



Challenged by IoT Security?

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

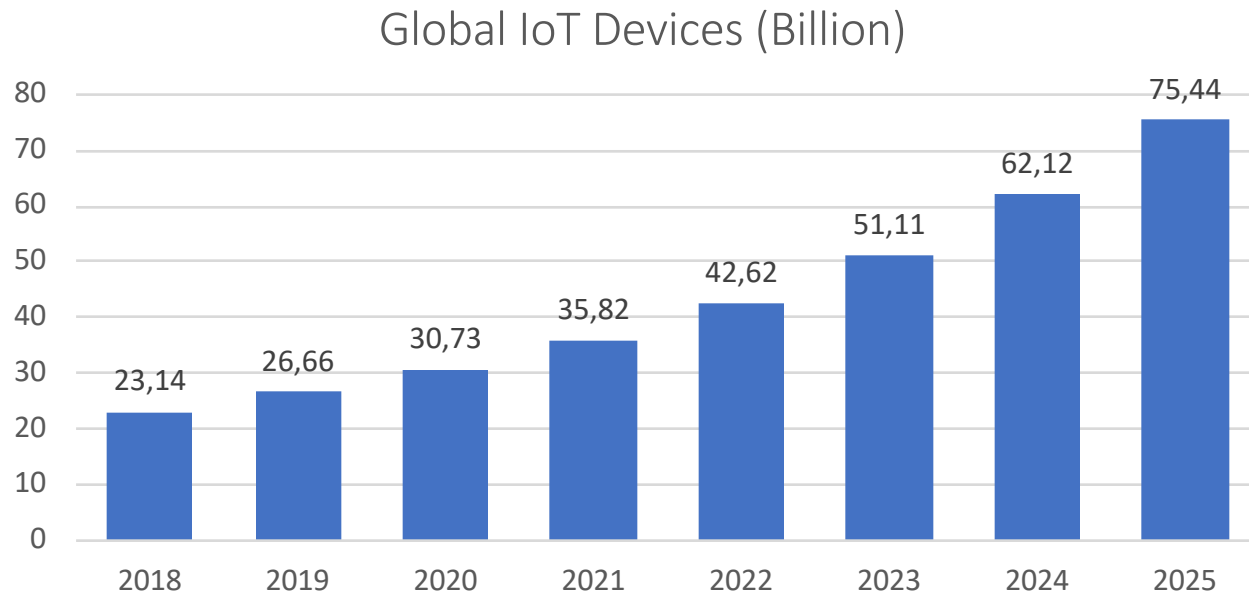
Hisham Lamei

VIBE Cybersecurity International LLC

IoTSF 2019 : 26 November 2019 – London



Setting the Stage for IoT



Source: Statista 2019

Deployed IoT devices projected to be 75.44 billion by 2025.

The IoT Opportunity



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



**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.

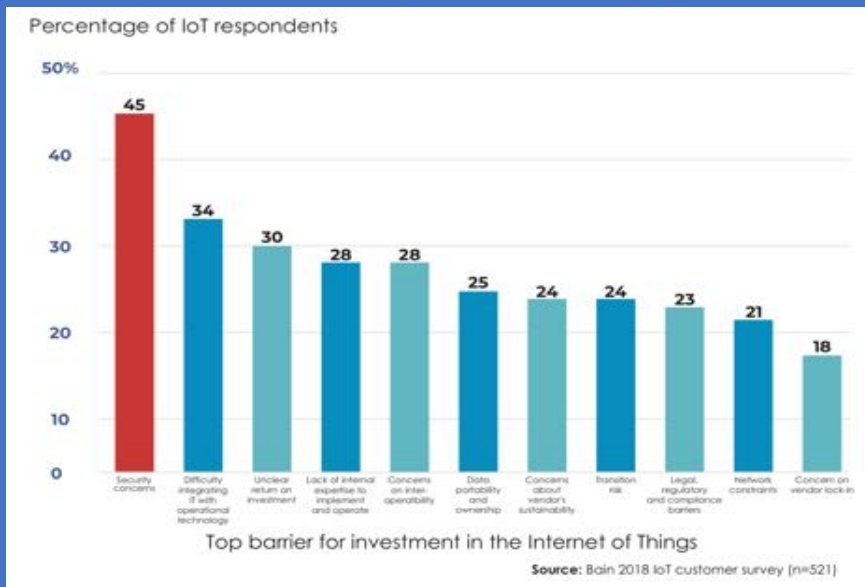
Security – The Critical IoT Barrier

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.



Security is the Leading Barrier to IoT Adoption

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.



Another IoT Adoption Barrier - Scalability



In the Cybersecurity Industry, scalability means the ability to

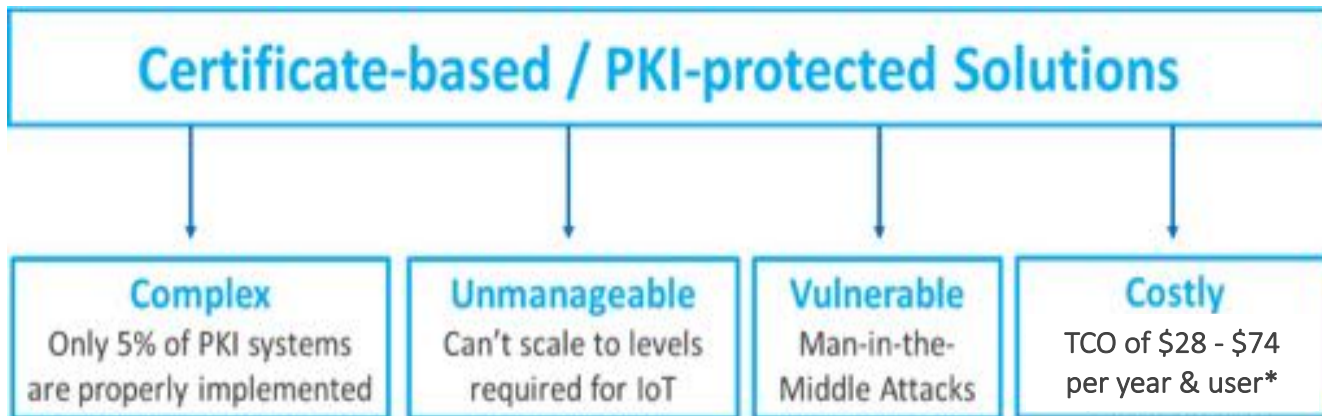
- Seamlessly deploy and manage the rapid growth of devices within a given application, and to do so economically, while adapting to operational requirements

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 ...



(*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



- 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)



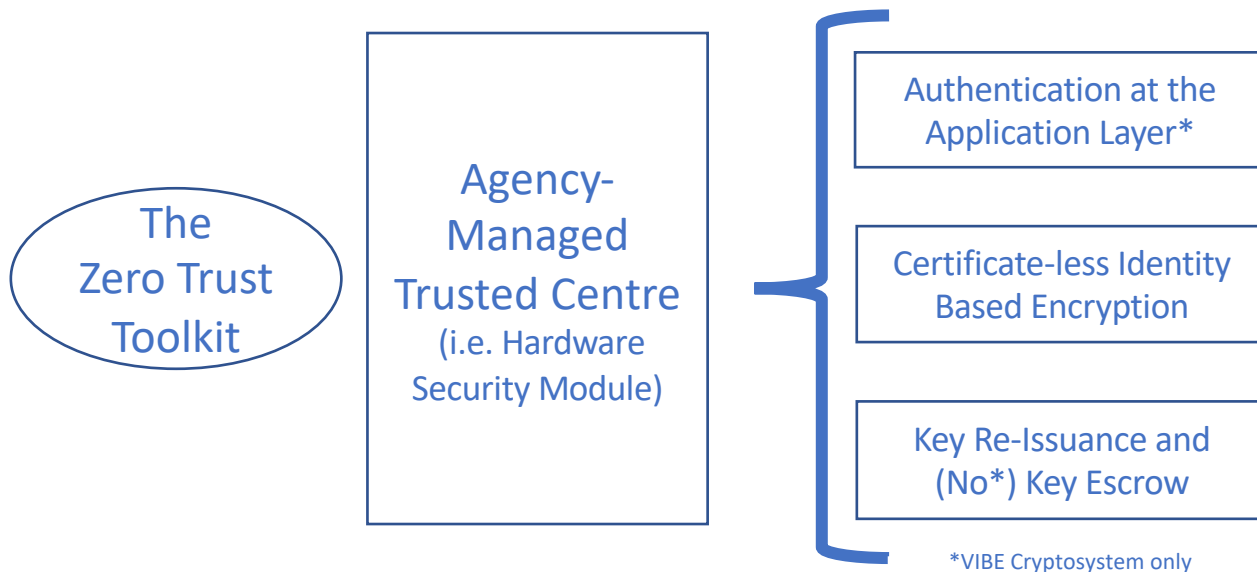
**A UK parliamentary committee said late last year that it’s
“impossible to protect critical infrastructure from cyber attacks.”**

WE RESPECTFULLY DISAGREE

The “Zero Trust” Approach



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



“Zero Trust” – applied to IoT

- 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



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”



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

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 (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

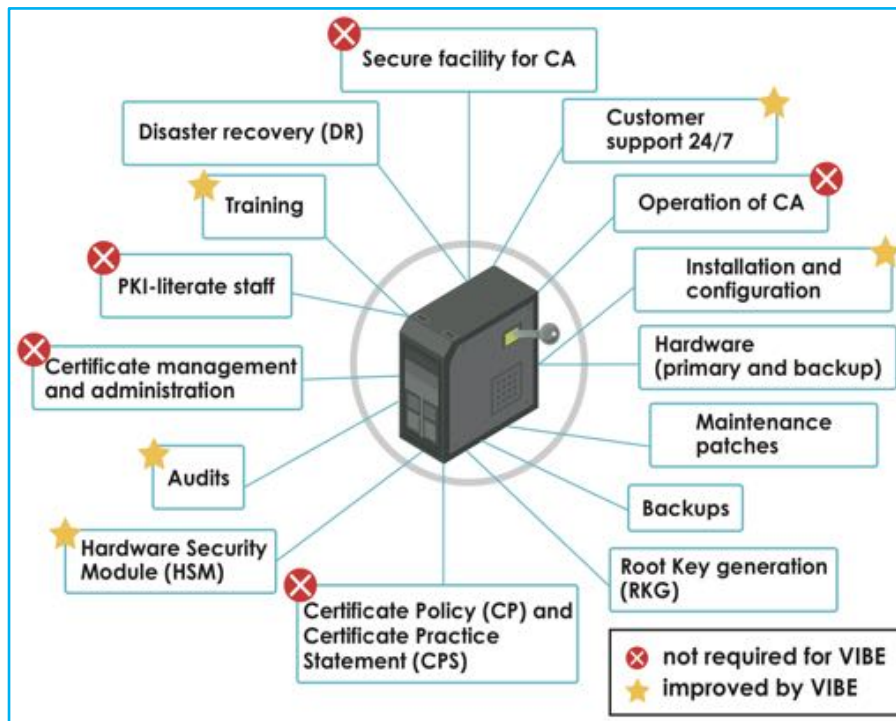
VIBE Eliminates Key-Escrow

Eliminating risk of Privacy Infringements

VIBE Total Cost of Ownership

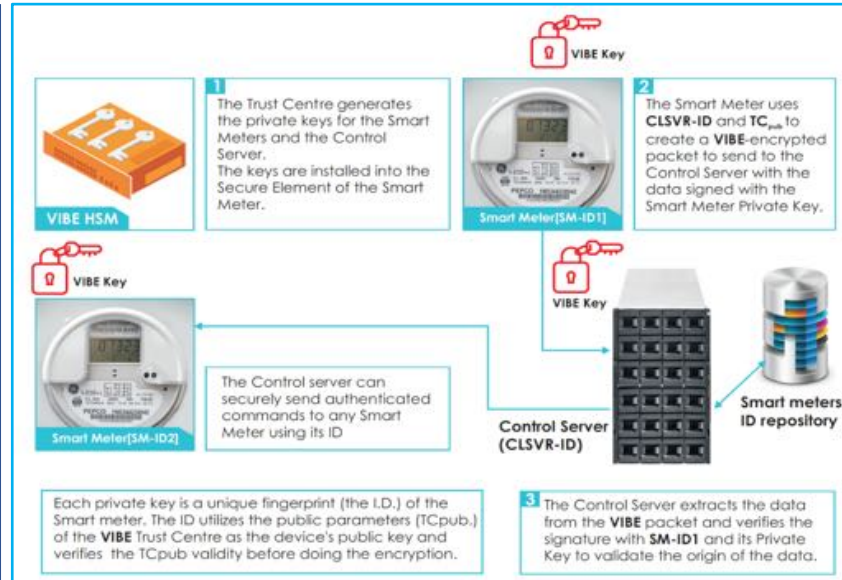
Compared to PKI,
VIBE's reduced
communications and
infrastructure costs, and
ongoing operational
improvements yield:

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



VIBE Use Case – Building Automation

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



The background of the slide features a large, glowing blue globe on the left side, composed of a grid of dots. To the right of the globe, there is a series of hexagonal icons arranged in a grid-like pattern. These icons represent various concepts such as a factory, a magnifying glass, a person, a cloud, a bar chart, and a target. The entire background is set against a dark blue gradient with a diagonal split between a lighter blue and a darker blue.

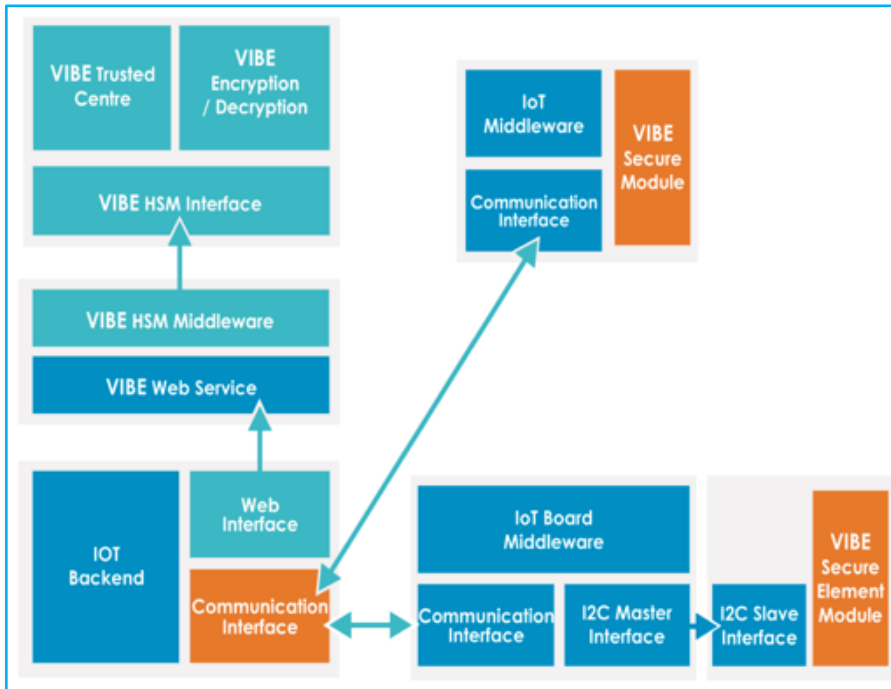
 Back Up Slides



VIBE Software Architecture

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

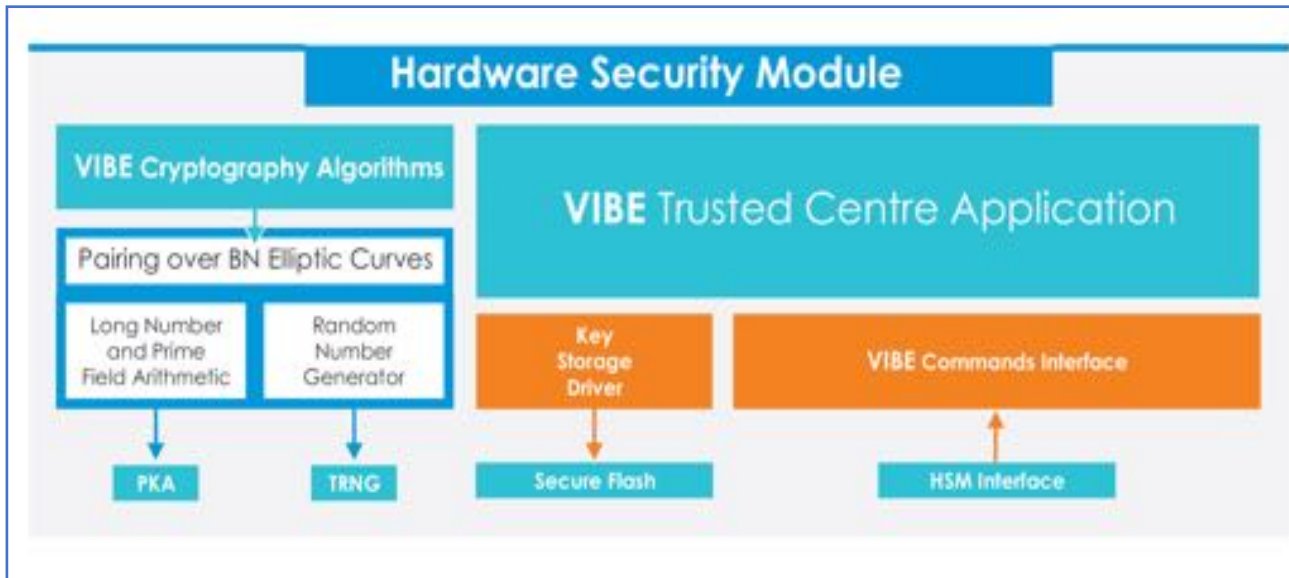
The uniqueness of VIBE is that this superior level of security can also be achieved over a non-secure communication channel.



VIBE Hardware Security Module

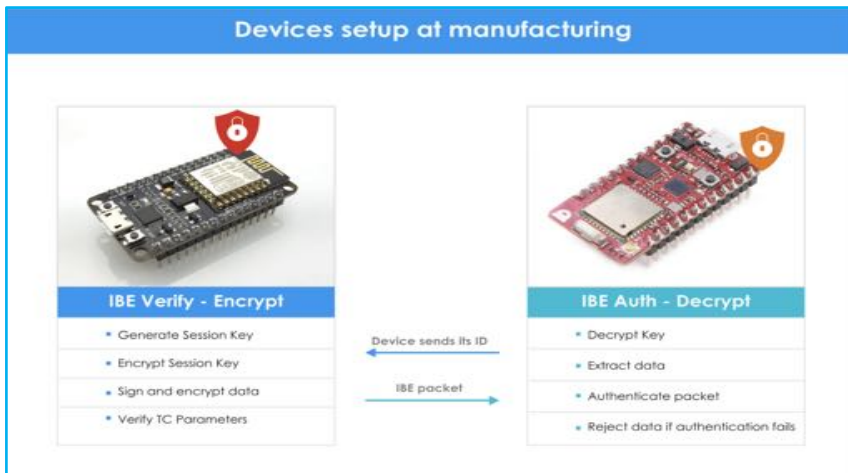


An HSM is a powerful, Trusted Execution Environment which enables high-level security for back-end applications. It is the recommended security device to house the VIBE TC that provides the root of trust in a VIBE-enabled system.



VIBE Message Exchange

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



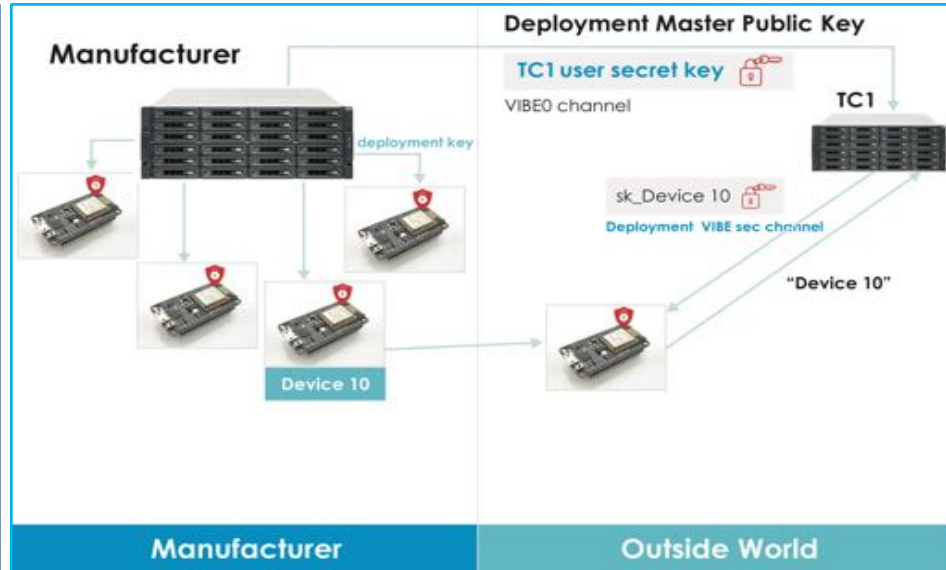
The VIBE key exchange mechanism is impermeable to a man in the middle attack as the public key is the ID of the device and the TC parameters are verified before the encryption, making the peer-to-peer communication fully authenticated.

Implementing VIBE

VIBE'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

GRACE: Graceful Remediation with Authenticated Certificateless Encryption


QuantumCiel, Cyber Security Agency of Singapore, Government Technology Agency of Singapore
VIBE Cybersecurity and University of Glasgow

PROJECT GRACE

- Public Key Infrastructure (PKI) is inadequate for the current scale of the Internet and IoT.
- PKI is costly to operate. Client certificates are rarely used in the applications due to costs.
- PKI is difficult to operate. Many implementations are error-prone because of the certificates.
- Project GRACE** implements a security architecture using an advanced form of pairing-based cryptography called Verifiable Identity-based Encryption (VIBE) to provide a simple, scalable and secure key management.

AIMS AND OBJECTIVES

- VIBE as the core key management protocol for cloud services, IoT and critical infrastructures.
- A certificateless infrastructure that is secure, scalable and efficient.
- Integration of VIBE capabilities with all major security protocols (e.g. TLS) and the systems for greater efficiency.




KEY SECURITY CAPABILITIES

- An immutable digital identity in the private key stored in the secure hardware.
- All crypto functions and the private keys are used only within the secure hardware.
- All main CPUs/memorys are protected to be free of malicious processes to run other applications securely.
- TLS is GRACE-enabled to provide transport security among devices and virtual machines (VMs).

SMART METERING INFRASTRUCTURE


- Smart meters are deployed to each household to measure the energy use of electrical appliances that form a Home Area Network (HAN).
- A Field Area Network (FAN) is a wireless mesh network where a group of smart meters and concentrators are interconnected to aggregate the collected energy usage data and then forward to the Meter Data Management System (MDMS).



Advanced Metering Infrastructure Architecture and Components


SECURITY REQUIREMENTS

- Authentication of smart meters and concentrators.
- Authorization of access to the billing data and access to the smart meters and concentrators.
- Auditing and Accounting of the energy use for billing purposes.
- Privacy of the energy usage for each household.
- Secrecy of private keys which facilitates the protection of the environments against the cyber physical attacks.



SECURE METERING INFRASTRUCTURE


- Each pair of communicating devices shall securely establish a secure session key to protect their communication without using certificates.
- All devices have a secure hardware to protect the private key and execute all crypto functions.
- The smart meter shall establish a new session key with the concentrator to protect the energy consumption data using VIBE and secure hardware.



An Example of Establishment of a Secure Communication Channel

- Other security channels shall be established securely and efficiently between smart meter and the cloud MDMS, smart meter and the user's mobile device, concentrator and MDMS.
- Session keys shall be renewed and updated according to the security requirements.

PROJECT CONSORTIUM



What Smart Lamp Post's Can Do

Autonomous vehicle

Real-time kinematic technologies mounted on lamp posts will provide line-of-sight connection to self-driving vehicles, to determine their precise location for navigation and to avoid collisions.

Environmental sensors

Sensors mounted on lamp posts will be able to collect environmental data, including temperature, humidity, air quality and rainfall. The data is sent to self-driving cars to improve their situational awareness of road conditions.

Personal mobility device

Camera and artificial intelligence-based video analytics systems mounted on lamp posts will be able to determine if a mobility device or bicycle is travelling at more than 15km/h on footpaths, which is illegal. The data will be captured and an alert will be sent to the relevant agency.

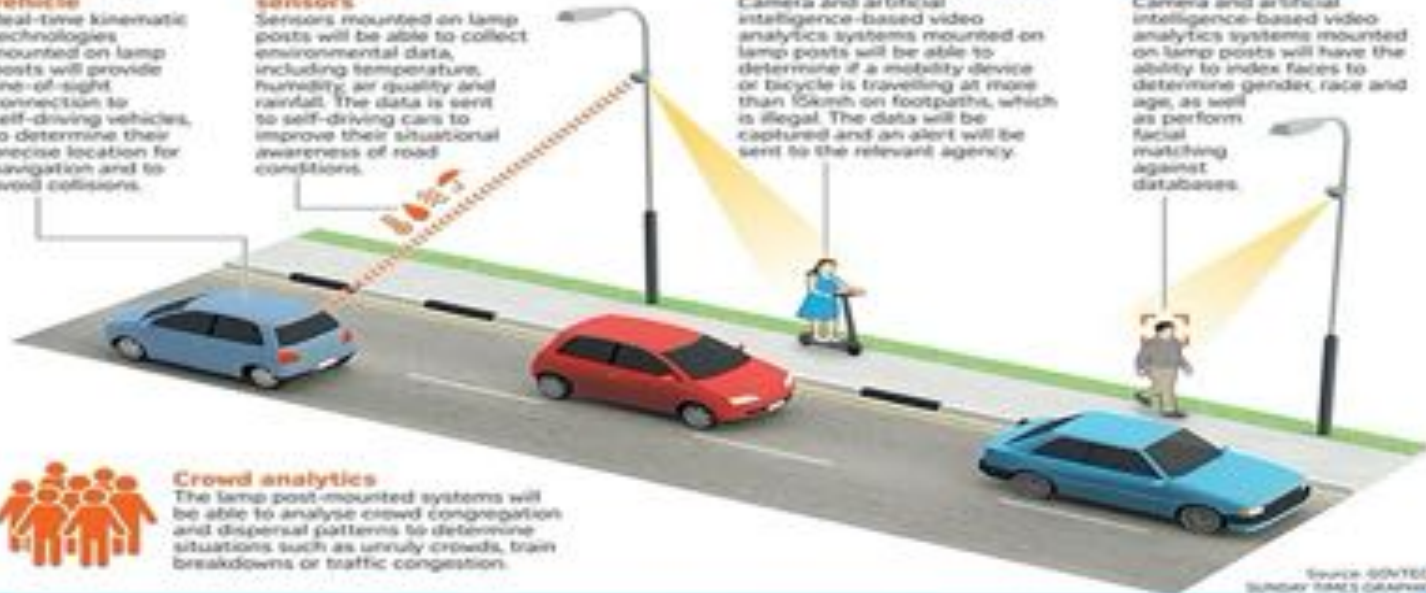
Facial detection

Camera and artificial intelligence-based video analytics systems mounted on lamp posts will have the ability to index faces to determine gender, race and age, as well as perform facial matching against databases.



Crowd analytics

The lamp post-mounted systems will be able to analyse crowd congregation and dispersal patterns to determine situations such as unruly crowds, train breakdowns or traffic congestion.



Source: SCHTECH
BUILDING TRAILS GRAPHICS

GRACE TLS replaces PKI with VIBE