

Official CPE Dictionary

Discussion

Agenda

- CPE Dictionary Debrief
- CPE Dictionary Interfaces
- CPE Dictionary Content
- CPE Lifecycle Process
- CPE Content Contribution

CPE Dictionary Debrief

Dictionary Content - Statistics

- Focused on products from 250 widely used vendors
- Final dictionary contains 15,000+ CPE names
- 3000+ products
- 58 OVAL inventory definitions
- 2.0 CPE names included with deprecated attributes

CPE Dictionary Issues / Decisions

- Marketing versions vs. software versions

Software Product 2008 vs. Software Product 7.1

- The year often pertains to multiple versions
- Using software versions allows correlation between multiple versions

Decision: `cpe:/a:software:product:7.1`

CPE Dictionary Issues / Decisions (cont.)

- Is firmware a hardware version or an OS/Application?

Hardware Router rev4 1.2.3

- Vendors refer to firmware as the version of the router.
- Some hardware has a revision
- The firmware does not have a distinct name from the hardware

Decision: `cpe:/h:hardware:router_rev4:1.2.3`

CPE Dictionary Issues / Decisions (cont.)

- The same product version exists for two vendors resulting from acquisition

Vendor, inc Product 1.1

Newvendor, inc Product 1.1

Decision: `cpe:/a:vendor:product:1.1` and
`cpe:/a:newvendor:product:1.1`

Resulting in duplicate CPEs for the same product.
Is this a problem?

CPE Dictionary Issues / Decisions (cont.)

- What to do where little information exists for old products?

Decision: Use legacy NVD product data where no other information is available. Rely on data within CVEs that reference these products.

CPE Dictionary Issues / Decisions (cont.)

- Product families vs. full enumeration of specific products

Cisco 2600 Series

Decision: `cpe:/h:cisco:2621`, `cpe:/h:cisco:2691`,
etc.

CPE Dictionary Issues / Decisions (cont.)

- When should an OS be used as part of a product name or as an edition?

Vendor Adapter for Mac OS X

Vendor Adapter for Enterprise Systems

- Both products represent different code bases, release cycles, etc.

Decision: `cpe:/a:vendor:adapter_for_mac_os_x`
and
`cpe:/a:vendor:adapter_for_enterprise_systems`

CPE Dictionary Issues / Decisions (cont.)

- How do you write a CPE name for the initial software release when subsequent updates have been provided?

cpe:/a:vendor:product:1.0 (all updates)

cpe:/a:vendor:product:1.0:sp1 (sp1 update)

cpe:/a:vendor:product:1.0:sp2 (sp2 update)

What about the initial release prior to the first update?

What if the vendor does not provide a name for the initial update such as: ga, rtm, gold, etc?

Future discussion point: Implicit vs. explicit matching using wildcards

CPE Dictionary Issues / Decisions (cont.)

- What to do when you can't find a specific version?

Decision:

- If evidence indicates that version 1.4 exists, then there is no harm including 1.3

CPE Dictionary Issues / Decisions (cont.)

What if software is not versioned?

Not including a version implies all versions

Discussion point:

What if the vendor does not version their software?

CPE Dictionary Issues / Decisions (cont.)

- Inconsistent vendor version references are found

12.1.2 vs 12.1(2)

Decision: Use the most prevalent scheme, when vendor input is not available.

CPE Dictionary Issues / Decisions (cont.)

Should a standard be adopted for language components?

Decision: We are using ISO 639-1

CPE Dictionary Interfaces

Multiple methods will exist to retrieve CPE Dictionary data

- Official CPE Dictionary–XML Format
- Web Search Interface
 - HTML Formatted CPE Dictionary
 - Ability to download search results in XML dictionary format
 - Permits custom creation of CPE Dictionaries
- Web Services Interface
 - Querying capability
 - CPE name
 - Official and repository metadata
 - Results are in CPE dictionary format wrapped by SOAP headers

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

```
<FindItemsRequest xmlns="http://scap.nist.gov/schema/cpe-dictionary-service/0.1"
```

```
  xmlns:cpe-meta="http://scap.nist.gov/schema/cpe-dictionary-metadata/0.1"
```

```
  xmlns:scap-core="http://scap.nist.gov/schema/scap-core/0.1">
```

```
  <criteria>
```

```
    <cpe-meta:include-cpe-with-status>
```

```
      <cpe-meta:cpe-status>final</cpe-meta:cpe-status>
```

```
    </cpe-meta:include-cpe-with-status>
```

```
    <cpe-meta:include-deprecated-cpe>false</cpe-meta:include-deprecated-cpe>
```

```
    <cpe-meta:include-cpe-modified-since>2008-01-01T00:00:00</cpe-meta:include-cpe-  
modified-since>
```

```
    <cpe-meta:include-products>
```

```
      <scap-core:cpe-name>cpe:/a:Microsoft:Office:2000</scap-core:cpe-name>
```

```
      <scap-core:cpe-searchable-name>cpe:/o:Microsoft:Windows*</scap-core:cpe-  
searchable-name>
```

```
    </cpe-meta:include-products>
```

```
  </criteria>
```

```
</FindItemsRequest>
```

Repository
Metadata

CPE Name

Wildcard
CPE Name

CPE Dictionary Content

The CPE dictionary schema does not support all user interface use cases

Problem:

- Building a CPE name from individual components
- Presenting meaningful component titles

Solution:

- Hierarchical component tree
- Associating metadata with specific components
 - Titles
 - References

```
<component-tree xmlns="http://scap.nist.gov/schema/cpe-dictionary-  
  metadata/0.1">  
  <vendor value="microsoft">  
    <title xml:lang="en">Microsoft Corporation</title>  
    <product value="office" part="a">  
      <title xml:lang="en">Office</title>  
      <version value="2000">  
        <title xml:lang="en">2000</title>  
        <update value="sp1">  
          <title xml:lang="en">Service Pack 1</title>  
        </update>  
      </version>  
    </product>  
    <product value="windows-xp" part="o">  
      <title xml:lang="en-US">Windows XP</title>  
      <version value="sp1">  
        <title xml:lang="en">Service Pack 1</title>  
      </version>  
    </product>  
  </vendor>  
</component-tree>
```

The CPE dictionary schema does not support a CPE name lifecycle

Problem: the `<cpe-item>` does not contain any status or change information

```
<cpe-item name="cpe:/a:microsoft:ie:7.0">  
  <title xml:lang="en-US">Microsoft ie 7.0</title>  
</cpe-item>
```

Solution:

```
<cpe-item name="cpe:/a:microsoft:ie:7.0">  
  <title xml:lang="en-US">Microsoft ie 7.0</title>  
  <meta:item-metadata modification-date="2007-10-01T15:16:59.160-  
    04:00" status="DRAFT" nvd-id="68457" />  
</cpe-item>
```

Each CPE name in the dictionary has a maintenance cost

- Titles
- Checks
- Deprecation
- Bandwidth
- Processing
- Change history

There is a potential for exponential growth when enumerating products

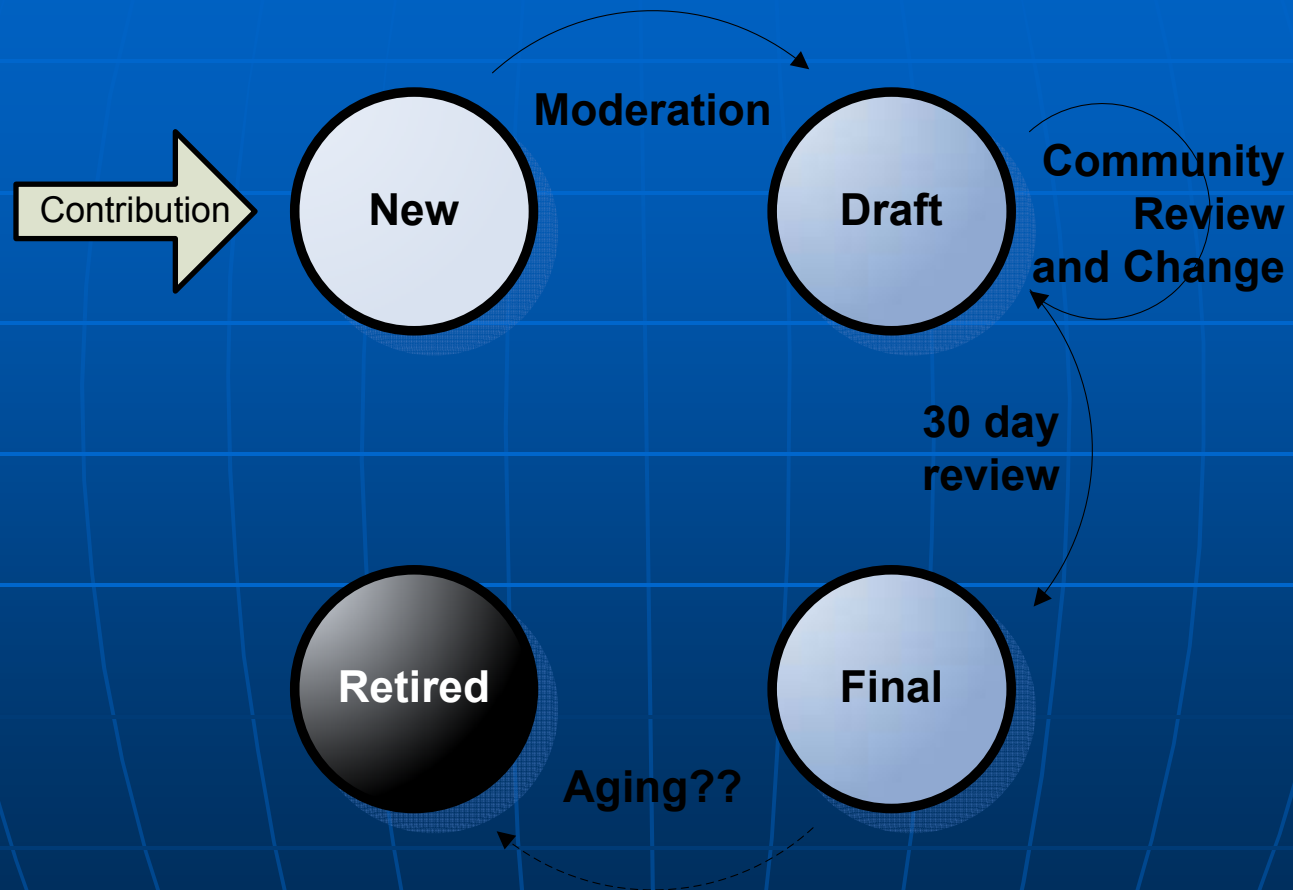
- $2^n - 1$ where n is the number of components
- `cpe:/part:vendor` = 3
- `cpe:/part:vendor:product` = 7
- `cpe:/part:vendor:product:version` = 15
- `cpe:/part:vendor:product:version:update` = 31
- `cpe:/part:vendor:product:version:update:edition` = 63
- `cpe:/part:vendor:product:version:update:edition:language` = 127

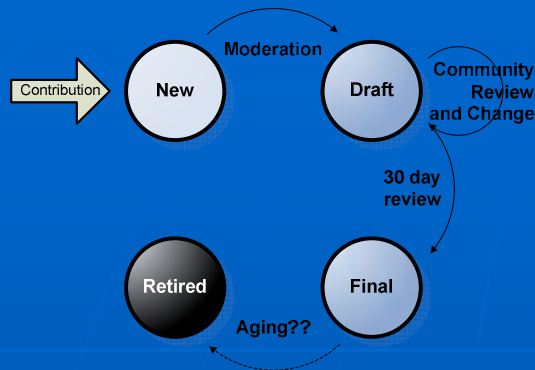
The solution: enumerating every possible CPE name is not necessary

- Leaf nodes provide all data necessary to generate every possible variation
- Variations are only needed where additional metadata is required
 - Checks
 - Notes
 - References
 - Titles
- Does not prevent the use of CPE name matching

CPE Lifecycle Process

A possible lifecycle process

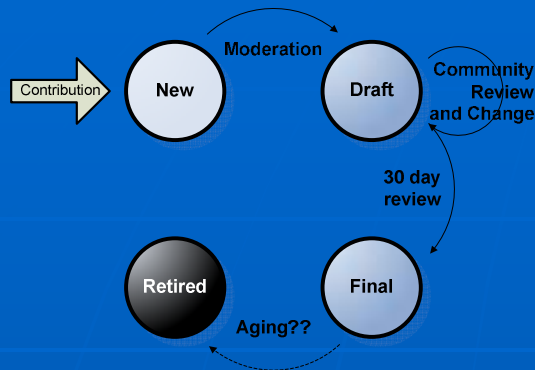




CPE Name Creation

- Each CPE name is assigned a tracking identifier - *nvd_id*
 - Used for change tracking
- Community contributed, non-authoritative CPE names are assigned a **NEW** status.
- Vendor contributed, authoritative names are assigned a **DRAFT** status

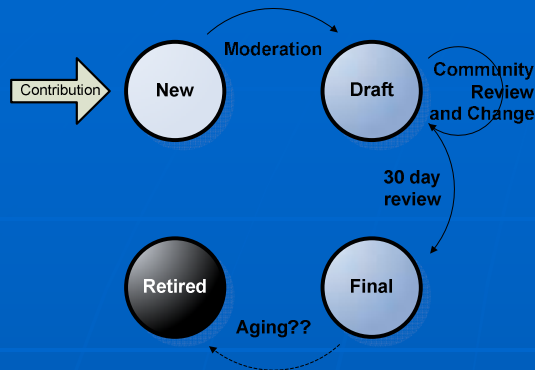
NEW



- Name is subject to change at any time
- CPE name is not included in the dictionary
- Review by the CPE moderation authority is required to transition the state to **DRAFT**.

Criteria for transition to **DRAFT** status:

- CPE name must follow the specification
- Must not reference a product covered by an existing CPE name
- All components must be normalized with similar names

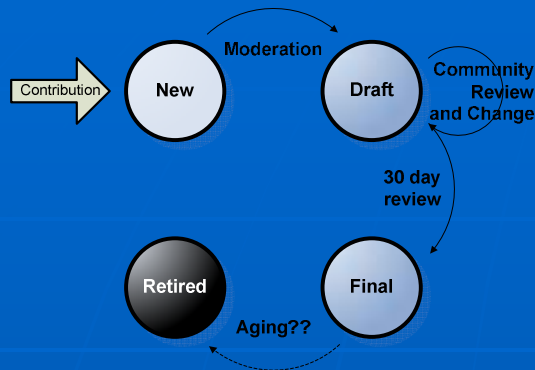


DRAFT

- CPE name is added to the dictionary
- Available for public review and comment, final quality assurance check
- Allows time for metadata to be created (checks, references, etc)
- Name is subject to change at any time
- Any change to the CPE name resets the 30 day clock

Criteria for transition to **FINAL** status:

- No CPE name change for a 30 day period
- Addition of metadata does not reset the clock

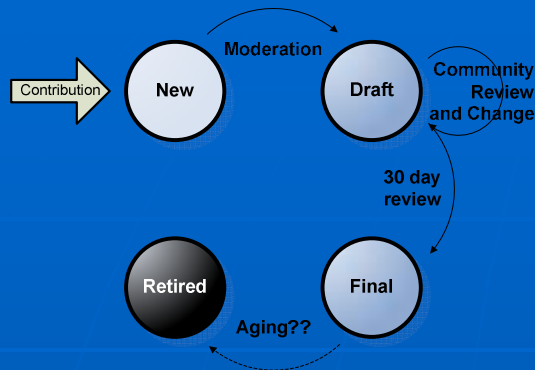


FINAL

- The name is now frozen
- The *nvd_id* is removed
- Metadata can be added, removed or updated resulting in a change to the modification date

Criteria for transition to **RETIRED** status:

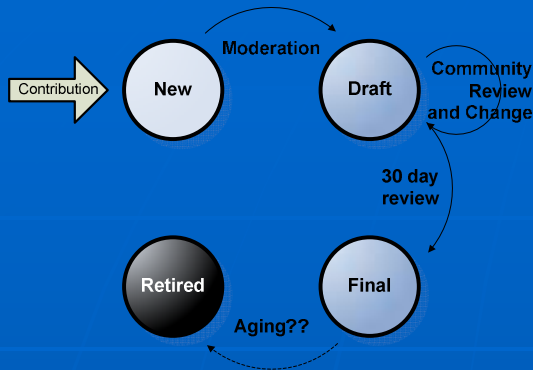
- Deprecation date greater than 1 year



RETIRED

- Reserved for deprecated CPE names
- The name remains frozen
- The name is removed from the dictionary, but remains in the repository
- Metadata can be added, removed or updated resulting in a change to the modification date – **Why?**

Deprecation



- A CPE name may be deprecated due to replacement by another CPE name
- A bogus CPE name may be deprecated without a replacement
- The CPE moderation authority must approve all deprecation requests

Future Workflow

- Content will be managed through web and web service interfaces
- Vendor access will be provided on an authenticated basis for authoritative CPE name management

CPE Content Contribution

CPE Content Contribution

- What is needed:
 - Corrections
 - Authoritative content from primary source vendors
 - CPE name and component titles
 - Checks - inventory definitions
 - References to product info

Contact Info

- CPE Dictionary Page

<http://nvd.nist.gov/cpe.cfm>

- Staff

Peter Mell - mell@nist.gov

- Support

David Waltermire - David.waltermire@nist.gov

Harold Booth - Harold.booth@nist.gov

John Banghart - John.banghart@nist.gov