



# A Method for Determining EALs for TOEs

Erkut BEYDAĞLI  
CC Evaluator / OKTEM Laboratory

22 September 2010

# CONTENT

- Introduction
- EAL (**E**valuation **A**ssurance **L**evel) Description
- EAL Statistics since 1997
- Current Approach for Determining EALs to TOEs (**T**arget **o**f **E**valuations)
- Proposed Methodology
- Examples
- Conclusions
- References

## INTRODUCTION (1/2)

- CC (**C**ommon **C**riteria) Consumer/Customer asks the following question:
  - "Which EAL is appropriate for my TOE to protect my critical assets?"
- Since CC standard does not provide any methodological approach to guide consumers in deciding the most appropriate EAL, determining appropriate EALs for TOEs is still an open problem.“
- At this presentation, a methodological approach is proposed as a solution to the problem.

## INTRODUCTION (2/2)

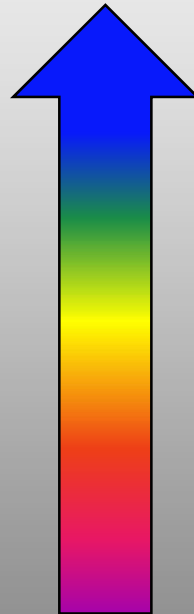
- TOE's goal is to protect Customer's critical assets.
- So, EALs of TOEs are much important.
- While determining EAL:
  - EAL should be determined by Customer.
  - Vendor should not determine the EAL instead of Customer.
  - Because critical assets belong to Customer, Vendor does not know the value of Customer's critical assets.

# EAL MEAN: DIFFERENCE BETWEEN EALs (1/3)

## DEVELOPMENT PHASE BASED:

HIGH QUALITY

- EAL7:
- EAL6:
- EAL5:
- EAL4:
- EAL3:
- EAL2:
- EAL1:

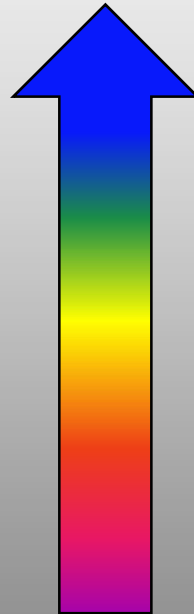


# EAL MEAN: DIFFERENCE BETWEEN EALs (2/3)

## EVALUATION PHASE BASED:

### WHITE BOX TEST

- EAL7:
- EAL6:
- EAL5:
- EAL4:
- EAL3:
- EAL2:
- EAL1:

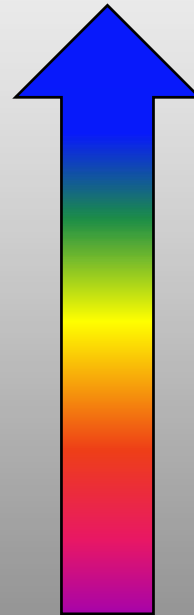


# EAL MEAN: DIFFERENCE BETWEEN EALs (3/3)

## OPERATING PHASE BASED:

### ATTACK POTENTIAL

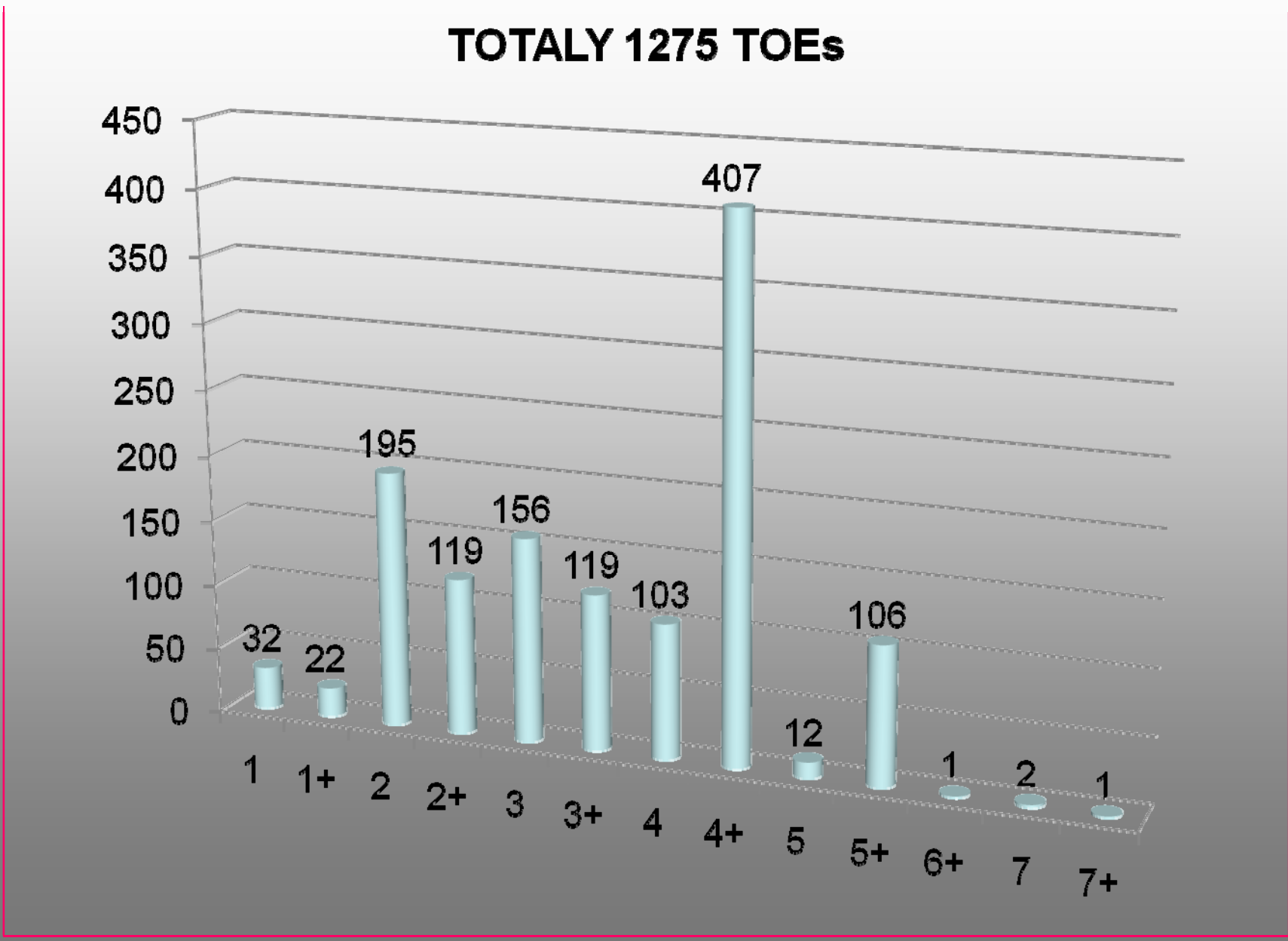
- EAL7: HIGH
- EAL6: HIGH
- EAL5: MODERATE
- EAL4: ENHANCED BASIC
- EAL3: BASIC
- EAL2: BASIC
- EAL1: BASIC



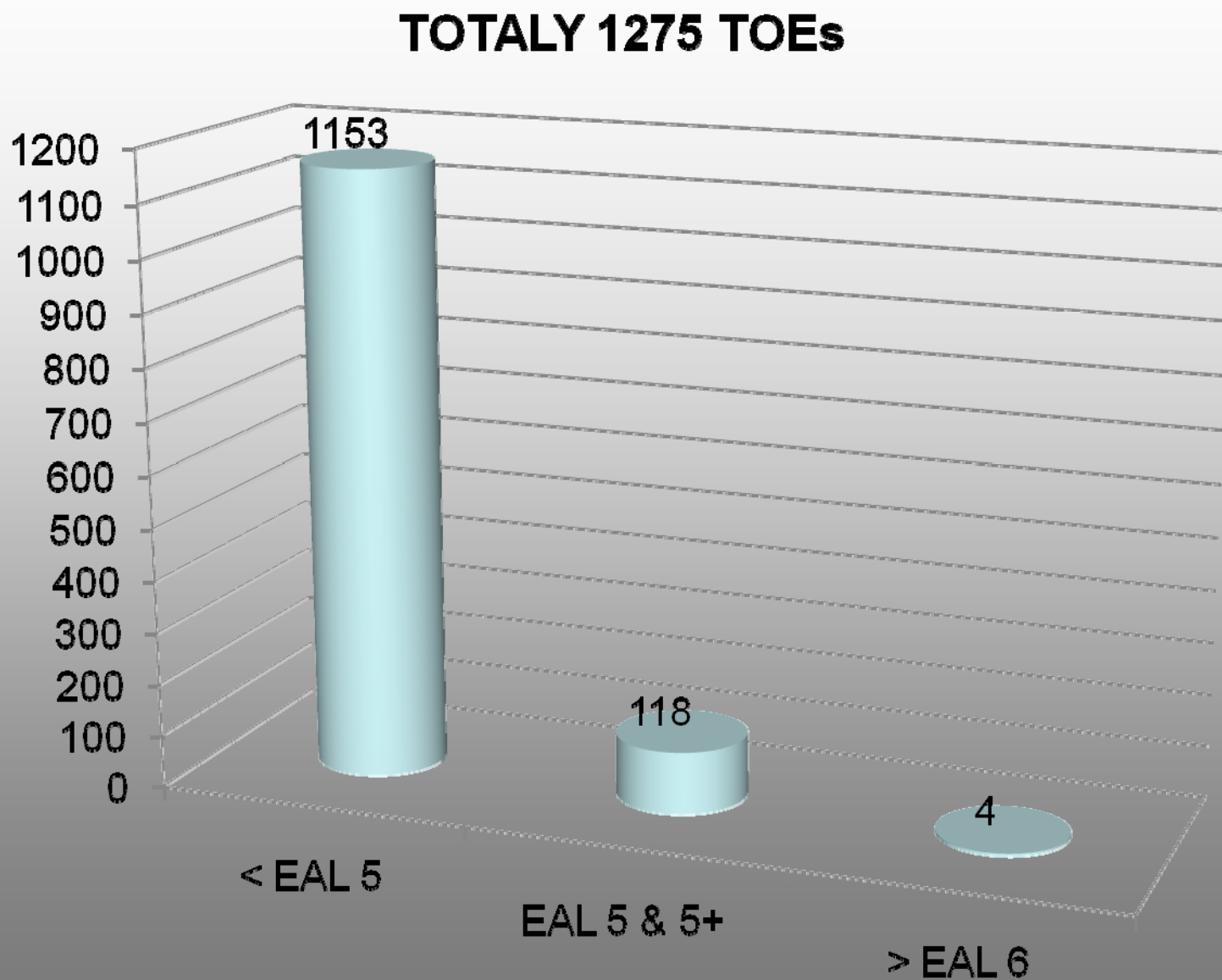
## OPERATING PHASE BASED, CONTINUE...

- EAL 6-7: Resistant to HIGH attack potential
- EAL5: Resistant to MODERATE attack potential
- EAL4: Resistant to ENHANCED BASIC attack potential
- EAL 1-2-3: Resistant to BASIC attack potential
  
- So **RESIDUAL VULNERABILITY** is much important. It means:
  - If a TOE has a CC certificate at EAL 4 level:
    - » This TOE may not be resistant to MODERATE and HIGH level attack potential.
    - » This TOE may include vulnerability that will be exploitable by attackers who have MODERATE or HIGH level attack potential.

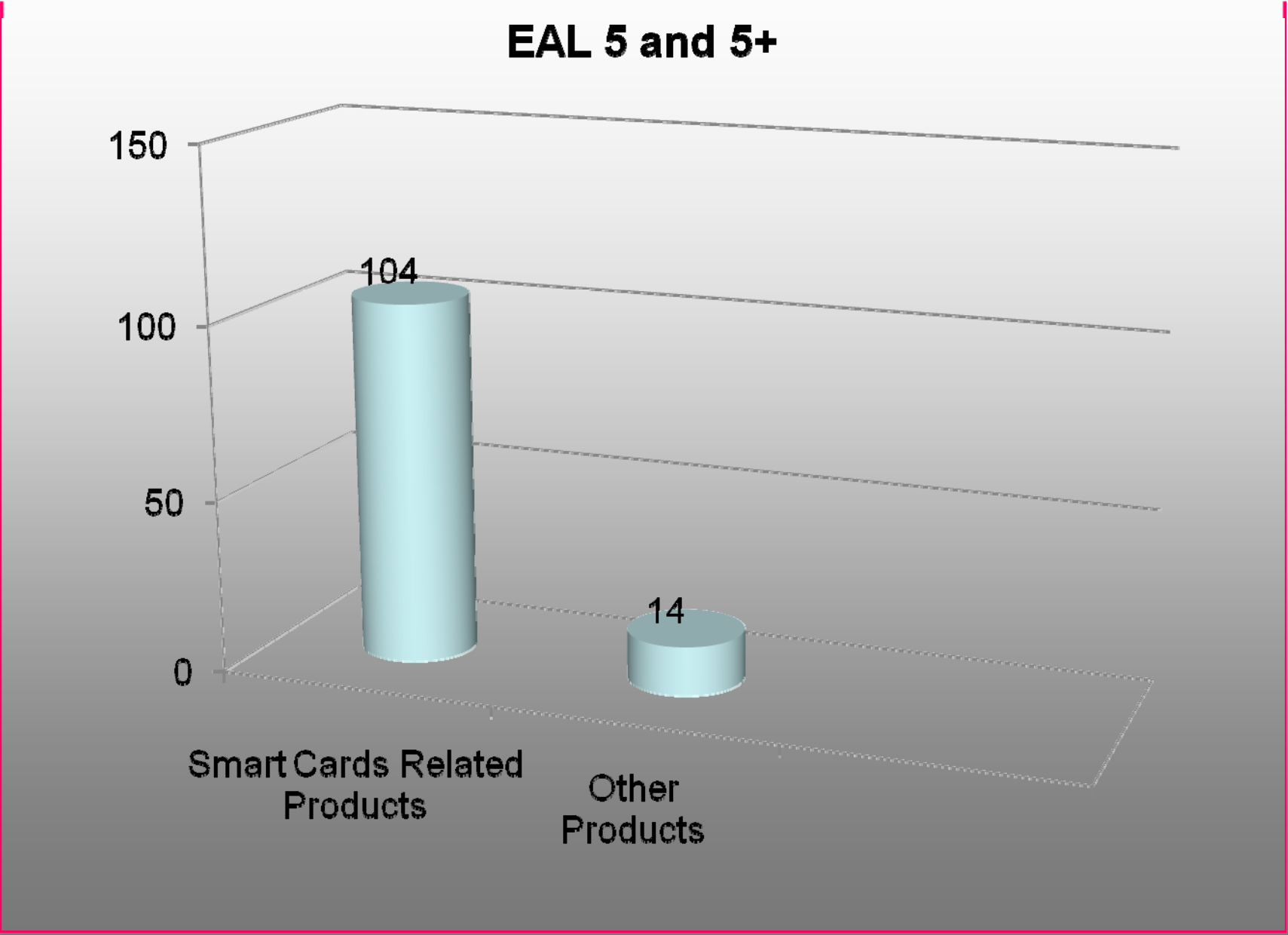
# EAL Statistics between 1997-2010 (1/4)



# EAL Statistics between 1997-2010 (2/4)

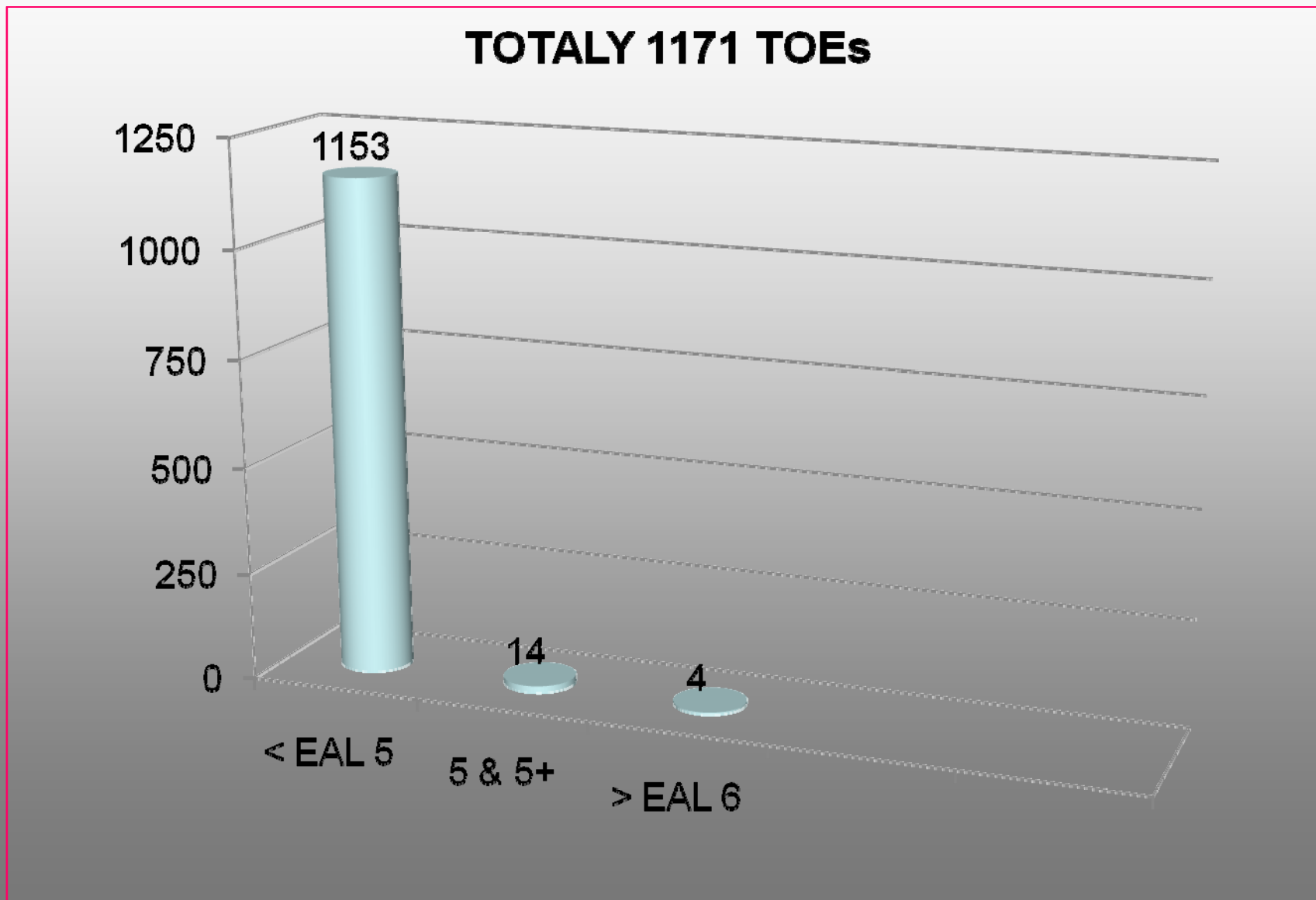


# EAL Statistics between 1997-2010 (3/4)



# EAL Statistics between 1997-2010 (4/4)

- Without smart card related products.



## Current Approach for Determining EALs

- No familiar methodology have been used to determine the EALs of 1275 products since 1997.
- Since there is no familiar methodology, everyone used different methods to determine EAL. The popular non technical methods are below:
  - **Previously certified similar TOEs**
  - **Test Period**
  - **Test Cost**
- To determine the accurate EALs for TOEs, we need a validated common methodology as a supporting document at CC.

## PROPOSED METHODOLOGY INTRODUCTION (1/2)

- CC addresses protection of assets from:
  - unauthorized disclosure,
  - unauthorized modification, or
  - loss of use.
- The categories of protection relating to these three types of failure of security are commonly called confidentiality, integrity, and availability, respectively

## PROPOSED METHODOLOGY INTRODUCTION (2/2)

- Within CC, assets are protected by TOEs. In order to determine the appropriate EAL for TOEs, a relation between asset value and EAL is required:
- To determine the asset value, **CIA**:
  - Confidentiality (C)
  - Integrity (I)
  - Availability (A)
- and **IMPACT LEVELS** can be used:
  - High (H)
  - Moderate (M)
  - Low (L)

## CIA DESCRIPTION

- **CONFIDENTIALITY:** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- **INTEGRITY:** Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
- **AVAILABILITY:** Ensuring timely and reliable access to and use of information.

## IF the potential impact is LOW:

- The loss of confidentiality, integrity, or availability might:
  - *cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;*
  - *result in minor damage to organizational assets;*
  - *result in minor financial loss; or*
  - *result in minor harm to individuals.*

## IF the potential impact is MODERATE:

- The loss of confidentiality, integrity, or availability might:
  - *cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;*
  - *result in significant damage to organizational assets;*
  - *result in significant financial loss; or*
  - *result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.*

## IF the potential impact is HIGH:

- The loss of confidentiality, integrity, or availability might:
  - *cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;*
  - *result in major damage to organizational assets;*
  - *result in major financial loss; or*
  - *result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.*

# PROPOSED METHODOLOGY

- ASSETS which are protected by TOEs,
- CIA
- IMPACT LEVELS

are considered as the most basic inputs to the proposed methodology.

# SCORE TABLE

- To determine the appropriate EAL for a TOE, the first step is to define the assets that are protected by the TOE.
- After this process, CIA values for each asset should be calculated. The following score table can be used to calculate these asset values.

Confidentiality				Integrity			Availability		
NA	L	M	H	L	M	H	L	M	H
0	1	2	3	1	2	3	1	2	3

**Note: Not Applicable (NA) is only applicable for confidentiality.**

# FORMULA

Confidentiality				Integrity			Availability		
NA	L	M	H	L	M	H	L	M	H
0	1	2	3	1	2	3	1	2	3

The **FORMULA** to calculate the score for asset value is:

$$= \{(\text{confidentiality, impact})_{\text{score}} + (\text{integrity, impact})_{\text{score}} + (\text{availability, impact})_{\text{score}}\}$$

# FINAL TABLE

- After calculation, the appropriate EAL level for the TOE can be determined based on the highest score and the highest impact level of assets. Following table can be used:

	HIGHEST CIA LEVEL		
	Low	Moderate	High
Calculated score = 2	EAL 1	NA	NA
Calculated score = 3	EAL 2	EAL 3	NA
Calculated score = 4	NA	EAL 4	EAL 4+ (AVA_VAN.5)
Calculated score = 5	NA	EAL 4+ (AVA_VAN.4)	EAL 4+ (AVA_VAN.5)
Calculated score = 6	NA	EAL 5	EAL 5+ (AVA_VAN.5)
Calculated score = 7	NA	NA	EAL 5+ (AVA_VAN.5)
Calculated score = 8	NA	NA	EAL 6
Calculated score = 9	NA	NA	EAL 7

# EXAMPLE 1

- A financial organization managing routine administrative information determines that:
  - the potential impact from a loss of confidentiality is low,
  - the potential impact from a loss of integrity is low,
  - and the potential impact from a loss of availability is low.
- The resulting score for this asset (administrative information) is calculated as:

Confidentiality				Integrity			Availability		
NA	L	M	H	L	M	H	L	M	H
0	1	2	3	1	2	3	1	2	3

- Asset value<sub>routine administrative information</sub> = {(confidentiality, L) + (integrity, L) + (availability, L)} = **3**

# EXAMPLE 1

- Asset value routine administrative information = **3** and the highest CIA level is Low.

	HIGHEST CIA LEVEL		
	Low	Moderate	High
Calculated score = 2	EAL 1	NA	NA
<b>Calculated score = 3</b>	<b>EAL 2</b>	EAL 3	NA
Calculated score = 4	NA	EAL 4	EAL 4+ (AVA_VAN.5)
Calculated score = 5	NA	EAL 4+ (AVA_VAN.4)	EAL 4+ (AVA_VAN.5)
Calculated score = 6	NA	EAL 5	EAL 5+ (AVA_VAN.5)
Calculated score = 7	NA	NA	EAL 5+ (AVA_VAN.5)
Calculated score = 8	NA	NA	EAL 6
Calculated score = 9	NA	NA	EAL 7

- Using methodology, we can determine that **EAL 2** is appropriate for the TOE which claims to protect routine administrative information for CIA risks.

## EXAMPLE 2

- An organization managing public information on its web server determines that:
  - there is no potential impact from a loss of confidentiality (i.e., confidentiality requirements are **not applicable**),
  - a **moderate** potential impact from a loss of integrity,
  - and a **moderate** potential impact from a loss of availability.
- The resulting score for this asset (public information) is calculated as:

Confidentiality				Integrity			Availability		
NA	L	M	H	L	M	H	L	M	H
0	1	2	3	1	2	3	1	2	3

- Asset value<sub>public information</sub> = {(confidentiality, NA) + (integrity, M) + (availability, M)} = **4**

# EXAMPLE 2

- Asset value<sub>public information</sub> = 4 and the highest CIA level is Moderate.

	HIGHEST CIA LEVEL		
	Low	Moderate	High
Calculated score = 2	EAL 1	NA	NA
Calculated score = 3	EAL 2	EAL 3	NA
<b>Calculated score = 4</b>	NA	<b>EAL 4</b>	EAL 4+ (AVA_VAN.5)
Calculated score = 5	NA	EAL 4+ (AVA_VAN.4)	EAL 4+ (AVA_VAN.5)
Calculated score = 6	NA	EAL 5	EAL 5+ (AVA_VAN.5)
Calculated score = 7	NA	NA	EAL 5+ (AVA_VAN.5)
Calculated score = 8	NA	NA	EAL 6
Calculated score = 9	NA	NA	EAL 7

- Using methodology, we can determine that **EAL 4** is appropriate for the TOE which claims to protect public information for integrity and availability risks.

# EXAMPLE 3

- A law enforcement organization managing extremely sensitive investigative information determines that:
  - the potential impact from a loss of confidentiality is high,
  - the potential impact from a loss of integrity is high,
  - and the potential impact from a loss of availability is moderate.
- The resulting score for this asset (investigative information) is calculated as:

Confidentiality				Integrity			Availability		
NA	L	M	H	L	M	H	L	M	H
0	1	2	3	1	2	3	1	2	3

- Asset value<sub>extremely sensitive investigative information</sub> = {(confidentiality, H) + (integrity, H), (availability, M)} = **8**

# EXAMPLE 3

- Asset value<sub>extremely sensitive investigative information</sub> = 8 and the highest CIA level is High.

	HIGHEST CIA LEVEL		
	Low	Moderate	High
Calculated score = 2	EAL 1	NA	NA
Calculated score = 3	EAL 2	EAL 3	NA
Calculated score = 4	NA	EAL 4	EAL 4+ (AVA_VAN.5)
Calculated score = 5	NA	EAL 4+ (AVA_VAN.4)	EAL 4+ (AVA_VAN.5)
Calculated score = 6	NA	EAL 5	EAL 5+ (AVA_VAN.5)
Calculated score = 7	NA	NA	EAL 5+ (AVA_VAN.5)
<b>Calculated score = 8</b>	NA	NA	<b>EAL 6</b>
Calculated score = 9	NA	NA	EAL 7

- Using methodology, we can determine that **EAL 6** is appropriate for the TOE which claims to protect extremely sensitive investigative information for CIA risks.

## CONCLUSIONS (1/2)

- “Which EAL for my TOE?” is still an open problem at CC.
- Without a methodology, to define the required EAL for TOEs is difficult. Therefore, a common methodology is muchly required.
- Lack of methodology is encouraging Customer or Sponsor to use the following non technical methods:
  - **Previously certified similar TOEs**
  - **Test Period**
  - **Test Cost**
- This presentation describes a technical methodology for common use.

## CONCLUSIONS (2/2)

- The proposed technical methodology bases on:
  - Highest IMPACT LEVEL (Low, Moderate, High) of assets
  - Highest SCORE (2,3,4.....,9) of assets.
- Customer's critical assets are under risk with the usage of non technical methods. To eliminate the usage of them:
  - A methodology (as a mandatory supporting document) should be prepared by a CC working group.
  - An evaluation step (additional to APE\_REQ.2.12 and ASE\_REQ.2.12) should be added to PP and ST evaluation to check EAL level accuracy.

# REFERENCES

- Common Criteria Standard v3.1 rev 3
- Common Evaluation Methodology v3.1 rev 3
- NIST Special Publication 800-60 version 2.0 Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories

**THANKS FOR YOUR ATTENTION !**

**Any Comments or Questions**