

# Collaborative efforts in Malaysia: **Producing Protection Profile for Internet Banking Application**



Ahmad Dahari Bin Jarno  
*Senior Analyst & MySEF Evaluator  
CyberSecurity Malaysia-MySEF (Malaysia)*

Co.Author:  
*Zarina Musa & Norahana Salimin*

# The “Menu | Outline” of the Day



Overview,  
Concept & Ideas



Roadmap  
& Activities



Vision, Mission  
& Fulfilling the Need's



Step into

# “Startup | Overview”

Perspective’s



The **IDEA** are proposed by MyCC Scheme to initiate a projects called **Protection Profile Working Group (PPWG)** under the framework of the 10<sup>th</sup> Malaysian Plan & SRI 2012/2013



The **Concept & Strategies** is by inviting local industry players, educational researchers, product testers and evaluators from the local labs thus, most importantly, implementers and enforcers from the Government to merge as Committee Members



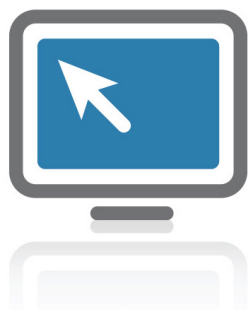
Step into Perspective's  
“Startup | Overview”



**PPWG#1** Data Protection  
Protection Profile Working Group



**PPWG#2** Network Devices  
Protection Profile Working Group



**PPWG#3** Internet Banking Apps  
Protection Profile Working Group



**PPWG#4** Smartcard Devices (MyKad)  
Protection Profile Working Group





# “Startup | Overview”



**PPWG#3** Internet Banking Apps  
Protection Profile Working Group

## “Objectives”

To develop a list of security functional requirements as a baseline, guidance & guidelines, references, roots of similar understanding and agreements on all aspects and perspectives of internet banking applications including the scope of “mobile apps”.

## “Road to Success?”



All industry, developers, implementers, enforcers, testers and evaluators has the same common understanding of IT security components and concepts in all types of internet banking applications that may differs from its types, usage and implementation in making sure of these components uphold:

- Confidentiality of Users Credentials
- Integrity of Data (internally/externally of the apps) is preserved
- Availability on Accessibility & Information Is Protected



# Roadmap & Activities

[Journey into the PP Dev.Adventures]

# The Beginning into the Adventures “Roadmap | Step’s”

As the proposal goes according to plans, all four (4) Protection Profile Working Groups have got the CSM Management & Malaysian Minister **APPROVAL** to initiate the starting line up programs/plans of developing minimum of four (4) propose documents known as list of security requirements and specification that shall support the objectives, mission and vision of Malaysian Government in the busting the awareness of IT | IT Security industry locally (**buying local product & IT security awareness**).

## “Lineup Tasks”

- a) Selection of the Committee Members & Secretariat Members;
- b) Appointing the Managerial Committee (Board of Approval);
- c) Appointing the Technical Committee (Industry, Labs, Educational, Governments & etc.)
- d) Drafting the Term of Reference, JD & outline of the activities
- e) Project Kick-Off & follow up meetings (regularly on monthly basis)



The Beginning into the Adventures  
“Roadmap | Step’s”



**PPWG#3** Internet Banking Apps  
Protection Profile Working Group



## “Determine PP Scope”

Software Desktop Internet Banking  
Browser Web Application Internet Banking  
Mobile App Internet Banking



## “Perspective in Depth”

Covering Platform (Android, iOS and BB)  
Programming Codes Guidelines  
3<sup>rd</sup> Supporting Environment & Apps



# The Beginning into the Adventures “Roadmap | Step’s”

## “Endorsement Committee”

MOSTI  
CyberSecurity Malaysia BoD  
PEMANDU  
SRI Committee  
Voting Representative of PPWG  
ISCB | MyCB



MIMOS  
CyberSecurity Malaysia MySEF  
BAE Detica  
IRIS Technology Malaysia  
Pannell Kerr Forster Malaysia  
Multimedia University Malaysia  
Chief Government Security Office  
ISCB | MyCB

## “Technical Committee”

# “Roadmap | Activities”

## 1<sup>st</sup> & for most: ESR form

ESR (Evaluation Security Requirements) is the form to be fill in by Secretariat of PPWG#3 to determine:

**Scope of Technology**  
**Boundary scope of PP** and  
**Coverage of the PP/TOE**

The document shall list the SPD, SO & SOE, SFR's & SAR's and EAL\* requirements; thus agreed to be a baseline blueprint for the PP drafting

## 2<sup>nd</sup> & continuing: PP Drafting

As the chairperson (leader) of the PP Technical Committee agreed with the content of the ESR as the blueprint of the PP, the draft PP shall be executed either with these options:

**Hiring CC Consultant and/or**  
**Experience the Hardship of writing PP**





In the Middle

Executions & GO!

# “Roadmap | Activities”

## 3<sup>rd</sup> & the trills: PP Evaluation

As the completion of drafting the PP, the document will be send to Malaysian Security Evaluation Facility under MyCC Scheme to be evaluated and next to be endorsed  
**CyberSecurity Malaysia MySEF**  
**BAE System Detica**

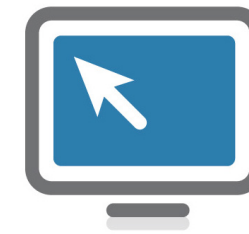


## 4<sup>th</sup> & finally: PP E&E

“E&E stands for Endorsed & Enforcement”  
Once the PP document is evaluated and certified by MyCC Scheme, the PP shall be awarded to respective owner of the project, which is either key player of industry or government agencies  
**For PPWG#3 – MIMOS is the Owner of the Project**

# Protection Profiles Development Journey

[The Team Hardship & Efforts]



**PPWG#3** Internet Banking Apps  
Protection Profile Working Group

# “In Depth | PP Content”

## Protection Profile Overview

Mobile banking is a system that allows customers or users (Data Users) of a financial institution to conduct financial transactions through a mobile device such as a smartphone or tablet. The financial transactions can be done through SMS, mobile web or application downloaded and installed to the mobile device.



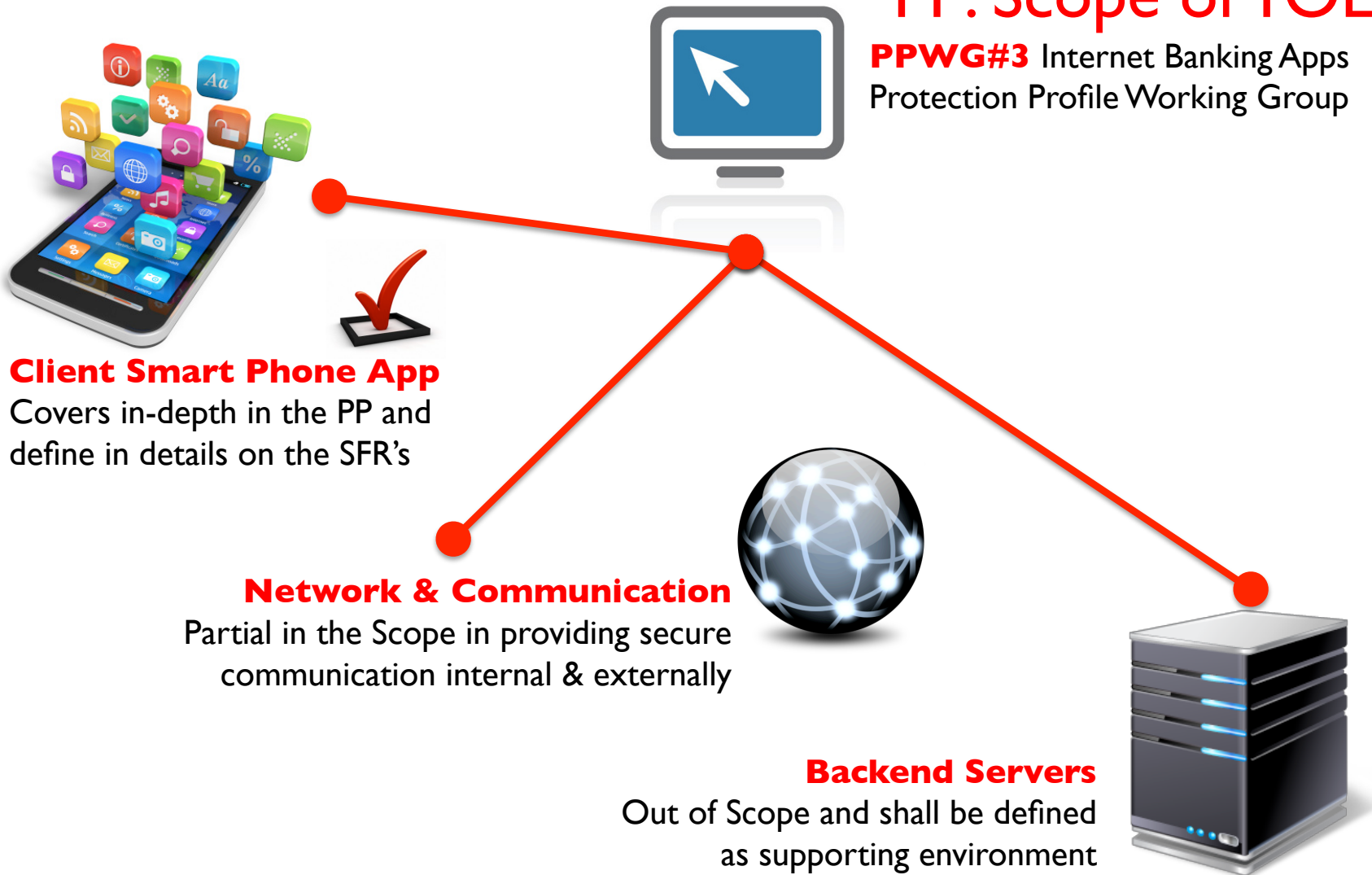
## Boundary of PP Overview

- ◆ The product shall be installed **in authorized platform** that is able to provides secure operational environment
- ◆ Users that will be using the product have **adequate knowledge** of the product operations
- ◆ Operations of the product are **securely managed by its own operation and protected** from any interference from other 3<sup>rd</sup> party apps.
- ◆ Scope of product only focusing at **client/users/consumers side mobile app** excluding the back-end servers operations
- ◆ Transactions financials are **protected via authentication** process using username, password, OTP and Token

# "In Depth | PP Content"

## PP: Scope of TOE

**PPWG#3** Internet Banking Apps  
Protection Profile Working Group



# “In Depth | PP Content”

## PP: Logical Scope of TOE



**PPWG#3** Internet Banking Apps  
Protection Profile Working Group

### Security Management

Main components that governs the whole operations of the product

### Authentication & Identification

Access control protection by enforcing the usage of OTP,Token or UAP



### User Data Protection

All data in motion and at rest are protected by enforcement of encryption & secure RAM

### Trusted Path Communication

Securely protecting data in motion from client to the banking server

# “In Depth | PP Content”



## PP: SPD (Assets)

**PPWG#3** Internet Banking Apps  
Protection Profile Working Group

### Personal Information

User/s credential that crucial that are transmitted in motion from client mobile device to banking backend servers

### Authentication Credentials

Credential that holds User/s to their banking information and as the authentication variables

### Account Details

Information holds by the banker that relates to user/s financial status and values that needs securely transmitted and dismiss when required

### Audit Details & Sessions Management

Logs of all and specific transaction performed, thus monitoring each sessions are securely managed





# “In Depth | PP Content”



## PP: SPD (Assumptions)

**PPWG#3** Internet Banking Apps  
Protection Profile Working Group

### ✦ Supporting Capabilities

- TOE has sufficient network access to transaction server of interest.
- TOE operates independent of physical location and means of connectivity.
- The processing resources of the TOE will be located within controlled environment.



### ✦ Trust on User/s

- The user is competent to operate the TOE and is able to exercise due care of the information required to operate the TOE inclusive of his credentials.
- The user is not careless, will fully negligent, or hostile, and will follow and abide by the terms and conditions pertaining to the use of the TOE, and instructions provided by the TOE documentation.

# “In Depth | PP Content”



## PP: SPD (Threats)

**PPWG#3** Internet Banking Apps  
Protection Profile Working Group

### ✦ Integrity & Confidentiality

- Unauthorized party attempts to compromise integrity of TOE upon service interruption on mobile platform.
- An unauthorized party which intercepts, modifies and/or disrupts data communications between TOE and transaction server, resulting in loss of confidentiality and/or integrity.

### ✦ Malfunctions

- An unauthorized party may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.
- User interaction which results in transaction outcome (or lack thereof) which can result in subsequent disputes with service provider.



# “In Depth | PP Content”



## PP: SPD (OSP)

**PPWG#3** Internet Banking Apps  
Protection Profile Working Group

### ❖ **Single Active Instance**

- Single active instance of the TOE shall be installed on one mobile platforms owned by specified user, as authenticated by means of credential demonstration.

### ❖ **Fresh Demo of Credential**

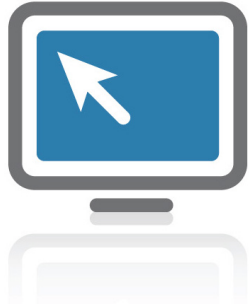
- TOE requires fresh demonstration of credential or demonstration of fresh credential by specified user for each session with transaction server of interest.

### ❖ **Accurate Timestamp**

- The TOE shall accurately record events by using the reliable time stamps provided by the TOE operational environment.



# “In Depth | PP Content”



## PP: SFR's

**PPWG#3** Internet Banking Apps  
Protection Profile Working Group

### ✦ Security Audit

- The product as TOE shall be able to capture events and recorded into audit logs that securely managed by the client app, thus sync back to the backend servers.

### ✦ User Data Protection

- Information and user credentials are protected internal within the operations of the mobile phone as well as in motion, thus at rest in backend server storage.

### ✦ Security Management

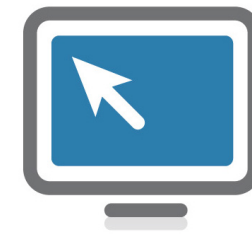
- Each functional and features of the app are securely managed contributing to secure operations of the app in handling data and user credential.

- ✦ TOE Access
- ✦ Trusted Path & Channel
- ✦ Communication



# Protection Profiles PPWVG#3 Projections

[ The GOALS & MISSION ]



**PPWVG#3** Internet Banking Apps  
Protection Profile Working Group

# “Challenges | Hold-up”

## Hold-up

- The members are more favorable on ISO language rather than CC facts and statements.
- Arguments on the practically of the product that will be develop using this PP.
- Always loose of focus due to lack in selection of SFR’s that is relevant or irrelevant for the PP content.



- Hard to get as many members especially the Developers and Government Agencies to join in the PPWG
- Sync facts and understanding among the ideas and scope of PP
- Short timeframe and everybody commitment in meetings.

## Challenges

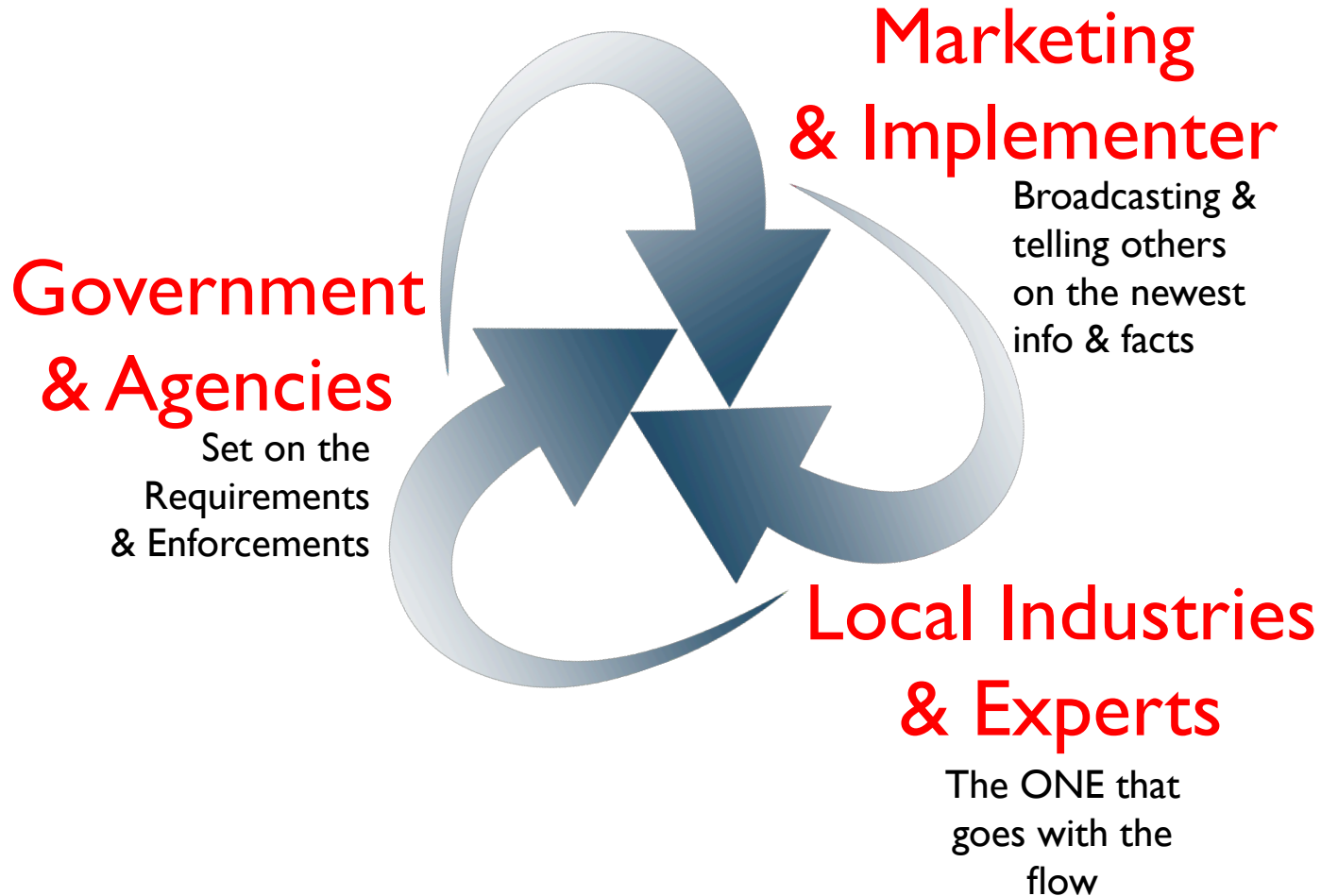




Almost the End

All the Trills & Experience

# “Mission | Finally”



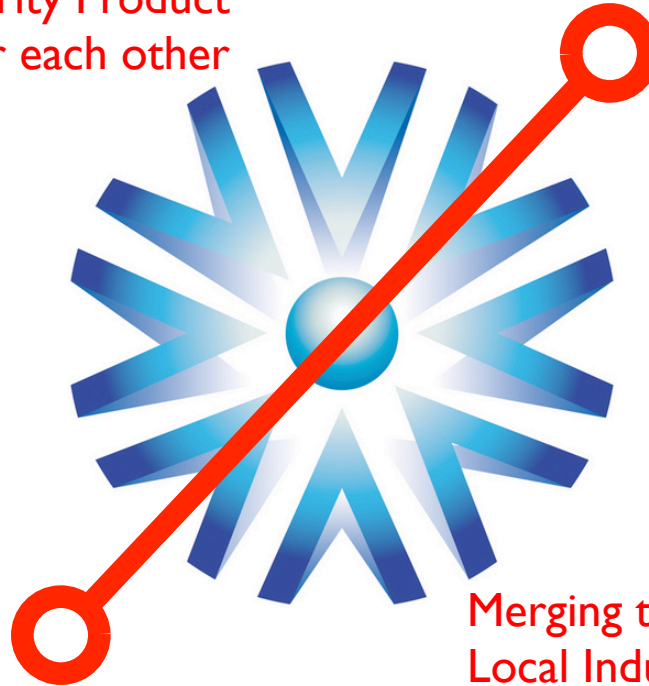
Almost the End

All the Trills & Experience

# “Vision | Way Up”

Seeing improvement at the local Government mindset, to see beyond borders that IT Security Product & Certification are meant for each other

# “Enforcement”



# “Better Sales”

Merging the gap between Test Lab & Local Industries as well as the Markets, to bond and merge from the depths of misleading info and facts on Evaluating & Certifying Products




**AHMAD DAHARI JARNO**

Senior Analyst & Evaluator, MySEF

Security Assurance, CyberSecurity Malaysia

Email: [dahari@cybersecurity.my](mailto:dahari@cybersecurity.my)

 [www.facebook.com/adj.hit](http://www.facebook.com/adj.hit)

 [@tenz\\_tensai](https://twitter.com/tenz_tensai)

# Thank you

**Corporate Office**

CyberSecurity Malaysia,  
Level 5, Sapura@Mines  
No. 7 Jalan Tasik  
The Mines Resort City  
43300 Seri Kembangan  
Selangor Darul Ehsan, Malaysia.

T : +603 8992 6888  
F : +603 8992 6841  
H : +61 300 88 2999

[www.cybersecurity.my](http://www.cybersecurity.my)  
[info@cybersecurity.my](mailto:info@cybersecurity.my)

**Northern Regional Office**

Level 19, Perak Techno-Trade Centre  
Bandar Meru Raya, Off Jalan Jelapang  
30020 Ipoh, Perak Darul Ridzuan, Malaysia

T: +605 528 2088  
F: +605 528 1905

 [www.facebook.com/CyberSecurityMalaysia](http://www.facebook.com/CyberSecurityMalaysia)

 [twitter.com/cybersecuritymy](https://twitter.com/cybersecuritymy)

 [www.youtube.com/cybersecuritymy](http://www.youtube.com/cybersecuritymy)

