

Who tells you that your secure product is actually secure?



Think about the time it stays on the field...



It went through a security evaluation

# Walking through the attack rating methodology to manage the trust

Hugues Thiebeauld – CEO of eShard

11<sup>th</sup> of September 2015

WISE Workshop



**eshard**



*Your trusted partner for the data  
protection  
in mobile and connected devices*



**Secure your app**



**Analyze your data**



**Ask the expert**



The job of risk manager is difficult

Needs to estimate the risk and to anticipate it

Needs to have a global picture

The time factor is a challenge

Require a tool for the right criteria

Make sure it meets the state-of-the-art and methodology was respected

Certification  
Body

Laboratory

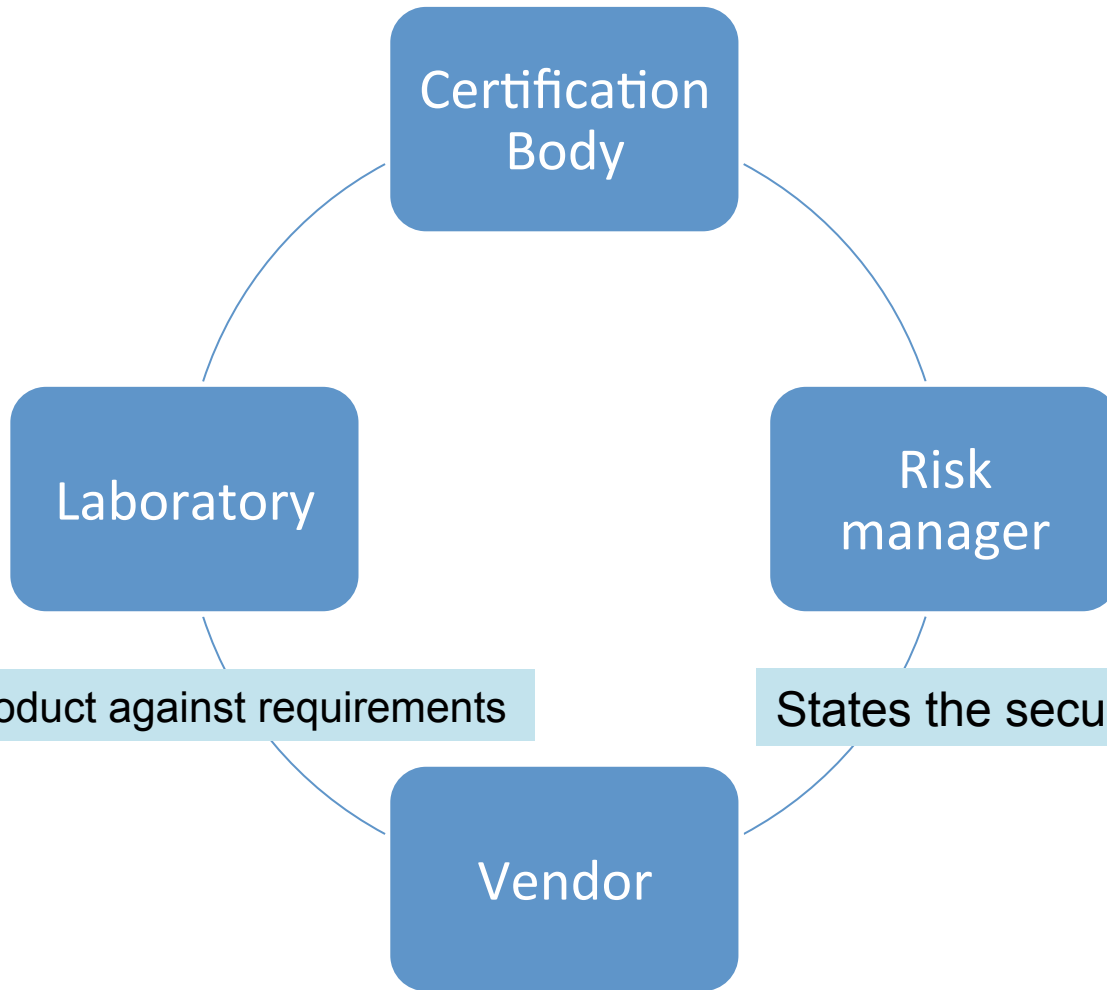
Risk  
manager

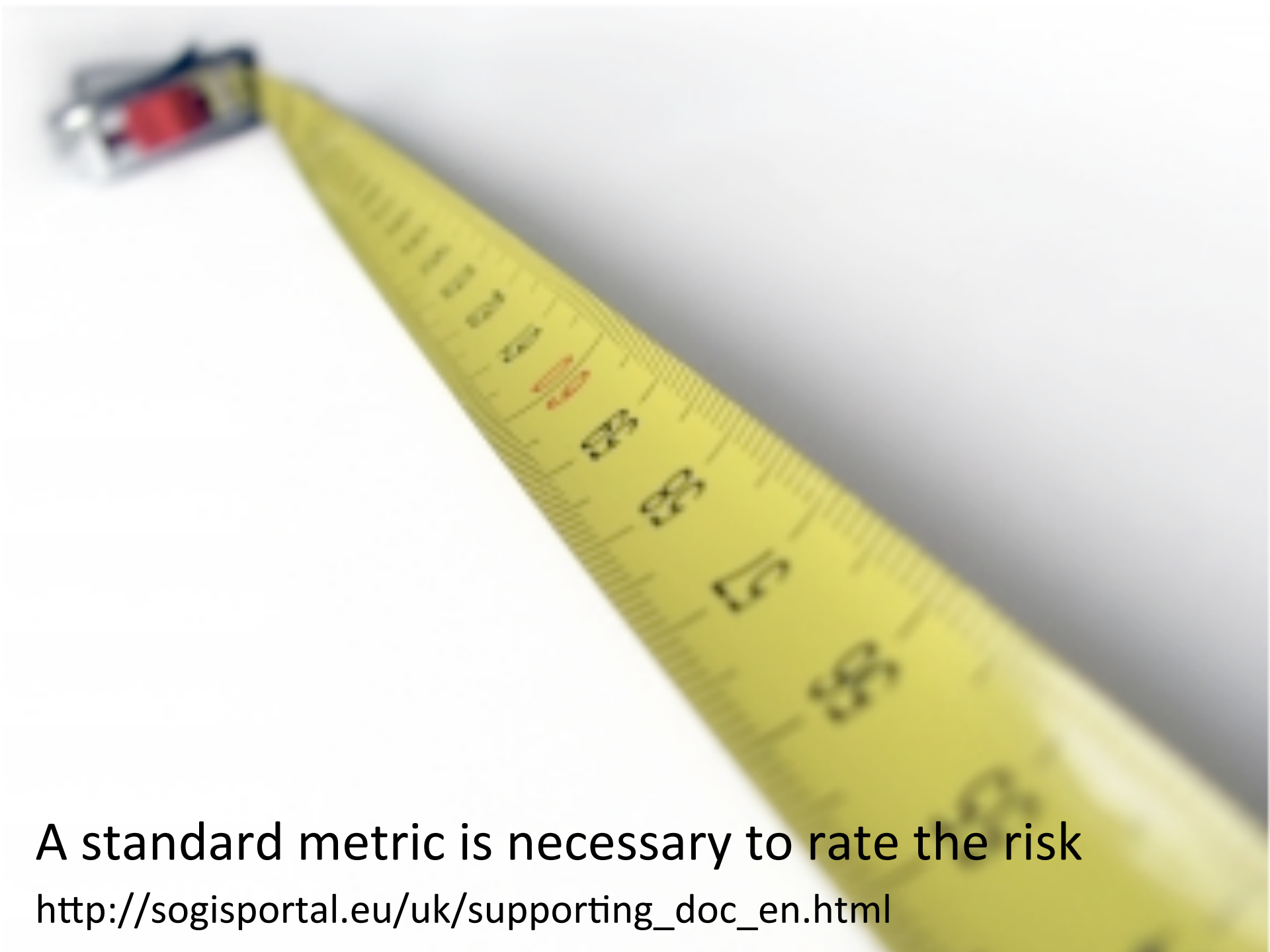
Ascertains the product against requirements

States the security requirements

Vendor

Designs and implements a secure product





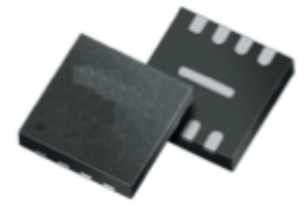
A standard metric is necessary to rate the risk

[http://sogisportal.eu/uk/supporting\\_doc\\_en.html](http://sogisportal.eu/uk/supporting_doc_en.html)

# JIL rating

	Identification	Exploitation
Elapsed time		
Expertise		
Knowledge		
Samples		
Equipment		
Technology specifics		





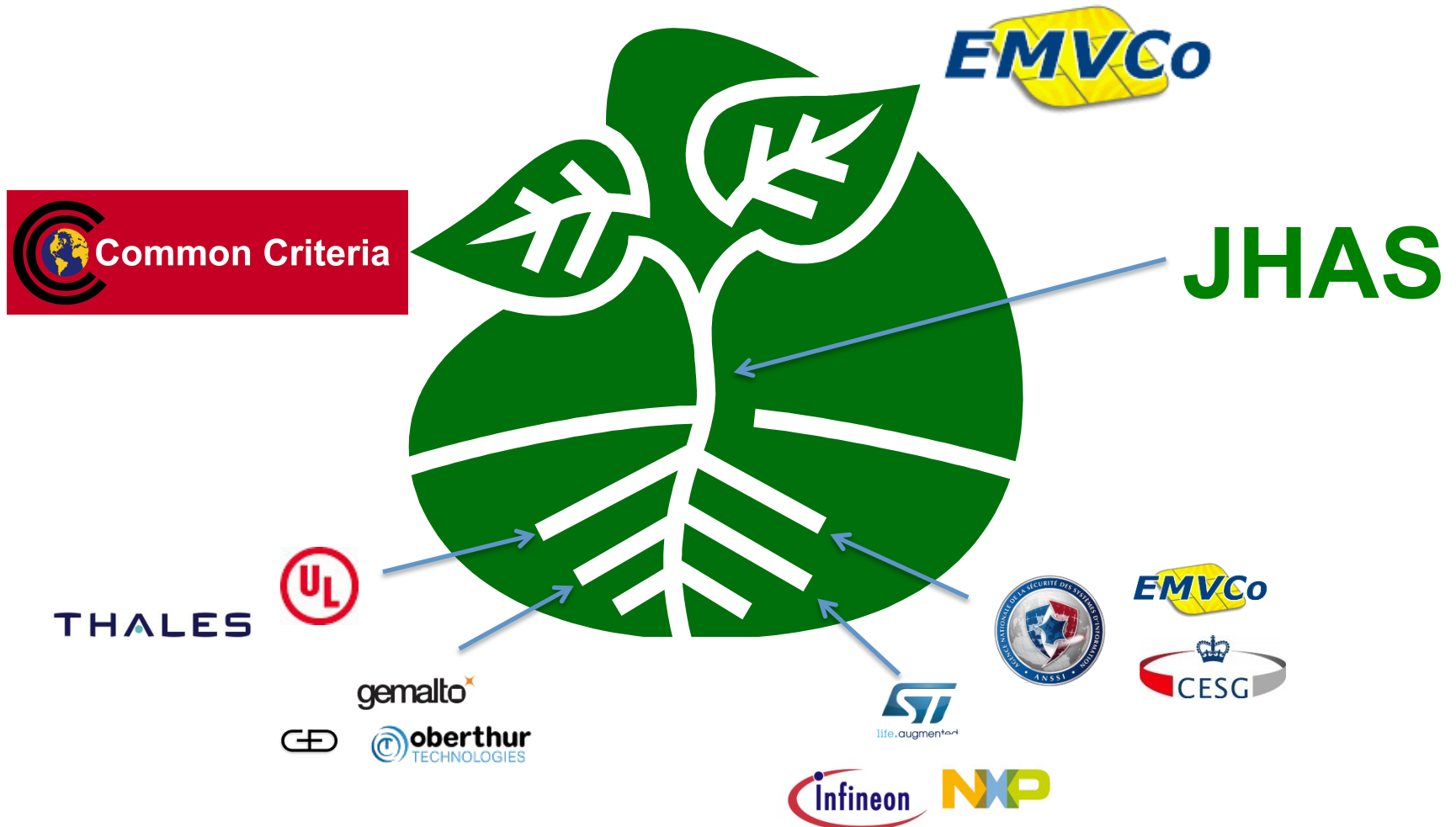
# JIL rating – Secure Element

An AES key is fully extracted with a statistical attack (eg CPA) from a SE

	Identification	Exploitation
Elapsed time	<1 month (3)	<1 day (3)
Expertise	Expert (5)	Proficient (2)
Knowledge	Critical (6)	Public (0)
Samples	<10 samples (0)	<10 samples (0)
Equipment	Specialised (3)	Specialised (4)

**Total: 26**

# Maintenance



# Maintenance



JHAS

public

PCI

private

JTEMS

public

VISA ready

private

BEAT





✓ or ✗

Certification  
Body

Laboratory

Risk  
manager

Vendor

Risk  
management

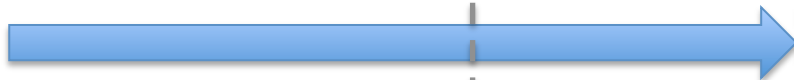
Requires 31

26



intermediate

highest



# Technology and scope

JIL rating is related to a technology

Evaluation takes care of a scope (list of assets)



A certificate does not necessarily mean that the whole product is secure

# Recap

Purpose of a security evaluation: bring assurance

Assurance concerns a scope of a product

Attack rating is technology specific and provides a link with an assurance level



Certificate is only valid at the issuance date

# Positive feedbacks

Global security level has dramatically increased

EMV payment cards, passports and terminals are running through the process. Many certificates are issued every year.

Experts can speak (almost) the same language.

harmonize the attack techniques across the industry





## A stone in the shoe

State-of-the-art attack change over the time

Renewal process is sometimes part of the process → a fail is difficult to manage

There is no obvious rule to manage the risk over the time

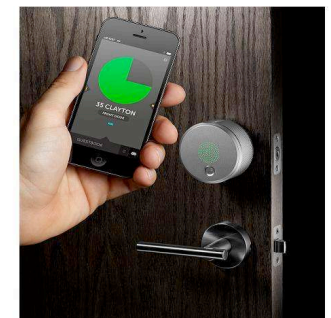
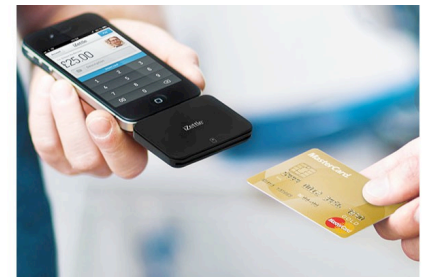
# Is it scalable?

Outside secure chips and terminals, there is no active committee

Perimeter must be defined to an affordable scope

Equation risk assurance versus cost and time to market

Rating an attack and managing the risk are closely tied together



# Some Android Exploits



**Stagefright : July 2015**  
**95% of devices vulnerable**  
**Remote exploitation (mms)**



**Towelroot: June 2014**  
**50% of devices still vulnerable**  
**Local kernel exploit**

**Rage Against the Cage: 2011**  
**3% of devices still vulnerable**  
**adb + Local exploitation (fork bomb)**

# Secure chip environment

**Confined and closed**

**Manufacturing and  
development processes  
can be controlled**

**Full coverage is  
affordable**

**Depth is possible**



**Assessment methodology  
established and mature**

**→ Global level of trust remains strong**

# Mobile environment is different

Open environment  
(interfaces, access, etc)

Involved number of  
stakeholders for the  
design and the  
manufacturing

Full coverage is not  
possible



Depth is hard to achieve  
exhaustively

No assessment methodology

→ How to create a good level of trust?

→ More pressure for time to market

# Connected and mobile devices

Communities of hackers

Level of information  
available is much higher  
(hardware, SDK,  
tutorials,)



Multi faces threats

Legal protection is the  
same?

Device: trust in the host?

→ Risk management: need to change the model?

## Some gaps to fill...



JIL rating is still missing for several technologies



Where most of exploits are published nowadays




# Software security and mobile

Mobile app are OS- and not handset specific



Assurance can change with a new exploit

How managing the multiple release?



Risk management should not rely only on a set of security requirements

Back-end is there for most of connected and mobile solutions → can be adaptive

More forensics to monitor the risk on the field



## Conclusion

JIL rating is an effective tool to rate an attack

It requires to have technical expert committees

Risk management relies on security evaluations

Model shall certainly change for latest technologies

New usage, new technologies are emerging in IoT



**Questions?**

**[contact@eshard.com](mailto:contact@eshard.com)**