

# SECUREMAG

SECUREMETRIC TECHNOLOGY GROUP

FORMULA FOR STRONG DIGITAL SECURITY



**FINTECH**  
The Disruption in Digital Finance  
PAGE 14-15 INFOGRAPHIC



**TECH** DAYS 2016  
PAGE 4-5



**The Next Big Thing**  
by Andreas Philipp  
PAGE 6-7

SECUREMETRIC TECHNOLOGY

A DECADE IN  
**ADVANCING &  
EMPOWERING  
GLOBAL  
DIGITAL SECURITY**

THE BEST

**10**  
YEAR

ANNIVERSARY  
- Since 2007 -

**CENTAGATE**<sup>®</sup>  
Centralized Authentication Gateway

SECUREMETRIC JOINED

# BANKTECH ASIA KUALA LUMPUR 2016



## Kuala Lumpur, Malaysia

- After a series of organizing Banking Technology event in Jakarta and Manila, Knowledge Group of Companies Malaysia held its final regional series of Banking & Technology Conference in Kuala Lumpur Malaysia. BankTech Asia 2016 was held at Nexus Connexion Ballroom last November 8 - 9. SecureMetric is proud to be a Gold Sponsor for this event.

After years of preparation on SecureMetric's latest technology authentication product, SecureMetric introduced CENTAGATE at the BankTech Asia event. CENTAGATE is a fully owned and developed product by SecureMetric.



With the support of Mr. Sea from MIMOS, together with SecureMetric Technology's CEO, Mr. Edward Law, SecureMetric conducted an interesting panel discussion during the breakout session with the topic "Meeting Requirements & Combating Threats with latest Authentication Technology". More than 50 delegates were present during the Day 2 session on November 2, 2016.

These 2-day event were attended by more than 150 delegates from the banking sector of Malaysia and other Asian region. CENTAGATE captures the interest of the delegates. They've visited SecureMetric booth to have a glimpse of the demo for both CENTAGATE on-premise and CENTAGATE UAP versions. A lot of follow-up meetings have been setup to further discuss clients requirement after the event.

SecureMetric is looking forward to introduce this remarkable solution for the banking industry in Malaysia and to urge them the banking sector in Malaysia to actively look into upgrading their authentication platform based on the requirement set by Bank Negara Malaysia



# CENTAGATE®

## NEXT GENERATION AUTHENTICATION GATEWAY *with* ADAPTIVE INTELLIGENCE

- CENTAGATE® On - Premise
- CENTAGATE® UAP
- CENTAGATE® Public Cloud

Technology Recipient

Supported by

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



ORGANISED BY PRIMEKEY,  
19TH – 20TH SEPTEMBER 2016

# PKI TECH DAYS 2016 @ STOCKHOLM, SWEDEN



**This** year's PrimeKey PKI Tech Days gathered approximately 80 International PKI professionals from around the globe at the nice and cozy Huvudsta Gärd Conference Centre, situated in Solna, just a few minutes outside of Stockholm City.

The event has a good combination of interesting presentations from PrimeKey and from various customers and partners from their extensive network. It is difficult to think of a place where you can listen and talk to many experts within the PKI field at the same time.

IoT and Blockchain were certainly an

interesting topic in the market today. Chris Adriaensen from ForgeRock talked about on how to Identify Relationship Management and how PKI evolve in the age of IoT. Primekey's Chief Technology Officer, Tomas Gustavsson discussed about his inspiration and reflection on Blockchain vs. PKI. Both experts definitely blew our minds through interesting in-depth presentations and knowledge sharing.

We are privileged to listened to Ryan Hurst from Google talk and it was even more interesting since he talked about Certificate Transparency and a

C2 Company from USA shared about the ICT and PKI landscape in Silicon Valley. Furthermore, we learned on how to Benefit from e-Signatures and leverage on eIDAS (a PKI directive by the European Union, EU) from Cryptomathic, Guillaume Forget.

As always, when we discuss IT security, we need to know about possible cyber-attacks. This matter was covered as Najwa Aaraj from DarkMatter shared her presentation regarding the Modern Crypto Systems and Practical Attacks. In the same line, we had a well-known cryptographer, PHD Vladimir Soukharev,

who shared on How To Be Ready for Tomorrow's Quantum Attacks. Mr. Soukharev showed us an examples of cryptographic algorithms that can, in fact, resist quantum attacks.

During the event, PrimeKey's team gave the audience a comprehensive product roadmap update for EJBCA Enterprise, SignServer Enterprise and for their PKI Appliances. It was very interesting to learn about how PrimeKey's R&D could incorporate both technology trends and customer demands in different roadmaps. It is not hard to imagine why EJBCA is "probably the best PKI" in the market now.

Last but not least, we were proud to witness Sea Chong Seak from MIMOS (R&D Agency of Malaysia) who talked about his research experiences in the space of PKI for MyKad and the New Trend in Authentication.

In addition to all the interesting presentations, we were invited to a special cruise dinner hosted by PrimeKey. While enjoying a good meal, we were given an opportunity to see Stockholm City, known as "Venice of the North", from the seaside.

All in all, PrimeKey PKI Tech Days is definitely one of the best PKI event we have attended and surely it has already become a "MUST GO" event on our every year calendar.



**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

**utimaco**<sup>®</sup>[hsm.utimaco.com/en](http://hsm.utimaco.com/en)

## WHY ENCRYPTION FALLS SHORT, THE NEXT BIG THING! SURE?



**Andreas Philipp** is Vice President of Business Development with Utimaco, the innovation leader in Hardware Security Modules. With over 15 years of experience in software development, project management and system implementation, Andreas changed to technical sales for HSMs and finally ran the worldwide sales team of Utimaco for over 10 years.

With an overall extensive experience in the Security Module Business of 25 years, Andreas has become a well-known industry expert and a frequent conference speaker.

**The** Internet of Things offers great opportunities in a world where we are connected and online 24 hours a day. Whether in industrial applications, such as medical, automotive and automation technology, or in the private sphere, with its smart TVs and the omniscient fitness bracelet. In all areas of the IoT, we are dealing with data streams containing sensitive information which, in many areas, might even affect privacy.

For years, companies have been busy issuing security policies and the corresponding IT measures such as policies, instructions, procedures and technologies. Even in the private sphere, we have learned how to deal with our data in the virtual world, e.g. when disclosing personal information in online shopping sessions or social networks.

Should all this become obsolete with the IoT? With the introduction of intelligent

connected objects, the doors opened up to connected shop floor systems and Distributed Control Systems. Does this mean established security procedures become obsolete?

Even in the private sector, data collection and transfers happen between a multitude of objects, from our Smart TVs connected to the internet to Smart Watches on our wrists. Where is this collected data stored and who has access to it? Basically, the fundamental question is: Where is my digital self-determination?

The increasing number of security issues over the last years shows that this is not part of a science fiction novel. Examples are the unprotected remote maintenance access to industrial facilities and private homes or the various attacks on automobiles.

Many experts predict that the real IoT



world is still ahead: Consumers and businesses are only willing to activate the IoT concepts they have already prepared after strong IT security measures have been introduced and implemented.

Nonetheless, due to the value proposition and promised cost reduction, we can certainly say that IoT is real today!

### **Cost pressure and IT Security**

A question to start with: How likely is the identification of a potential security flaw that causes product liability consequences for the device manufacturer of a webcam? A webcam today costs approximately 100\$, with a profit margin of 10% - which puts high pressure on the costs of adding appropriate IT security to the device.

This concerns IoT devices for end-consumers but equally applies to the



area of mechatronics and automation, where aspects of cost pressure often drive a cost reduction spiral and may result in low cost = low quality.

The question arises whether considering the security functionalities of IoT devices from a regulatory perspective is not more appropriate? What if there was a kind of technical inspectorate to periodically check whether these “IoT devices” and implementations are secure and trustworthy?

#### **Information Security – Where to start and how to realize it?**

Information security is a very wide and complex domain with different facets to consider. As for the IoT and IoT decides, we observe that economic interests come before security. An HP study from 2015 about IoT devices clearly shows this and

brings the following vulnerabilities to light:

- Poorly secured web applications which are allow cross-site scripting or SQL injection
- Weak user and device authentication
- Unsecured communication channels
- Unsafe pre-configurations
- Basic vulnerabilities in hardware and software

Sure, we can address the symptoms with appropriate countermeasures but – much more important – the causes need to be eradicated. Why are the device web applications so poorly secured? Why are errors that have been corrected long ago (when company websites started emerging) made again?

Do we give too little attention to security and safety when it comes to software development? Agile software development methods allow us to minimize the administrative burden and enable highly dynamic creation of software. But what is required is an appropriate security concept & measures across the entire lifecycle of an application or product.

But let's get back to the vulnerabilities that had already been addressed in the past. The change in software development is certainly one of the reasons why these "old" faults re-occur. But more generally speaking, dedicated security testing is needed in addition to common test pattern. These tests range from classic scanning of known vulnerabilities to detecting even unknown vulnerabilities by using fuzzing tools (confrontation of a system with random values to produce a misbehavior).

#### **Embedded or not?**

Let's now look at IoT devices and hardware. Basically, we are dealing with computer systems embedded into devices, systems or machines and the very special task of control, take over control to communications. These embedded devices – as opposed to personal computers – do not have the "usual" peripherals like mouse or keyboard.

With the introduction of embedded system such as Arduino or Raspberry Pi, it is now a days possible to start into the adventure of embedded programming directly. The focus here should be on the facet of security, where security problems subliminally but steadily open up due to faulty implementations in software and hardware:

- What if a programming error causes a command to target a wrong part in a supposedly protected RAM area?
- Vulnerabilities that are located in the hardware design of such units are very hard to detect.

Another important point to consider is whether IoT devices are designed on hardware that withstands side channel attacks and of which level – which brings us back to the importance of security testing.

Protection of privacy versus self-determined action

Basically, you can extend this list of security issues in the area of IoT eternally. Depending on the IoT system and the application, security measured need to be taken accordingly. However, at this point, we should take a look at another player in this game: the user!

Why should businesses invest in security when – on the other side – millions of users in social networks spread personal and private information (about holiday destinations and timing) and reveal their entire consumer behavior for loyalty programs like “Miles and More” or PayPal?

Let's say that, as a conclusion, IT security together with safety and privacy measures should certainly be implemented via regulations and inspections. But on the other hand, it is hard to deal with the stupidity of end-consumers...

# TALE OF TWO SYSTEMS

## UNIQUE COMBINATION BETWEEN SWIFT AND SECUREOTP APPLICATIONS

**SWIFT** is a global member-owned cooperative and the world's leading provider of secure financial messaging services. SWIFT's messaging services are used and trusted by more than 11,000 financial institutions in more than 200 countries.

With recent hacking involving SWIFT infrastructure, millions of dollar could be "transported" to cross boundaries and even in continents. The financial impact will be un-imaginable; SWIFT itself, usually deployed as its own island within the financial institution network but still hackers manage to gain access to SWIFT via impersonation.

Naturally Financial Institution wants to increase the security accessing SWIFT application and one of the requirement is to implement MFA (Multi-Factor Authentication).

This is unusual applications that requires authentication that is meant for external customers such as Retail or Corporate Internet Banking.

The case below is one of the exceptions:

SecureMetric had been requested by BankA to propose a solution for SWIFT to increase the security authentication for it's own personnel via Multi-Factor

Authentication.

With the limited knowledge of SWIFT Alliance Access (SAA) application, we need to look in-depth to the software for any supported interfaces. The best solution provided needs to observe the following factors:

1. Should reduce the system down time
2. Minimize the development work or modifying the software source code (in this scenario, any development is out of question)
3. Minimize impact to users experience,
4. Reduce integration time

With the assistance from Bank A, we





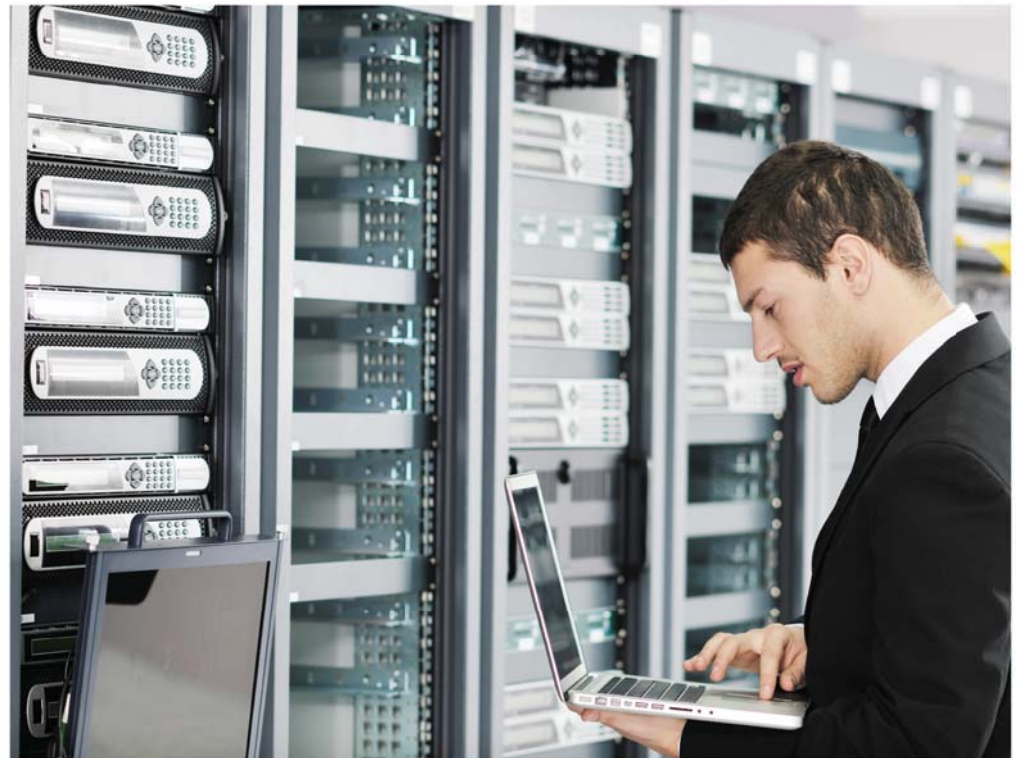
notice that SWIFT application does support Radius Protocol by default and so does Secure Metric's product, SecureOTP. One-time Passwords? Words that sounds familiar to us ?

Let's differentiate the meaning of One-Time Password and RADIUS.

One-time passwords (OTP) is a password that is only valid for only one login session, certain time or transaction, which may assist by OTP tokens. OTP tokens can display some length of digits and always change with some criteria such as time, click event etc. Every OTP has different seed code and that's the reason every OTP tokens will generate different OTP even the tokens that is manufactured by same factory.

Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized Authentication management for users who connect and use a network service. All the data communication is encrypted by shared key that was agreed by RADIUS server and client.

With support of OTP and RADIUS, we proposed a solution that uses our SecureOTP Authentication Server with OTP token to integrate with SAA. SecureOTP Authentication Server provides authentication service to the client. No code changes or any file changes to the SAA software, but only configuration changes from administrator console.



Technically, the SAA will be configured to forward authentication via RADIUS to SecureOTP Authentication Server. SecureOTP Authentication Server will perform authentication and return authentication result back to SAA. SAA will digest the result and will allow or reject SAA user login based on the result.


The integration was seamless, UAT was flawless and implementation was smooth. Each SWIFT user were presented with an OTP token and they would used it whenever they need to login into SAA.

Bank A then decided to integration the other payment gateway with SecureOTP

for MFA. The payment gateway vendor was able to integrate with SecureOTP using web services (SOAP). SecureOTP then has become Bank A's internal enterprise authentication platform for payment gateway related application.

This is a tale of how a simple request to implement MFA for an internal payment gateway application has grown into an enterprise wide internal authentication platform for payment related gateway system.

We encourage you to talk to us today and who knows, there might be another tale to tell.



**Trustworthy Voice and Message Encryption**

For more information please visit • [www.securemetric.com](http://www.securemetric.com)

# HOW CAN BANKS PROTECT THEIR CLIENTS AGAINST IDENTITY THEFT/FRAUD?

**I**N a recent report, 55 million Filipino voters information were leaked in the internet and those with bank accounts are now susceptible to fraud and other risk similar to identity theft. Names, Addresses and Birthdates that are considered vital and valuable were exposed to the public which can be used to identity fraud. Identity fraud occurs when fraudsters have an enough information about person's identity which engage to the misuse of personal data in order to commit crime and it has a huge impact on personal finances. Some of the identity theft and fraud are not only done through online, at times having someone's information is enough to steal identity and assets.

Bank industry are thinking of possible solutions in fighting this hideous crimes, one of the top banks in the Philippines is considering Fingerprint Verification in order to protect their clients who were affected by the said data breach.

Fingerprint Verification. Authentication and Verification techniques are now leaning towards the use of fingerprint since it is harder to fake something you are than to fake something you have or something you know. Fingerprint recognition is a common technique that is widely used and becoming a popular form of account access.

Fingerprint Verification can help bank clients against breach of information. Fingerprint verification have a higher security in authentication and verification of account holders, it ensures the



confidentiality of information in storage or in transit. Also, it will protect institutions for making the transactions as non-repudiation which in turn will be deterrent to identity theft. It is convenient, safe, non-intrusive, and reduced administration costs compared to passwords and other way of verification such as ID Cards.

As a South East Asia's market leader in the digital security industry and serving clients across the world, SecureMetric Technology offers Secugen Biometrics Solutions' Hamster Pro 20 fingerprint scanner. Hamster Pro 20 is an ultra-compact and rugged design USB Based fingerprint scanner industrial grade device which can easily be deployed on the branches.

#### Hamster Pro 20 Benefits and Features:

1. Create confidence and high trust to your client that you are using a high quality and certified fingerprint scanner.
2. Fast and Easy deployment to different branches

3. Rugged, Heavy Duty and Maintenance Free

4. Makes customers at ease that their sensitive information are highly secured  
FBI and STQC Certified, FIPS 201 Approved List and FAP 20 Compliant  
Ultra-compact, lightweight and portable  
IP65 rated for dust and water-resistance  
Sensor resistant to scratches, impact, vibration and electrostatic shock  
Encryption of fingerprint templates (with SecuGen Proprietary templates)  
Latent print image removal (does not accept prints left behind)

5. Auto-On™ (Automatic Finger Placement Detection) Scan your finger as soon as you touch the sensor – all without having to prompt the system.

6. Smart Capture™ (Automatic Image Adjustment to Accommodate Moist & Dry Fingers) Ensures quality fingerprint scanning of difficult fingers

7. Low Cost  
Quality & solid built-up but comes in a competitive pricing

# STAY PROTECTED AND AVOID HACKERS FROM STEALING YOUR INFORMATION

## BUSINESSES

like hospitals, governments, banks, academies and corporations are mostly affected by cyber attack and fraudulent transaction since these industries has a vital data that provide precise, timely and absolute personal information shared by their customers. With the wide digital transformation, there are a lot of ways cyber criminals are using in stealing such data. Stealing of information can be through email and online account (e.g social media, online banking and the like).

Having a weak code is one cause of security breach, password are use to restrict unauthorized person to utilize their personal account and to protect their data from cyber criminals. Through password, the security of personal data is assigned to users of particular system rather than the administrators, that's why people are always reminded to have a lengthy and intricate password which it will be harder for the attacker to gain access to user's credentials. Most of people reuse passwords for their different accounts and this is risky as hackers could access their personal account. But can a single password is enough to secure people from hacking? Strong passwords are essential to protect someone's online accounts but having two-factor authentication is more secure than relying on a single password. Having a password alone is not enough to be protected since it is easy to guess and to

crack.

Two-factor authentication adds an extra step in basic log-in procedure and it can reduce the rate of online fraud. It requires both something you know which is the password and something you have which can be a phone or a token .By using an One Time Password Token it could be the best choice of authentication method to strengthen system security.

Security is extremely important today and companies whether big or small can no longer be safe from any cyber attack. In the world of

technology, change is inevitable and it is important to stay ahead of the curve, by using two-factor authentication is a big step to keep away from hackers. Also, people should be aware and educated on the possible ways on how their credentials can be protected and make sure that they use distinctive and secure password for each of their online account.



# SOFTWARE SECURITY THROUGH HARDWARE

**Security** is an issue that everyone would want to have and attain — may it be personal security, national security, network security and information security, but in the advanced world of software industry the most vital of things to secure is the intellectual property. It is necessary for every Software Developers to have a solid grasp of intellectual property rights and apply it to the Software Industry.

Software Developers need to have a broad knowledge about their rights to develop and to protect their product. They have to ensure exclusive ownership, confidentiality of their work to have an advantage in the competitive market. With the rapid growth of technology, software firms are looking for a simple and cost effective way

on how software can be protected.

Now, you might be wondering what could be the most effective, possible way of protecting software's — is it by using encryption code which among others is most commonly used by developers as it allows them to decrypt the code or is it much more secured if the developers have a software security through a hardware? Protecting software using codes and license can be effective and more cheaper, however, it may not provide full security that a software needs. Today, encryption system can be hard for people to crack or decode, but the advances in technology and software development could make it effortless for them to pirate the software.

Industry experts agree that the

hardware-based protection provides maximum security as it avoids to abuse the software. This hardware protection is known as a dongle or USB hardware key, a device incorporated with the software. It controls the end-user on how to use the software and the end-user's access to the software is managed by the dongle. Security based upon hardware is more convenient, functional and it is harder to modify.

Whichever security protection you decide to make use of, be sure that it matches your software's need and you have a good knowledge of how it works and how will it be beneficial for you or your business. And of course, you have to consider the level of security that your software requires.

**THE DANGEROUS WORLD OF SOFTWARE PIRACY**

Commercial Value of Unlicensed PC Software, 2013 (B\$)

Country	Value (B\$)
United States	\$9,737
France	\$2,685
China	\$8,767
India	\$2,911
Brazil	\$2,851

Incident Rates

Category	Rate
Software Piracy	16%
Malware	75%
Phishing	14%
Denial of Service	>5%

Incident Rates

Category	Rate
Software Piracy	77%
Malware	60%
Phishing	36%
Denial of Service	28%

Direct Download

Waste, Ingress, Misconfig, Redundancy

**Smarter Way To Protect Your Software**

For more information please visit • [www.securemetric.com](http://www.securemetric.com)

# THE IMPORTANCE OF SOFTWARE PROTECTION IN THE INDUSTRY AND ECONOMY

**According** to software alliance, “more than four out of ten software programs installed on personal computers around the world were stolen, with a commercial value of more than \$51 billion.” In this case, not only the revenue of the company is affected by this illegal activity but the economy as well.

Most software firm in different countries have problem on illegally distributed software. Some of the businesses buy licenses for a limited number of computers and install it to more than the number of computers allocated for them. Piracy has a big impact to software industry, making it less profitable, that’s why software

industry are taking serious actions in protecting their revenues and if piracy will lessen, the economic benefit will increase. It also devalue the work of Software Developers which can lead to loss of jobs. Study shows that lowering software piracy by just 10 percent would create bigger amount of employment rate.

So, the question is how can we resolve this piracy issue? Software Developers are implementing different means of lessening piracy by changing on how software is distributed to make it harder to decrypt the code. With a wide range of security options, developers also considering the cost will be in terms of resources and time

on deciding on what possible security system should they implement. Software Developers use the profit from selling the software’s in continuing research and development for continuous advancement and innovation of technology. Developing software is a team effort from the developers, sharing their creative ideas to develop useful software’s. At the end of the day, educating staff on this matter is one of the most important ways in helping to ensure software compliance to benefit all developers and organizations affected by this piracy issue.



# FINTECH LATEST TRENDS



**SERVICE-BASED INVESTING**  
Upcoming industry of paid services around low-cost investing



**DIGITAL-BASED EQUITY CROWDFUNDING**  
Digital platforms offering accredited investors the option to fund seed and early stage companies



**ROBO INVESTING**  
Online wealth management service providing automated, algorithm-based portfolio management advice without using human financial planners

# THE TRENDING FINTECH STARTUPS



**18.8%**  
Data analysis for better decision making



**14%**  
Payments and International Transfers



**13.4%**  
Lending



**11.3%**  
Small Business Financial Solutions



**6.5%**  
Bitcoin



**6.5%**  
Identity



**6.5%**  
International Transfer



**5.9%**  
Mobile



**5.9%**  
Shopping



**5.9%**  
Blockchain



**5.4%**  
Personal Finance



**1.6%**  
Banking

# TOP REASONS WHY CONSUMERS ADOPT FINTECH SOLUTIONS

**1.8%**  
Greater level of trust than the traditional institutions

**5.5%**  
More innovative products than available from traditional bank

**10.3%**  
Better quality of service

**11.2%**  
Better online experience and functionality



**43.4%**  
Easy to set up an account

**15.4%**  
More attractive rates/fees

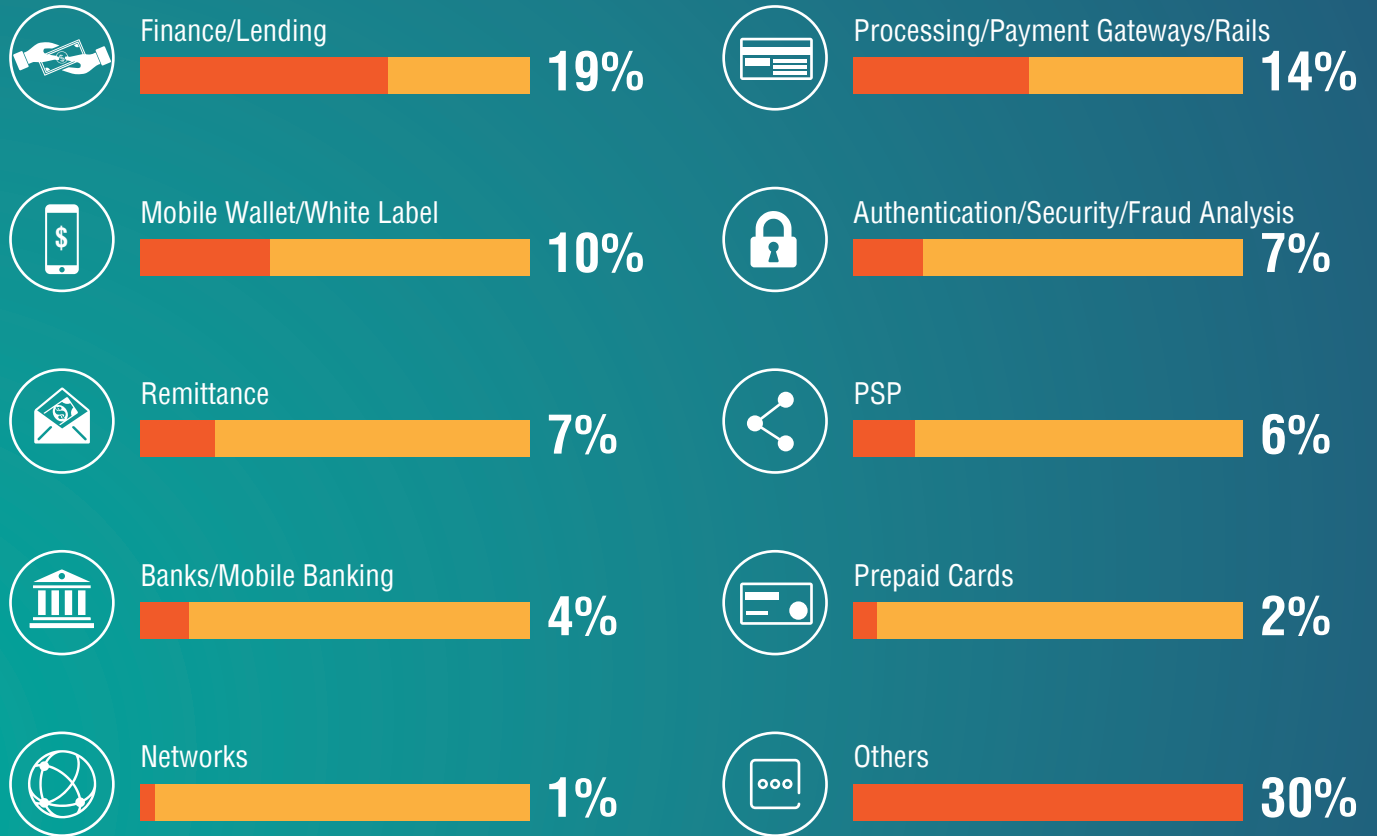
**12.4%**  
Access to different products and services

# FINTECH

The Disruption in



# FINTECH INVESTMENT CATEGORIES



IN 2013 & 2014



## FINANCE/ LENDING COMPANIES

Attracted **\$567 million** in funds, the largest compared to other categories



## PAYMENT RAILS COMPANIES

Raised **\$416 million**



## MOBILE WALLET COMPANIES

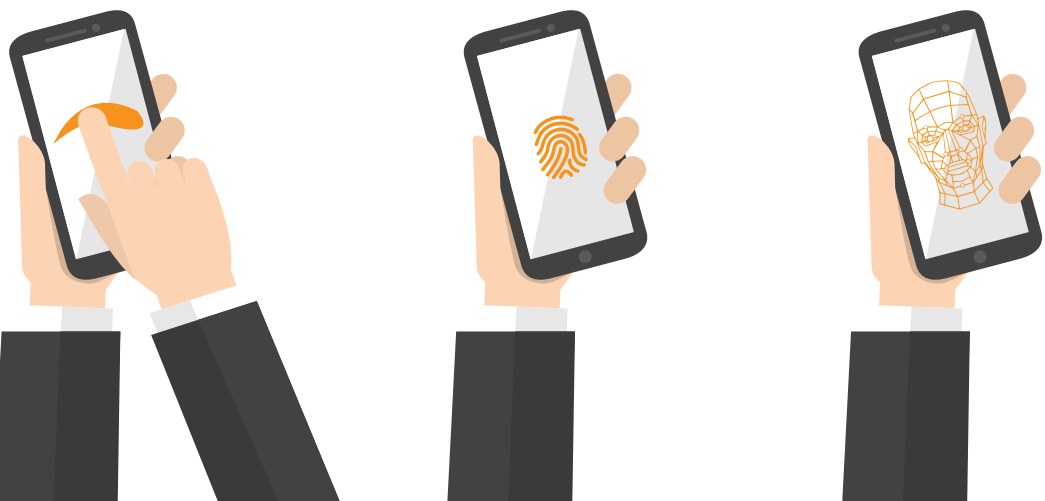
Raised **\$286 million**

# ECH

Digital Finance

## PAYMENTS IN THE BLINK OF AN EYE

PAYMENT AS EASY AS A **TAP, TOUCH** OR A **BLINK**





## CENTRAL BANK UPDATE A NEW POLICY

**I**n the beginning of 2016, there is a surge of requests from financial institutions to upgrade the security features these requests ranges from enabling Multi-Factor Authentication (MFA) for Retail and / or Corporate Internet Banking Portals to Secure Remote Access Applications.

The surge of requests may be attributed to the recent internet hacking incidents that made it to the worldwide headlines, prompting the various central banks to issue instructions for financial institutions to further enhance the security feature for both customer facing application such as internet banking or remote access applications egvpn / remote desktop service.

According to Wikipedia.com, “In February 2016, instructions to steal US\$951 million from Bangladesh Bank,

the central bank of Bangladesh, were issued via the SWIFT network. Five transactions issued by hackers, worth US\$101 million and withdrawn from a Bangladesh Bank account at the Federal Reserve Bank of New York, succeeded, with US\$20 million traced to Sri Lanka (since recovered) and US\$81 million to the Philippines (about \$18 million recovered). The Federal Reserve Bank of NY blocked the remaining thirty transactions, amounting to US\$850 million, at the request of Bangladesh Bank”. This incident must be one of the biggest heist of all-time, prompting a string of resignations from the governor of Bangladesh Bank to the presidents of banks that were implicated in the scam. This is probably the first incident that involves government agency with private financial institutions via a global banking network.

Key weaknesses have been attributed to lack of proper anti-virus software for desktops, used to fulfill the transactions in-adequate network protection devices such as firewall and lack of remote access control procedures.

We need to be aware that SECURITY for both local and remote user access is no longer an afterthought or just barely fulfilling a checklist for compliance purposes. The impact can cost hundreds of millions, and hackers are using more complicated methods and tools of gaining access or trust to global financial network.

Investing into network protection devices is compulsory and highly recommended to secure user access via Multi-Factor Authentication. Username and password is insufficient to access high value transactions related applications. We need to wake up and face realities.





## SECUREMETRIC JOINED ISOG SUMMIT 2016

### MANILA, Philippines

- Information Security Organization Group (ISOG) aim to build a culture of Information Security through ISOG Summit held last September 29-30 at SMX Convention Center, Taguig. ISOG is a team of Chief Information Security Officers (CISO) from different financial institutions with a mission to strengthen information security through awareness and education programs within Philippines' banking and financial sector.

This two-day event addresses cyber-threats to the advances of technology and how these threats can be resolved. The event was a success attended by more than 250 delegates from public and private sector, vendors & service providers, policy makers, government and leading associations with the latest industry standards with regard to cyber-security. Fraud Management, Establishment of Cyber-Forensics Teams, Security Incidents and Events Management (SIEM), Establishment of Security Operations Centers (SOCs) were some of the topics highlighted during the summit and has been tackled by thirty-five (35) resource speakers that is comprised of law enforcement, corporate world, legal specialization of cyber law and industry leaders.

Mr. Manuel Joey Regala, ISOG's president and founding member delivered the opening remarks, he explained that constant vigilance by way of policies, procedures, technology solutions and total participation by all of an organization's stakeholders is the most effective antidote to digital threats. "Organizations must now connect and collaborate with other organizations in their respective industries as well as with other organizations in other industries, they must also coordinate with government policymakers and law enforcers", he also added.

Over 30 exhibitors joined the summit and as a South East Asian market leader in the

digital security industry, SecureMetric Technology was one of the exhibitor who participated in this historic event organized by ISOG and was privileged to be part of it. Numerous delegates visited SecurMetric booth and showed interest on the solution and products that are suitable for organizations of different industries and of any size. SecureMetric offers a wide array of digital security solutions to help clients defend their business against the latest security threats and risks.

ISOG Summit was a good avenue to learn and be aware of strategies and methods with regard to information security



# IMPROVEMENTS ON ELECTRONIC TRANSACTIONS

## HANOI, Vietnam-

The South East Asia's market leader in digital security, SecureMetric Technology together with Malaysia's Information and Communications Technology Research Center, MIMOS and the worldwide supplier of professional cyber security solution, UTIMACO, joined forces to present a seminar that focuses on the analysis of Centralized Authentication Gateway solution (CENTAGATE) with UAP, a new authentication technology that integrates many different authentication methods that helps to mitigate network attacks. The seminar theme is "Authentication in full Information". It was held last August 2, 2016 at Intercontinental Hotel, attended by IT Directors (CIO) from the bank, Officials in charge of Safety Information from Financial Institutions and Insurance in Vietnam.

Mr. Kang Siong, an expert from Center for Research and National Development of Malaysia (MIMOS) mentioned that today and in the near future, the use of traditional authentication method (eg: User Name and Password) will still be common in any online transaction and this basic authentication has a lowest form of security unlike with One-Time Password(OTP), Certificate, Token, Bar Codes and the like. By using a weak password there will be a big chance of hackers to steal personal information that can be used to any cyber crime. There were issues raised that using a multiple separate authentication method in similar transaction will be difficult for the user since it will take more time and still have the risk of any vulnerability. Mr. Kang Siong shared his knowledge on how CENTAGATE with the new UAP

authentication technology could play a vast role to overcome this kind of vulnerability.

CENTAGATE integrates different authentication method. For instance, using smart phones to create a password and a barcode to be scanned through laptop camera to identify and to have access.

IT Director of Prime Minister office, Mr. Ahmad Zulkfi is one of the speaker who discussed his experience in using authentication solution for the Agency of the Government of Malaysia specifically in the Finance Ministry. According to him, the Government of Malaysia is using Centralized Authentication Solutions since 2013, "This solution has a high stability, continuous 24/7 operation, fast response time, reduce costs and no incidents happened since I used the application", Mr. Zulkfi added.

Evaluation of information security incidents takes place in Vietnam in recent times. CIO office, Malaysian Prime Minister and SecureMetric Technology's Chief Executive Officer, Mr. Edward Law shares the security concerns of full information that the agencies and organizations in Vietnam are currently experiencing. They stated that since 2013, the agencies and organizations of Malaysia also suffered from numerous hacker attacks on the



service system.

A strategy for security and safety information that is applicable to the agencies and organizations has developed by the Malaysian government in which it emphasizes the authentication solution. Hence, Malaysia has lessened the attacks on network.

Questions from the delegates were entertained by technology experts, most of delegates concern is about the feasibility of solutions, compatibility with the software being used in the organization. Delegates express their interest in the new Authentication Solution offered by SecureMetric Technology.

SecureMetric Technology develops robust enterprise security solution with all the essential product and service to meet client's needs in the most cost and time effective manner, based in Kuala Lumpur with subsidiaries in Hanoi, Ho Chi Minh City, Jakarta, Yangon, Singapore and Manila. With more than 15 years of security experience in serving clients across the world.

SecureMetric Technology has successfully implemented many projects for Multi-Factor Authentication and Public Key Infrastructure(PKI) security projects both private and public sector.

## 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



South East Asia Value Added Reseller Partner



# Signing Hub

www.ascertia.com  
www.signinghub.com  
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, all 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 airmail.

I approve this document  
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

## SECUREMETRIC JOINED ITIP NATIONAL CONFERENCE 2016

### BAGUIO CITY, Philippines

I.T Interaction Philippines (ITIP) held their 13th Annual National Conference last November 10-12, 2016 at Camp John Hay Trade and Cultural Center in Baguio City. I.T Interaction Philippines (ITIP) is a non-stock and non-profit professional organization of large IBM users whose members are represented by high-level management from companies belonging to the top local and multi-national corporations. These three (3)-day event intended to strengthen the organization's objective, which is to serve as a venue and opportunity for exchange of common IT-related professional interests among its members.

More than 300 delegates from banking and finance, utilities, telecommunications, manufacturing, distribution, retail, government and software integrators were present during the event to broaden their knowledge on the New Trends in Technology that they can utilize in their respective industry. This year's convention theme was "ITIP Cognitive Convergence: A Meeting of Minds and Technologies". During the first day, 2016 ITIP President, Mr. Roseller Lim welcome the delegates. Opening remarks was delivered by IBM Philippines' President & Country General Manager, Mr. Luis Pineda and DICT Chief Atty. Rodolfo Salalima conducted the keynote presentation. Baguio City Mayor, Hon. Mauricio Domogan was also present during the event.

There were twenty-six (26) foreign and local influential speakers talked about current issues, management, new developments in technology that has an impact in the business industry. One of the topic discussed is about the new cloud era

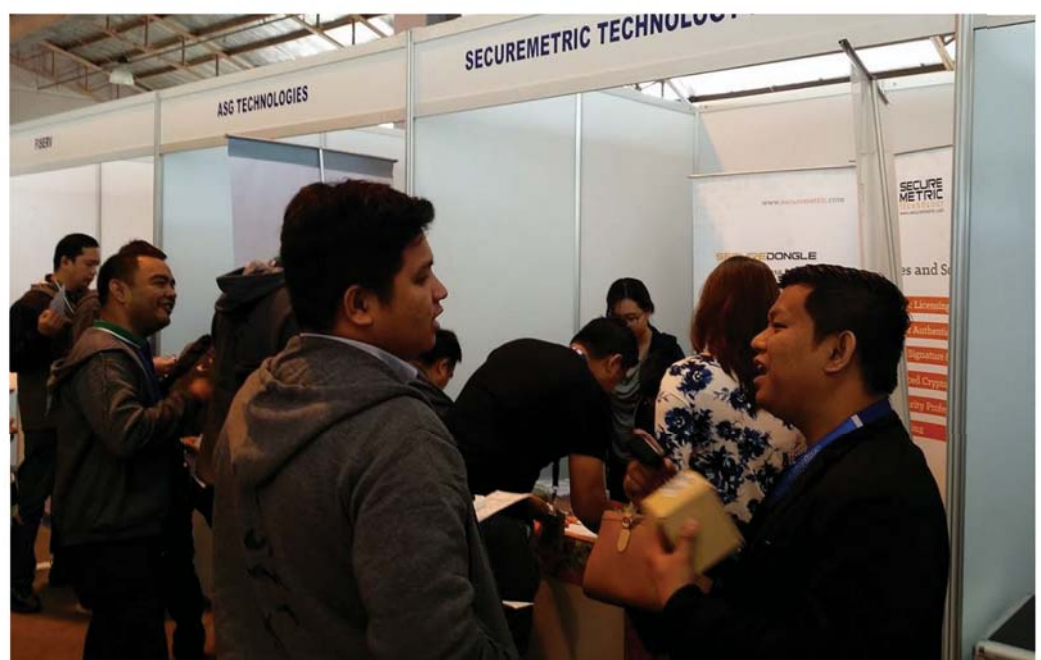


and big data storage, the speakers explained on how these advancement in technology can be a benefit in their business strategies. Delegates were also educated on the cyber security and its transformation.

There were twenty-one (21) companies from diverse industries sponsored the

event to show support to ITIP and as a digital security provider, SecureMetric Technology participated as one of the exhibitor in the said event. SecureMetric Technology was able to informed people from varied business about the importance of cyber security in their industry. These three(3)-day event helped Securemetric Technology to addressed and understand clients digital security needs that will help to improve SecureMetric's products and services. With wide-array of products and solution that SecureMetric Technology has to offer, delegates from the event showed interest on SecureMetric's Two-Factor Authentication Token ,CENTAGATE, Biometric Solution and Signature Pad.

With the vast cyber attack that is happening in the business industries, SecureMetric Technology will continue to identify technology trends and will develop solution that can help their clients to defend them against latest security threats and risk.



# SECUREMETRIC JOINING TECHMART HANOI 2016

## Hanoi, Vietnam

Technology and equipment fair was held annually with the aim of supporting and connecting organizations to have the technology and equipment be recognized by the companies. Techmart organized exhibitions which products were introduced and promoted through media activities and trade promotion before, during and after the fair. Domestic and foreign firms also have the chance to introduce and sell their products and technology on the event. With the collaboration between Hanoi City People's Committee and the Ministry of Science and Technology, Technology & Equipment Fair 2016 (Techmart 2016) was held at the Museum of Hanoi, Pham Hung street, Me Tri, Nam Tu Liem District, Hanoi.

Techmart Hanoi 2016 took place from 28

September to 01 October, 2016. The convention has more than 430 booths displaying their products and technology. There were more than 30 booths from foreign countries such as Japan, Germany, China, Korea. There were also participating booths from the provinces, cities, universities, colleges, research institutes of defence ministry, state institutions, enterprises, organizations and individuals with products and new technology.

Products and Technologies were introduced at Techmart Hanoi 2016 focused on the information technology field, electronic products, production line automation, mechanical products, manufacturing machinery for agriculture, industrial, transportation, urban management, preservation technology, agro-forestry-fishery, food, high-tech

agriculture, plant varieties, animal breeds of high economic value, environmental treatment technologies, technology and equipment for ancillary industries.

SecureMetric joined Techmart Hanoi 2016 to introduce its security solutions and products to the Vietnam market and Southeast Asia region. SecureMetric also introduced PKI in a Box, Centagate, Software License Protection, Fingerprint Reader, and Card Reader to delegates and visitors who visited the booth. Our products and solutions caught the attention of the visitors during the exhibit. SecureMetric has been invited to several follow up meetings after the event. SecureDongle, RFID reader were among the top enquire products in this event and SecureMetric is looking forward to close some of its leads they got from the event.



## SECUREMETRIC JOINED THE 3RD CYBERCRIME SUMMIT



### MANILA, Philippines

– Last March 15-16 2016, the Anti-Cybercrime Group (ACG) and the Philippine National Police (PNP) cybercrime unit, in partnership with Philippine Computer Emergency Response Team(PhCert), Philippine Institute of Cyber Security Professionals(PICSPRO), Bank Security Management Association (BSMA) and

Information Security Officers Group (ISOG) helped hand in hand in organizing the 3rd Cybercrime Summit at the PNP Multi-Purpose Center in Cramp Crame, Quezon City. These two-day event focused on the theme “Sustainable Economy through Cyber Security”. PNP Anti-Cybercrime Group Acting Director, Police Senior Superintendent Guillermo Lorenzo Eleazar welcome the Top

Top Executives and Senior Information Security Officers from Business Sectors, Government, Civil Society and Academe.

The delegates were informed on the latest forms of cybercrime and how it affects the economy during the summit. There were twenty-three expert resource speakers who shared their thoughts on how businesses can be protected from the harm that these cybercrime can cause. Online Scams, Impact of Intellectual Properties in Cybercrime and Technical Perspective of Cyber Security were the topics that has been given the utmost importance during the seminar. Nonetheless, all the other topics that were discussed are useful especially now a days that cybercrime has continued to grow and has become a serious problem with an immense effect on individuals, businesses and national economies. There was a panel discussion where delegates were able to provide an opportunity to ask questions to the speakers about cyber security and also, give their different point of view on the said topic.

Having the capacity to protect its clients from the latest threats and risks, SecureMetric Philippines participated as a Silver Sponsor on this two-day event. SMPH was able to market and introduce its products and solutions to the attendees as the convention is relevant to the service and product that SMPH offers.

SecureMetric Philippines’ Vice-President & Country Manager, Ms. Aimee Asanza received a plaque of appreciation had the privilege to award the Samsung A5 hand phone to the raffle winner.

**CRYPTOMATHIC**

**Key Management Solution**

For more information please visit • [www.securemetric.com](http://www.securemetric.com)

## SECUREMETRIC JOINED CHAMBER OF THRIFT BANKS ANNUAL CONVENTION 2016

### MANILA, Philippines

SecureMetric Technology has participated as a minor sponsor to the 2016 Chamber of Thrift Banks Annual Convention last March 18 at Dusit Thani Manila, Makati City. Chamber of Thrift Banks is the umbrella organization of the country's thrift banks and was organized primarily to provide an institutional medium through which members can collectively assist and cooperate with one another, as well as with other members of banking sector, the national government and its instrumentalities, more particularly the Bangko Sentral ng Pilipinas (BSP). It aims to promote, develop, expand and strengthen the role of savings and loan associations, private development banks and savings and mortgage banks (otherwise known as thrift institutions).

This year's convention theme is "Sustaining the Momentum for Inclusive Growth", attended by different members bank, information technology experts and other institutions. Tech-enabled consumer lending, credit bureau services, economy, banking facility/technology for thrift banks and credit information system were the highlighted topic during the event. The ribbon cutting ceremony was conducted by Bangko Sentral Deputy Governor, Mr. Nestor Espenilla Jr., RCBC's President & CEO and CTB President, Mr. Rommel Latinazo, City Savings Bank's President & CEO and the Convention Chairman, Mr. Catalino Abacan to open the exhibit followed by the keynote address delivered by Bangko Sentral ng Pilipinas Governor, Hon. Amado Tetangco JR. Chamber of Thrift Banks' induction of officers was also held during the convention.

SecuMetric's Senior Manager for Pre-Sales, Mr. Chew Eng Siong is

privileged to explained to the delegates on how to prevent and defend their business from cyber attack through CENTAGATE, since bank industry has always been a victim of fraud and scams. He also share the recent security breaches and how cyber criminals are getting innovative, exploiting security loopholes, taking advantage of the unawareness of the

people about cyber security.

The convention has been an excellent avenue for exchange of ideas, knowledge and perspective not only to promote well-being of the thrift banking sector but also to see possibilities toward contributing to the country's social and economic goals.



# BANK TECH ASIA 2016: WHERE BANKING MEETS TECHNOLOGY

## MANILA, Philippines

With an impressive track record in developing and running cutting edge business related events, conference, workshops and in-house training program, Knowledge Group of Companies is behind the success of the 8th Annual Premier Banking Technology Event held at Dusit Thani, Makati last May 24-25.

Endorsed by Malaysia Digital Economy Corporation (MDEC), Banking Technology Asia is a conference for banking technology and fintech enthusiast to have a better idea and anticipation of the banking technology future.

More than 60 delegates from Top Management, Business Units & Supporting Units and Information Technology of different banks in Singapore, UAE, Malaysia, Vietnam, Pakistan, Bangladesh and Philippines were present during the event. Bank Tech Asia's organizing chairperson, Mr. Vincent Fong welcome the delegates. These 2-day



event address various topics on the opportunities and strategies on how technology can integrate in the banking industry, expert speakers also explained that the advances in technology allows the bank products and services more convenient and effective to use.

SecureMetric's Chief Executive Officer,

Mr. Edward Law together with eProtea MSC's Managing Director, Mr. Jeffrey Fok-Boon Hung, iPay88's Technical Director, Mr. Khong Kok Loong shared their insights about FSI versus Cyber Criminals. Akati Consulting's Chief Executive Officer, Mr. Krishna Rajagopal facilitated the panel discussion. In the discussion, it was intricate that the cyber criminals usually involve illegal access on one or more computer systems to steal information and it is currently experiencing by the banking industry. By having an intensive background in btechnology, panelist gave their opinion on how to prevent and resolve this hideous crime.

SecureMetric Technology participated as one of the event's exhibitor and took the opportunity to market its products and services that would meet security requirements of the banking industry compliance. CENTAGATE, is a SecureMetric solution that can help to prevent and defend bank industry from cyber attack.





## SECUREMETRIC JOINED RSA CONFERENCE 2016

### SINGAPORE- RSA Conference 2016

The world's largest information security event, was held last July 20-22, 2016 at the Marina Bay Sands Singapore. RSA Conference conducts information security events around the globe that connects business people to industry leaders.

This three-day event have informative sessions with five tracks which tackled Cloud, Mobile, Iot Security, eFraud, Law Enforcement, Global Perspective, Security Strategy, Data Security, Threats and Threat Actors. The event was attended with around 6,200 registrants that featured more than 85 speakers and has an intensive learning sessions that focuses on the latest information security issues and strategies. Attendees were informed about the swift changes currently happening in the industry and keeping them in line with the advanced defence against cyber threats.

Opening address was delivered by Singapore's Minister for Home Affairs & for law, Minister K Shanmugam, in which he highlighted the Ministry of Health Affairs' strategy in fighting cybercrime by arranging future plans and priorities. RSA President Amit Yoran was the keynote speaker during the event, whilst the closing keynote was led by Bob Geldof, a well renowned musician known for his political activism particularly in his anti-poverty efforts.

Another part of this event was a panel discussion wherein one of the topics discussed was about, "Asian nation get smarter, but are they more secure?". The panellist included were International



Association of Privacy Professionals Chairman Hilary Wandall, Ernst Young Asia Pacific Cyber Security Leader Mr. Paul O' Rourke, Head of Cyber, Commercial Solutions, JAPAC, Bae Systems' Mr. Alex Traverer and RSA's Chief Technology Officer Mr. Zufikar Ramzan.

More than 100 eminent exhibitors in different region showcased their current cyber security products and solutions. SecureMetric Technology and UTIMACO were one of the various

exhibitors that exposed their innovative technologies that can help secure and protect businesses against digital threats and risk.

Primekey was also present during the event and visited SecureMetric and UTIMACO booth. Primekey has been in partnership with SecureMetric Technology and UTIMACO. These companies joined forces together to defend their clients in any possible cyber attacks.



# CENTAGATE UNIFIED AUTHENTICATION PLATFORM

Adaptive Multi-Factor User Access and Transaction Security

Organisations with multiple enterprise systems require optimised and centralised multi-factor authentication with single sign-on capabilities across a wide variety of business units and functions. The complexity of managing user IDs is moving towards seamless identity management using a trust model as a framework.

## What is CENTAGATE® UAP?

The research and development of CENTAGATE® UAP based on SAML 2.0 Specification addresses problems related to the increase of operational risks attributed to users and system administrators who control and provide cross-application functionalities in heterogeneous applications.

The growth of heterogeneous applications in an enterprise is inevitable due to the proliferation of web-based applications available; within a firewall in an Intranet or even outside a firewall in the Internet to run application services.

CENTAGATE® UAP is designed to manage front-end application authentication using an established protocol, Secure Assertion Markup Language (SAML) protocol, which provides a centralised authentication framework and aims to reduce significant application changes at the backend.



## Advantages



Containment of Operational Risks

Identification of usage and activities can be centrally tracked and traced. This delivers organised data integrity whereby a single source of information can be properly managed for a user life cycle i.e. registration, activation, deletion, termination and so on.



Reduced Cost

Minimise multiple changes result to less impact and reduced cost as the platform is managed centrally.



Amplified Productivity

Cross-functions features enable stakeholders to benefit enterprise-wide from system owners, to system administrators, to system developers and system users. These benefits can be translated from resources into terms of time and money.

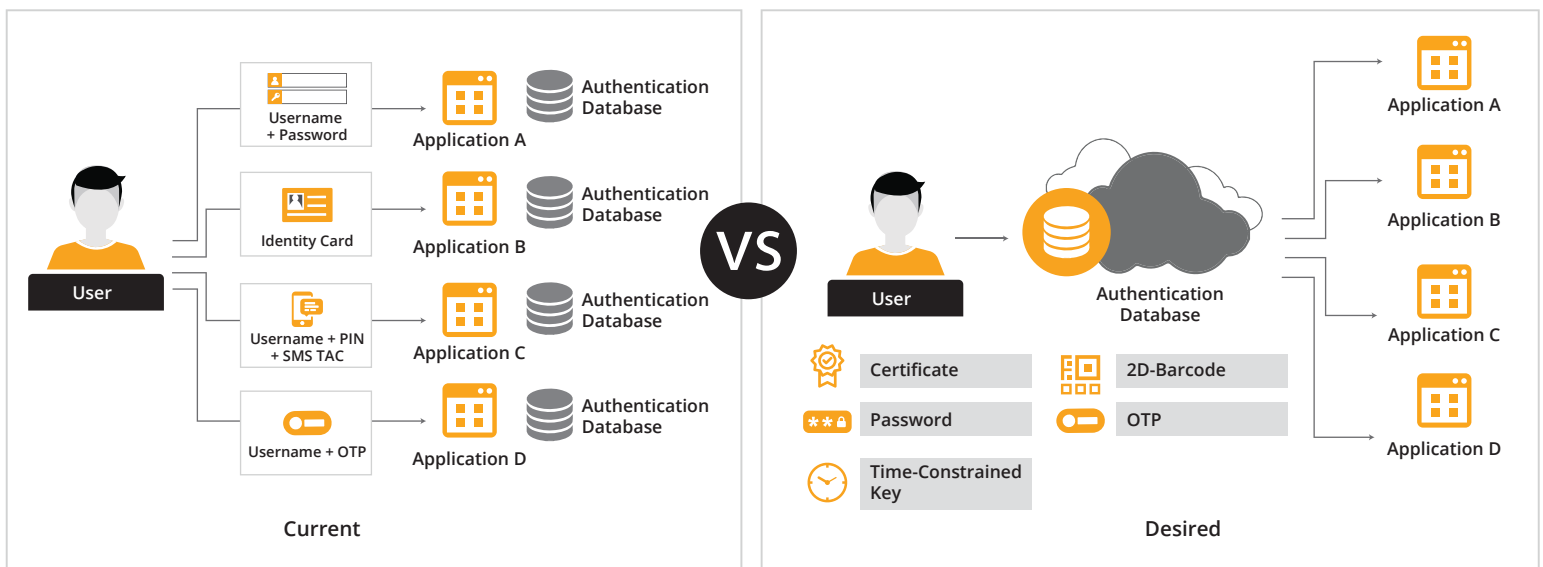
## Present Challenges: Big Data And Security

The world is currently enduring a “big data” boom, hoping that an explosion of data will bring solutions to a myriad of problems, from preventing terrorist attacks to anticipating the next technology trend and mitigating natural disasters before they happen.

In retrospect, not a day has gone by that cyber espionage campaigns are uncovered, shadowy hacker groups infiltrate prominent websites and endless streams of riveting disclosures occur involving

various government agencies across the globe.

As a result, standard security measures such as Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are not to be fully relied on as they are at risk of eavesdropping. It is here the management of privacy and the security of information of the very people that reside in the system that is key.



Common Scenario vs Desired Scenario

## Scalable High Trust Financial Systems

Federal financial planning, budgeting, monitoring and reporting systems need enhanced authority over expenditure management given limited resources. Streamlining of access is necessary to

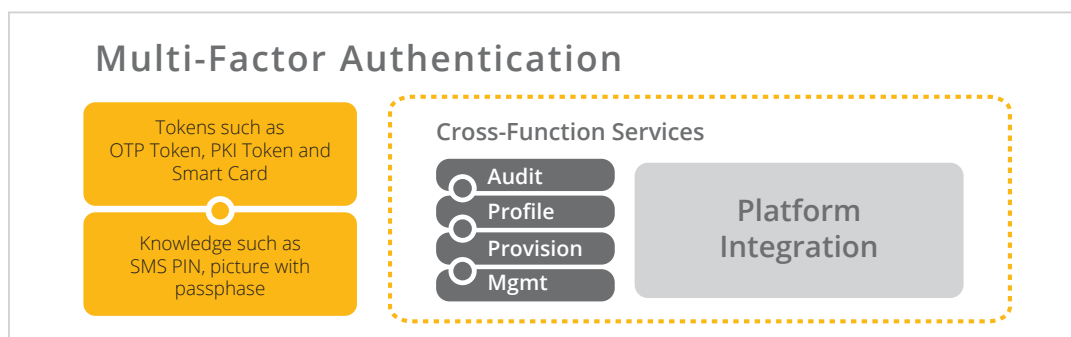
reduce the risk of information leaks, fraud and ensure security. CENTAGATE® UAP supports this via:

**Adaptive Authentication**

Within an enterprise environment, for example, applications pertaining to budget approval that are set at a higher trust level may require additional methods of authentication which is provided by CENTAGATE® UAP. In addition, based on the login behaviour of the user such as a change in device location or login time, CENTAGATE® UAP may request user for additional authentication.

**Multi-Factor Authentication**

CENTAGATE® UAP comprises multiple authentication methods with different trust values. Therein, enterprise systems can have the flexibility to set the type of authentication method to facilitate secured user access. Users also have the option to choose their preferred method to login to the system.



CENTAGATE® UAP System Architecture



SECUREMETRIC & UTIMACO

# HARI RAYA OPEN HOUSE @ MANDARIN ORIENTAL

**Raya** have been the biggest celebration of all Muslims in Malaysia. As a multi racial country, this remarkable holiday is celebrated by all races. This year, SecureMetric together with their close partner, Utimaco, organised their first Raya Open House dinner for all their clients and partners. This event was held at Mandarin Oriental Hotel in Kuala Lumpur, Malaysia last 14 July 2016. SecureMetric invited more than 80 people from different industries such as software and system integrators, banking and security. Everyone enjoyed the sumptuous buffet dinner served by the hotel. There were so much joy and SecureMetric staff get a chance to share their knowledge to all attendees. We are looking forward to organise another Hari Raya Open House next year.

