

# SECUREMAG

SECUREMETRIC TECHNOLOGY GROUP

FORMULA FOR STRONG DIGITAL SECURITY

**GETTING LOST  
IN THE  
CLOUD?**

PAGE 16-17 INFOGRAPHIC

**PKI CONFERENCE 2015**  
Kuala Lumpur | 9-10 June | Hotel Royale Chulan

**ASEAN FIC**  
ASEAN Financial Institution Conference

PAGE 12-15

**PAGE 28-31**

**2015**

**Invest In The Solution  
Creation Process As  
The Foundation To  
Project Success**

by YuWin PAGE 10-11



**{ ADAPTIVE  
INTELLIGENCE }**

**CENTAGATE®**  
Centralized Authentication Gateway

## A NEW GENERATION SECURED UNIFIED AUTHENTICATION GATEWAY WITH ADAPTIVE INTELLIGENCE

**CENTAGATE (Centralized Authentication Gateway)** Adaptive Intelligence works based on the combination of user's previous login data and rules defined by the system administrators. The more the user logs-in using the system, the better CENTAGATE will be able to predict the threat level of the authentication attempt.



# CENTRALIZED AUTHENTICATION GATEWAY

Next Generation Secured & Unified

Authentication Gateway with Adaptive Intelligence

CENTAGATE is a gateway that provides various kind of authentication services for corporate web or a client / server applications. One of the main features of CENTAGATE is the Adaptive Intelligence. It implements a risk and rule based approach with additional Identity assurance.

## Why does CENTAGATE have multi-Factor, multi-Step, multi-Layer with Adaptive Intelligence features ?

The answer is simple – we need to detect and defend various attack methods used by Cyber-Criminals. Cyber-Criminal deploys complex and multiple attack methods to gain access into user’s private information and / or device information.



Threat Name	Attack Description	Resolution
Man-in-the-middle Attack	Man-in-the-middle attack is an attack that intercepts the communication between two systems by acting as a proxy. It is able to read, insert, and modify data in the intercepted communication. Man-in-the-middle attack is very effective because of the nature of the HTTP protocol and data transfer which are all ASCII based. It also can be done over HTTPS protocol by establishing 2 independent SSL sessions over both client and server connection.	End-to-end message encryption using hardware PKI or PKI mutual authentication will ensure that data are not transmitted in clear text and only the intended party are able to decipher the message using the recipient’s Private Key. Sender will use recipient’s Public Key to encrypt the message.
Man-in-the-Browser attack/ Browser Poisoning	Man-in-the-browser (MITB, MitB, MIB, MiB) is a security attack related to Man-in-the-middle attack. Man-in-the-browser uses trojan horse to intercept and manipulate calls between main application’s executable (web browser) and the browser security mechanisms or library. The main objective of this attack is to cause financial fraud by manipulating transactions of internet banking systems, even two-factor authentication has been used.	If the computer is infected with MITB malware code, the most effective countermeasure is to use another channel or “Out of band” transaction verification. The transaction verification should be done such as mobile device. Call or SMS transaction verification are common but the verification via mobile application is gaining acceptance.

Threat Name	Attack Description	Resolution
<p>Man-in-the-OS/ Mobile Attack</p>	<p>Man-in-the-mobile are allows attacker to leverage malware placed on the mobile devices to get around the verification system that sends codes via SMS to user's phone for the confirmation. ZitMo is a mobile malware that works similar to proxy function that all incoming SMSes in mobile phone. This attack can completely bypass Out of Band transaction verification.</p>	<p>Secure Mobile Security Token in the mobile such as Device, Signing and Encryption Keys that bind to an authentication server will help to detect such attacks the moment the uses different environment (e.g. different IP, location, device). Together with Adaptive Intelligence, we are able to use user's behavior to protect from future attacks.</p>
<p>Replay Attack</p>	<p>Replay attack (also known as playback attack) is an attack where the attacker captures the valid messages and re-uses the messages at a later time to trick the cryptography protocol. The captured messages are sufficient enough to gain access to the network even though the messages may be encrypted, and the attacker may not know what is the actual key or passwords.</p>	<p>A multi-factor authentication such as SMS / Mobile OTP and PKI (with unique transaction ID, to prevent multiple usage) will prevent such attacks.</p>
<p>Android SMS Sniffer Trojan Attack</p>	<p>The objective of many financially motivated malicious mobile apps is to steal the out-of-band passwords organizations use to provide an additional layer of user authentication. A typical example is a one-time password (or passcode) that is sent by the bank to the users via SMS which later on needs to be entered to confirm high-risk online transactions such as wire transfers. Fraudsters and cybercriminals have developed SMS sniffers (or SMS hijacking apps) that are designed to work with Trojans installed on PCs. The SMS sniffer intercepts the SMS messages and steals the out-of-band password to enable fraudulent transfers from the victim's bank account.</p>	<p>Secure Mobile Security Token in the mobile such as Device, Signing and Encryption Keys that bind to an authentication server will help to detect such attacks the moment the user a different environment (e.g. different IP, location, device). Together with Adaptive Intelligence, we are able to use user's behavior to protect from future attacks.</p>
<p>IOS Malicious Profiles</p>	<p>IOS profile / mobile config file is use by mobile applications to configure key system level settings of IOS device such as WI-FI, VPN, Email, and APN settings. Mobile config files are usually used for constructive needs and thus provide a lot of value, these capabilities are able to be used by malicious attacker to circumvent Apple's security model and perform significant damage to their victims. A malicious profile can be used to remote control mobile device, monitor and manipulate user activity and hijack user session.</p>	<p>Secure Mobile Security Token in the mobile such as Device, Signing and Encryption Keys that bind to an authentication server will help to detect such attacks the moment the user a different environment (e.g. different IP, location, device). Together with Adaptive Intelligence, we are able to use user's behavior to protect from future attacks. Similarly, deploying Mobile PKI will also prevent future attacks.</p>
<p>Phishing Attack</p>	<p>Phishing is an activity to trick people into divulging sensitive information such as username, password, and credit card accounts by pretending to be a trustworthy entity in an electronic communication. It is basically a fraud, whereby the potential victims are contacted via email, instant messaging, text message or phone.</p>	<p>There are multiple solutions to protect against phishing attacks by implementing PKI, Mobile PKI, OTP Challenge Response and Secure Mobile Security Token.</p>
<p>Pharming Attack</p>	<p>Pharming is a form of online fraud that is very similar to Phishing. Pharming will redirect a website to another fake website by changing the host file in the victim's computer or by exploiting the DNS server vulnerability. Pharming requires an unprotected access to target a computer such as home computer rather than a corporate business server.</p>	<p>There are multiple solutions to protect against pharming attacks by implementing PKI, Mobile PKI, OTP Challenge Response and Secure Mobile Security Token.</p>

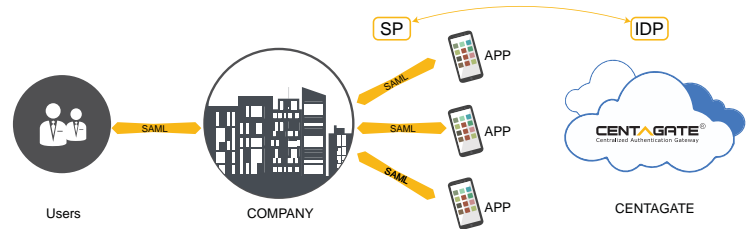
CENTAGATE has 2 features, which are:

**1** Centralized Identity Management

**2** Centralized Device Management

**1** Centralized Identity Management

Supports open-standard data format by exchanging authentication and authorization data between parties through SAML (Security Assertion Markup Language) based SSO (Single Sign-On). Widely deployed in cloud-based applications such as Microsoft Office 365, Sharepoint and Google Applications.



**Benefits of using CENTAGATE's SAML SSO:**

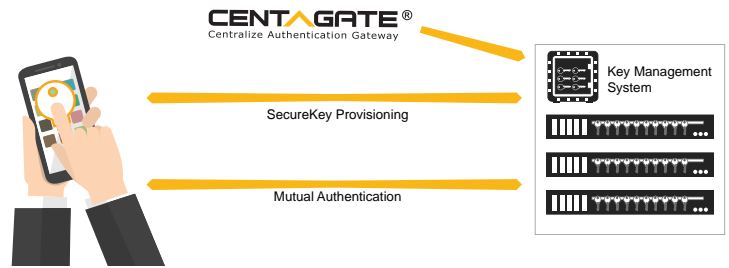
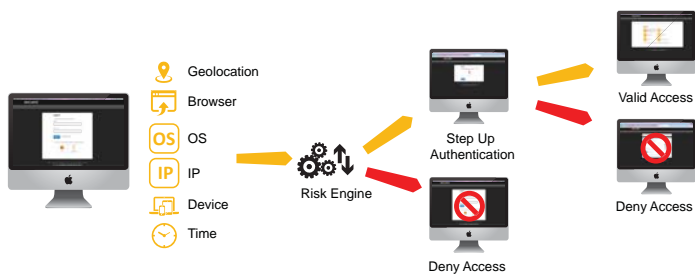
- **Centralized User Management for the Administrator**
- **Convenience for users, a single sign-on to multiple applications**
- **Ease of integration for developers as it removes the complexity of dealing with authentication and authorization from application code**
- **Provides encryption to protect authentication and authorization among all parties. Data exchange between SP (Service Provider) and IdP (Identity Provider) is not shared with user.**
- **IdP (Identity Provider) can be connected to retrieve user information via ADFS (Active Directory Federated Services) or LDAP (Lightweight Directory Access Protocol) Farms**
- **Supported by many popular web browsers such as Internet Explorer, Firefox and Chrome**
- **Multi-Factor Authentication options for user to select (the most convenient)**
  - i. What User Knows – Username and Password
  - ii. What User Have – Hardware Tokens or Software / Mobile Tokens / OTP / Mobile PKI / Mobile Cert
  - iii. What User Is – Biometric scanner such as finger, iris or voice



- **Strong Protection**  
CENTAGATE deploys military grade encryption solution such as support for Hardware Security Module (HSM) with high level of security protection and international standard certifications. Security keys are stored in HSM. Mobile apps and user accounts are used to generate secure key for mutual authentication.

● **Adaptive Intelligence Authentication**

Adaptive Authentication is a comprehensive authentication and fraud detection platform. It is designed to measure the risk associated with a user's login and post-login activities by evaluating a variety of risk indicators such as Geo-location, Operating System, Browser Type, IP Address, Device and Time. Using a risk and rules based approach, the system then requires additional identity assurance, such as out-of-band authentication, for scenarios that are high risk and violate a policy.

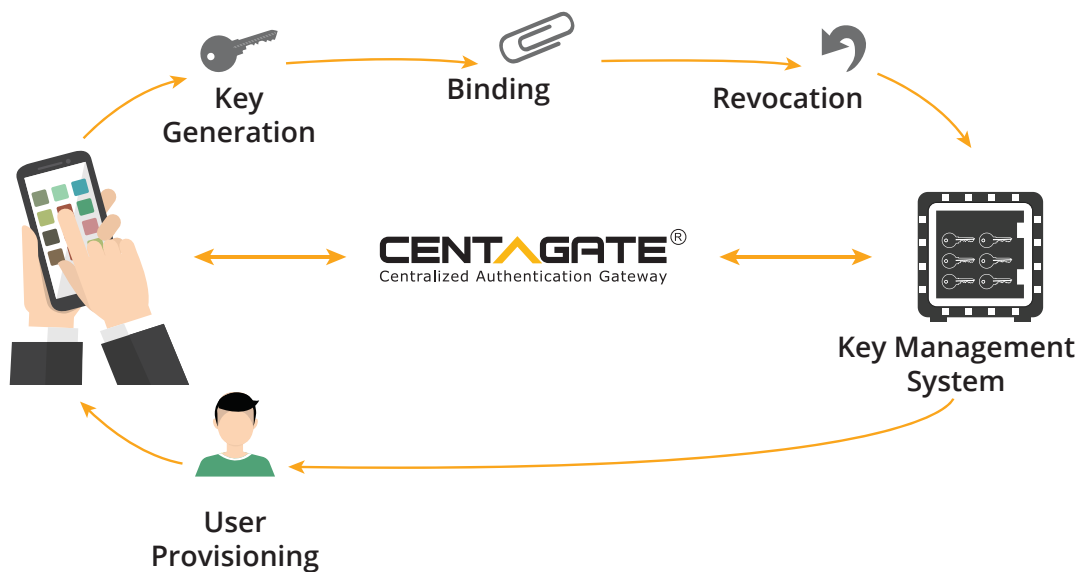


● **Adaptive Intelligence Authentication that Detects & Defends Against Attacks**

The essential part is the risk engine, which detects the threats on every authentication request. A request from the authentic user credentials and its attributes results to a lower risk thus logon access is permitted. Whenever the risk engine detects a request from non-genuine origin by an attacker, a validation of its strange / unusual login attributes against user's transaction history will result to failure, thus original user credentials are defended by this solution.

● **Reporting and Notification**

Real time fraud detection response against attacks. With its' active watch, it will continuously checks for remote attack. Any suspicions attacks are detected and a real-time notification are sent to registered recipients and administrations



**2 Centralized Device Management**

CENTAGATE provides the capability to manage people's devices and access to Web or Mobile Apps, to achieve better security efficiently, centrally.

● **Secure and Flexible BYOD solution**

BYOD or Bring Your Own Device offers flexible option for end user to utilize their own devices as security tokens. Currently

supports Android and iOS.

● **Security Does Matter**

In mobile platforms (BYOD), not all authentication solutions offer high security to ensure user credentials are protected. In CENTAGATE, user information is processed and secured by using our advanced tokenization technology. Security keys are generated and bound with the device. Key life-cycle will cover its revocation for disposal.



**CRYPTOMATHIC**

www.cryptomathic.com

## ACHIEVING CRYPTOGRAPHIC KEY MANAGEMENT COMPLIANCE

# THE IMPORTANCE OF KEY MANAGEMENT COMPLIANCE

### ORGANIZATIONS

are facing various challenges during implementation of cryptography on both new and legacy systems. Improper key management can lead to key leakage, where an attacker obtains the key and recovers the sensitive information from the encrypted data, which can lead to significant financial losses.

Regardless of which system or solution is used, the cryptographic keys will always need to be managed using secure processes. Ensuring and being able to demonstrate that keys are managed securely is essentially what key management compliance is all about.

Traditionally end-to-end lifecycle key management was, and still is, achieved through inefficient paper based procedures and highly resource intensive tasks performed by 4 or 5 employees, but this inefficient process can lead to human errors, high operational costs and difficulties in demonstrating compliance to auditors. Streamlining and automating processes help to eliminate human error, which is a real threat since humans are prone to making mistakes.

Key management compliance relies heavily on secure design, which will not work properly, and as intended, if it can be

The two most important factors to ensure compliance are to:

01

Understand what is needed to meet the minimum requirements

02

Implement techniques that effectively enforce these rules for all environments and processes within scope

### Security Compliance Requirements in Key Management

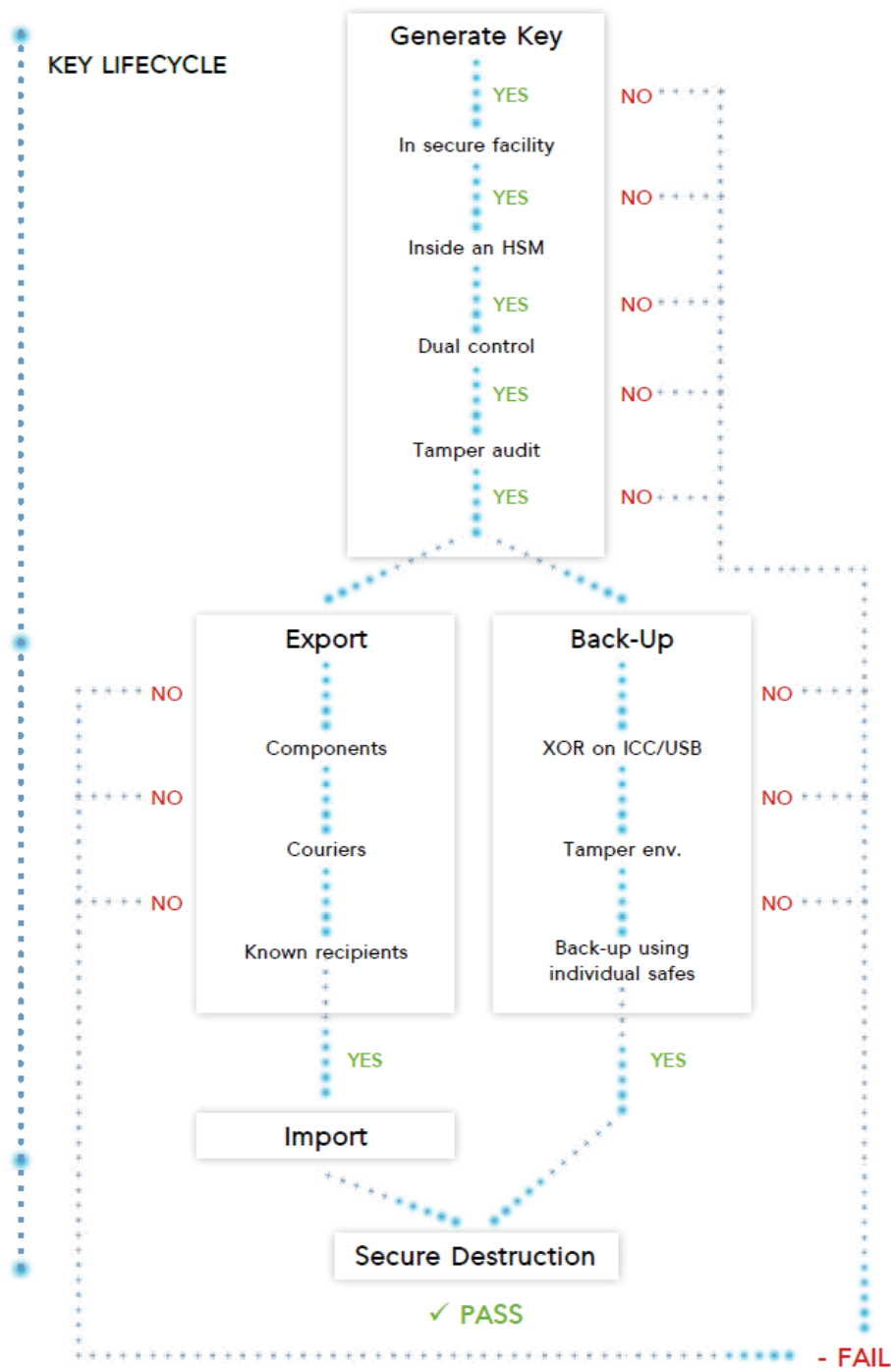
One of the best practices for key management is the documentation of standards-based compliance requirements. It aims at increasing security and is written based on both theoretical speculations on how to counter unwanted activities and also on practical experiences.

Most key management compliance documentation will include requirements such as:

- + Updating keys on predetermined regular intervals
- + Splitting knowledge: Split secrets between multiple persons
- + Logging all activities
- + Ensure keys are never seen in the clear
- + Implementing dual control for access to sensitive information or systems: Grant access only on a need-to basis after approval from a second authorized person
- + Keys must be generated and stored in a tamper resistant environment

misused or incorrectly implemented. Such a list can be very long, very detailed and technical. In summary, compliance can be a major hassle and is therefore an issue which organizations must deal with in the most practical way possible.

Ensuring compliance through centralized and automated crypto operations is considered to be much easier. Below is an example of the key management steps taken during the life cycle of a key in order to pass audits and achieve compliance.



Automating operations eliminates the time-demanding manual key management procedures, since automation can be made for key import or export where systems can exchange keys electronically via a push-pull protocol. Controlling everything centrally is the most simple and efficient way to manage keys and enables compliance auditing to be done in one place.

Cryptomathic's CKMS (Crypto Key Management System) provides a centralized and automated solution which ensures compliance and improves security workflow. Centralized controls allow the business to restrict access to cryptographic functions and enforce policies on key length, rotation, mode of operation and so on. These features help in meeting regulations, industry guidelines and controls.

Compliance is highly dependent on industry so it is important to determine which compliance authorities that are relevant to key management of each individual business. It is always worth to keep in mind that compliance offers a means to controlling risk by highlighting and subsequently minimizing it significantly, even if compliance is not a legal requirement of direct business obligation.

In the light of severity of compliance failure not all compliance authorities are equal. Some attract more serious consequences upon failure to comply, some mean you don't get to play in the security game at all. Having the right systems, processes and knowhow in place is 'key' to obtaining compliance.



## Why Key Management

The Key Management System (KMS) uses a client-server based architecture, with shared HSMs, to provide a centralized key management solution. The system is accessed by operators using desktop computers equipped with secure PIN pads for key component entry. An extremely flexible 'key-push' protocol allows the KMS server to securely connect with practically any secure host system that supports exchange of cryptographic keys.

**Key Advantages**

- Streamline Processes
- Cost Saving – Eliminate Custodians
- Avoid Human Error
- Centrally Managed Upgrades HSM
- Fewer HSMs



For any enquiries on key management product, please contact us at 03-8996 8225 or visit [www.securemetric.com](http://www.securemetric.com)



**utimaco**<sup>®</sup>

hsm.utimaco.com/en

## WHY ENCRYPTION FALLS SHORT, 5 QUESTIONS AUTOMOTIVE DESIGNERS SHOULD BE ASKING ABOUT HACKING

**BY** 2020, three quarters of all cars shipped globally will be built with internet-connection hardware. In the average modern car, more than 80 microcomputers communicate internally to control everything from the stereo to steering wheel, and all those internally connected devices interface with the outside world via Wi-Fi or mobile telephony. But when the car turns into the “Internet on Wheels,” how do we keep it safe from crashes, hackers and privacy breaches?

Risks associated with rapidly growing connectivity include unauthorized access and malicious control. Just recently, white-hat hackers proved how they could remotely commandeer a Jeep Cherokee to come to a dead halt, blast the music and max the air-conditioning. Though the means of securing any connected device boils down to the same core technology solution, the threat of a hacked car becomes far more severe and complex as we trust the integrity of these connections with our lives.

One of the main benefits of the connected car is the very fact that it enables over-the-air (OTA) updates. With OTA, mandatory updates can be loaded remotely into the vehicles’ systems without requiring costly recalls and unpleasant visits at the dealership for the customer. On the flip side, this capability adds another attack surface. Remote software updates require a process of verification to

identify and block communication commands before they find their way into the vehicle system.

### Securing Connected Devices, Why We Need To Go Beyond Encryption

Securing connections and providing authentication as well as non-repudiation in IoT is a highly complex and multifaceted challenge that the embedded industry is already taking steps to outline and define. The same security challenges that apply to connected devices in general also apply to the connected car. A typical go-to answer is encryption: encrypt everything and you’ll be secure. In the case of securing commands and communication in the connected car, however, encryption won’t help. How do we secure over-the-air updates and critical in-car communications like steering, brakes, airbags and tires, as well as non-critical ones like entertainment and climate control?

Encrypting data means encoding information in such a way that only authorized parties can read it. In IoT, the critical security element consists of validating the communication commands between different and multiple connected components, i.e. the moment when the device unlocks the encrypted transmission from another device to execute the action required.

Validation occurs by 1) ensuring that all connected components that constitute the car be kept secure and untampered with,



despite multiple suppliers and throughout the lifetime of a car in the hands of different owners, and 2) ensuring that the cryptographic keys that unlock the device transmissions are created and managed in such a way that they remain unique and uncompromised. These challenges come into play once the car is connected, which occurs in the field when the cars’ firmware is updated—not in the secure production environment.

### Assigning a Birth Certificate to the Connected Car’s Components

Cryptographic keys work as digital signatures that provide connected devices with a chain of trust, a trust anchor if you will, that ensures authenticity and integrity in all device communications. These unique keys work as “birth certificates” to provide undisputable identity and guarantee that every action a smart device



## Related articles:

- <http://electronicdesign.com/blog/car-hacked-flaw-jeep-revealed> (hyperlinked in body)
- <http://electronicdesign.com/blog/what-does-it-mean-secure-internet-things> (hyperlinked in body)



initiates is authenticated and reliable, without third-party obstruction. Properly deployed in the case of the Jeep Cherokee hack, the hackers' signaling device would have been identified as a false sender of the command, making the remote commandeering impossible.

The connected car's chain of trust begins with validating the components at the manufacturing level and throughout the supply chain. By coding a cryptographic key into the connected device, seeding the chip, at production time, identity—and trust—become embedded into the connected component before it even leaves the device vendor's facility. But how can automotive designers maintain that security from the point of manufacturing to commercial deployment?

To maintain the integrity of the car's

cryptographic key material from point of production to commercial deployment, automotive designers need to consider continued key management to avoid compromised, cloned or mismanaged keys. To handle the distribution and use of cryptographic material embedded within the vehicle system, an embedded key management system will manage both code signing and verification of firmware updates, including automatic upgrades via OTA connections.

#### Where Did I Put My Crypto Car Keys?

There are different means of creating a cryptographic key via pseudo (software engineered) or true random number generation (based on randomly occurring anomalies in physics), and of storing a cryptographic key.

Hardware security module technology offers secure key storage even in the most hostile environments. The module can detect when any attack toward the key storage is happening, including drilling, heat, power blackout or chemical attack, and automatically delete the keys immediately. In comparison, software-based cryptographic keys can be captured in the moment of unlocking, offering attackers the ability to learn the software, exploit vulnerabilities and run attacks remotely.

In the connected car, computer systems (ECUs) embedded in the car need to have a physically secured area to store these unique crypto keys with which the systems can prove the identity of all the components and sign command messages. At the other end, the receiving ECU needs to have the ability to verify and unlock those crypto keys to validate the command before executing it. With hardware-based crypto key storage and management, the various systems communicating over the central bus in the vehicle can communicate while maintaining the chain of trust via identifiable crypto keys.

Complementary next-generation solutions to secure the connected car include innovations such as that of ethernet over fiber, enabling cryptographic solutions that

scale with complex automotive systems, and mobile software management solutions that securely manage all software in the car, including head units, ECUs and telematics boxes—whether on the production line, at the dealer's lot or the owner's driveway.

#### Looking Forward, 5 Questions to Avoid the Next Car Hack

For automotive designers working to ensure that a hack like the one on the Jeep Cherokee never happens again, there are five questions they should be asking about securing the connected car:

1. Is the supply chain secure? Can you be sure all the car's components are real and not counterfeit?
2. Does the car's embedded computer system have a physically secure area to store certificates and cryptographic IDs? And does the receiving computer system have the ability to verify those signed messages by checking them against a chain of trust?
3. Once the components are embedded into the larger ecosystem that is the car, how can you ensure the various systems communication over the central bus in the vehicle can communicate in a trusted manner?
4. How can you ensure all processes related to the software function of the car are covered by safeguarding measures, including development and production, at dealerships and service organizations?
5. Does your security solution cover all V2X communications? Including car-to-car communication, car-to-infrastructure communication, and roadside to vehicle communication? Or what about over the air updates? And lifecycle management?

The connected car is a thing of beautiful engineering and I'm sure it will make for some truly enjoyable road trips, aided by innovative command control and increased safety. With a hardware-based trust anchor, each connected device is supported from the point of production throughout its lifecycle, providing the root of trust that both vendors and drivers demand and anticipate before they hit the road.

# INVEST IN THE SOLUTION CREATION PROCESS AS THE FOUNDATION TO PROJECT SUCCESS



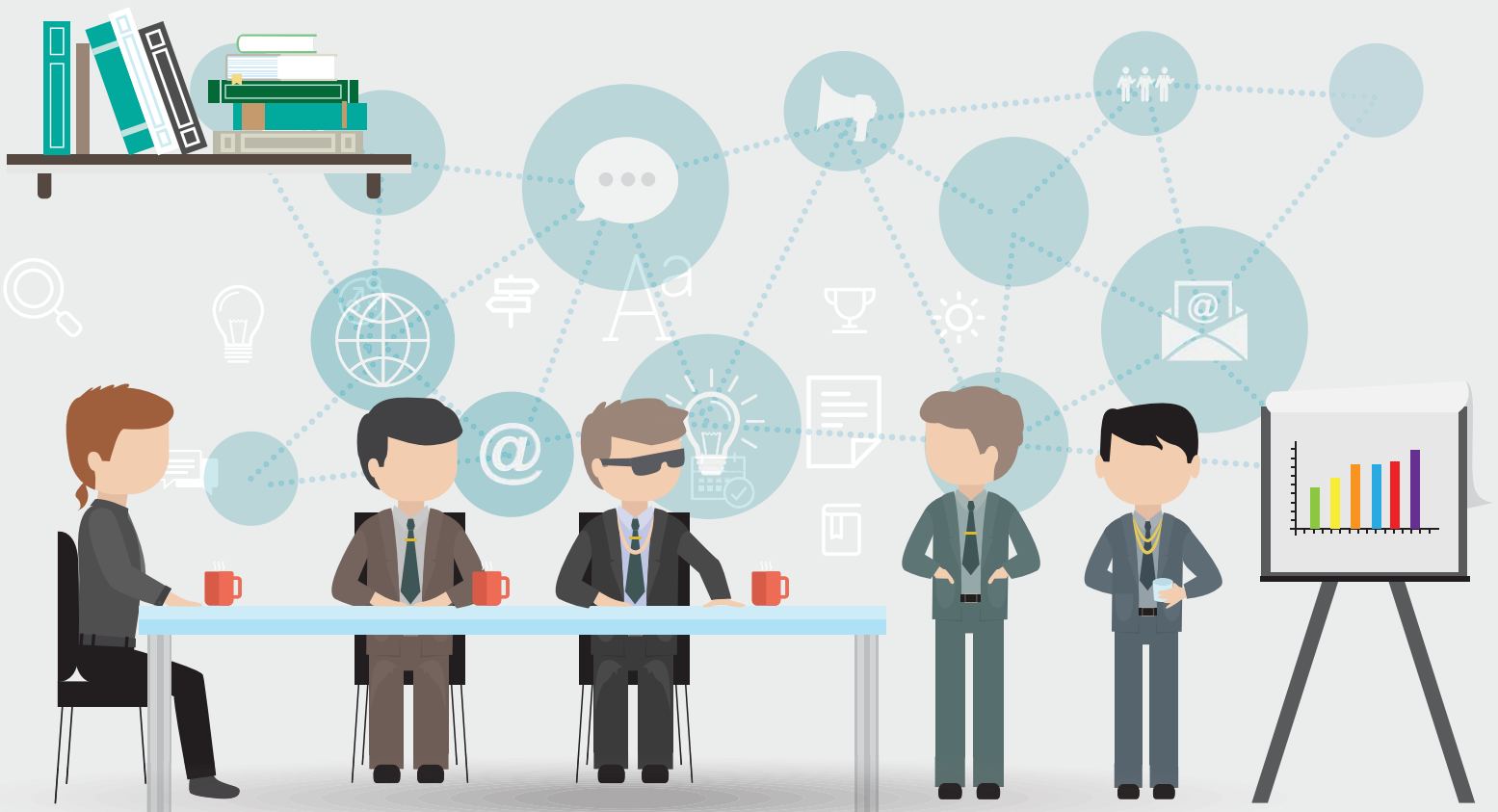
YuWin Tan joined SecureMetric in January 2014 as VP of Project Management and Support. Having 14 years experience in the PKI industry, YuWin Tan is responsible for the Project Delivery, Pre-sales Consultancy and Post-sales customer support teams in SecureMetric. YuWin's 14 year career in the PKI industry has taken him on numerous PKI Implementation and Consultation projects all over the world including a 2 year stint in Beijing. He firmly believes that doing the right things will ultimately lead to doing things right.

**SO**, you say that the vendor working on your project has got a super star sales team, world-class project managers and hardcore engineers. Successful project delivery should be a piece of cake right?

Well if it's not, you might want to look at how your vendors are putting together their solutions. "Solutioning", while not recognized as an official word by most dictionaries, refers to the process where business problems (Business/technical needs) get solved by deploying a combination of Hardware, Software and Processes (The solution creation process).

As a customer, you would want your vendor to get the "Solution" right so that it addresses your business problem in the most effective way and at the right cost. Therefore when deciding on a solution vendor, always choose a vendor who puts a greater emphasis on getting the solution right rather than somebody with the cheapest price.

Have you ever completed a project only to discover that the project had not addressed key business needs? How about systems that had features nobody ever uses? Remember that time when you had to upgrade or add features to your system about one month after go-live?





This could be because not enough attention was given during the solution creation process. It's like hammering a square peg into a round hole while saying "As long as it fits!"

Besides this, how many people consider Change Management needs as part of their solution creation process? Change Management is often the overlooked portion of most "Solutions". People tend to forget that their solution will most definitely invite change and, change needs to be managed. A solution that views the problem from a purely technical perspective might fail miserably because the change that it introduced was rejected by the people or resulted in an undesirable side effect much worse than the problem it was trying to solve!

To be fair, Customers sometimes contribute to the lack of focus in the solution creation process. This usually happens when there are unrealistic price expectations, insufficient time, communication breakdowns or just plain not knowing the difference between a "need" and a "want". Its funny how many people focus so much on what they "want", that they ignore what they "need". This happens not just in business but life in general as well. In this situation, uncovering and fulfilling the actual "need" becomes quite a challenge. However, it is the fulfilling of these "needs" that usually results in long term success of the solution.

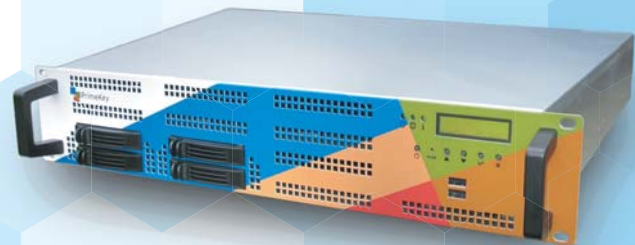
At SecureMetric, our team of professionals takes pride in fitting the right Solution to your business needs. For us, knowing that we got the "Solutioning" part right is just as important as winning the deal. We would rather decline an opportunity then propose a solution that doesn't fit.

Oops, please don't tell our sales team that ;)

**PrimeKey**

**EJBCA**

Probably the best PKI in the world.



**PKI in a BOX**



Faster and easier deployment



Much lower total ownership cost



Scale up or scale down options



Simplified Support & Maintenance and Efforts



Single Point of Supply for both Hardware and Software



CC EAL 4+ Certified CA Core & FIPS 140-2 Level 3 Validated HSM



Visit [www.securemetric.com](http://www.securemetric.com) for more information

**ASEANFIC**  
ASEAN Financial Institution Conference



# THE 10TH EDITION OF ASEANFIC 2015 AMAZED BANKERS AT PHNOM PENH

Organized by



Supported by



Local Hosted by



Partners



**ASEANFIC** starts the year with the 10th edition at Phnom Penh, Cambodia. It was held at Sofitel, Phokeethra, Phnom Penh. A young, talented group of professionals from Idealink Consulting was the event's local host in Phnom Penh. With their great effort, ASEANFIC garnered a total of 90 high level banking officers from every bank in Cambodia who participated in the event.

ASEANFIC is proud and grateful to have along our partners namely UTIMACO from Germany, PT Aprisma from Indonesia, and EPIC, CyberSecurity & Molla Technologies from Malaysia who spoke and share their expertise to local bankers from Cambodia.

Mr. Lim Chin Wan, the Chairman of ASEANFIC and Chief Business Development Officer of SecureMetric started the event with a warm welcome speech and followed by a talk of Mr. Ou

**30** 5th March 2015  
8 am - 5.30 pm



**Sofitel Phnom Penh Phokeethra Hotel**

No. 26, Samdech Sothearos Blvd (3), Sangkat Tonle Bassac, Khan Chamkar Morn, 12301 Phnom Penh, Cambodia



**10th Edition Phnom Penh, Cambodia**

Phannarith, Director of Ministry of Post and telecommunications of Cambodia and Chief Inspector Majoy Jay D. Guillermo, Chief Intelligence and Investigation Anti-Cybercrime Operations and Training Division From Philippine National Police, Anti Cyber Crime Group as our Keynote Speaker.

Cambodia's economy has been captivating in the past 2 years and has a great potential in Information Technology Industry where software and technology requirement drastically increase to cater the development of the economic growth of the country.

ASEANFIC Phnom Penh 2015 ended with a high tone, knowing all the participants are satisfied and now well informed with Threats that their company might face. Besides that, some guests won an Ipad Mini and Power Banks from the raffle draw.

ASEANFIC was a real success that everyone is looking forward for next year's edition.





- 1 ASEANFIC Cambodia gathers more than 80 delegates from banking industry around the Phnom Penh City.
- 2 Mr. Poh Soon from Utimaco making his presentation about PKI and Payment Security.
- 3 Delegate engaging IDEALink, SecureMetric local partner on the showcased products.
- 4 Banking delegates enjoying their beer & drink after a full day conference.
- 5 Delegates are happy and cheer during the end of the session.
- 6 Puan Maslina of CyberSecurity Malaysia is presenting security certification standards to the delegates.
- 7 Local partner IDEALink presenting souvenir to Mr Viraj from Epic Malaysia.
- 8 Delegates sharing the view among each other regarding banking technologies.
- 9 Lucky draw session where Mr Lim Chin Wan is picking up a lucky winner.
- 10 Speaker and Delegates are sharing their thoughts with joy.
- 11 Delegates enjoying their coffee on morning coffee break session.



**ASEANFIC**  
ASEAN Financial Institution Conference



# THE 11TH EDITION OF ASEANFIC 2015 GOES BACK TO MAKATI CITY, MANILA

**THREE** months after the successful organizing of ASEANFIC in Phnom Penh, ASEANFIC continues its journey on its 11th edition to Manila on this 30th June 2015. ASEANFIC again gathers 120 top levels officers from the banking industry to join us in this event.

Again, ASEANFIC is proud to have our partners from UTIMACO and Epic Malaysia to join the event. More to add on this year, ASEANFIC successfully invited local Philippines companies to join the event as a speaker on sharing their new products and ideas to the banking industry experts. PMTI Inc and Globe Labs were the 2 companies being invited to join us at our event.

Ms. Janette Toral, e-commerce Advocate of Digital Filipino, Philippine presented her keynote session about the Framework of e-commerce in the Philippines.

As the local host and organizer of the event, SecureMetric's Chief Business Development Officer, Mr. Lim Chin Wan presented CENTAGATE to the audience. Being an intelligent centralized authentication platform, CENTAGATE successfully attracted the eyes of the security officers.

This 11th edition of ASEANFIC event added in 2 Workshop sessions for the bankers at the afternoon session, where they can choose to attend any one of the topics that would be hosted and talk by Nickson Yau, CTO of SecureMetric Technology and Mr. Virash, CEO from Epic Malaysia.

Again, ASEANFIC Manila ended with a cocktail session with lucky draws to our delegates. 5 of the lucky delegates won 5 iPad mini and everyone left home with a big smile on their faces.

Organized by



Supported by



Supporting Organisation



Partners



**30** 30th June 2015  
8 am - 5.30 pm

**Shangri-La Hotel, Manila**  
Ayala Avenue Corner  
Makati Avenue, Makati City,  
1200, Philippines

**11th Edition  
Manila, Philippines**





2



3



4





5



6

- 1 Mr. Luis "Chito" A. Jacinto, represent Information Security Officer Group (ISOG) Philippines, presenting ISOG to the delegates.
- 2 Mr Viraj from Epic Malaysia introducing Mobile Banking Technologies to the delegates.
- 3 Mr Edward presenting souvenir to Mr Teo Poh Soon after his speech about PKI Security.
- 4 ASEANFIC Manila 2015 is about to start.
- 5 Delegates getting ready to listen to the next speaking session.
- 6 Mr Lim Chin Wan speaking about SecureMetric new product, CENTAGATE to banking delegates.





**ASEANFIC**  
ASEAN Financial Institution Conference  
[www.aseanficc.org/2015](http://www.aseanficc.org/2015)

**Thank You for being part of our team at ASEANFIC 2015!**

We are a non-profit organization that provides an opportunity for Banking and Financial Institution to cope up with all the technological trends today.

# GETTING LOST IN THE CLOUD?

With information flowing more freely than ever in today's increasingly digital economy, findings from a new perspectives survey show that IT Professionals admit to having limited visibility into where all their organization's sensitive data resides.

## TRANSFORMING BUSINESS IT WITH PRIVATE CLOUD

Gartner predicts a **10x increase** in Private Cloud deployments, driven by speed and agility benefits

**58%** of companies move to Private Cloud for AGILITY gain and SPEED

When Private Cloud is working, IT becomes a business enabler

**40%** say their biggest Private Cloud Challenge: INTEGRATION with existing systems

### HOW DOES CLOUD COMPUTING RATE?

**1/3** of the organisations include cloud computing in their top 3 priorities

## TOP 3 BUSINESS PRIORITIES

01 Delivering Operational Result

02 Reducing Enterprise Costs

03 Improving Efficiency

Private Cloud enables speed, agility and innovation. You need to move from the drawing board to deployment. **But is your organization ready to adapt?**

### PRIVATE CLOUD

deployment may outpace Public Cloud use by 2 times within the next 12 months

## GARTNER: PROCESSES UNDERPIN IT SUCCESS

Make the Shift From Service Provider to Strategic Business Partner With Mature IT Management Processes

### SERVICES

- 01 IT as a Service Provider
- 02 Defined Services, Classes, Pricing
- 03 Understand Costs
- 04 Guarantee SLA's
- 05 Measure and Report Service Availability
- 06 Integrate Processes
- 07 Capacity Management

### VALUE

- 01 IT as a Strategic Business Partner
- 02 IT and Business Metric Linkage
- 03 IT/ Business Collaborator Improve
- 04 Business Process
- 05 Real-time Infrastructure
- 06 Business Planning

Source :

<sup>1</sup> Based on 597 customer responses to Data<sup>3</sup> research, June 2013

<sup>2</sup> Based on 341 responses. Palmer Research, April 2013. <http://www.prweb.com/releases/2013/6/prweb10833469.htm>

<sup>3</sup> Forrester, July 2012 [http://resources.idgenterprise.com/original/AST-0089434\\_private-cloud-more\\_than\\_just\\_virtualization.pdf](http://resources.idgenterprise.com/original/AST-0089434_private-cloud-more_than_just_virtualization.pdf)



## WITHOUT SECURITY, CLOUDS CAN'T REIGN

Survey results from 130 security professionals from the RSA conference show companies are not being proactive enough to protect sensitive data in the cloud

## IN THEIR OPINION, THE CLOUD IS...

No Different To Secure Than On Premise

18%

66%

Much More Difficult To Secure Than On Premise

16%

Less Difficult To Secure Than On Premise

## A MIDDLE GROUND IS NEEDED

Organizations are not aggressively using cloud systems because of privacy and security concerns

52%

of respondents trust their CSP

RELYING ON A CSP FOR DATA COMPLIANCE AND PROTECTION MAY NOT BE ENOUGH

## TO TRUST OR NOT TO TRUST IN YOUR CLOUD SERVICE PROVIDER

Do IT professionals trust their Cloud Service Provider (CSP) to take care of protecting and controlling enterprise data for them?

IT'S A SPLIT DECISION

48%

of respondents do not trust their Cloud Service Provider

THIS CAN LIMIT CLOUD ADOPTION, AND HARM THE BUSINESS

## CURRENT ENTERPRISE MENTAL MODEL: PRIVATE CLOUD = SECURE CLOUD

### The Majority of Respondents Still House Less Than a Quarter of Their Data in Public Cloud Environments

Private is the home of highly sensitive data, but this information will continue to make its way into the public cloud as enterprises learn about what encryption and tokenization can do for them.

### Regulatory Compliance and Security Concerns are The Primary Inhibitors to Cloud Adoption

67%

prefer to store the enterprise data in the cloud if data privacy and compliance regulations could be address

50%

say data privacy regulations impact up to 50% of their cloud strategy

33%

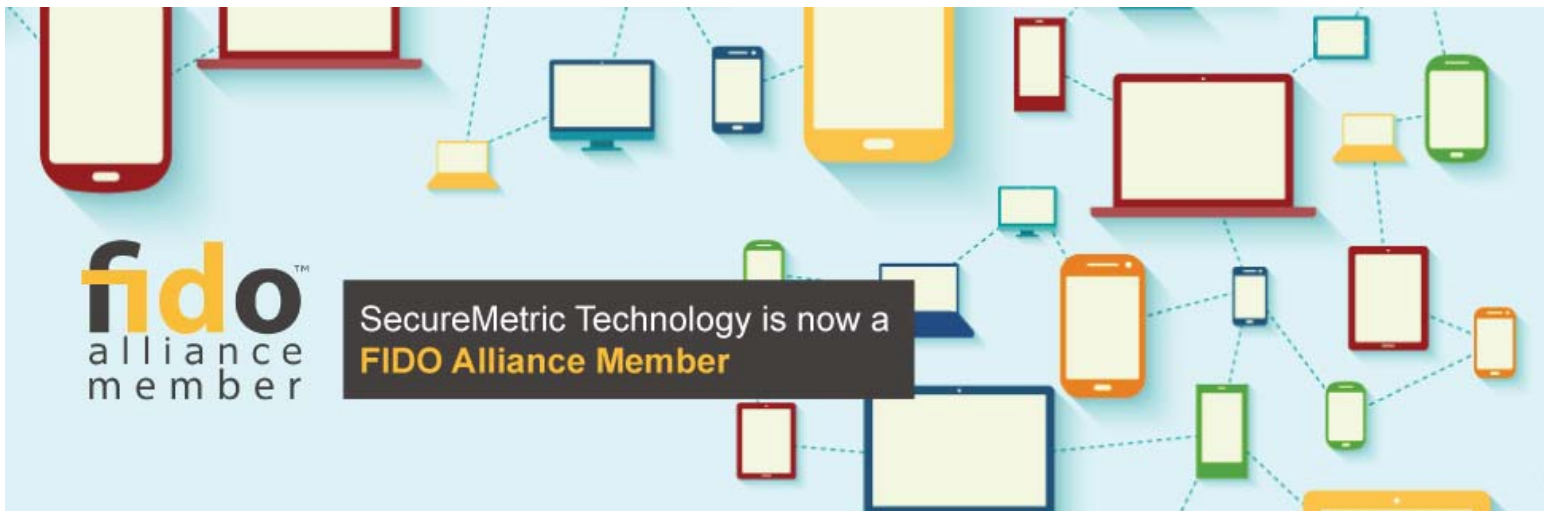
claim no public cloud use, as far as they know (IaaS, PaaS, or SaaS)

Source :

<sup>4</sup> <http://technology-news-hub.com/cloud-computing/the-true-value-of-the-private-cloud/>

<sup>5</sup> [http://cloudtweaks.com/wp-content/uploads/2015/05/Perspecsys\\_Final-e1431626616155.jpg](http://cloudtweaks.com/wp-content/uploads/2015/05/Perspecsys_Final-e1431626616155.jpg)

<sup>6</sup> [www.PerspecSys.com](http://www.PerspecSys.com)



## SECUREMETRIC TECHNOLOGY ANNOUNCES MEMBERSHIP IN THE FIDO ALLIANCE

### SECUREMETRIC

Technology proudly announces that they have joined the FIDO (Fast Identity Online) Alliance in March 2015.

The FIDO (Fast Identity Online) Alliance was formed to address the lack of interoperability among strong authentication technologies, as well as the problems individual users face in creating and remembering multiple user names and passwords. FIDO Alliance membership includes global leaders in technology and industry.

Being the PKI Expert in the region, SecureMetric plans to cultivate innovative and more secure authentication by using FIDO specifications which defines an open, scalable, interoperable set of mechanisms that supplant reliance on passwords to securely authenticate users of online services.

“The FIDO Alliance is proud of our associate member SecureMetric Technology for its dedication to the vision of industry standards for strong authentication. They join a powerful FIDO ecosystem vital to widespread adoption of interoperable, strong authentication that simplifies the user experience while raising security and privacy at the same time,” said Brett McDowell, FIDO Alliance executive director. “FIDO Alliance members embody the innovation that FIDO specifications enable.”

#### About SecureMetric

SecureMetric, [www.securemetric.com](http://www.securemetric.com), is Southeast-Asia’s market leader in digital security industry with more than 17 years of experience in serving clients across the region. On top of supporting more than 3,000 software companies worldwide in protecting their software copyright and licensing, SecureMetric has successfully

implemented high profile 2-Factor Authentication and Cryptography projects for well-known financial institutions and government agencies.

#### About the FIDO Alliance

The FIDO (Fast Identity Online) Alliance, [www.fidoalliance.org](http://www.fidoalliance.org), was formed in July 2012 to address the lack of interoperability among strong authentication technologies, and remedy the problems users face with creating and remembering multiple usernames and passwords.

The FIDO Alliance is changing the nature of authentication with standards for simpler, stronger authentication that define an open, scalable, interoperable set of mechanisms that reduce reliance on passwords. FIDO authentication is stronger, private, and easier to use when authenticating to online services.



Philippine Software Industry Association

# SECUREMETRIC TECHNOLOGY FORMALLY JOINED PHILIPPINE SOFTWARE INDUSTRY ASSOCIATION (PSIA)

## SECUREMETRIC

Technology Inc. has formally inducted as an official member of Philippine Software Industry Association (PSIA) at their 1st General Members Assembly for 2015 last March 23, 2015 at Fairmont Hotel, Makati City.

The Philippine Software Industry Association is a non-stock and non-profit organization dedicated to promote the growth and development of the software industry in the Philippines and increase its

overall competitiveness in the global scene. For 26 years now, it has been closely working with the government, the academy and the IT community, to further the country's success in this rapidly expanding industry.

With SecureMetric and PSIA joining forces to promote not just the software industry but the digital security awareness campaign, we can expect our country to progress in the digital age and catch up with our ASEAN neighbours in cyber digital race.

SecureMetric is Southeast-Asia's market leader in digital security industry with more than 17 years of experience in serving clients across the region. On top of supporting more than 3,000 software companies worldwide in protecting their software copyright and licensing, we had successfully implemented high profile 2-Factor Authentication and Cryptography projects to well-known financial institutions and government agencies.

## SafeGuard® CryptoServer

- Terminal Control Center
- CVCA & DVCA
- Random Number Generator
- Basic Access Control
- Extended Access Control
- Key Management



For more Information, contact us at [sales@securemetric.com](mailto:sales@securemetric.com)



South East Asia Value Added Reseller Partner



utimaco  
a member of the Sophos Group



**Signing Hub**

ascertia  
[www.ascertia.com](http://www.ascertia.com)  
[www.signinghub.com](http://www.signinghub.com)  
[sales@ascertia.com](mailto:sales@ascertia.com)

Sales Contract 2015

*No Waivers, Cumulative Remedies.* A party's failure to insist upon strict performance of any provision of this Agreement is not a waiver of any of its rights under this Agreement. Except if expressly stated otherwise, all remedies under this Agreement, at Law or in equity, are cumulative and nonexclusive.

*Severability.* If any portion of this Agreement is held to be unenforceable, the unenforceable portion must be construed as nearly as possible to reflect the original intent of the parties, the remaining portions remain in full force and effect, and the unenforceable portion remains enforceable in all other contexts and jurisdictions.

*Notices.* All notices, including notices of address changes, under this Agreement must be sent by registered or certified mail or by e-mail.

*John Clarke*  
I approve this document  
[john.clarke@signinghub.com](mailto:john.clarke@signinghub.com)  
London, United Kingdom

IN WITNESS WHEREOF, the parties execute this Agreement as of the Effective Date. Each person who signs this Agreement below represents that such person is fully authorized to sign this Agreement on behalf of the applicable party.

## The Most Secure Way to Sign

- Document Signing
- Signature Verification
- eID Validation
- Timestamping & Archiving
- Approval Workflow



**AKATI CONSULTING**  
MALAYSIA • UK • MEXICO • HONG KONG

[www.akati.com](http://www.akati.com)

by Krishna Rajagopal



# ARE YOU ON THE ROAD TO GETTING HACKED?

YES! You can get hacked easily regardless of the size or reputation of your organization. Sometimes the lack of knowledge about certain basic security measures could result in cyber attacks, large financial losses or being cheated by so called information security vendors.

With the emerging trend of online business, many small business owners have waded into the waters of e-commerce since it's a cost effective and fast way to grow a business. It's not just the start-ups, business habits of many established firms and governments are also changing as they become cognizant of the immense benefits of conducting business online. Well, online transactions are great but there is one crucial aspect that most entrepreneurs and organizations forget - Information Security!

You're not expected to become a security expert to secure your network and business. You can hire a reputed Information Security service provider to upkeep the security of your IT infrastructure. However, to be able to select a firm who will not presume on your ignorance, you need to know the basic differences of certain security mechanisms. First of all let's get this straight - It's imperative to test any internet-facing site for vulnerabilities.

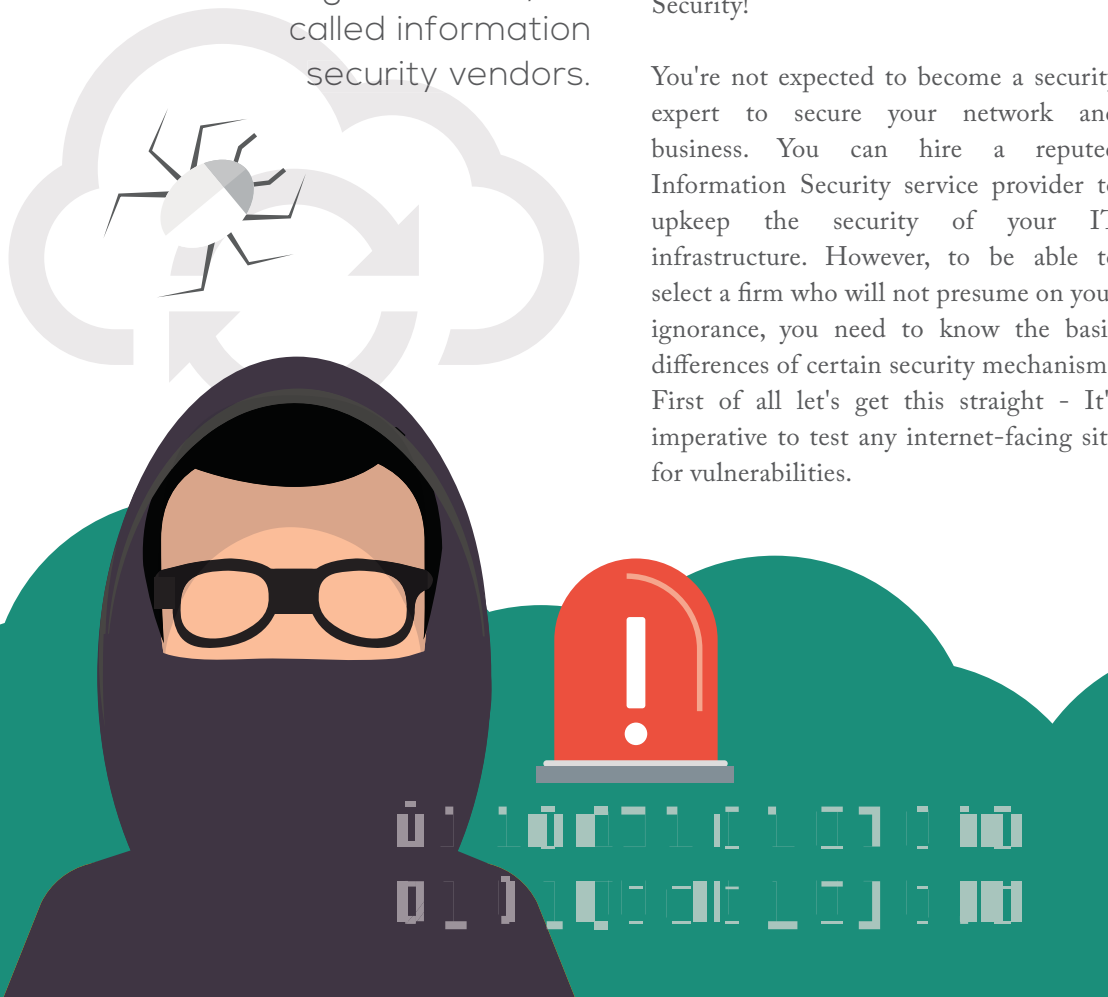
"Vulnerabilities are the gateway by which threats are manifested" is the SANS definition of vulnerabilities. Essentially, these are weaknesses found in systems that can open up your network to a range of threats such as data breaches, information theft and credit card fraud.

How are these vulnerabilities caused? Many systems and software are shipped with known and unknown security holes or bugs and default configurations that are not secure. There are also vulnerabilities caused due to misconfigurations by system administrators.

## What Can You Do About It?

Systems have to be checked for vulnerabilities. Then the vulnerabilities have to be assessed to see if they can be exploited in your particular environment. Afterwards, the impact of the identified vulnerabilities in your organisation must be ascertained. These three different processes are what entail Vulnerability Assessment, Penetration Test and Risk Analysis respectively. Information Security is not a one-time operation so you may have to run these tests periodically.

Having a sound understanding of what these security mechanisms really mean can be quite useful when deciding the best way to secure your network and systems which form a significant part of your business.



# SECUREMETRIC ST3 ACE FIPS 140-2 LEVEL 3 CERTIFIED



## SECUREMETRIC

Technology’s USB token ST3 ACE received the FIPS 140-2 Level 3 certificate; a U.S government computer security standard last January 12, 2015. This recognition reflects SecureMetric’s innovative approach in developing security products and assuring the market the credibility and quality of its services offered.

SecureMetric ST3 Ace FIPS 140-2 Level 3. SecureMetric ST3 Ace is a USB token containing FIPS-COS cryptographic operating system. The FIPS-COS is embedded with IC chip and has been developed to support ST3 Ace Token. ST3 Ace is designed to deliver strong authentication and identification to support network log-in, online transactions, digital signatures and

sensitive data protection. The FIPS 140-2 level 3 certification provides a great opportunity for SecureMetric. With this, we can now provide a highly secured cryptographic IC chip USB tokens to the security markets in the region; thus makes us more competitive more than ever.

### About FIPS 140-2 Level 3 Certificate

FIPS 140-2 defines four levels of security, simply labeled “Level 1” up to “Level 4”. Physical security mechanism required at Security Level 3 provides high probability of detecting and responding to attempts at physical access and use or modification of the cryptographic module. The physical security mechanism includes the use of strong enclosures and tamper detection/response circuitry that zeroes all plain text CSP’s when the removable covers/doors of the cryptographic module are opened.

### About SecureMetric

SecureMetric is one of the fastest growing digital security technology companies in the market. On top of supporting more than 3,000 software companies worldwide in protecting their software copyright and licensing; we had successfully implemented high profile 2-Factor Authentication and Cryptography projects to well-known financial institutions and government agencies across the region. With our commitment on R&D, we can assure our partners that we continuously improve our products and solutions. We aim to be the leading digital security provider in South East Asia.



# SECUREMETRIC HQ HAS MOVED!



## SECUREMETRIC

Technology has officially moved to a new office in Technology Park Malaysia on 11 June 2015.

A small party was hosted for friends and partners from all around the world to enjoy buffet and also some short session to introduce SecureMetric products and solutions.

The new office is larger and capable to fit our expanding workforces, in addition we now have a dedicated server room, multiple meeting rooms of various sizes and also bigger inventory space for our products.

SecureMetric pledges to not stop growing

and we managed to expand thanks to our loyal customers support and also our strong R&D team on continuing to improve and develop new solutions to solve our customer concerns on digital security.

We will continue to strive on providing the best digital security solutions and products, with our new office we hope we will be able to expand our presence further and offer the best service which we are already providing to our customers.

SecureMetric Technology contact details remain the same although our office location has moved so it will be convenient for our existing customer and our potential customer to contact us.



**+603 8996 8225**

9 a.m. - 6 p.m. local time  
Monday - Friday



**Website**

[www.securemetric.com](http://www.securemetric.com)



**Our New Address**

Level 5 L5-E-6, Enterprise 4,  
Technology Park Malaysia  
Lebuhraya Sg. Besi - Puchong,  
Bukit Jalil, 57000 Kuala Lumpur,  
Malaysia.

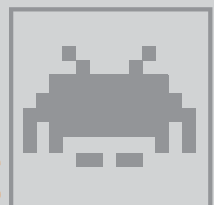
In SecureMetric Technology, we pay attention to every feedback or enquiry. We promise will response to you within 24 Hours within our working hour.

**SECURITY WARNING!**

**DID YOU KNOW THAT 59%  
OF EMPLOYEE STEALS  
PROPRIETARY CORPORATE  
DATA WHEN THEY  
QUIT OR FIRED**



**MALWARE  
MASS  
ATTACKS  
INCREASES & ADAPTS**



# SECUREMETRIC JOINING VIETNAM ICT SUMMIT 2015 IN HANOI



**THE** 25th June, SecureMetric took part in Vietnam ICT Summit 2015 in Hanoi. This is the most important event in Vietnam ‘s software and ICT industry which organized annually by VINASA.

This year, ICT summit once again achieved wonderful accomplishment with more than 500 delegates from ICT and software companies in Vietnam. Comprising with several meetings and conferences this year, Vietnam ICT Summit is designed to discuss the application of ICT in major sector and social service management.

With the theme of: “ICT and Smart Management” this summit forum is tailored for high level national information technology and communications professionals. The summit plays a very important role targeting in a new vision and strategic solution for national development based on IT and telecommunication. Four major topics were on agenda at the forum – ICT empowers healthcare capacity, Develop Vietnam ICT Young Talent, ICT enhances public services efficiency and ICT empowers Smart Cities and Smart Transportation”.

SecureMetric Technology was presented as co-sponsor for this event. By attending this event, SecureMetric showcased an overview about software protection solution – SecureDongle. SecureDongle is the market most wanted Software License and Copyright Protection dongle that offer maximum security but minimum learning and investment. Many software companies were impressed by SecureDongle product and its solution. SecureMetric brought to event a good solution for software developers to directly keep revenue loss due to software piracy.

In summary, ICT Summit was an ideal forum to share information and to present SecureMetric product to Vietnam’s customers. We have met good potential customers who, for sure will trust on our dongle in the near future.

## SECUREMETRIC TECHNOLOGY JOINED CARDS AND PAYMENTS, MANILA

**SEPTEMBER** 2015, SecureMetric together with Ziaplex co-sponsored at the Cards and Payments Asia, the region's biggest event dedicated to payments innovation & technology. Knowing the big potential of the Philippine market, the organizer, Terrapinn has launched its first Cards and Payments Philippine event that was held at SMX Convention Centre, Manila.

After generating, 2000 attendees, 50 exhibitors and 120 conference speakers, the event was a huge success. C-level executives and heads of cards, payments, retail banking, prepaid, security, marketing, loyalty, transit and IT attended the conference from different industry such as Banks and Financial Institutions, Government, Transport and Telco Operators, Manufacturers, Healthcare, Retailers, Shopping Malls and Supermarkets retailers across Philippines.

The conference tackled many issues including: Payment disruption and innovation, Payments and the customer experience, Digital currencies and wallets, Improving customer experience with mobile wallet, Bitcoin and digital currencies, Opportunities in carrier billing for the Philippines, New opportunities created by data analytics, Financial inclusion in the Philippines, Impact of alternative currencies and payments, Cyber security threats to payments and banks.

SecureMetric has showcased its different Security Solutions such as SecureDongle - Software Licensing Protection Dongle, Centagate - Centralized Authentication Gateway and PKI (Public Key Infrastructure) in a Box. With a growing industry of Cards and Payment in the Philippines, produces more reason for fraudsters and cyber criminals to target this country.

Knowing this, many delegates showed interest on the security solutions featured by SecureMetric as a lot of questions was generated. Delegates from different industry wanted to know more how they can secure their solutions and platforms against different cyber-attacks that may occur in the future and SecureMetric was successfully given them awareness how they can overcome it.

To strengthen SecureMetric's push for Digital Security Awareness in ASEAN Region, our Chief Business Development Officer, Mr. Lim Chin Wan, participated to be one of the speakers on the event with topic titled "Enhancing System Security using PKI".

Overall, it was another fruitful event that let SecureMetric showcase their vision in providing a Strong Digital Security for the Cards and Payments Industry.



Mr. Lim Chin Wan, Chief Business Development Officer of SecureMetric Technology is making his presentation at the Cards & Payment Event.



Joining together with Ziaplex Inc., SecureMetric makes our appearance in Cards & Payment Philippines.





SECUREMETRIC TECHNOLOGY  
FORMALLY JOINED  
**SOFTCON PH**

**WITH** the continuing support of SecureMetric Technology to the Philippine Software Industry Association or PSIA, SecureMetric has yet again take part of the Softcon.ph event as a Bronze Sponsor. As a company that teaches and creates awareness about software protection into the software industry, SecureMetric Technology has sponsored this event two years in a row.

SOFTCON.ph is the country’s premier event for promoting and celebrating the world-class products and services of the Philippines’ Information Technology industry. With last years’ success, PSIA create this year’s event more exciting by making it a two day expo that happened on November 4-5, 2015. Day 1 focused more on the business side which tackled the truth about digital businesses as a key theme, by exploring technology trends and taking a look at how technology is driving today’s businesses. The 2nd day focused on the theme of breaking beyond the hype of emerging technologies, with industry experts sharing practical technical advice that can be immediately applied to current work.

The venue was held at the Marriott Grand Ballroom which is simply the Philippines largest hotel ballroom. The venue brought

in excitement and good ambience to the delegates which was a big success by seeing a full packed crowd of attendees.

SecureMetric Technology is dedicated at to fight against software piracy by featuring SecureDongle software piracy. SecureMetric teaches and opens software industries mind about the importance of protecting their intellectual property as well as gaining more income by stopping unauthorized use of their software. Also, to make the event more exciting, SecureMetric Technology gave away free tumblers for every delegates who will

answer the Software Protection Awareness Survey. By doing this, it gave us an idea on how important is it for us to continue helping and partnering with the software industry in protecting their software against cloning, crackers, piracy and more.

Aside from SecureDongle, as we pushes the awareness about Digital Security, SecureMetric also showcased 2 Factor Authentication Tokens, Biometric Solutions and our latest innovation Centagate – Centralized Authentication Gateway which makes SecureMetric the most visited booth on the event.



Mr. Bryan Soler, Sales Manager of SecureMetric, is explaining to the customer about SecureMetric products.



## SOFTWARE Security Seminar with software developers at Ho Chi Minh City

SecureMetric Technology and Vietnam Software & IT Services Association had jointly organized a successful seminar, Software Security Workshop at Ho Chi Minh City on this 24th November, at Grand Hotel Saigon.

This half day seminar gathered 45 different delegates from software development industries that really do concern about protecting their software licenses and security. The seminar started with a welcome speech to all the VINASA member who participate in this seminar from the Deputy Director of VINASA, Mr. An Ngoc Thao. An overview of software piracy and protection was done Mr. Sio Chun Jia, Marketing & Sales Manager SecureMetric Technology, then followed by a presentation by Mr. Lim Chin Wan, Chief Business Development Officer of SecureMetric Technology about Securing Business Application with SSL.

The seminar continued with a detailed introduction to SecureDongle. SecureMetric software license protection dongle. Mr. Tan Jian Yau, Senior Engineer of SecureMetric Technology explained the details and features of SecureDongle to the delegates. Before the presentation, Mr. Tan also made an impressive demo on how easily can a software been hacked in just 15 minutes.

# SECUREMETRIC TECHNOLOGY SOFTWARE WORKSHOP HO CHI MINH CITY

Before the closing lunch and lucky draw session, the floor was being passed to Ms. Tuyen, the Manager of Sales at SecureMetric Ho Chi Minh City to answer

questions from the delegates. At the end, the seminar was closed with a good lunch with smiles from all the participants.





SECUREMETRIC ATTENDED  
EVENT AT JAKARTA

# PAYMENT SECURITY & AUTHENTICATION -ASIA

**SECUREMETRIC** Technology attended its first event of the year entitled “Payment Security & Authentication- Asia” at Jakarta, Indonesia. The event captured roughly 200 delegates around the region who specialized in mobile payment and security. The event was organized by Clarions UK.

The conference was done simultaneously with “Mobile Money & Digital Payments” at Ritz Carlton Hotel. Representatives from different organization’s interest on digital security provided by us proved to improve as we are the only security authentication solution company among 15 exhibiting sponsors. We introduced our services to them such as PKI in a Box, Cryptomathic Key Management System and CENTAGATE. Among all of our solutions, CENTAGATE made the most impact as the adaptive intelligence feature fits to present market needs. Our opportunity

paved way for delegates to explore and to know the latest security trend today.

Having the largest population in South-East Asia; Indonesia poses a great market opportunity for companies around the globe; and as this conference brings together payments’ professionals from all across the region to share insights and strategies; it is vital to create partnership to promulgate the purpose of the event and ensure to take advantage of the true potential of this country.

This conference brings together payments professionals from across the region to share the insight, opinions and strategy and form the partnerships fundamental to ensure the success of their initiatives on creating crucial services for the citizens through mobile business opportunities.

**1 PRIVATE INFRASTRUCTURE**  
Virtually owned a private infrastructure without any investment.

**2 LATEST TECHNOLOGY**  
Enjoy strong protection module, such as multiple authentication methods SMS, OTP, PKI token, FIDO, and etc in a single platform that continuously update to the latest technology.

**3 FLEXIBILITY & INTEROPERABILITY**  
Easy integration to any client app such as WEB API, Single Sign On (SSO), RADIUS, and LDAP/AD.

## 5 REASONS

To Move Authentication To Private Cloud

More and more cloud-based services are becoming an integral part of the enterprise, lowering cost and management overhead while increasing flexibility

**AUTHENTICATION AS A SERVICE IS NO EXCEPTION**

**4 MEETING BUDGET EXPECTATION**  
Private cloud authentication is based on a simple, user based subscription model, without any hardware & software investment

**5 NEEDS OF GROWTH**  
Private cloud authentication provide a secure environment that will grow together with your organization

**CENTAGATE®**  
Centralized Authentication Gateway



PKI CONFERENCE 2015  
Kuala Lumpur | 9-10 June | Hotel Royale Chulan

PKI CONFERENCE 2015 JOINTLY ORGANIZED BY

# SECUREMETRIC TECHNOLOGY & ASIA PKI CONSORTIUM

**THE** PKI Conference is the brand new forum for the presentation, sharing and discussing about the PKI technology. It offers a unique opportunity for organizations to research, gain feedback and establish collaborative relationships with an international audience of PKI and business leaders in the Asia PKI Conference.

This year, SecureMetric Technology & Asia PKI Consortium (hereinafter APKIC) are proud to jointly organizing this conference in Kuala Lumpur on the 9th and 10th of June at Royale Chulan Hotel with Malaysia Communication & Multimedia Commission (MCMC) being the official government sponsor for this event.

PKI Conference was proud to have 25 industrial and governmental experts across Asia and Europe to join the conference as speakers. Among the speakers they are, Dr. Phillip Leung, Dato' Mohd Ali Hanafiah, Ms. Eva Chan, Mr. Lars Bagnert, Mr. Liaquat Khan, Ms Phoebe Yip, Mr. Reynaldo Joseph Jr. Callao, Ms. Pitinan Kooarmornpatana and others.

PKI Conference is a 2-days conference with workshop session, which provide more targeted topics for the delegates to discuss in further details. The conference was proud to have the Deputy Minister of the Science, Technology and Innovation, Datuk Dr. Abu Bakar Bin Mohd Diah,



Official Government Partner



Endorsed by



Supported by



Organised by



Co-Organised by



Platinum Sponsor



Sponsor



MSC Company



giving an interesting welcome speech to all the delegates. Followed by keynotes presented by CEO of Cybersecurity Malaysia, Dr. Amirudin Abdul Wahab, regarding cyber security development in Malaysia. The event was followed by a coffee break with a VIPs tour at the exhibition area. Right after the coffee break session, Chief Officer of Content, Security & Innovation of the Malaysia Communication & Multimedia Commission, Dato' Mohd Ali Hanafiah Mohd Yunus presented "Trusted Ecosystem as a Major Component of Smart Nation".

The presentation captures the eyes of all the national governmental representatives and the security experts. The conference received huge positive feedbacks on the content where the speakers and content were informative and interesting. PKI Conference were proud to have representative across Asia participating the event namely, China, Macao, Hong Kong, India, Japan, Philippines, Thailand, Laos, Myanmar, Singapore, Indonesia and Vietnam.

The event started with panel discussion and received valuable insights and answers from the panels. The crowd was engaged as well where some critical questions were raised and ideas were given on certain topics.

The first day was ended with a special networking session with all the governing bodies around Asia together with the

sponsors. This special networking session was sponsored by MCMC, the event official government partner.

2nd day of PKI Conference's content are more towards industrial professional insights. PKI Conference Platinum sponsors, Primekey and Ascertia gave their presentations about PKI and digital signatures implementation to the audience, which attracted very much interest of the delegates who visited their booth later on. Mr. Krishna Rajagopal presented the last keynote from Akati Consulting. He highlighted a few interesting hacking cases around the world which related to the PKI industry. These incidents were then analyzed and discussed together with his co-speaker, Mr. Anders from Comfact AB Sweden.

After the lunch, the workshop session began with different topics for detailed discussion. The conference was ended with gala dinner with closing speech from the Deputy Minister of Communication & Multimedia, Datuk Jailani Johari. The conference ended with a smile on everyone's faces especially those who were lucky to win the lucky draw prizes.

PKI Conference will be planning the next edition next year 2016 again on June. A lot of parties from different ASEAN countries are interested to become the host for next year. The organizing committee will announce the next PKI Conference by end of the year 2015.

## THE CONFERENCE IS SET TO HAVE THE OBJECTIVE OF:

- 1 Learn from PKI & digital security experts around the world with the latest PKI technology and industry updates.
- 2 Promote and accelerate PKI technology standardization and interoperability among Asian countries.
- 3 Establish effective networking platform to strengthen co-operation among PKI industry among Asia & across other region.

# PK CONFERENCE 2015

Kuala Lumpur | 9-10 June | Hotel Royale Chulan



# PKCONFERENCE 2015

Kuala Lumpur | 9-10 June | Hotel Royale Chulan





**BEST GLOBAL MARKET AWARD** | **Star SOBA**  
STAR OUTSTANDING BUSINESS AWARDS

SECUREMETRIC RECEIVE AWARD AT  
**THE STAR OUTSTANDING BUSINESS AWARD (SOBA)**



**THE** Star Outstanding Business Awards (SOBA) is The Star's awards recognizing up-and-coming enterprises and their contributions to the Malaysian economy. In line with the Government's commitment to develop homegrown enterprises, SOBA seek to inspire and encourage local businesses to promote Malaysia and showcase its products and services to the world.

On the prestigious night, SOBA awarded 3 levels of winners namely Silver, Gold, & Platinum in 7 Top of the Class Award and 3 Outstanding Achievement Award. Announcement of winners were only made during the actual award night of which not

all categories would have a winner for all levels.

With that, SecureMetric Technology is honoured to be presented the Silver Award for Best Global Market Categories. This particular category attention was given to local businesses that export their products or services, as they help to promote Malaysia as a global center of commercial excellence.

Mr. Edward Law, the Chief Executive Officer of SecureMetric Technology, received the award from the hands of Minister in the Prime Minister's Department, Datuk Dr. Wee Ka Siong and The Star

Media Group Managing Director and Chief Executive Officer, Datuk Seri Wong Chun Wai.

SOBA has always been recognized as an avenue to help SMEs measure its competitiveness against the best in Malaysia. SecureMetric Technology humbly accepts the award and thanks SOBA for the noteworthy and gracious recognition of its work. Being recipient of this award motivates and drives SecureMetric even further to pursue greater accomplishments in its Global Market work so that SecureMetric Technology may one day achieve our vision on being the pioneer digital security service and solution provider in the region.