

Tool for Supporting a Common Criteria Evaluation

9th International Common Criteria Conference
Jeju, Korea – 25th September 2008





Instituto Nacional de
Técnica Aeroespacial



CESTI

Motivations

- Automate process and repetitive tasks
- Focus the evaluator effort on processes which require cognitive skills
- Understand potential automation in CC evaluations
- Learn about how XML and XSL transformations can assist in the process of automation
- *Not just less work, but smart work*



Instituto Nacional de
Técnica Aeroespacial



CESTI

Index

1. Automation
 1. Why
 2. How
 3. With What
2. Tool
 1. Inputs
 2. Processing
 3. Outputs
3. Current Status
4. Future Work



Instituto Nacional de
Técnicos Aeroespaciales



CESTI

Automation

1 Automation

1.1 Why

1.2 How

1.3 With What

2 Tool

3 Current Status

4 Future Work

- Reduce human intervention to a minimum
 - checking consistency
- Synchronize the results obtained for each evaluator
- Support the sponsor in avoiding typical mistakes
- Generate documentation using less time and effort
 - ETR from work units
 - OR from problems



Instituto Nacional de
Técnicos Aeroespaciales



CESTI

Why Automation?

Evaluators

1 Automation

1.1 Why

1.2 How

1.3 With What

2 Tool

3 Current Status

4 Future Work

- Reduce evaluation time and cost
- Detect errors earlier
- Focus on vulnerability search
- Track the evidences produced during the evaluation process



Instituto Nacional de
Técnicos Aeroespaciales



CESTI

Why Automation?

Developers

1 Automation

1.1 Why

1.2 How

1.3 With What

2 Tool

3 Current Status

4 Future Work

- Help sponsor to reduce common errors in documents
 - Check common errors before sending documentation
- Reduce the sponsor effort (time and cost)
- Improve sponsor satisfaction



Instituto Nacional de
Técnicos Aeroespaciales



CESTI

Why Automation?

1 Automation

1.1 Why

1.2 How

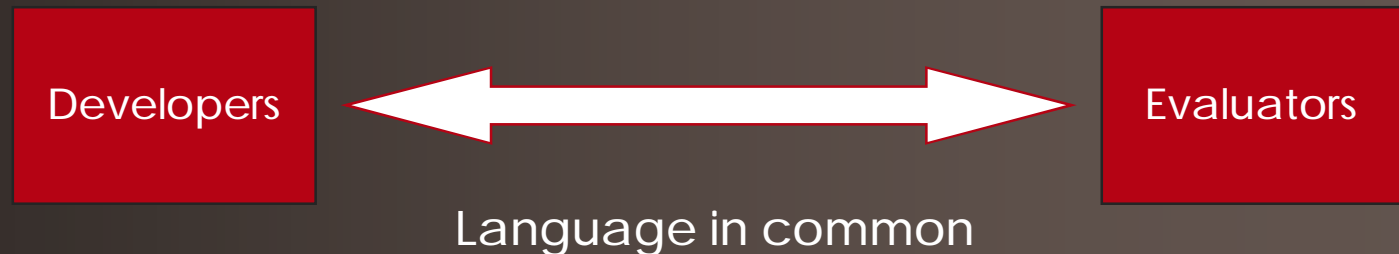
1.3 With What

2 Tool

3 Current Status

4 Future Work

- Agree on a language in common between Developer and Evaluator team
 - Establish fluent communication
 - Process automatically





Instituto Nacional de
Técnicos Aeroespaciales



CESTI

How Automation?

1 Automation

1.1 Why

1.2 How

1.3 With What

2 Tool

3 Current Status

4 Future Work

- XML
 - Structure independent from presentation
 - Source human and machine readable
 - Flexible markup language
 - Platform independent
 - Negotiated language between the man and the machine
- XSL Transformations
- Python Processing
- SVN
 - Open source version control system
 - Allow integration between evaluators



Instituto Nacional de
Técnicos Aeroespaciales



CESTI

What Tools?

1 Automation

1.1 Why

1.2 How

1.3 With what

2 Tool

3 Current Status

4 Future Work

- Python: Data processing
- PyQT: User Interface
- FOP: XSL Transformations to PDF files
- SVN: Configuration management tool

Python



PyQT



FOP



SVN



Instituto Nacional de
Técnicos Aeroespaciales



CESTI

SECT: Security Evaluation CC Tool

1 Automation

2 Tool

2.1 Inputs

2.2 Processing

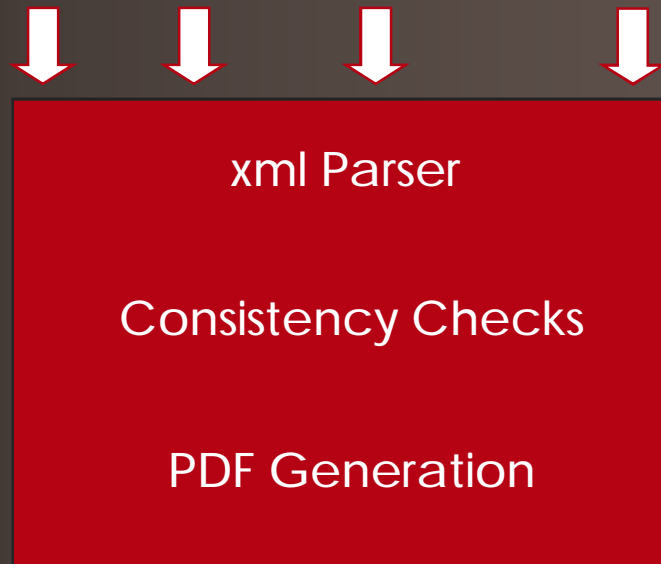
2.3 Outputs

3 Current Status

4 Future Work

Project
Information →

cc.xml st.xml checklist.xml macros.xml



→ Accountability

→ Audit

Work Unit

Observation

ETR



Instituto Nacional de
Técnicas Aeroespaciales



CESTI

SECT: Inputs

1 Automation

2 Tool

2.1 Inputs

2.2 Processing

2.3 Outputs

3 Current Status

4 Future Work

- Common Criteria Part 1-3 and CEM (from CCN, Spain)
 - cc.xml
 - cc2.xml

```
<m-workunit eal="all">  
  <ae-dc-element id="acm_aut.1.2c"/>  
  <para type="normal">  
    The evaluator shall check the CM documentation for  
    automated means to support generation of the TOE from  
    its implementation representation.</para>  
  <para type="normal" id="pgfId-710262">  
    In this work unit the term ``generation''  
    applies to those processes adopted by the developer to  
    progress the TOE from its implementation to a state  
    ready to be delivered to the end customer.</para>  
  <para type="normal" id="pgfId-710263">  
    The evaluator should verify the existence of automated  
    generation support procedures within the CM  
    documentation.</para>  
</m-workunit>
```



Instituto Nacional de
Técnicos Aeroespaciales



CESTI

SECT: Inputs

1 Automation

2 Tool

2.1 Inputs

2.2 Processing

2.3 Outputs

3 Current Status

4 Future Work

- Security Target
 - st.dtd (from CCN, Spain)

```

<!ELEMENT introduction      (identification,overview,cc-claim) >

<!ENTITY % parasequence    "(biblioentry|figure|glossentry|para|subclause|table) *">

<!ELEMENT identification    (st-reference,toe-reference) >
<!ELEMENT overview         (%parasequence;) >
<!ELEMENT cc-claim         (%parasequence;) >

<!ELEMENT st-reference     (st-title,st-version,st-revision,st-author,st-publication-date) >
<!ELEMENT toe-reference    (developer,toe-name,toe-version) >

<!ELEMENT st-title         (#PCDATA) *>
<!ELEMENT st-version       (#PCDATA) *>
<!ELEMENT st-revision      (#PCDATA) *>
<!ELEMENT st-author        (#PCDATA) *>
<!ELEMENT st-publication-date (#PCDATA) *>
<!ELEMENT developer        (#PCDATA) *>
<!ELEMENT toe-name         (#PCDATA) *>
<!ELEMENT toe-version      (#PCDATA) *>

```



Instituto Nacional de
Técnicos Aeroespaciales



CESTI

SECT: Inputs

- Checklists for each work unit
– checklist.xml

1 Automation

2 Tool

2.1 Inputs

2.2 Processing

2.3 Outputs

3 Current Status

4 Future Work

```
<assessment-method type="Examine">
  <select-from>
    <ol>
      <li>
        <foreach operation="=">
          <item>label.packagingOrMedia</item>
          <item>label.guidance</item>
          <item>label.operationalTOE</item>
        </foreach>
      </li>
      <li>
        <foreach operation="=">
          <item>reference.TOE</item>
          <item>TOEreference.ST</item>
        </foreach>
      </li>
      <li>
        <foreach operation="=">
          <item>label.operationalTOE</item>
          <foreach operation="+">
            <item>label.operationalTOEComponent</item>
          </foreach>
        </foreach>
      </li>
    </ol>
  </select-from>
</assessment-method>
```



Instituto Nacional de
Técnicos Aeroespaciales



CESTI

SECT: Inputs

- Macros
 - macros.xml

1 Automation

2 Tool

2.1 Inputs

2.2 Processing

2.3 Outputs

3 Current Status

4 Future Work

```

<basic>
  <ProductS>FNMT Crypto</ProductS>
  <ProductL>*****</ProductL>
  <ProductV>***</ProductV>
  <ProductC>*****</ProductC>
  <EALLevel>EAL 4</EALLevel>
  <EALAumentado><ul><li>ALC_FLR.1</li><li>AVA_VAN.5</li></ul></EALAumentado>
  <SponsorS>FNMT-RCM</SponsorS>
  <SponsorL>Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda</SponsorL>
  <SponsorA>FNMT-RCM<br/>Calle Odonnel<br/>28090 Madrid</SponsorA>
  <DeveloperS>FNMT-RCM</DeveloperS>
  <DeveloperL>Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda</DeveloperL>
  <DeveloperA>FNMT-RCM<br/>Calle Odonnel<br/>28090 Madrid</DeveloperA>
  <CBS>CCN</CBS>
  <CBL>Centro Criptológico Nacional</CBL>
  <CBA>Organismo de Certificación<br/>Avda. Padre huidobro s/n<br/>28023 Madrid<br/>http://
  <CCV>3.1 R2</CCV>
  <CEMV>3.1 R2</CEMV>
  <EvalLevel>EAL4+ AVA_VAN.5 y ALC_FLR.1</EvalLevel>
  <startDate>12-02-2008</startDate>
</basic>

```



Instituto Nacional de
Técnicas Aeroespaciales



CESTI

SECT: Processing

- Parsing XML: User writes in xml vs dtd
 - Using a XML parser (Python)

1 Automation

2 Tool

2.1 Inputs

2.2 Processing

2.3 Outputs

3 Current Status

4 Future Work

The screenshot shows the SECT tool interface. On the left is a tree view of the project structure, including folders like 'ase', 'ase_int.1', 'ase_cdi.1', 'ase_spd.1', 'ase_obi.2', 'ase_ecd.1', 'ase_req.2', 'ase_tse.1', 'ase_comp.1', 'agd', 'agd_ope.1', 'agd_pre.1', 'akc', 'alc_rmc.4', 'alc_rms.4', 'alc_del.1', 'alc_dvs.1', 'alc_fr.1', 'alc_lcd.1', 'alc_lst.1', 'ate', 'ate_cov.2', 'ate_dpt.2', 'ate_fun.1', and 'ate_ind.2'. The main window on the right displays a 'Guideline' section with the following text:

ASE_INT.1.1E:
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_INT.1.1C:
The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

Procedure:
The evaluator shall check that the ST introduction contains an ST reference, a TOE reference, a TOE overview and a TOE description.

The 'Result' section shows a 'PYSEC' error dialog box with the following message:

The following errors have been found in ase_int.1-1: Opening and ending tag mismatch: li line 8 and ul, line 12, column 10.
Trying to save the test. Good Luck!

The dialog box has an 'OK' button. The main window also has 'Source' and 'Preview' buttons at the bottom left and a 'Save' button at the bottom right.



Instituto Nacional de
Técnicos Aeroespaciales



CESTI

SECT: Processing

- Checking consistency

1 Automation

2 Tool

2.1 Inputs

2.2 Processing

2.3 Outputs

3 Current Status

4 Future Work

- ASE_REQ.2-3: The evaluator *shall examine* the ST to determine that all subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs are defined.
- ASE_OBJ.2-2: The evaluator *shall check* that the security objectives rationale traces all security objectives for the TOE back to threats countered by the objectives and/or OSPs enforced by the objectives.
- ASE_ECD.1-2: The evaluator *shall check* that the extended components definition defines an extended component for each extended security requirement.



Instituto Nacional de
Técnicos Aeroespaciales



CESTI

SECT: Processing

- Generating PDF (Report)
 - XSL: Using FOP

1 Automation

2 Tool

2.1 Inputs

2.2 Processing

2.3 Outputs

3 Current Status

4 Future Work

```
<?xml version="1.0" encoding="UTF-8" ?>

<!-- STYLESHEET FOR REPORTS -->

<xsl:stylesheet
  version="1.1"
  xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
  xmlns:fo="http://www.w3.org/1999/XSL/Format"
  xmlns:axf="http://www.antennahouse.com/names/XSL/Extensions"
  exclude-result-prefixes="fo">

  <xsl:include href="param.xsl"/>
  <xsl:include href="attribute.xsl"/>
  <xsl:strip-space elements="table tr td program"/>

  <xsl:template match="report">
    <fo:root xmlns:fo="http://www.w3.org/1999/XSL/Format">
      <fo:layout-master-set>
        <fo:simple-page-master master-name="PageMaster">
```



Instituto Nacional de
Técnicos Aeroespaciales



CESTI

SECT: Outputs

1 Automation

2 Tool

2.1 Inputs

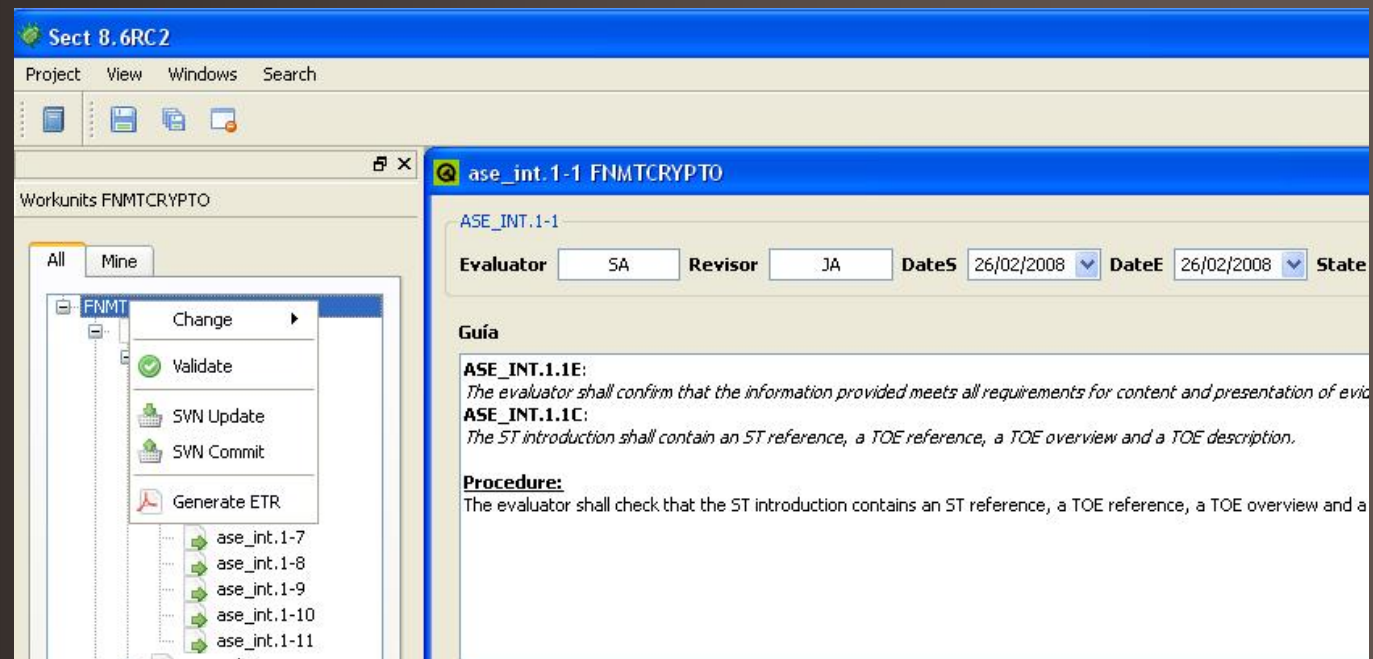
2.2 Processing

2.3 Outputs

3 Current Status

4 Future Work

- Work Unit / Subactivity / Activity Report
- Observation Report
- Evaluation Technical Report





Instituto Nacional de
Técnicos Aeroespaciales



CESTI

Current Status

1 Automation

2 Tool

3 Current Status

4 Future Work

- PDF Report Generation
 - Work Units
 - Observations
 - Evaluation Technical Report
- Intelligent Labels
- Work with XML Security Targets that meet a DTD
- Evaluation Process Management and Coordination
- Checklist (ALC_CMC.4)



Instituto Nacional de
Técnicos Aeroespaciales



CESTI

Future Work

1 Automation

2 Tool

3 Current Work

4 Future Work

- Checklists (ALC site visit)
- Reports signed with electronic signatures
- Generate Plans, Procedures and Reports automatically (ATE and AVA)
- Work with XML Documents that meet a DTD (not only the ST)
- Incorporate requirements from supporting documents



Instituto Nacional de
Técnica Aeroespacial



CESTI

Thank you

Maria Soraya Artiles Burgos
Security Technical Manager
artilesbs@inta.es