The Common Evaluation Methodology

Miguel Bañón

Representing the
National Cryptologic Centre
National Intelligence Centre

organismo.certificacion@cni.es

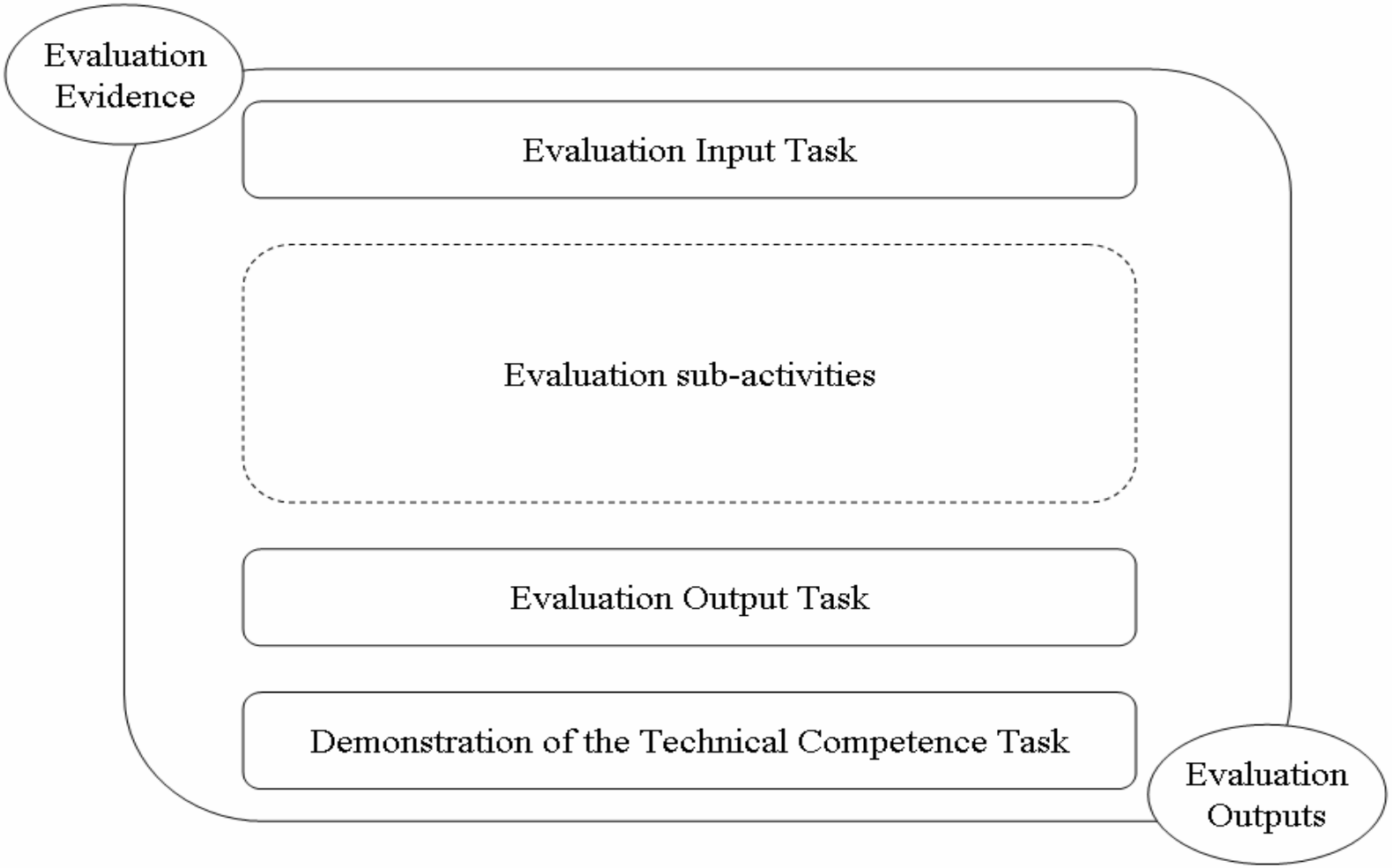
- Objectives
- New general evaluation tasks
- The actions catalogue
- Some numbers about EAL work units
- Questions welcomed

Objectives

The new CC/CEM assurance components are to be explained elsewhere in this conference.

This presentation provides an assurance class independent view of the new CEM, based on the work unit action verbs.

New general evaluation tasks



New general evaluation tasks

Each evaluation, whether of a PP or TOE (including ST), follows the same process, and has four evaluator tasks in common: the input task, the output task, the evaluation sub-activities, **and the demonstration of the technical competence to the evaluation authority task.**

In contrast to the evaluation sub-activities, input and output tasks have no verdicts associated with them as they do not map to CC evaluator action elements; they are performed in order to ensure conformance with the universal principles and to comply with the CEM.

New general evaluation tasks

The demonstration of the technical competence to the evaluation authority task may be fulfilled by the evaluation authority analysis of the output tasks results, or may include the demonstration by the evaluators of their understanding of the inputs for the evaluation sub-activities.

This task has no associated evaluator verdict, but has an evaluator authority verdict. The detailed criteria to pass this task are left to the discretion of the evaluation authority.

New general evaluation tasks

The matters that schemes may choose to specify include:

what is required in ensuring that an evaluation was done sufficiently - every scheme has a means of verifying the technical competence, understanding of work and the work of its evaluators, whether

• by requiring the evaluators to present their findings to the oversight body,

• by requiring the oversight body to redo the evaluator's work, or

• by some other means that assures the scheme that all evaluation bodies are adequate and comparable;

The actions catalogue

Whereas evaluator actions are briefly defined in the criteria, the evaluator real action is decomposed into work units in the methodology. We will study the action verbs for these work units.

ADV_FSP.1.1E	The evaluator shall **confirm** that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.1-1	The evaluator shall **examine** the functional specification **to determine** that it states the purpose of each SFR-supporting and SFR-enforcing TSFI.
	...
ADV_FSP.1-4	The evaluator shall **examine** the functional specification **to determine** that it states the purpose of each SFR-supporting and SFR-enforcing TSFI.

The actions catalogue

Work units are generally worded following a common pattern:

The evaluator shall <action> <input evidence> <verdict criteria>?

An analysis of the range of action verbs and the requirements they impose on the evaluator expertise/work load may provide some light on the assurance gained during a CC/CEM evaluation.

What do the CC/CEM evaluators do?

The actions catalogue

The evaluator shall **check** that all actual test results ...
The evaluator shall **conduct** testing ...
The evaluator shall **devise** a test subset ...
The evaluator shall **examine** the base component **to determine** ...
The evaluator shall **perform** all user procedures ...
The evaluator shall **produce** penetration test documentation ...
The evaluator shall **record** in the ETR the identified ...
The evaluator shall **report** a complete list that uniquely ...

The actions catalogue

The evaluator shall **check** that all actual test results ...

Check: to generate a verdict by a simple comparison. **Evaluator expertise is not required.** The statement that uses this verb describes what is mapped.

ADV_IMP.1-1	The evaluator shall **check** that the implementation representation defines the TSF to a level of detail such that the TSF can be generated without further design decisions.

Evaluator mood: Monday mornings

The actions catalogue

The evaluator shall **conduct** testing ...

ADV_IMP.2-5	The evaluator shall **conduct** a transformation of the implementation representation into the implementation.
ATE_IND.2-4	The evaluator shall **conduct** testing using a sample of tests found in the developer test plan and procedures.
AVA_VAN.2-7	The evaluator shall **conduct** penetration testing.
AVA_VAN.2-3	The evaluator shall **conduct** a search of ST, guidance documentation, functional specification and TOE design evidence to identify possible potential vulnerabilities in the TOE.

Evaluator mood: Monday evening

The actions catalogue

The evaluator shall **devise** a test subset ...

ATE_IND.1-3	The evaluator shall **devise** a test subset.
AVA_VAN.1-4	The evaluator shall **devise** penetration tests, based on the independent search for potential vulnerabilities.

Evaluator mood: Tuesday, lots of coffee, after nap

The actions catalogue

The evaluator shall **examine** … **to determine** ...

Examine: to generate a verdict by analysis using evaluator expertise. The statement that uses this verb identifies what is analysed and the properties for which it is analysed.

Determine: this term requires an independent analysis to be made, with the objective of reaching a particular conclusion.

The usage of this term differs from ``confirm'' or ``verify'', since these other terms imply that an analysis has already been performed which needs to be reviewed, whereas the usage of ``determine'' implies a **truly independent analysis**, usually in the absence of any previous analysis having been performed.

The actions catalogue

The evaluator shall **examine** ... **to determine** ...

ADV_ARC.1-1	The evaluator shall **examine** the architectural design **to determine** that the information provided in the evidence is presented at a level of detail commensurate with the descriptions of the SFR-enforcing abstractions contained in the TOE design document.
ATE_COV.1-1	The evaluator shall **examine** the test coverage evidence **to determine** that the correspondence between the tests identified in the test documentation and the interfaces described in the functional specification is accurate.

Evaluator mood: Wednesday morning, chill-out music

The actions catalogue

The evaluator shall **perform** all user procedures ...

AGD_PRE.1-5 The evaluator shall **perform** all user procedures necessary to prepare the TOE to determine that the TOE and its operational environment can be prepared securely using only the supplied preparative user guidance.

Evaluator mood: Wednesday evening, I need something to play with.

The actions catalogue

The evaluator shall **produce** penetration test documentation ...

ATE_IND.1-4	The evaluator shall **produce** test **documentation** for the test subset that is sufficiently detailed to enable the tests to be reproducible.
AVA_VAN.1-5	The evaluator shall **produce** penetration test **documentation** for the tests based on the list of potential vulnerabilities in sufficient detail to enable the tests to be repeatable.

Evaluator mood: Do I need to do this? Can I have a tool to produce the docs?.

The actions catalogue

The evaluator shall **record** in the ETR the identified ...

Record: to retain a written description of procedures, events, observations, insights and results in sufficient detail to enable the work performed during the evaluation to be reconstructed at a later time.

ATE_IND.1-6	The evaluator shall record the following information about the tests that compose the test subset: • identification of the interface behaviour to be tested; • ...
AVA_VAN.1-3	The evaluator shall record in the ETR the identified potential vulnerabilities that are candidates for testing and applicable to the TOE in its operational environment.

Evaluator mood: Do I need to do this? Can I have a tool to produce the docs?.

The actions catalogue

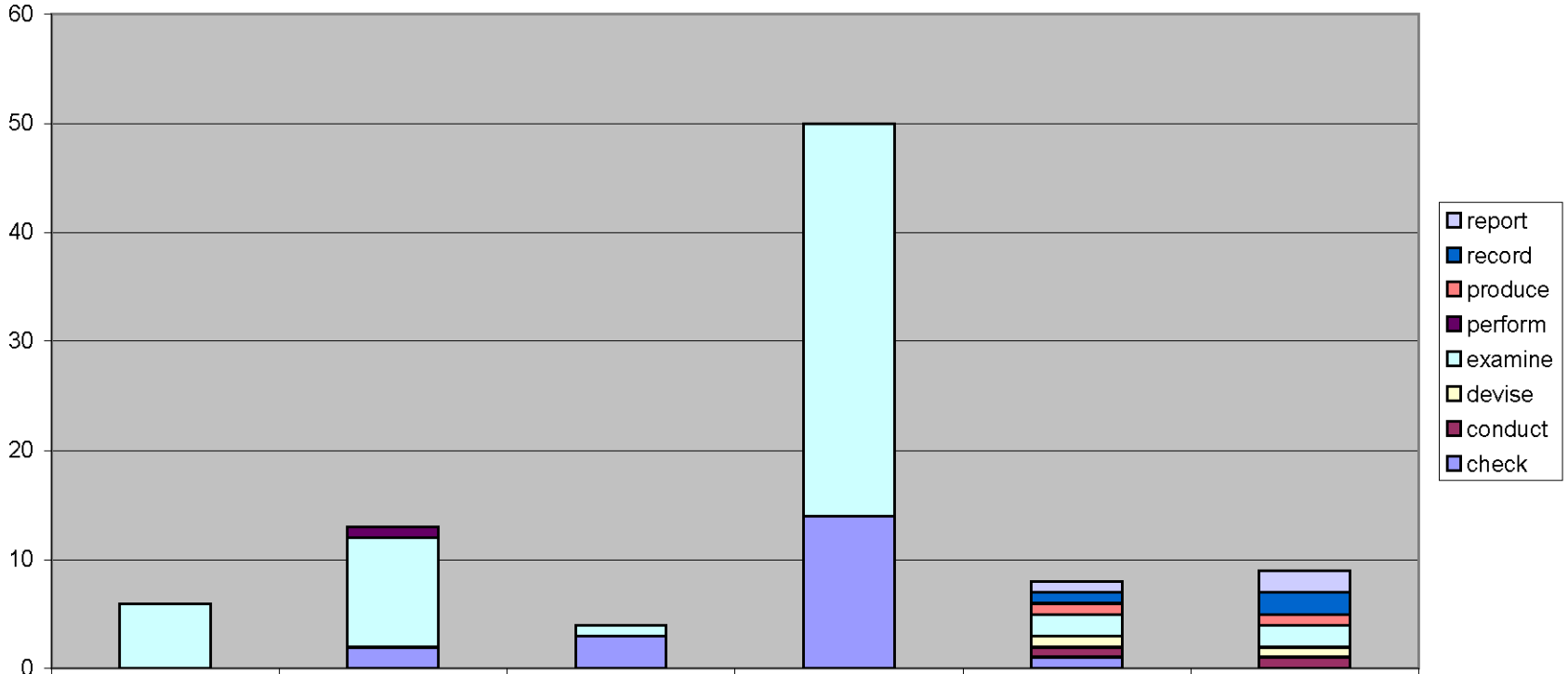
The evaluator shall **report** a complete list that uniquely ...

Report: to include evaluation results and supporting material in the Evaluation Technical Report or an Observation Report.

ATE_FUN.1-8	The evaluator shall **report** the developer testing effort, outlining the testing approach, configuration, depth and results.
AVA_VAN.1-8	The evaluator shall **report** in the ETR the evaluator penetration testing effort, outlining the testing approach, configuration, depth and results.

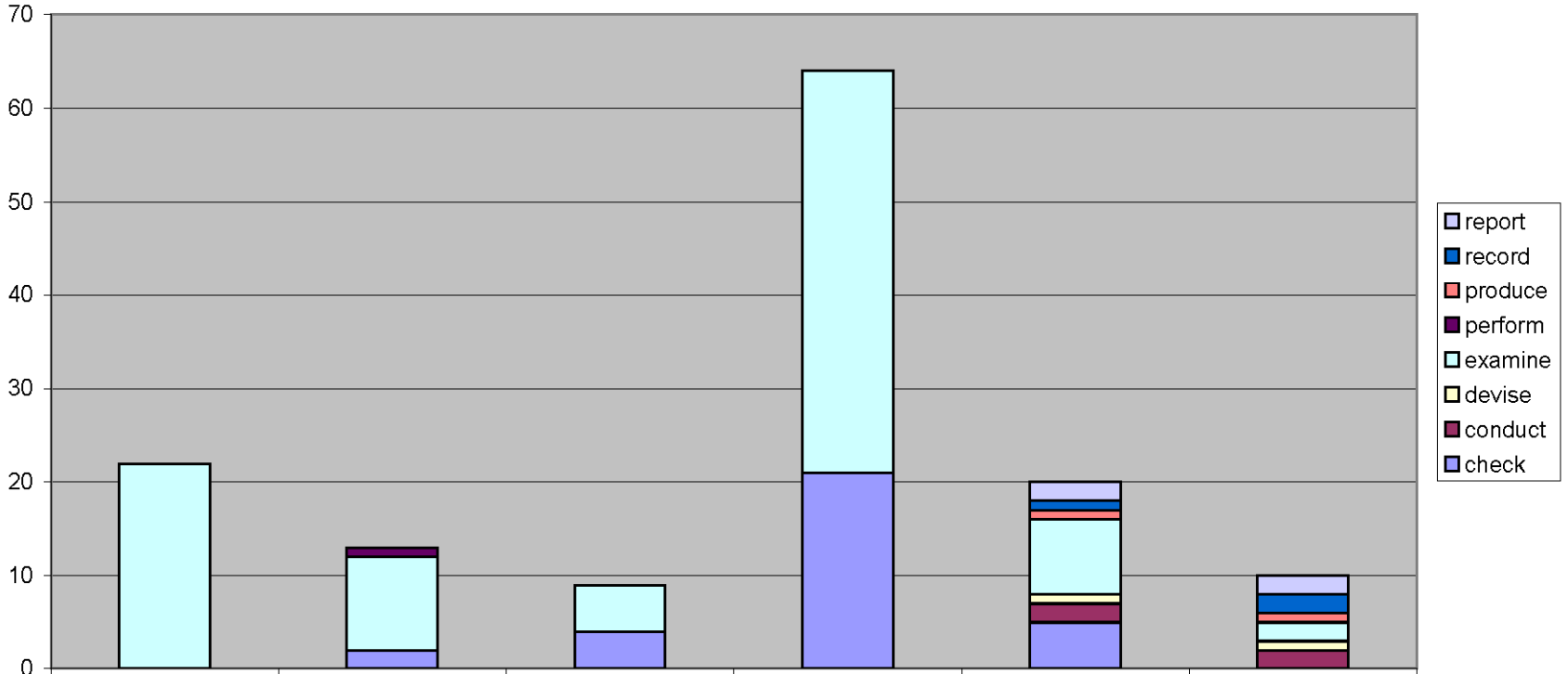
Evaluator mood: OK, only because it's Friday ...

EAL1



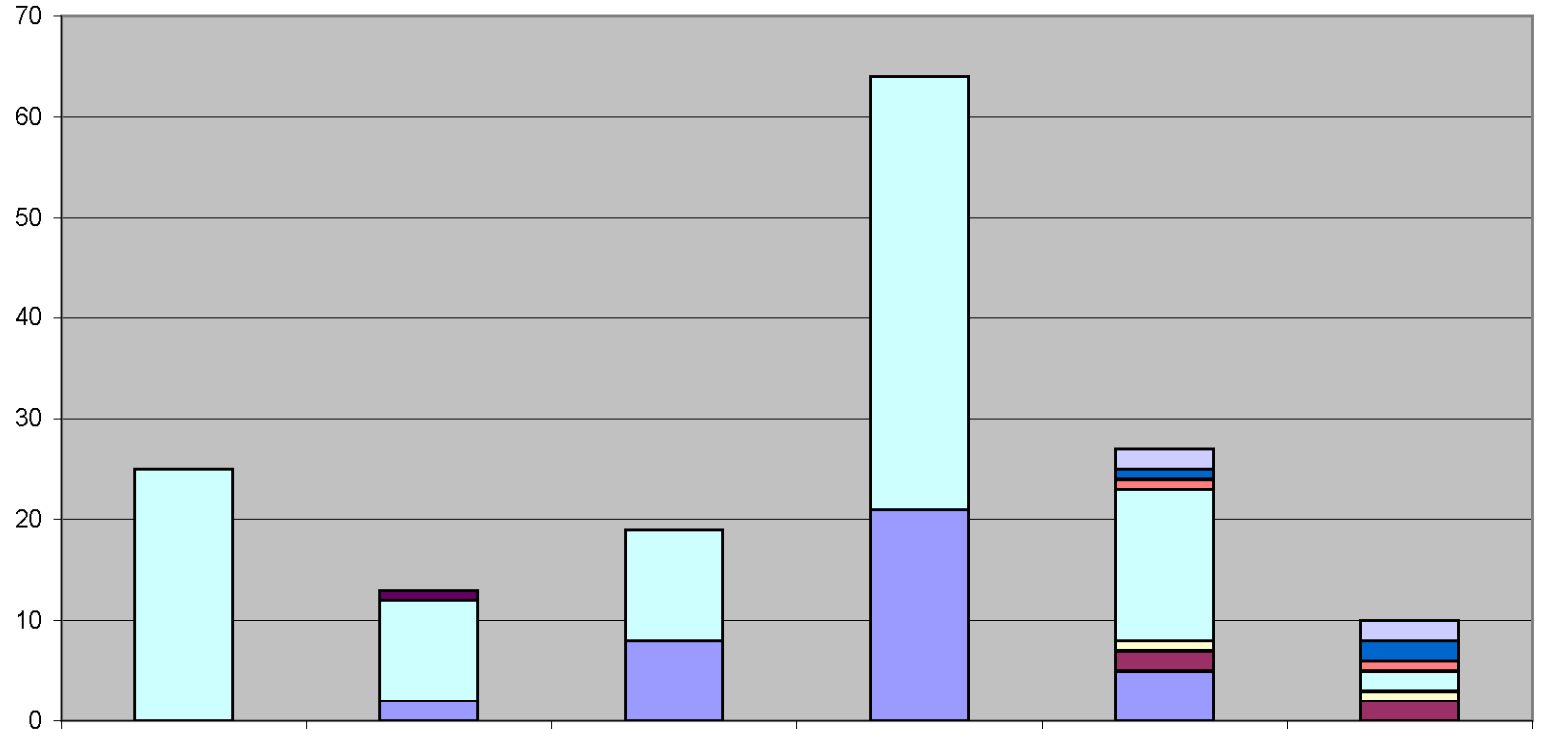
	ADV	AGD	ALC	ASE	ATE	AVA
report					1	2
record					1	2
produce					1	1
perform		1				
examine	6	10	1	36	2	2
devise					1	1
conduct					1	1
check		2	3	14	1	

EAL2



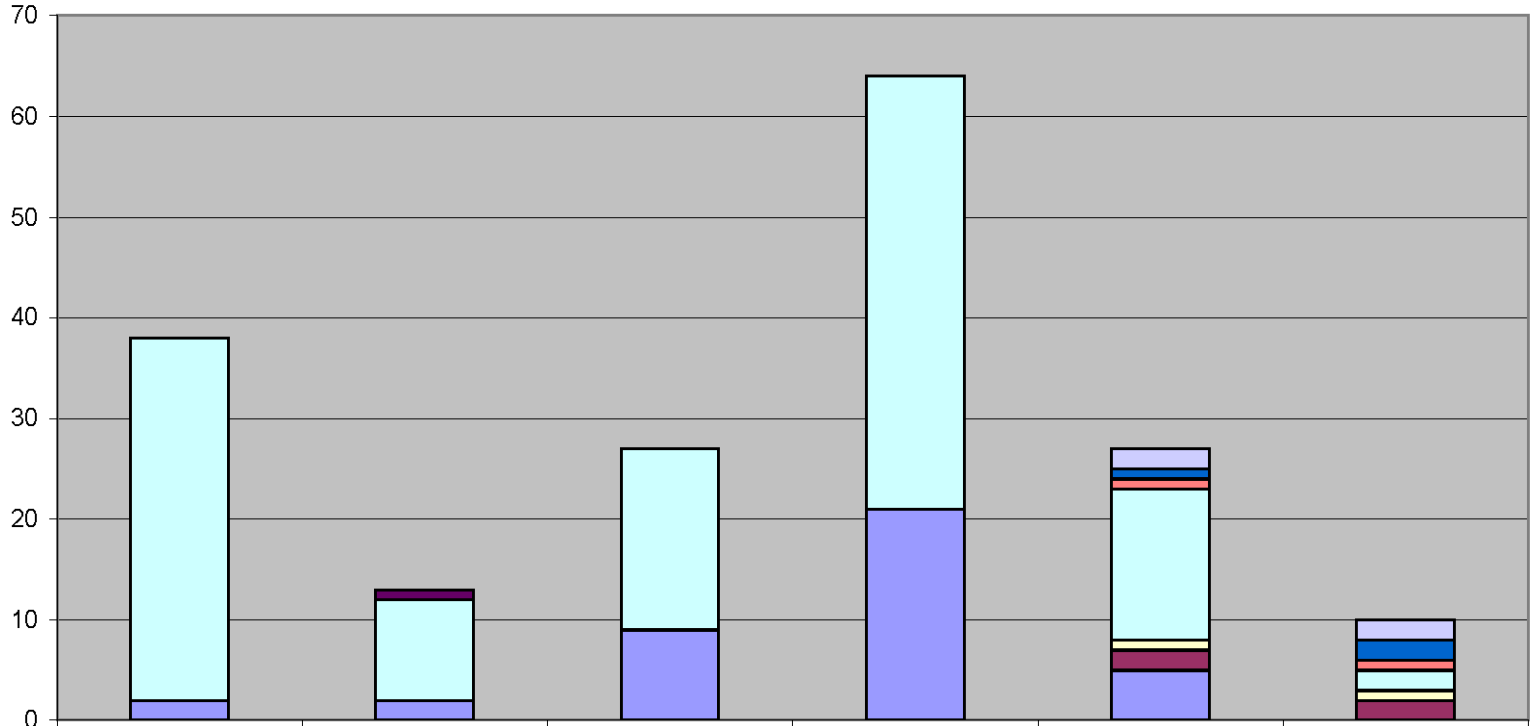
	ADV	AGD	ALC	ASE	ATE	AVA
report					2	2
record					1	2
produce					1	1
perform		1				
examine	22	10	5	43	8	2
devise					1	1
conduct					2	2
check		2	4	21	5	

EAL3



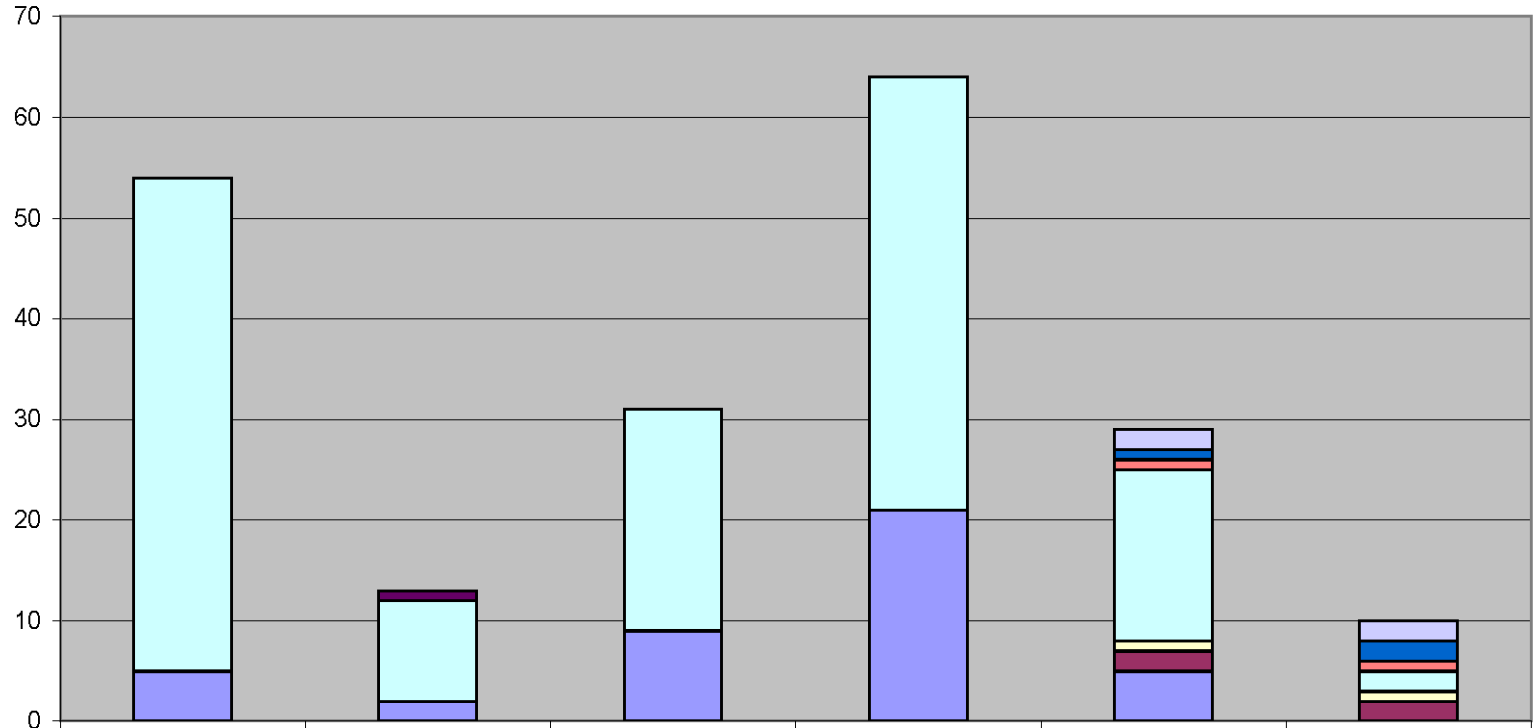
	ADV	AGD	ALC	ASE	ATE	AVA
report					2	2
record					1	2
produce					1	1
perform		1				
examine	25	10	11	43	15	2
devise					1	1
conduct					2	2
check		2	8	21	5	

EAL4



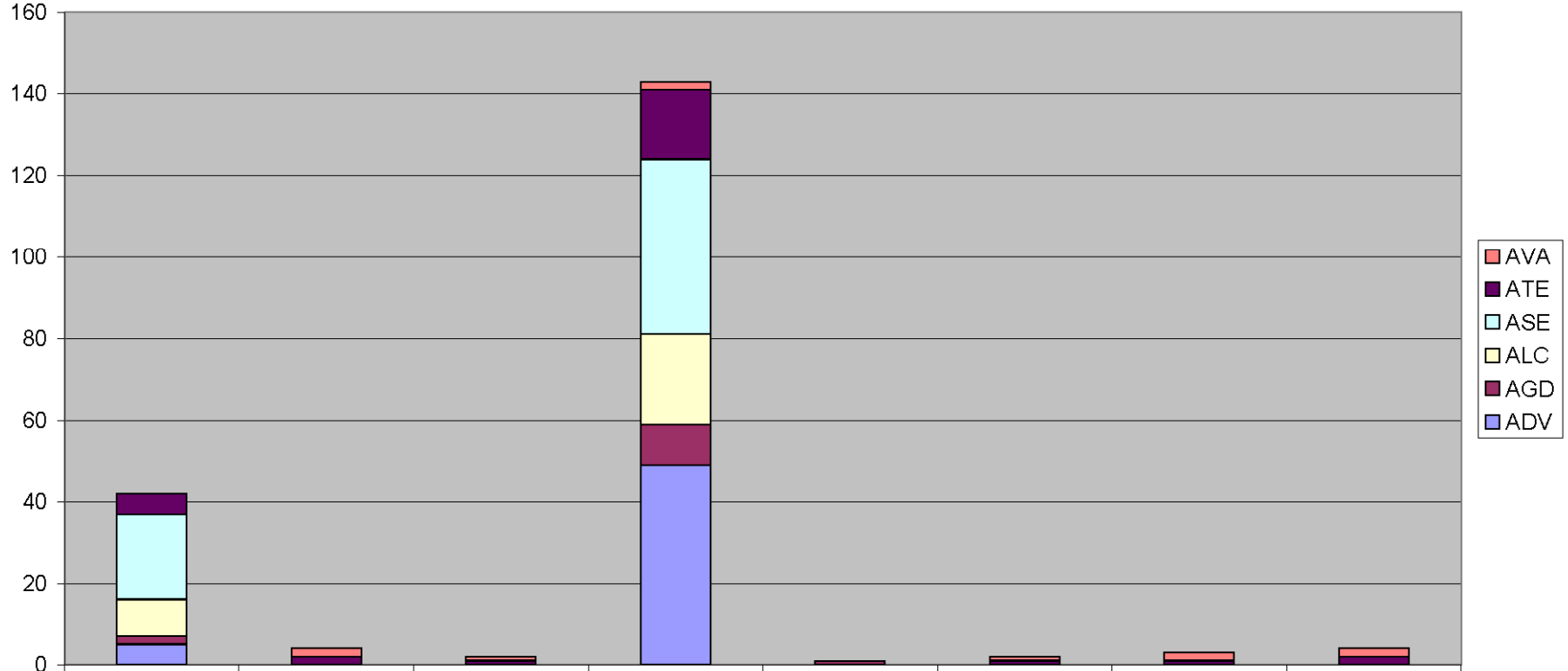
	ADV	AGD	ALC	ASE	ATE	AVA
report					2	2
record					1	2
produce					1	1
perform		1				
examine	36	10	18	43	15	2
devise					1	1
conduct					2	2
check	2	2	9	21	5	

EAL5



	ADV	AGD	ALC	ASE	ATE	AVA
report					2	2
record					1	2
produce					1	1
perform		1				
examine	49	10	22	43	17	2
devise					1	1
conduct					2	2
check	5	2	9	21	5	

EAL5



	check	conduct	devise	examine	perform	produce	record	report
AVA		2	1	2		1	2	2
ATE	5	2	1	17		1	1	2
ASE	21			43				
ALC	9			22				
AGD	2			10	1			
ADV	5			49				

Questions welcomed

Miguel Bañón

Representing the
National Cryptologic Centre
National Intelligence Centre

organismo.certificacion@cni.es