems (50% are vulnerable to cyberattacks)



A sample setup of a smart meter communication within a BAS environment is shown. The VIBE protected deployment is set up, and then taken offline, effectively eliminating threats from "online" attackers.

Thank You!

VIBE Cybersecurity International LLC

Email info@vibecyber.com
Web www.vibecyber.com

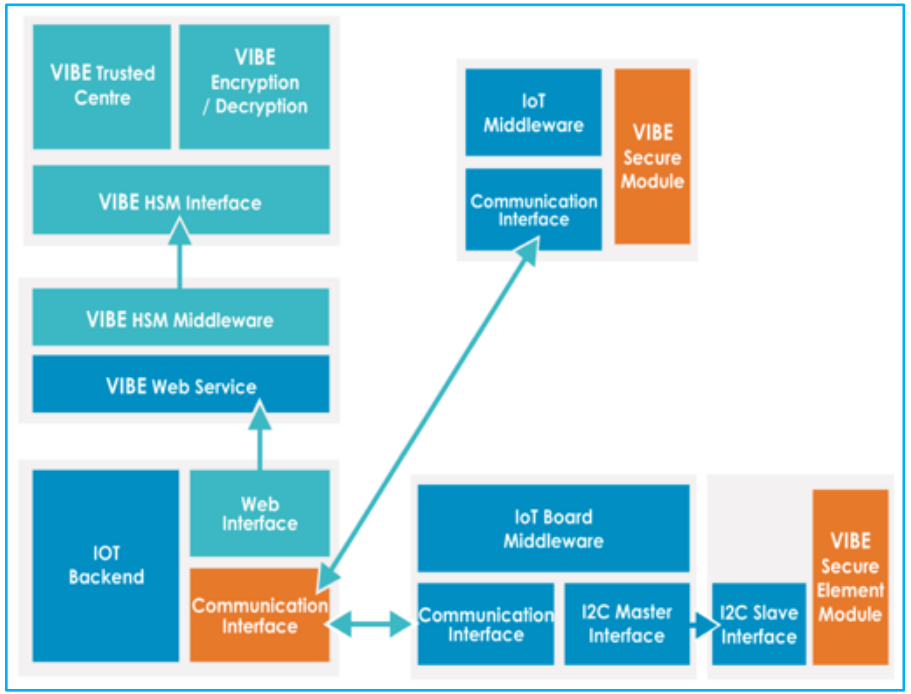
Back Up Slides

VIBE Software Architecture

VIBE Cyber
Trust Nothing. Authenticate Everything.

The software architecture of a VIBE Cryptosystem ensures end-to-end secure communication.

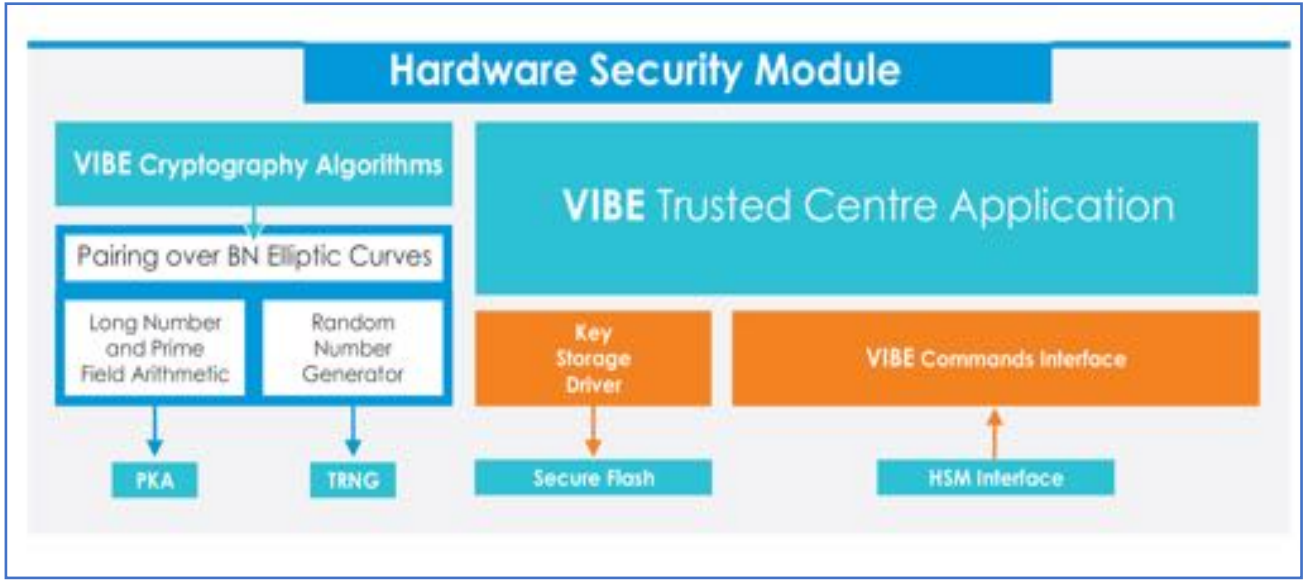
The uniqueness of VIBE is that this superior level of security can also be achieved over a non-secure communication channel.



VIBE Hardware Security Module

VIBE Cyber
Trust Nothing. Authenticate Everything.

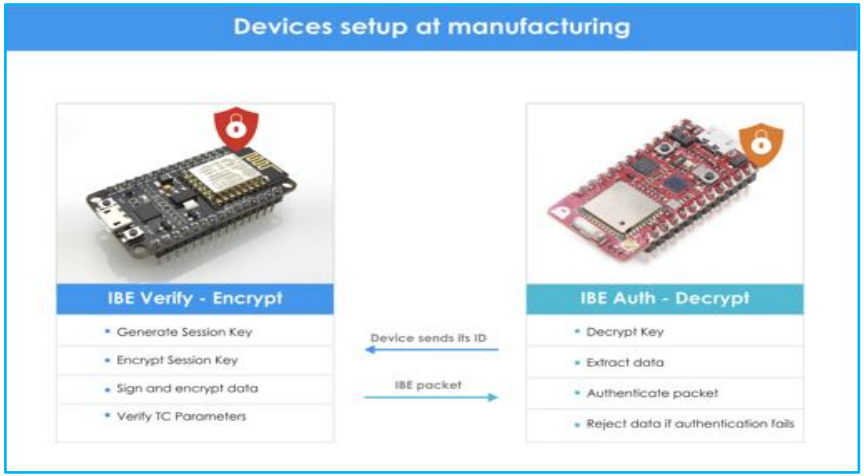
An HSM is a powerful, Trusted Execution Environment which enables high-level security for back-end applications. It is the recommended security device to house the VIBE TC that provides the root of trust in a VIBE-enabled system.



VIBE Message Exchange

VIBE Cyber
Trust Nothing. Authenticate Everything.

The VIBE-enabled communication process is fast, simple, and economical



The VIBE key exchange mechanism is impermeable to a man in the middle attack as the public key is the ID of the device and the TC parameters are verified before the encryption, making the peer-to-peer communication fully authenticated.

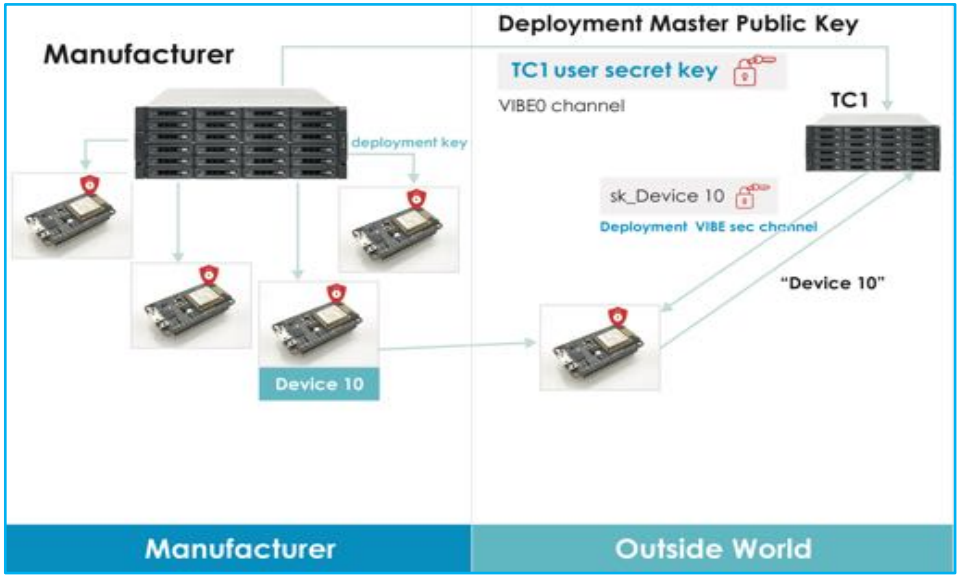
Implementing VIBE

VIBE Cyber
Nothing. Authenticate Everything.

VIBE's certificate-less schema affords its users the opportunity to easily and economically scale to any level on a peer-to-peer basis – including the massive deployment models that characterize IoT.

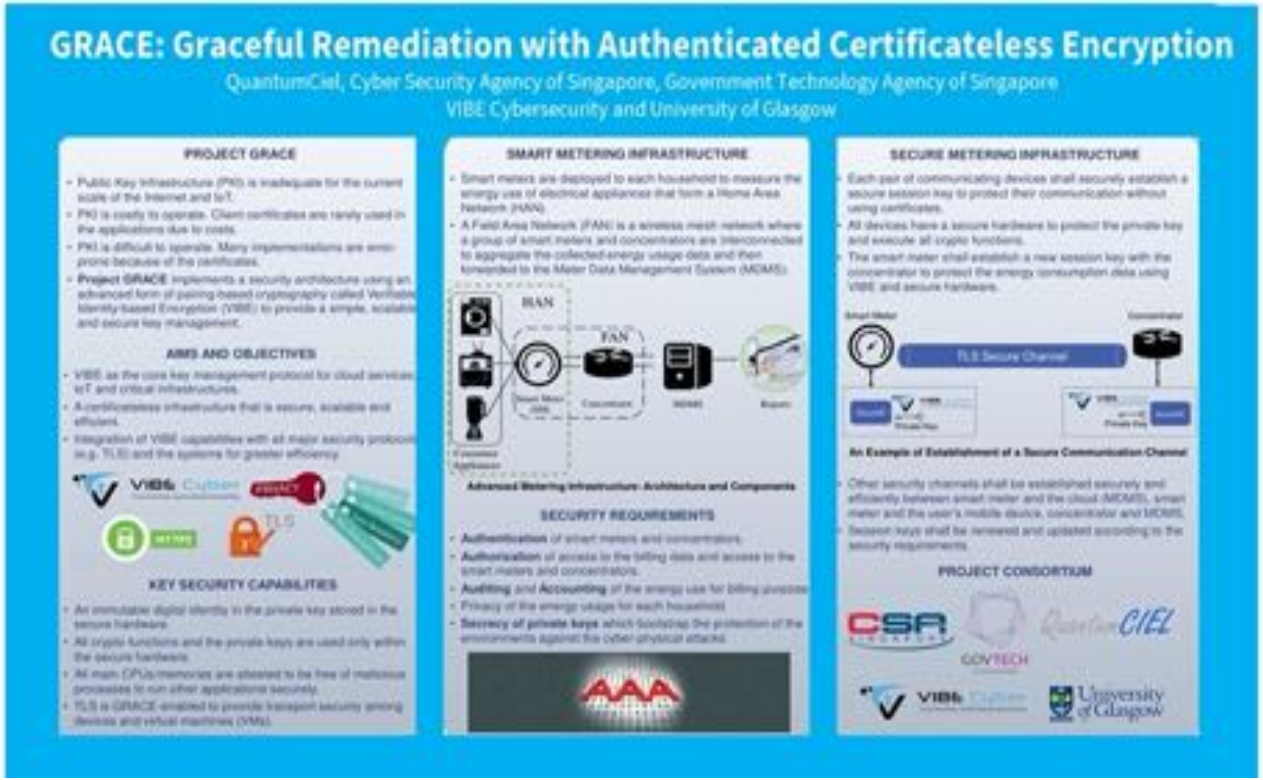
The VIBE deployment model for a manufacturer makes use of different, independent VIBE groups.

Setup keys are deployed during the Trusted Centre registration process.



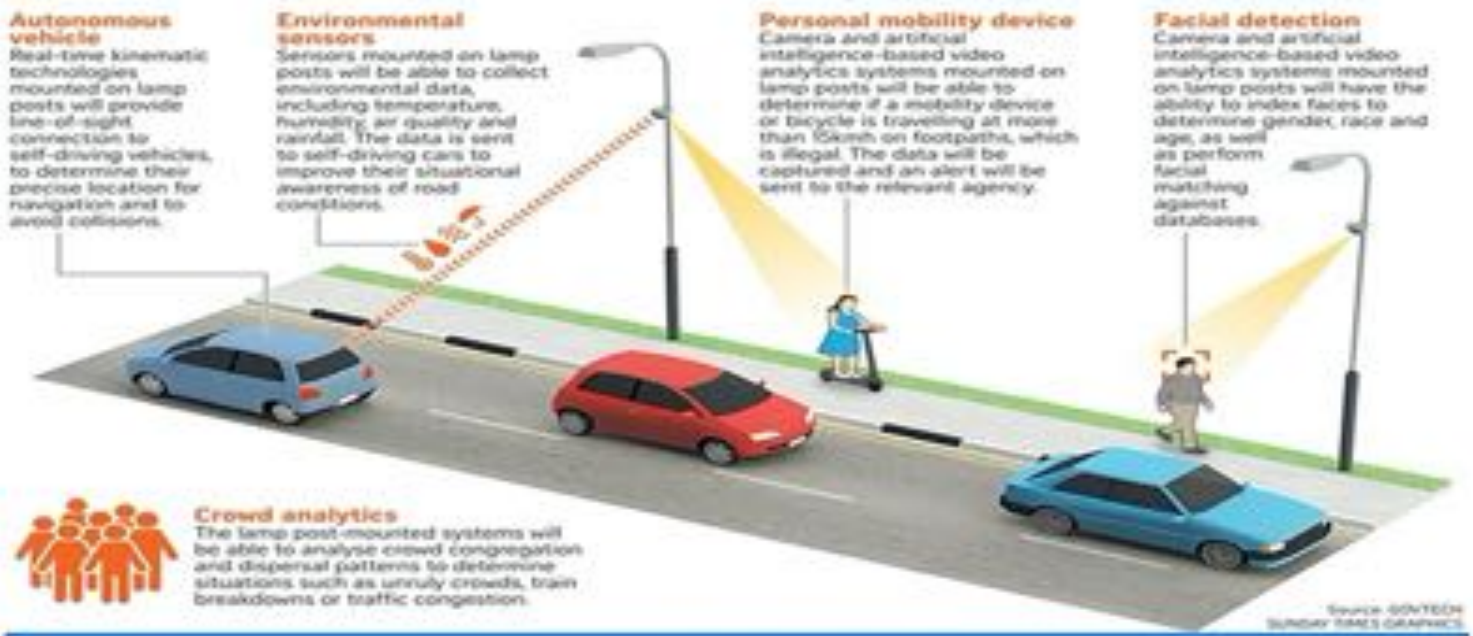
Project GRACE – VIBE is the “ACE” in GRACE

VIBE Cyber
Trust Nothing. Authenticate Everything.



Project GRACE Phase Two: GRACE TLS Technology validation/practical test – Q4 2019

What Smart Lamp Post's Can Do



GRACE TLS replaces PKI with VIBE