SCAP Content VALIDATION

Andrew Bove

AGENDA

- The Mission of SCAP Content Validation
- Relationship to The NCP
- Tiers and Why They are Important
- Why SCAP Content Validation is Important

Mission

- Explore methods that will ensure that published content will understood and by all SCAP validated tools.

Checklist Tiers* (I, II and II)

- **Tier I** checklists are prose-based, such as narrative descriptions of how a person can manually alter a product's configuration.

- **Tier II** checklists document their recommended security settings in a machine-readable but non-standard format, such as a proprietary format or a product-specific configuration script. These checklists may include some elements of SCAP (for example, they may contain CCE identifiers), but do not meet the Tier III requirements.

- **Tier III** checklists use SCAP to document their recommended security settings in ***machine-readable standardized SCAP formats that meet the definition of "SCAP Expressed" specified in NIST SP 800-126*** [29]. Tier III checklists can be processed by SCAP-validated tools, which are products that have been validated by an accredited independent testing laboratory as conforming to applicable SCAP specifications and requirements.

(*)NIST SP 800-70R1: NATIONAL CHECKLIST PROGRAM FOR IT PRODUCTS: GUIDELINES FOR CHECKLIST USERS AND DEVELOPERS

Checklist Tiers* (IV)

- **Tier IV** checklists include all properties of Tier III checklists. Additionally, Tier IV checklists are considered **production-ready** and have been validated by NIST or a NIST-recognized authoritative entity to ensure, to the maximum extent possible, interoperability with SCAP-validated products. Tier IV checklists also demonstrate the ability to **map low-level security settings (for example, standardized identifiers for individual security configuration issues) to high-level security requirements** as represented in various security frameworks (e.g., SP 800-53 controls for FISMA), and the mappings have been vetted with the **appropriate authority**.

(*)NIST SP 800-70R1: NATIONAL CHECKLIST PROGRAM FOR IT PRODUCTS: GUIDELINES FOR CHECKLIST USERS AND DEVELOPERS

Conventional Approach

- Validate an XML instance document using a grammar-based language (e.g. DTD, Relax NG, XML Schema)
- Validate using a rule-based language (i.e. Schematron)
- So, What's the problem(s)?

Well…

- Inter and Intra File / Document Relationships
- Style Impacts Understanding
- Derived versus Declared Meaning / Intention
- Normative versus Informative

The “Context” of Content

- Content Relationships – Double Edged Sword
  - Inter and Intra File / Document Relationships
    - Documents and Files need to move in Lock Step
      - Versioning at Fragment Level is not possible
    - Information sharing problematic
      - Re-use and Distributed Repositories
      - Clone Rules → Maintenance Chaos
    - The most ‘insignificant” change causes the reset to square-one
      - Version=N+1 even when there is no change
- Content Is Difficult To Validate Therefore Content Interpretation is Problematic
  - Schema Validation Barely Gets You in the Game
  - Style Impacts Understanding/Interpretation
  - Inter and Intra File/Document Relationships
  - Lack of a Ontology (Model)

IS SCAP REALLY A SPECIAL CASE?

1. XBRL and The SEC
   - “Companies will provide their financial statements to the Commission and on their corporate Web sites in interactive data format using (XBRL).” - April 13, 2009 http://www.sec.gov/rules/final/2009/33-9002.pdf

IS SCAP REALLY A SPECIAL CASE?

2. Health Level Seven (HL7) and Health Care
   - http://www.hl7.org/Library/standards.cfm
   - The CCOW standard exists to facilitate a more robust, and near **"plug-and-play"** interoperability across disparate applications.
   - CCOW Enables Context Management

Transacting The Business of Security

- Can I create a standard simple open format to describe my message structures and data content rules?
- Can my partners validate their transactions in test BEFORE they send them?
- How do people know what I will send them?
- I want something that's simple and standards based – leverages existing XML components
- Can I generate HTML documentation that is readable by business analysts?

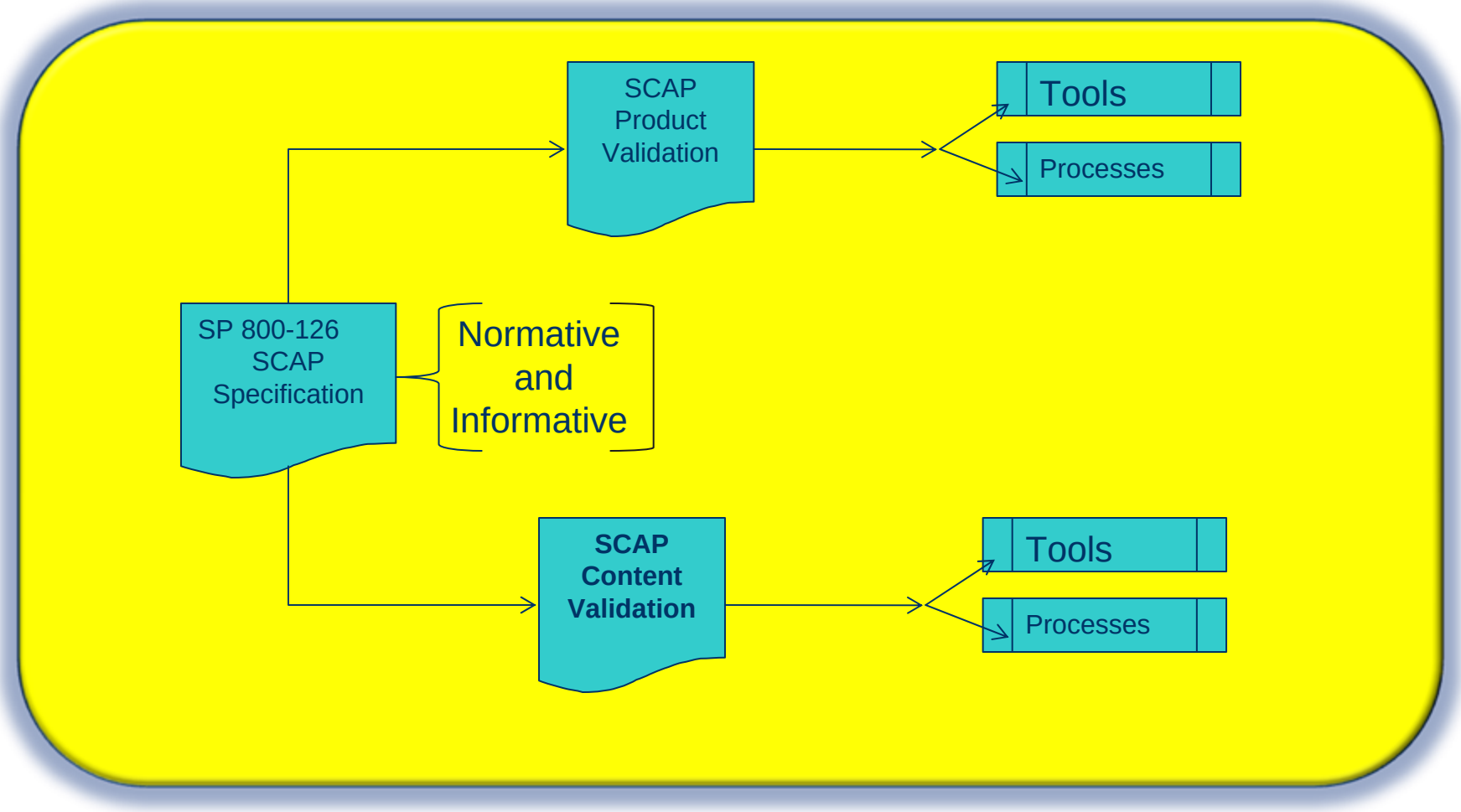
Expectations of Transacting Business

- Automatic information integration has been the Holy Grail of business systems since before XML was conceived.
  - Remember EDI?
- Lesson learned
  - the ability to design transactions consistently,
  - the ability to document their usage in a clear way
  - the ability to drive software that can apply rules and test information content to ensure correct compliance.

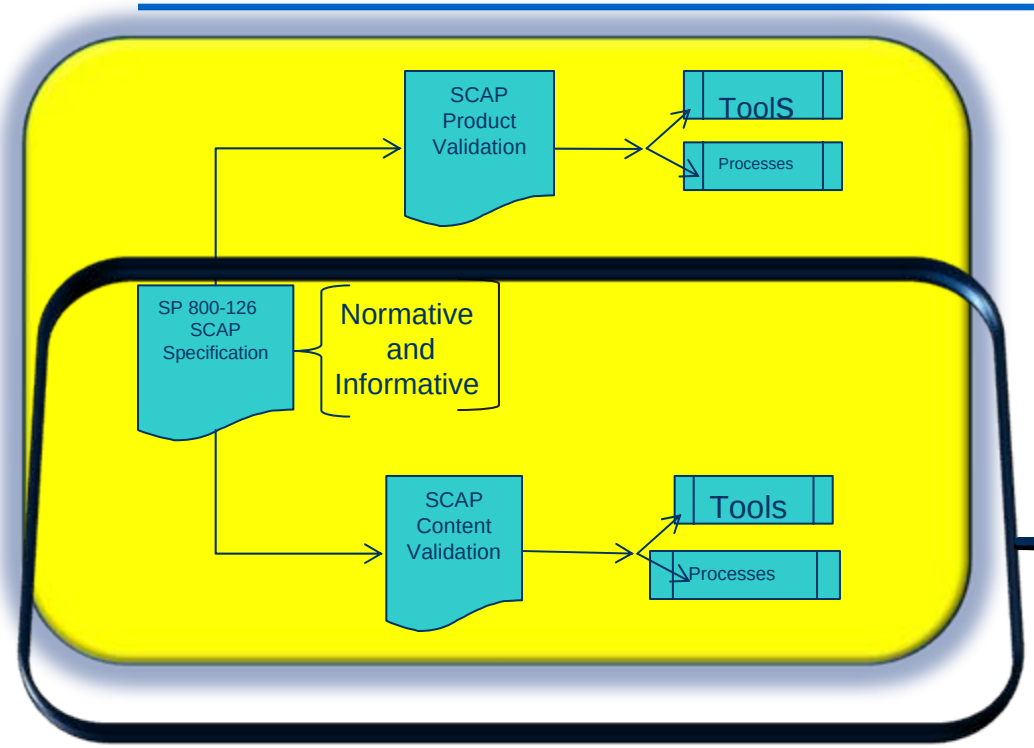
We Are Not Alone

- “The current semantical validation performs about 400 checks. These are checks to ensure references within the BPEL, to WSDL documents or to XSD Schemas are valid and there are checks to ensure the rules defined by the BPEL specification are not violated.”

What Are We Doing?

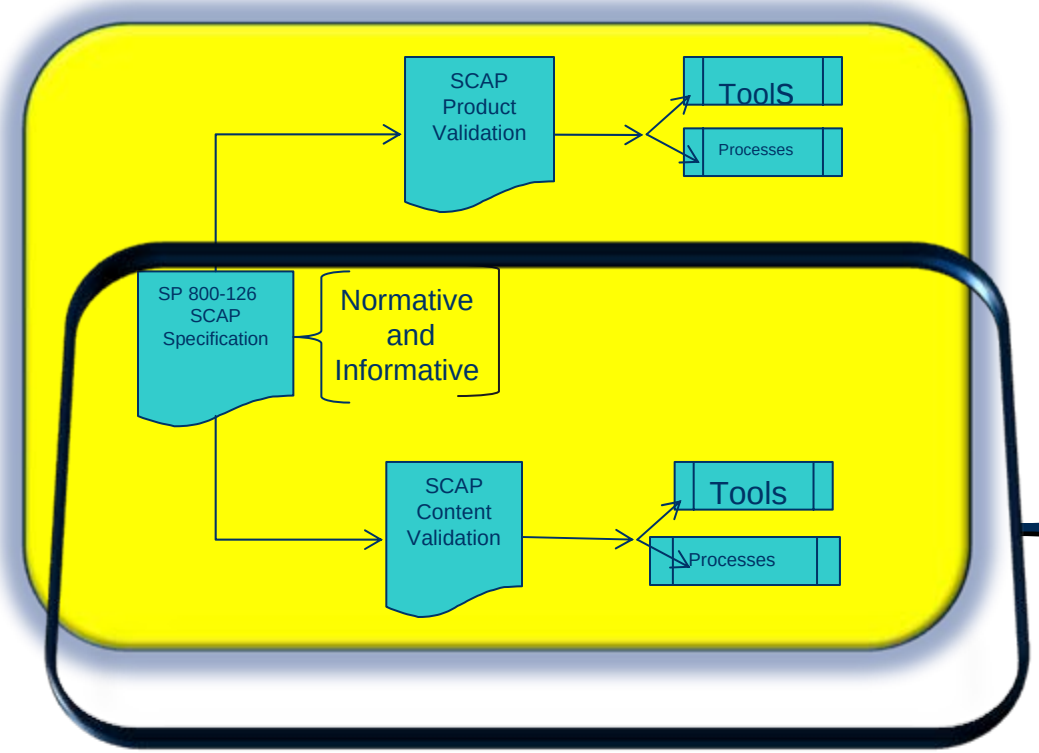


Content Validation Program



- ✓ Form
- ✓ Syntax
- ✓ Semantics

Products and By-Products

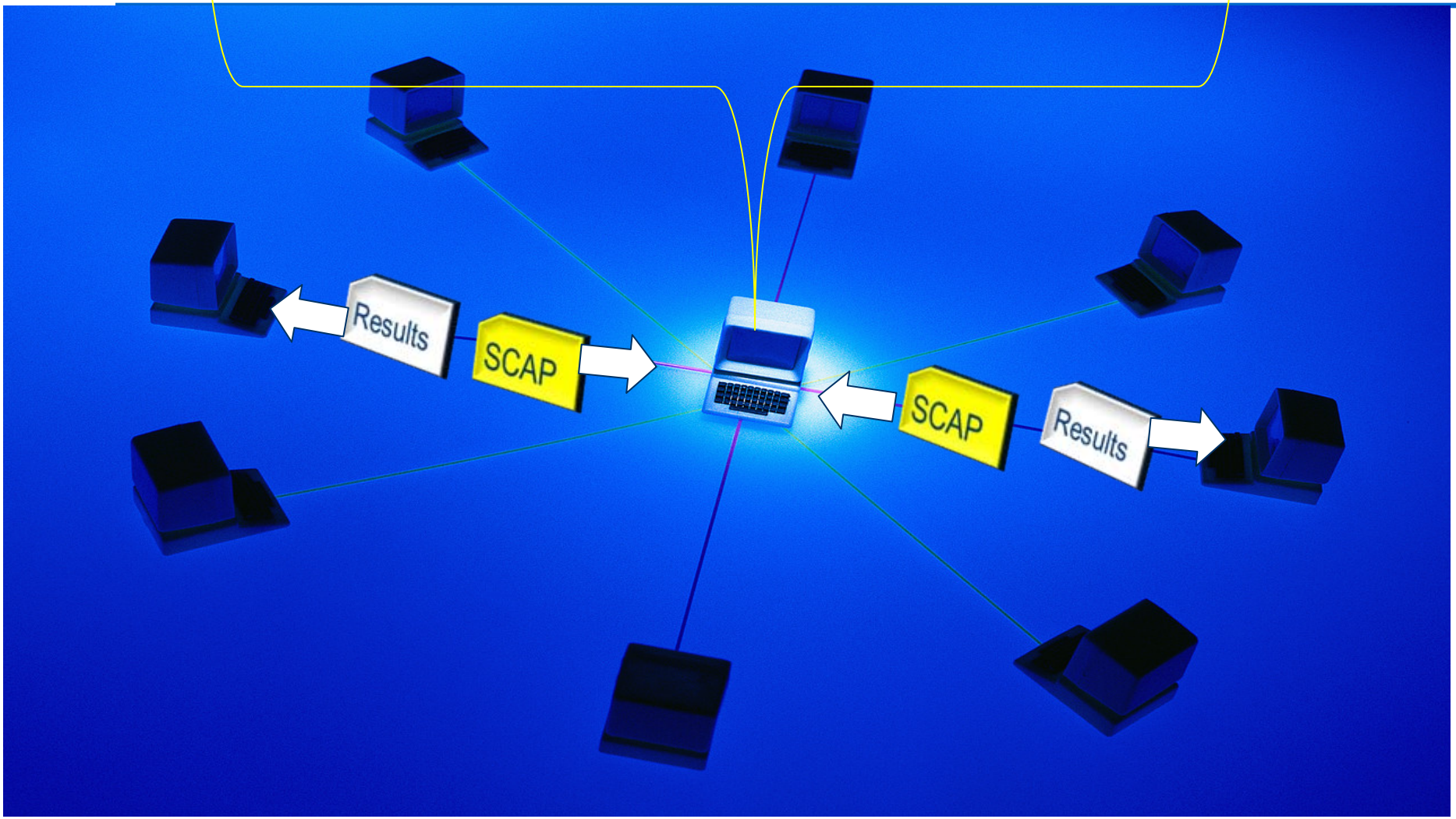


1. Feed Back:
   a. Errors
   b. Warnings
   c. Recommendations
2. Feed Forward:
   a. Augmented Metadata
   b. Cross Reference

SCAP Content Validation Service

- Validate
  - Form, Syntax, and Semantics
- For
  - Generic SCAP
  - Specific Use case
    - Configuration Verification
    - Vulnerability Assessment
    - Patch Validation
    - Inventory Collection
  - Tier III

SCAP Content Validation Service



SCAP Content Validation Service

- Ensures that checklists ***can be processed by SCAP-validated tools…***

Contact Information

Andrew.Bove@SecureAcuity.NET