Universal (Software) Product Identity: Solving a Hard Problem Twice Over

Art Manion (US)

Thomas Proell (Siemens ProductCERT, DE)

Thomas Schmidt (BSI, DE)

The naming problem

The naming problem

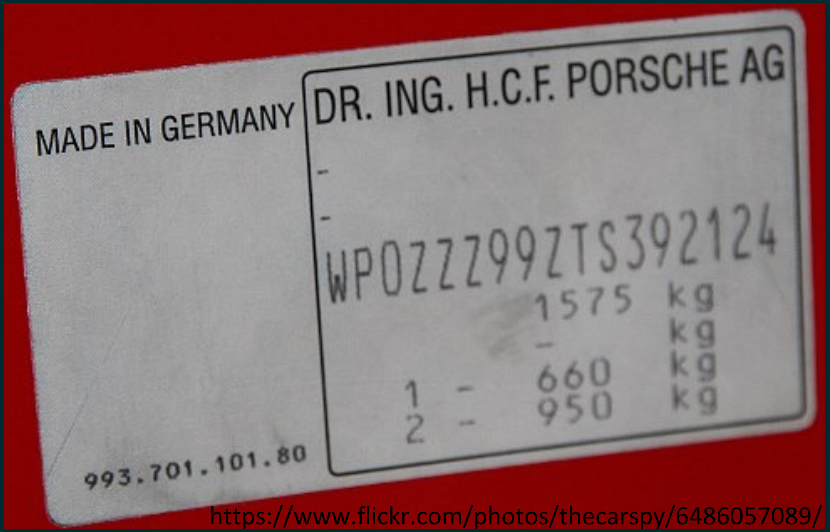
There are only two hard things in Computer Science: cache invalidation and naming things. (Phil Karlton)

The naming problem

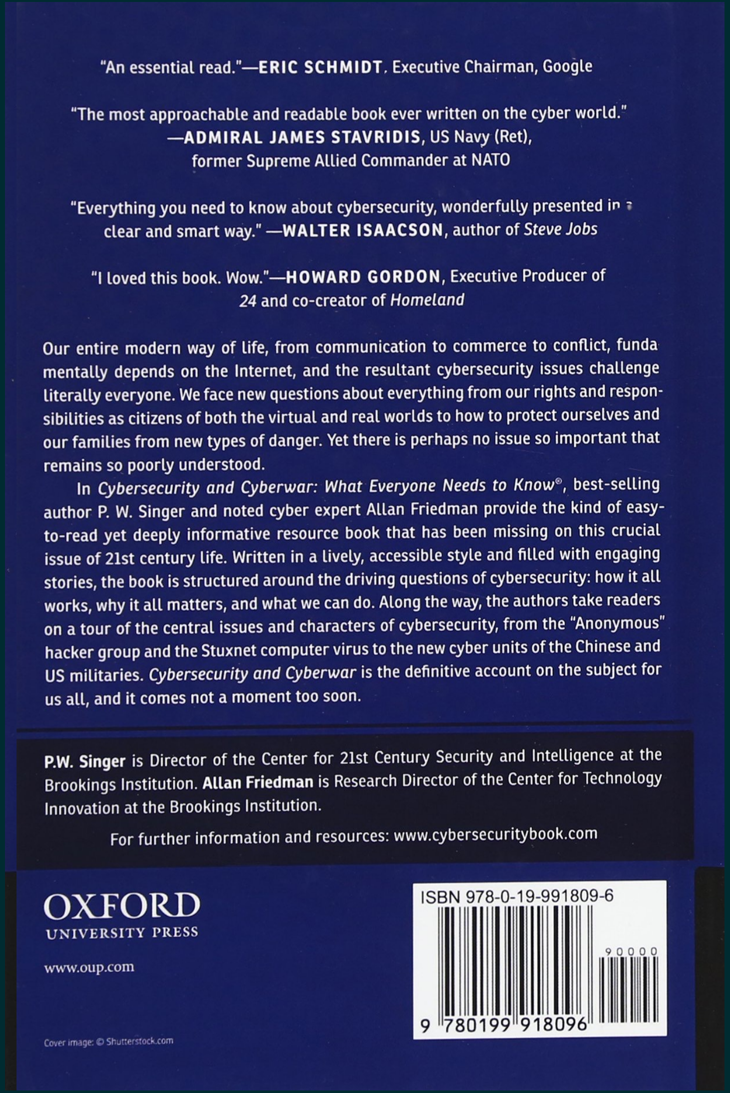
There are only two hard things in Computer Science: cache invalidation and *naming things*. (Phil Karlton)

Global identification systems

- VIN
- ISBN
- DNS



https://www.flickr.com/photos/thecarspy/6486057089/



"An essential read."—**ERIC SCHMIDT**, Executive Chairman, Google

"The most approachable and readable book ever written on the cyber world."
—**ADMIRAL JAMES STAVRIDIS**, US Navy (Ret),
former Supreme Allied Commander at NATO

"Everything you need to know about cybersecurity, wonderfully presented in a clear and smart way." —**WALTER ISAACSON**, author of *Steve Jobs*

"I loved this book. Wow."—**HOWARD GORDON**, Executive Producer of *24* and co-creator of *Homeland*

Our entire modern way of life, from communication to commerce to conflict, fundamentally depends on the Internet, and the resultant cybersecurity issues challenge literally everyone. We face new questions about everything from our rights and responsibilities as citizens of both the virtual and real worlds to how to protect ourselves and our families from new types of danger. Yet there is perhaps no issue so important that remains so poorly understood.

In *Cybersecurity and Cyberwar: What Everyone Needs to Know*®, best-selling author P. W. Singer and noted cyber expert Allan Friedman provide the kind of easy-to-read yet deeply informative resource book that has been missing on this crucial issue of 21st century life. Written in a lively, accessible style and filled with engaging stories, the book is structured around the driving questions of cybersecurity: how it all works, why it all matters, and what we can do. Along the way, the authors take readers on a tour of the central issues and characters of cybersecurity, from the "Anonymous" hacker group and the Stuxnet computer virus to the new cyber units of the Chinese and US militaries. *Cybersecurity and Cyberwar* is the definitive account on the subject for us all, and it comes not a moment too soon.

P.W. Singer is Director of the Center for 21st Century Security and Intelligence at the Brookings Institution. **Allan Friedman** is Research Director of the Center for Technology Innovation at the Brookings Institution.

For further information and resources: www.cybersecuritybook.com

OXFORD
UNIVERSITY PRESS

www.oup.com

Cover image: © Shutterstock.com

ISBN 978-0-19-991809-6

90000

9 780199 918096

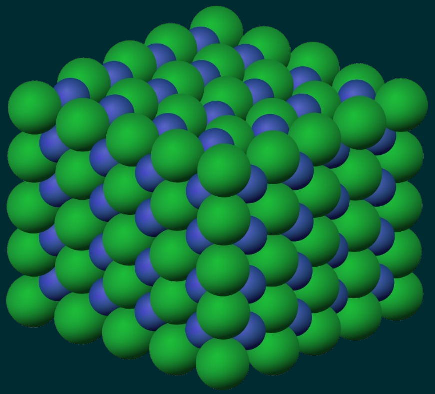
Why is it hard?

Name vs Identity

Why is it hard?

Name ≠ Identity

Intrinsic vs extrinsic naming scheme



NaCl

7647-14-5

Why is it hard?

Name ≠ Identity

Intrinsic vs extrinsic naming scheme

Different use cases

No market control

Why is it hard?

Name ≠ Identity

Intrinsic vs extrinsic naming scheme

Different use cases

No market control

Names change all the time

Current options

CPE

SWID

purl

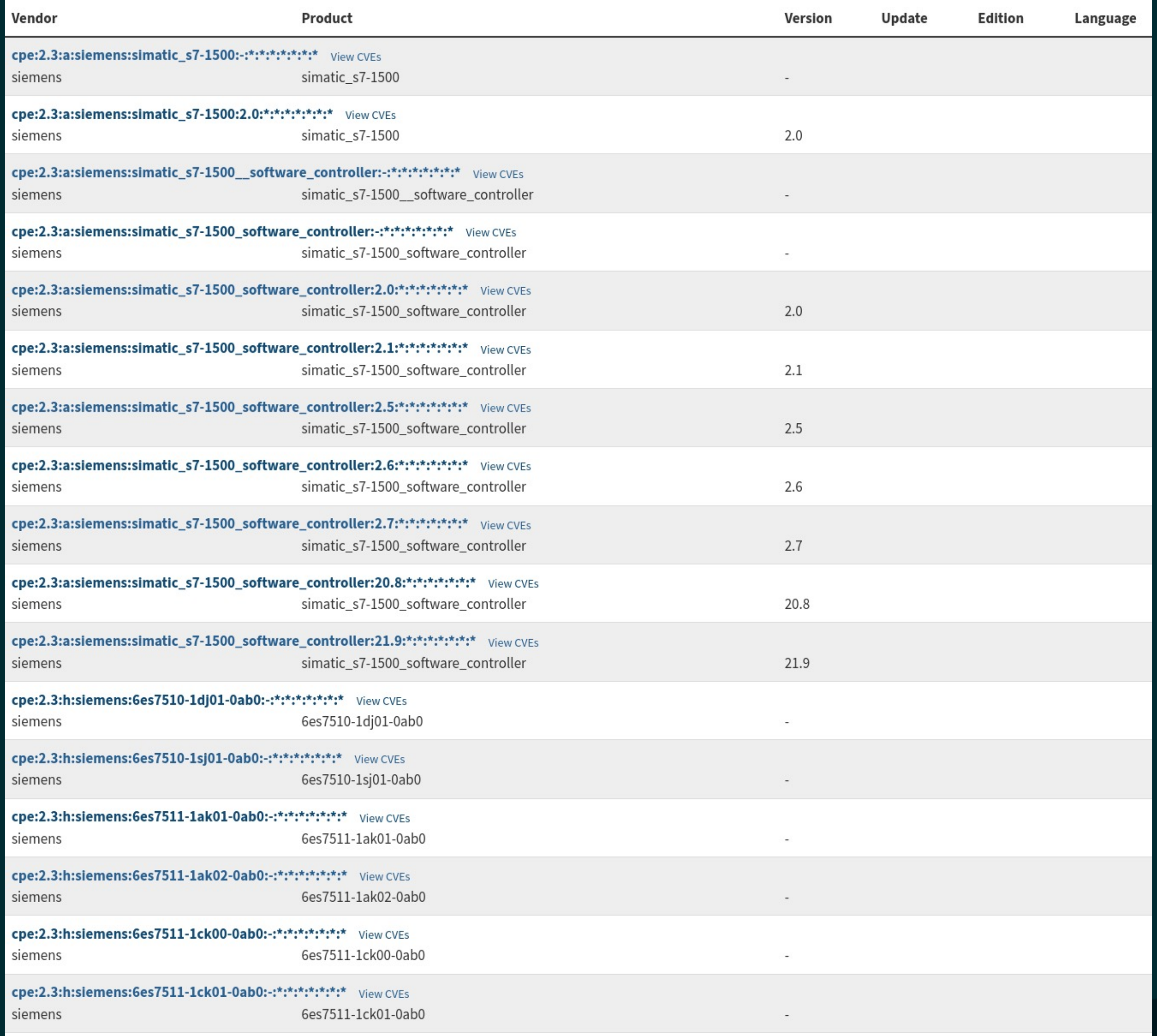
...

Common Platform Enumeration (CPE)

Maintained by NIST

Issues

- Difficult to search
- Product / vendor specific
- Specifically designed for vulnerabilities



Vendor	Product	Version	Update	Edition	Language
cpe:2.3:a:siemens:simatic_s7-1500:-:*:*:*:*:*:*:* View CVEs siemens	simatic_s7-1500	-			
cpe:2.3:a:siemens:simatic_s7-1500:2.0:*:*:*:*:*:*:* View CVEs siemens	simatic_s7-1500	2.0			
cpe:2.3:a:siemens:simatic_s7-1500__software_controller:-:*:*:*:*:*:*:* View CVEs siemens	simatic_s7-1500__software_controller	-			
cpe:2.3:a:siemens:simatic_s7-1500_software_controller:-:*:*:*:*:*:*:* View CVEs siemens	simatic_s7-1500_software_controller	-			
cpe:2.3:a:siemens:simatic_s7-1500_software_controller:2.0:*:*:*:*:*:*:* View CVEs siemens	simatic_s7-1500_software_controller	2.0			
cpe:2.3:a:siemens:simatic_s7-1500_software_controller:2.1:*:*:*:*:*:*:* View CVEs siemens	simatic_s7-1500_software_controller	2.1			
cpe:2.3:a:siemens:simatic_s7-1500_software_controller:2.5:*:*:*:*:*:*:* View CVEs siemens	simatic_s7-1500_software_controller	2.5			
cpe:2.3:a:siemens:simatic_s7-1500_software_controller:2.6:*:*:*:*:*:*:* View CVEs siemens	simatic_s7-1500_software_controller	2.6			
cpe:2.3:a:siemens:simatic_s7-1500_software_controller:2.7:*:*:*:*:*:*:* View CVEs siemens	simatic_s7-1500_software_controller	2.7			
cpe:2.3:a:siemens:simatic_s7-1500_software_controller:20.8:*:*:*:*:*:*:* View CVEs siemens	simatic_s7-1500_software_controller	20.8			
cpe:2.3:a:siemens:simatic_s7-1500_software_controller:21.9:*:*:*:*:*:*:* View CVEs siemens	simatic_s7-1500_software_controller	21.9			
cpe:2.3:h:siemens:6es7510-1dj01-0ab0:-:*:*:*:*:*:*:* View CVEs siemens	6es7510-1dj01-0ab0	-			
cpe:2.3:h:siemens:6es7510-1sj01-0ab0:-:*:*:*:*:*:*:* View CVEs siemens	6es7510-1sj01-0ab0	-			
cpe:2.3:h:siemens:6es7511-1ak01-0ab0:-:*:*:*:*:*:*:* View CVEs siemens	6es7511-1ak01-0ab0	-			
cpe:2.3:h:siemens:6es7511-1ak02-0ab0:-:*:*:*:*:*:*:* View CVEs siemens	6es7511-1ak02-0ab0	-			
cpe:2.3:h:siemens:6es7511-1ck00-0ab0:-:*:*:*:*:*:*:* View CVEs siemens	6es7511-1ck00-0ab0	-			
cpe:2.3:h:siemens:6es7511-1ck01-0ab0:-:*:*:*:*:*:*:* View CVEs siemens	6es7511-1ck01-0ab0	-			

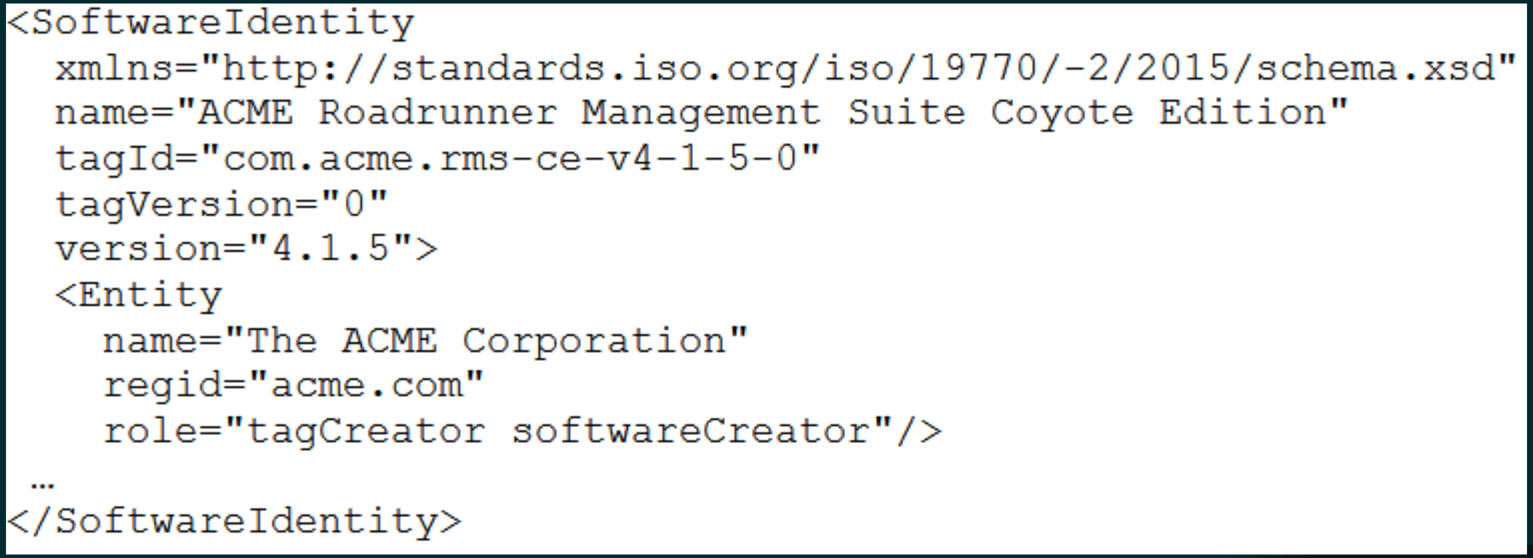
Software Identity (SWID)

ISO standard (ISO/IEC 19770-2)

Counterpart for hardware exists (ISO/IEC 19770-6)

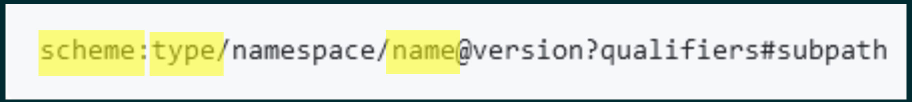
Issues

- Lots of backing but low adoption
- Version specific
- XML
- Tools?



```
<SoftwareIdentity
  xmlns="http://standards.iso.org/iso/19770/-2/2015/schema.xsd"
  name="ACME Roadrunner Management Suite Coyote Edition"
  tagId="com.acme.rms-ce-v4-1-5-0"
  tagVersion="0"
  version="4.1.5">
  <Entity
    name="The ACME Corporation"
    regid="acme.com"
    role="tagCreator softwareCreator"/>
 …
</SoftwareIdentity>
```

Package URL (purl)

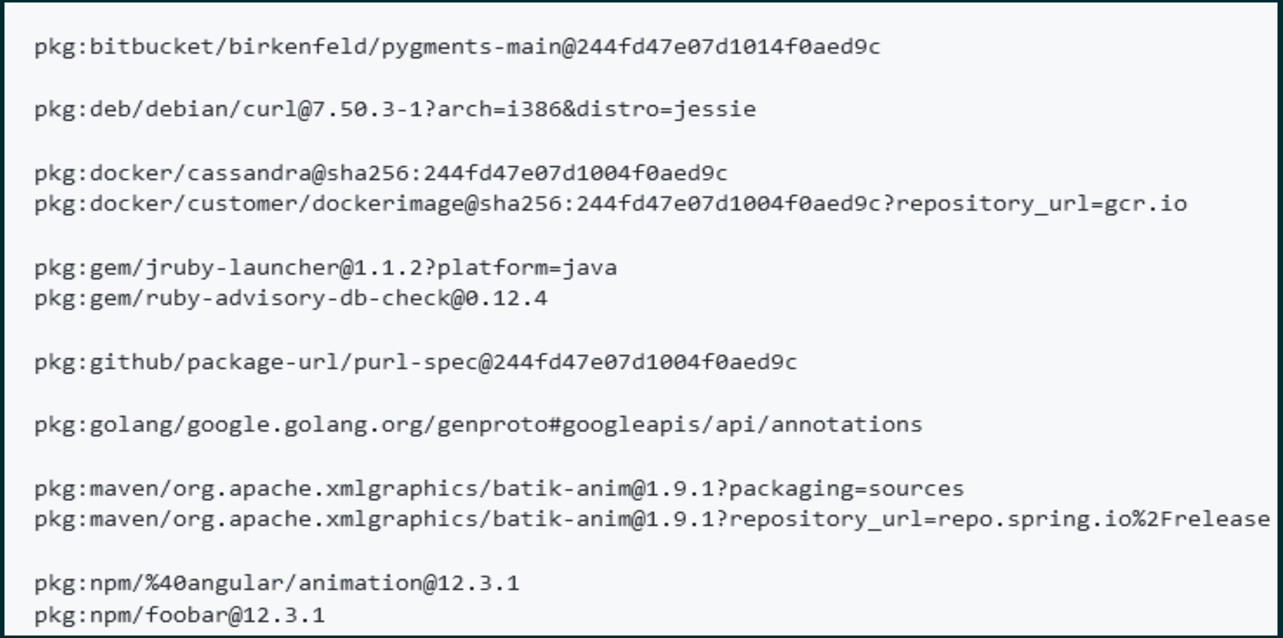


```
scheme:type/namespace/name@version?qualifiers#subpath
```

Community maintained

Issues:

- Works best for ecosystems with package managers (naming authority)
- Limited known / defined types
- Potentially different purls for same product
- Hard to incorporate hardware



```
pkg:bitbucket/birkenfeld/pygments-main@244fd47e07d1014f0aed9c

pkg:deb/debian/curl@7.50.3-1?arch=i386&distro=jessie

pkg:docker/cassandra@sha256:244fd47e07d1004f0aed9c
pkg:docker/customer/dockerimage@sha256:244fd47e07d1004f0aed9c?repository_url=gcr.io

pkg:gem/jruby-launcher@1.1.2?platform=java
pkg:gem/ruby-advisory-db-check@0.12.4

pkg:github/package-url/purl-spec@244fd47e07d1004f0aed9c

pkg:golang/google.golang.org/genproto#googleapis/api/annotations

pkg:maven/org.apache.xmlgraphics/batik-anim@1.9.1?packaging=sources
pkg:maven/org.apache.xmlgraphics/batik-anim@1.9.1?repository_url=repo.spring.io%2Frelease

pkg:npm/%40angular/animation@12.3.1
pkg:npm/foobar@12.3.1
```

Criteria

Readability

Distributed production

Reproducibility

Propagation model

Precision

Uniqueness

Transition

Inclusive

Standard scenarios

Rename a product / organization

Merges / Acquisitions

Sell-off

Whitelabel products

Correct false information

Solution #1

Global supplier registry

Design considerations

Globally unique identifiers (Universal Product IDentifiers, UPID)

All suppliers must be able to participate

Responsibility is coupled with authority

Local sphere of control

- Use your own names and other identifiers
- Interface only with adjacent participants

Rule following (or breaking) is observable

Rule #1: Partition by supplier

Supplier ID must be globally unique

“Supplier” is broadly defined: Developer, maintainer, vendor, producer, manufacturer, provider

- Includes intermediary code platforms and software identity ecosystems (GitHub, git, Maven, npm)
- Does not include reseller or retailer

Is “supplier” still the right term?

Rule #2: Supplier says

Supplier decides component names, versions, other identifiers, groups, hierarchies

- Some suppliers and ecosystems have significant influence

Rule #3: Use upstream identifiers

Using someone else's software?

- Must use their identifiers
- Do not make up identifiers for someone else

Rule #4: Provide identifiers downstream

Providing software to others?

- Must provide your identifiers (SBOM)
- This might mean publishing

Supplier changes

Suppliers come, and go, merge, are acquired

Projects are forked, archived, become stale

Supplier identification needs relationships too

- Ivanti *acquired* Pulse Secure
- Logitech *renamed* Logi

Rule support

Need more expressive SBOM relationships, such as

- *Uses*: incorporates component unchanged
- *Derived*: modifies upstream component, keep track of source
- *Identical*: same components
- *Alias*: additional name for same component

Rule violations

No identifiers?

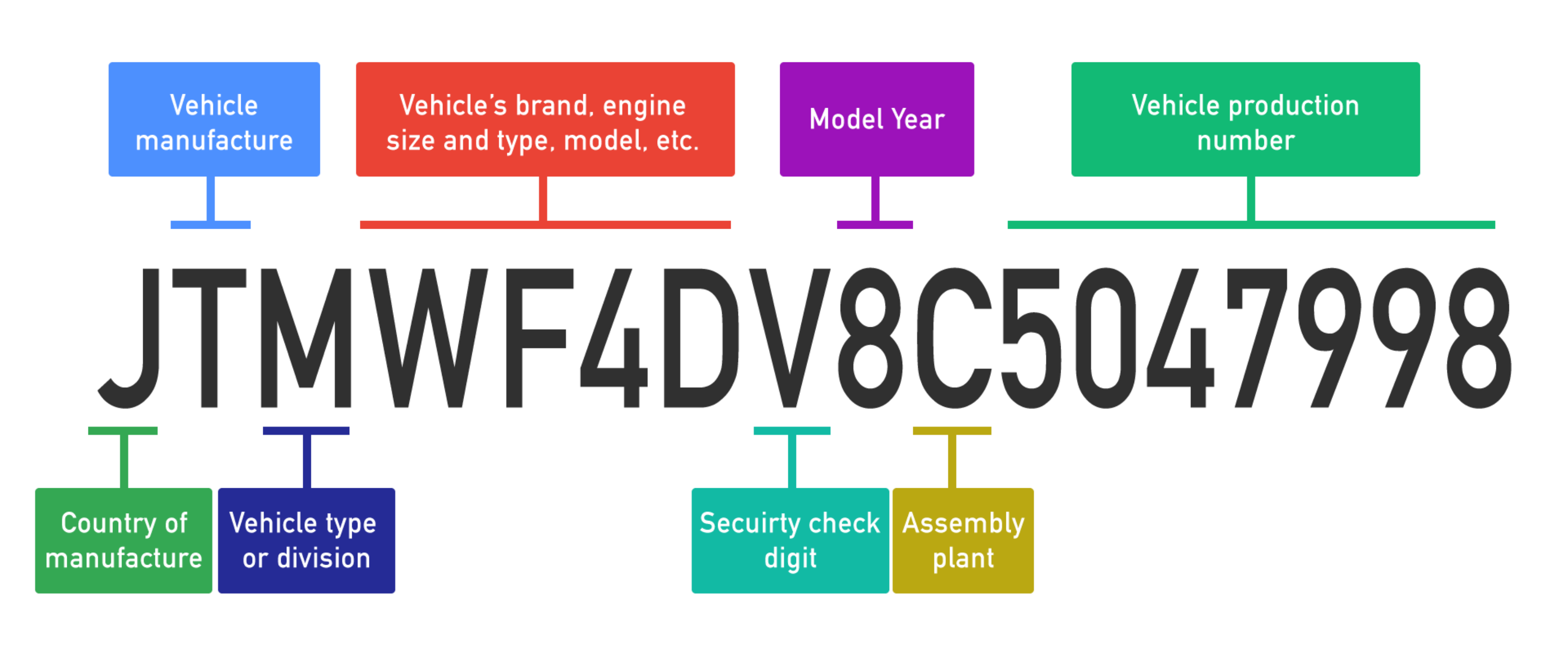
- Contact your supplier
- Reference the supplier (and their lack of identifiers)

No active supplier?

- Do you really want to keep using unmaintained software?
- Time to fork or accept risk

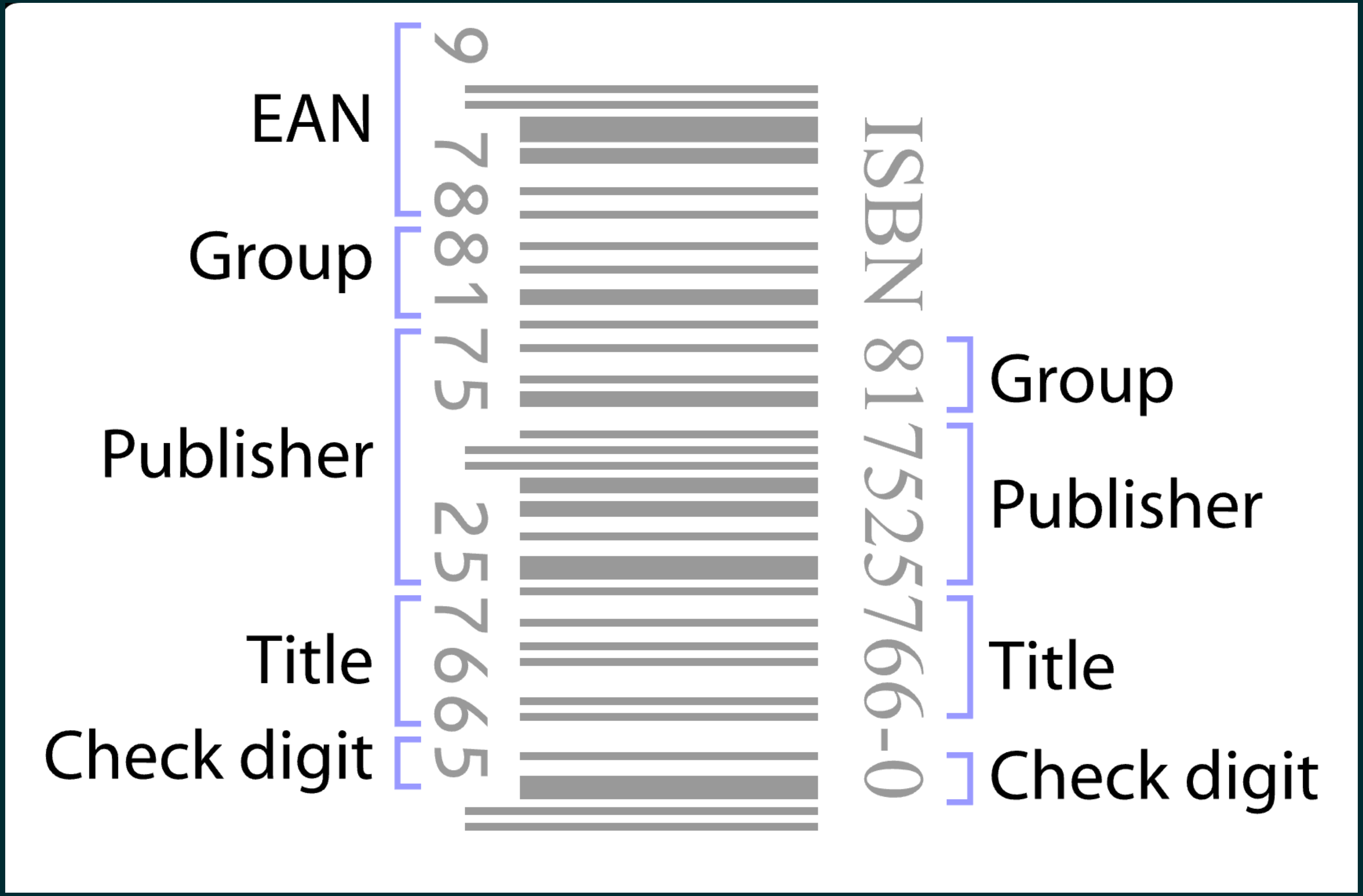
VIN: World Manufacturer Identifier (WMI)

Country of production, manufacturer, vehicle type



ISBN: Registrant Element

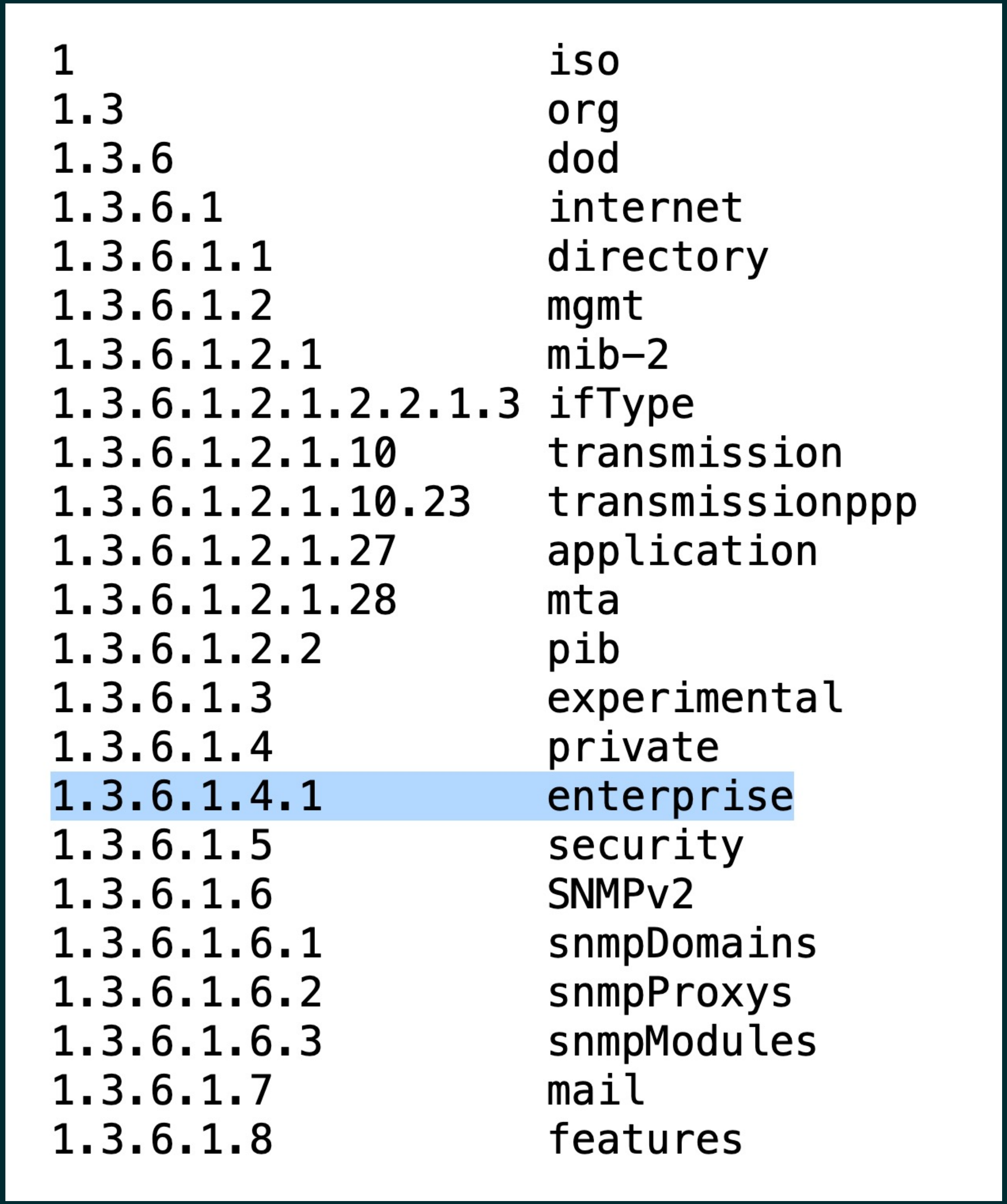
Publisher or distributor



1.3.6.1.4.1

IANA Private Enterprise Numbers

- Based on OID
- SNMP
- Old! But still in use?
- 60K+ entries

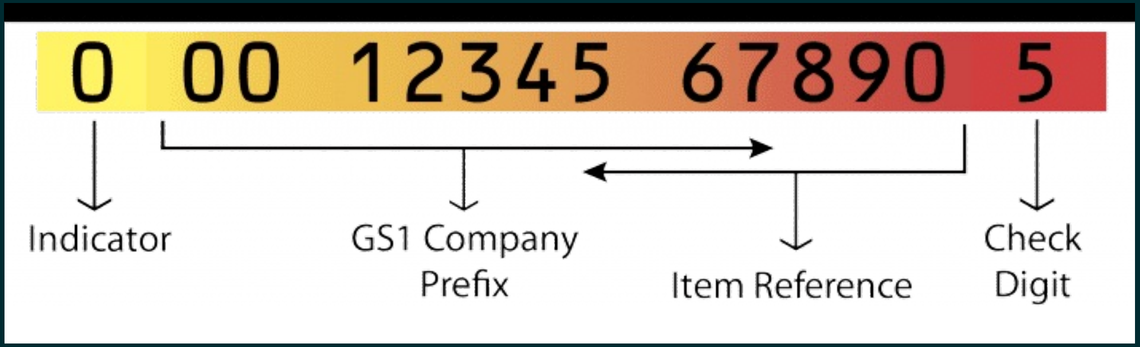


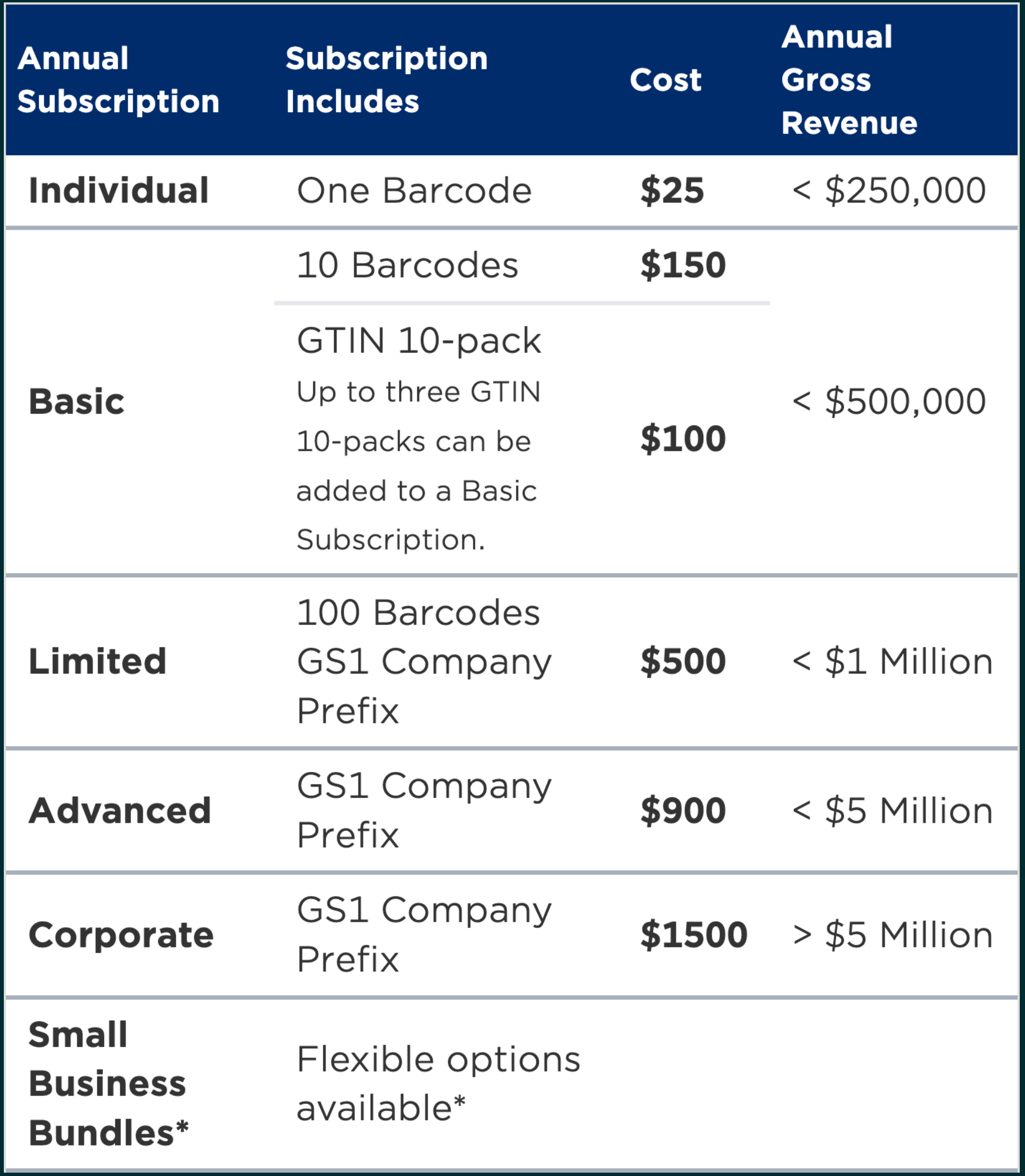
```
1                    iso
1.3                  org
1.3.6                dod
1.3.6.1              internet
1.3.6.1.1            directory
1.3.6.1.2            mgmt
1.3.6.1.2.1          mib-2
1.3.6.1.2.1.2.2.1.3 ifType
1.3.6.1.2.1.10       transmission
1.3.6.1.2.1.10.23    transmissionppp
1.3.6.1.2.1.27       application
1.3.6.1.2.1.28       mta
1.3.6.1.2.2          pib
1.3.6.1.3            experimental
1.3.6.1.4            private
1.3.6.1.4.1          enterprise
1.3.6.1.5            security
1.3.6.1.6            SNMPv2
1.3.6.1.6.1          snmpDomains
1.3.6.1.6.2          snmpProxys
1.3.6.1.6.3          snmpModules
1.3.6.1.7            mail
1.3.6.1.8            features
```

GS1, GTIN, GMN, UDI

For physical products, food, medical devices

- Required (UDI) medical device identification in EU and US
- (global) Company Prefix





Annual Subscription	Subscription Includes	Cost	Annual Gross Revenue
Individual	One Barcode	**$25**	< $250,000
Basic	10 Barcodes	**$150**	< $500,000
	GTIN 10-pack Up to three GTIN 10-packs can be added to a Basic Subscription.	**$100**	
Limited	100 Barcodes GS1 Company Prefix	**$500**	< $1 Million
Advanced	GS1 Company Prefix	**$900**	< $5 Million
Corporate	GS1 Company Prefix	**$1500**	> $5 Million
Small Business Bundles*	Flexible options available*		

Registrar concerns

Geopolitical

- Organization in DE might not want to register with a US registrar
- Use intermediary registrars, service providers

Costs for registrants

- No more difficult or costly than registering a domain

Sliding scale?

Minimum viable amount of bureaucracy

Transparency

- Registry is public

Resilience

- Replicate data

Registry is public

Funding

Governance

In DNS terms

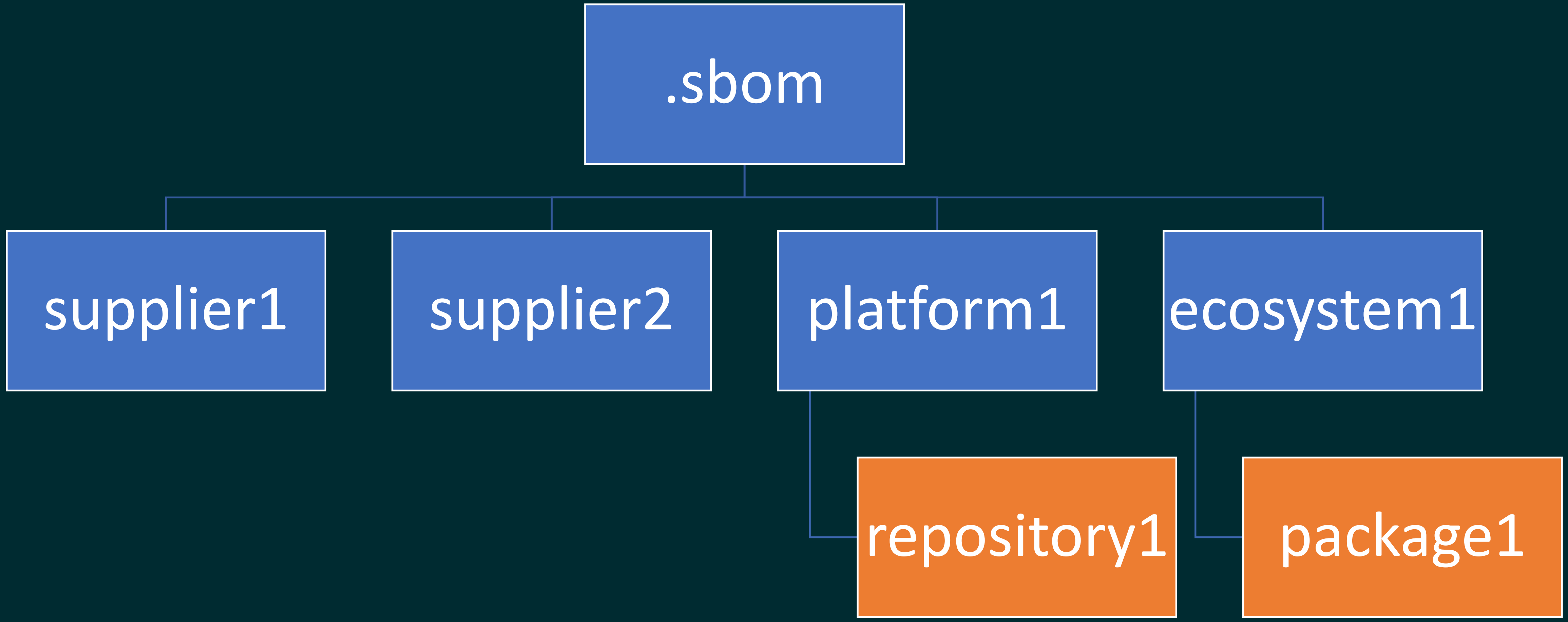
A new gTLD: .sbom

A registrar to manage .sbom

How about a new protocol? sboms://

- Or https:// with a not-yet-defined API

Supplier identity graph



.sbom

supplier1

supplier2

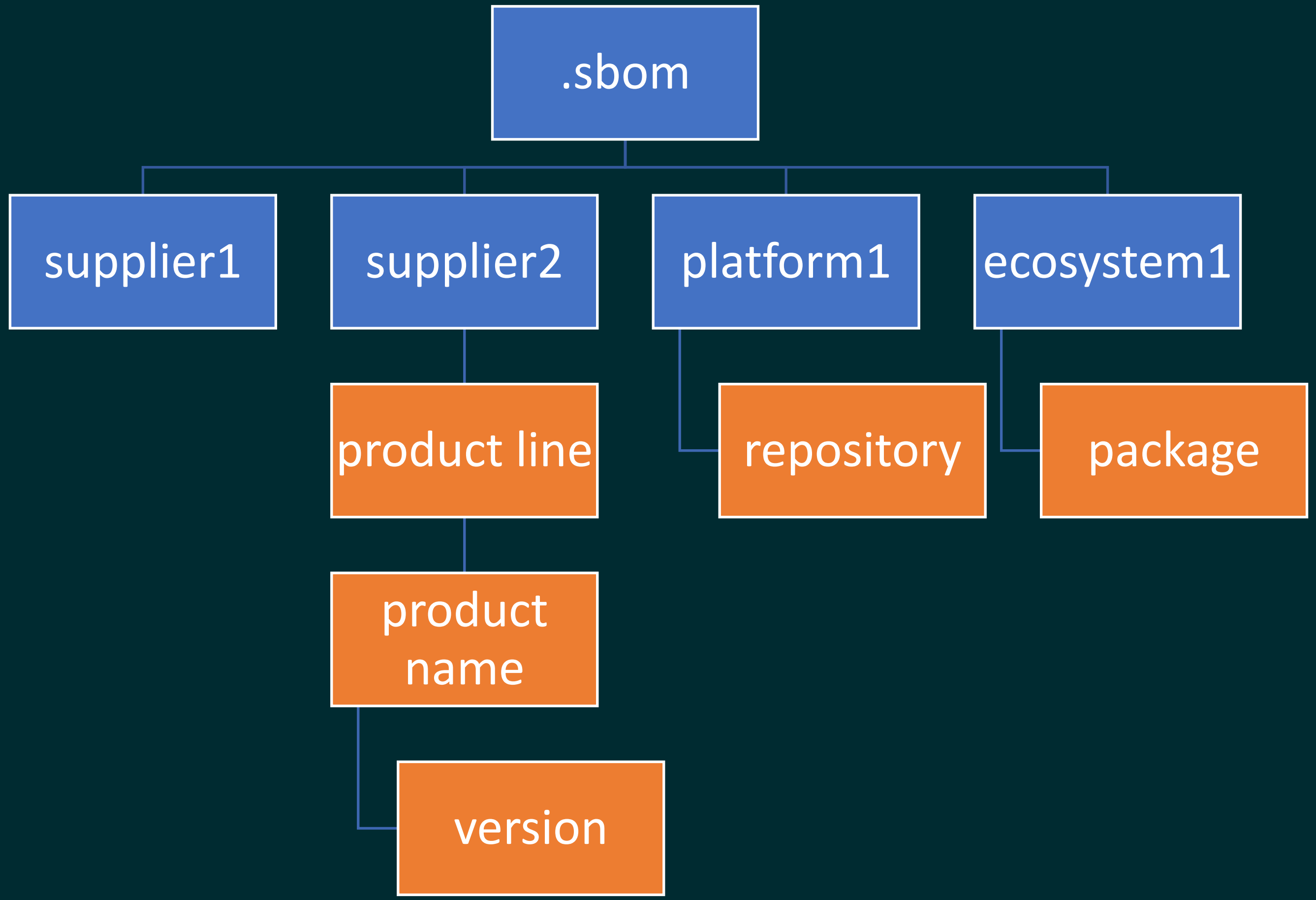
platform1

ecosystem1

repository1

package1

Component identity graph



.sbom

supplier1

supplier2

platform1

ecosystem1

product line

repository

package

product name

version

Examples

.sbom.microsoft.windows.server.2016.core
sboms://microsoft/windows/server/2016/core
https://microsoft.sbom/windows/server/2016/core

.sbom.github.vu-ls.advise.branch.'v1.1’
.sbom.github/vu-ls/advise/branch/v1.1
sboms://github/MISP/MISP/tag/2.4.168

sboms://openbsd/usr.sbin/smtpd/envelope.c/v/1.51
sboms://openbsd/src/commit/f748277

Examples

.sbom.microsoft.windows.server.2016.core
sboms://**microsoft**/windows/server/2016/core
https://**microsoft.sbom**/windows/server/2016/core

.sbom.github.vu-ls.advise.branch.'v1.1’
.sbom.github/vu-ls/advise/branch/v1.1
sboms://**github**/MISP/MISP/tag/2.4.168

sboms://**openbsd**/usr.sbin/smtpd/envelope.c/v/1.51
sboms://**openbsd**/src/commit/f748277

More examples

cpe:2.3:o:microsoft:windows_10_1507:-:*:*:*:*:*:x64:*

sboms://cpe/2.3/o/microsoft/windows_10_1507/-/*/*/*/*/*/x64/*

More examples

cpe:2.3:o:microsoft:windows_10_1507:-:*:*:*:*:*:x64:*

sboms://**cpe**/2.3/o/microsoft/windows_10_1507/-/*/*/*/*/*/x64/*

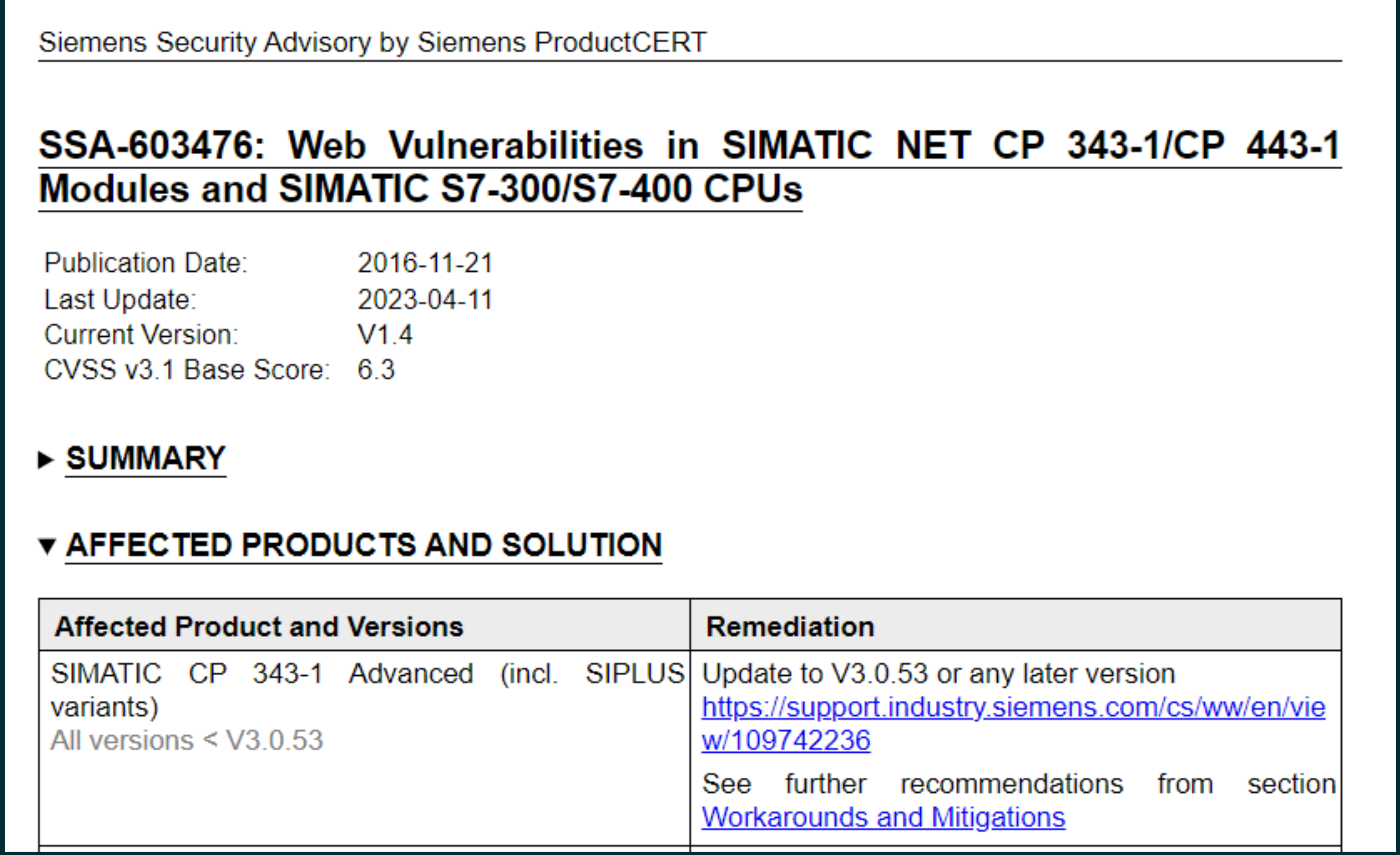
Solution #2

Vendor product tree

Introduction: Unique Product IDs

Unique Product IDs are important for

- Security advisories
- SBOM
- VEX
- CSAF
- Supply chain management



Siemens Security Advisory by Siemens ProductCERT

SSA-603476: Web Vulnerabilities in SIMATIC NET CP 343-1/CP 443-1 Modules and SIMATIC S7-300/S7-400 CPUs

Publication Date:	2016-11-21
Last Update:	2023-04-11
Current Version:	V1.4
CVSS v3.1 Base Score:	6.3

▶ **SUMMARY**

▼ **AFFECTED PRODUCTS AND SOLUTION**

Affected Product and Versions	Remediation
SIMATIC CP 343-1 Advanced (incl. SIPLUS variants) All versions < V3.0.53	Update to V3.0.53 or any later version https://support.industry.siemens.com/cs/ww/en/view/109742236 See further recommendations from section Workarounds and Mitigations

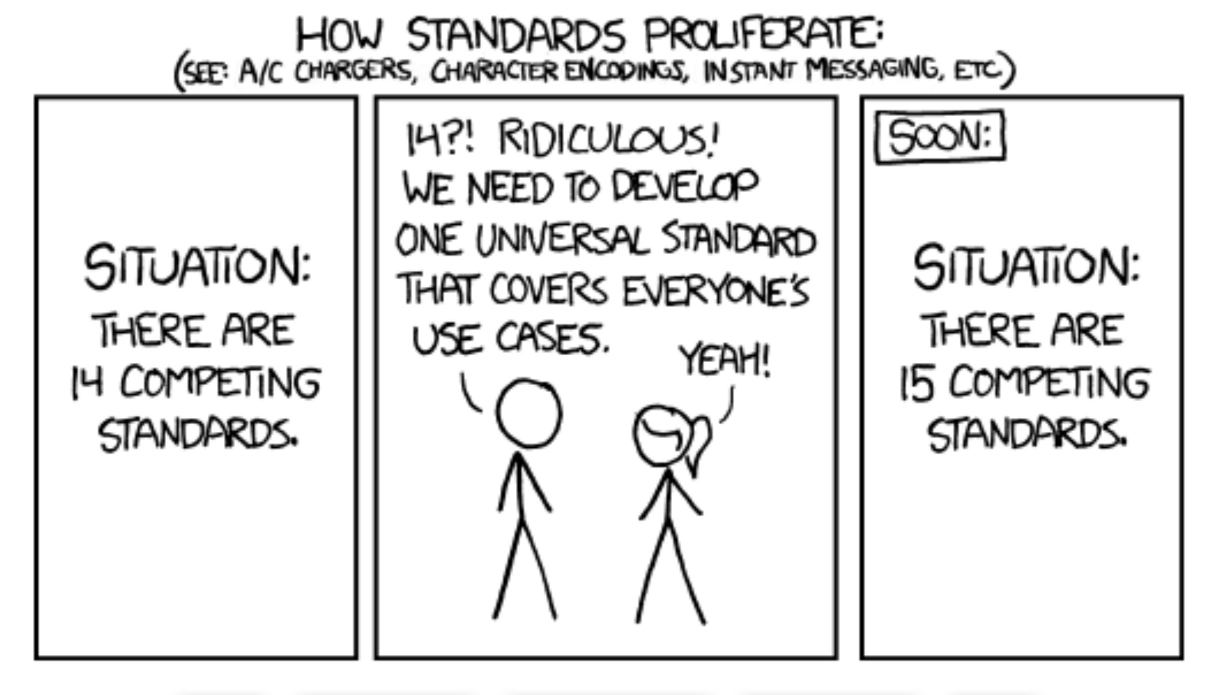
Things that do not work

Community approaches

- cpe:2.3:h:siemens:simatic_cp_343-1:-:*:*:*:standard:*:*:*

Forcing vendors into one standard

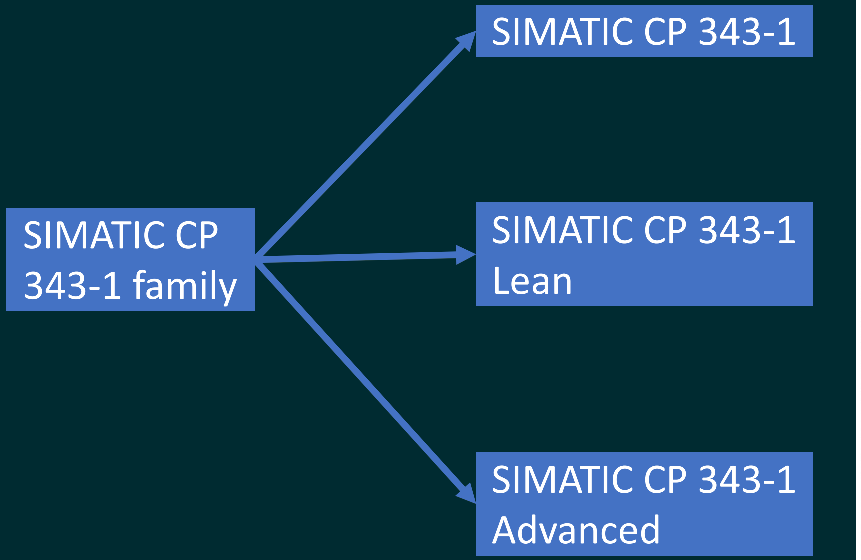
All 14 approaches we have today


HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC)
SITUATION: THERE ARE 14 COMPETING STANDARDS.
14?! RIDICULOUS! WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES.
YEAH!
SOON:
SITUATION: THERE ARE 15 COMPETING STANDARDS.

Vendor Graph – 2015

SIMATIC CP 343-1

Vendor Graph – 2018

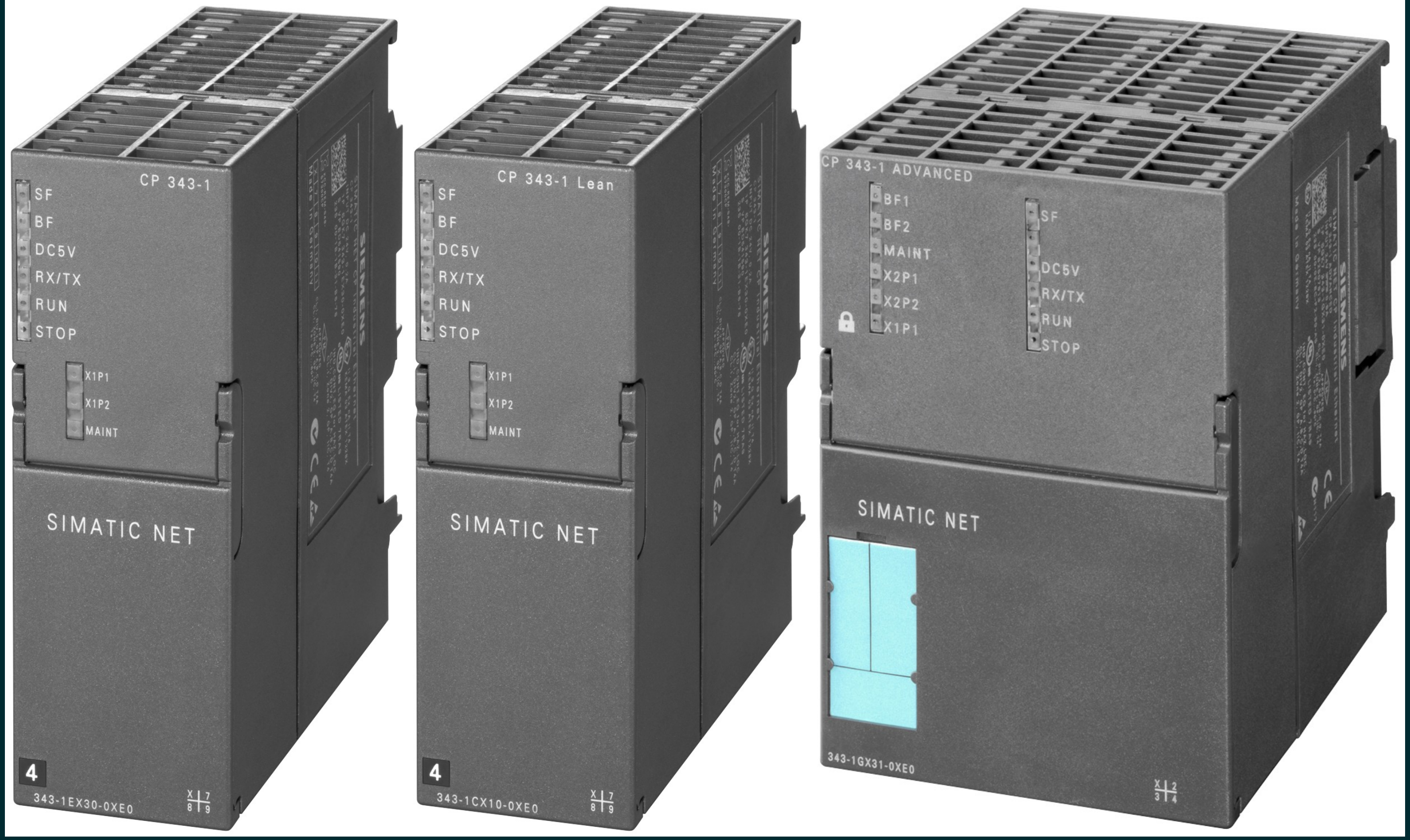


SIMATIC CP 343-1 family

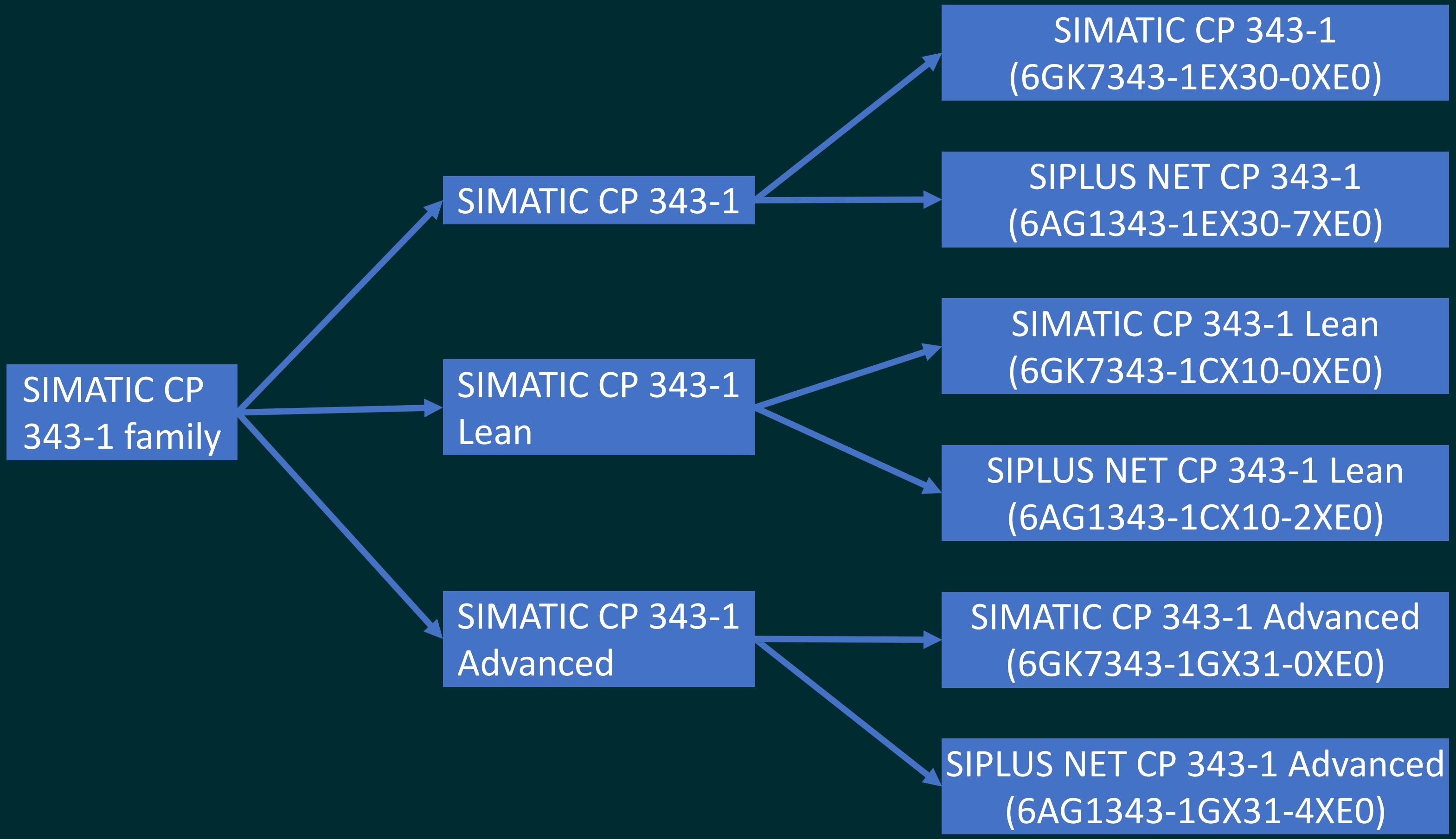
SIMATIC CP 343-1

SIMATIC CP 343-1 Lean

SIMATIC CP 343-1 Advanced



Vendor Graph – Status Quo



SIMATIC CP 343-1 family

SIMATIC CP 343-1

SIMATIC CP 343-1 Lean

SIMATIC CP 343-1 Advanced

SIMATIC CP 343-1 (6GK7343-1EX30-0XE0)

SIPLUS NET CP 343-1 (6AG1343-1EX30-7XE0)

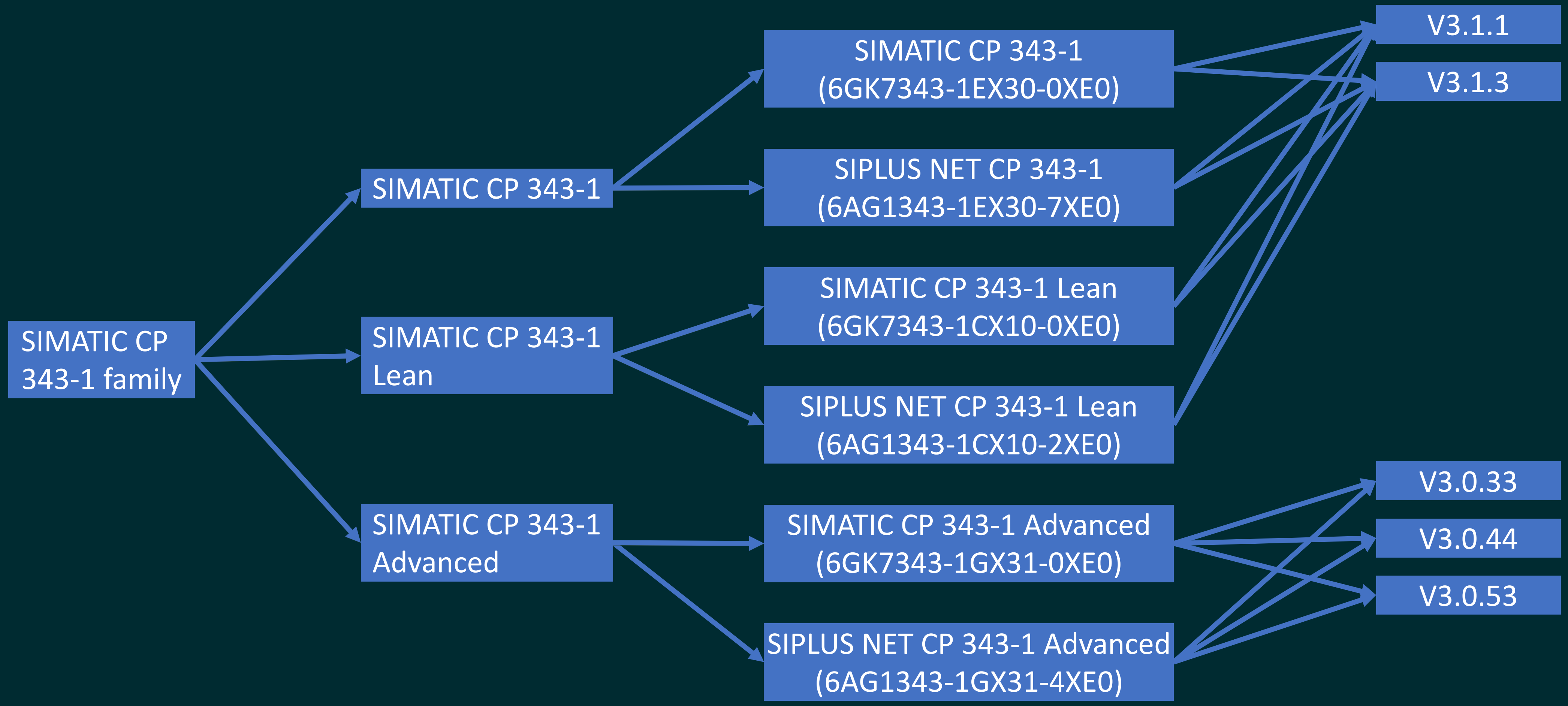
SIMATIC CP 343-1 Lean (6GK7343-1CX10-0XE0)

SIPLUS NET CP 343-1 Lean (6AG1343-1CX10-2XE0)

SIMATIC CP 343-1 Advanced (6GK7343-1GX31-0XE0)

SIPLUS NET CP 343-1 Advanced (6AG1343-1GX31-4XE0)

Vendor Graph – Hardware + Firmware



SIMATIC CP 343-1 family

SIMATIC CP 343-1

SIMATIC CP 343-1 Lean

SIMATIC CP 343-1 Advanced

SIMATIC CP 343-1 (6GK7343-1EX30-0XE0)

SIPLUS NET CP 343-1 (6AG1343-1EX30-7XE0)

SIMATIC CP 343-1 Lean (6GK7343-1CX10-0XE0)

SIPLUS NET CP 343-1 Lean (6AG1343-1CX10-2XE0)

SIMATIC CP 343-1 Advanced (6GK7343-1GX31-0XE0)

SIPLUS NET CP 343-1 Advanced (6AG1343-1GX31-4XE0)

V3.1.1

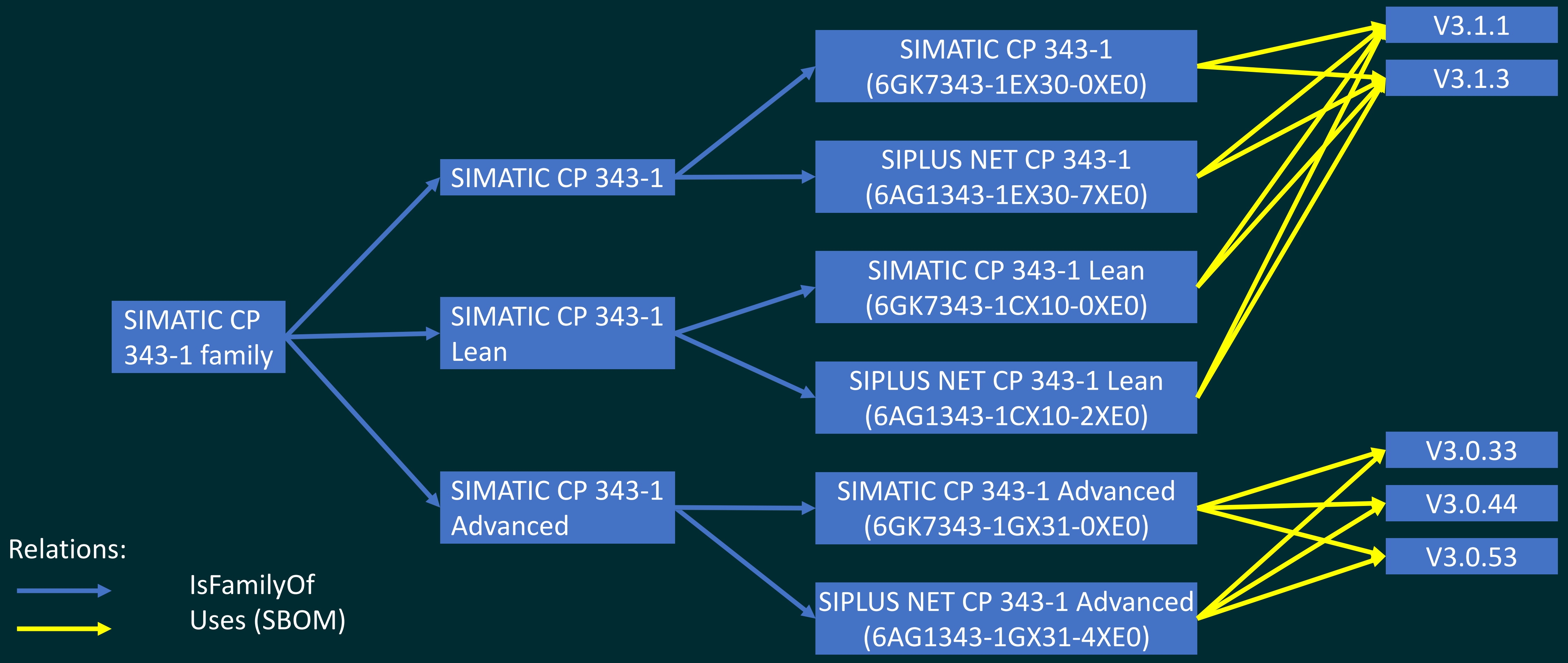
V3.1.3

V3.0.33

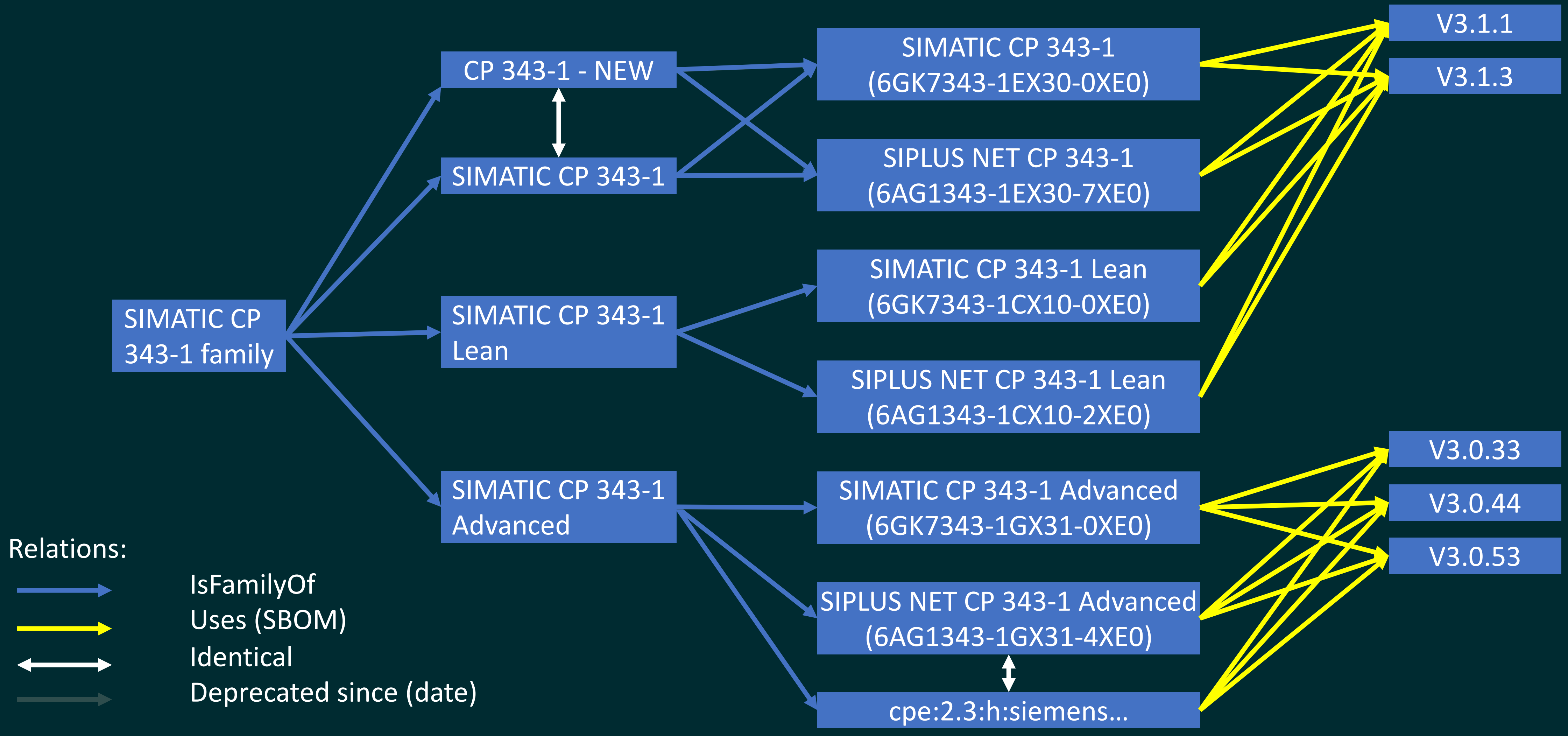
V3.0.44

V3.0.53

Vendor Graph – Relations

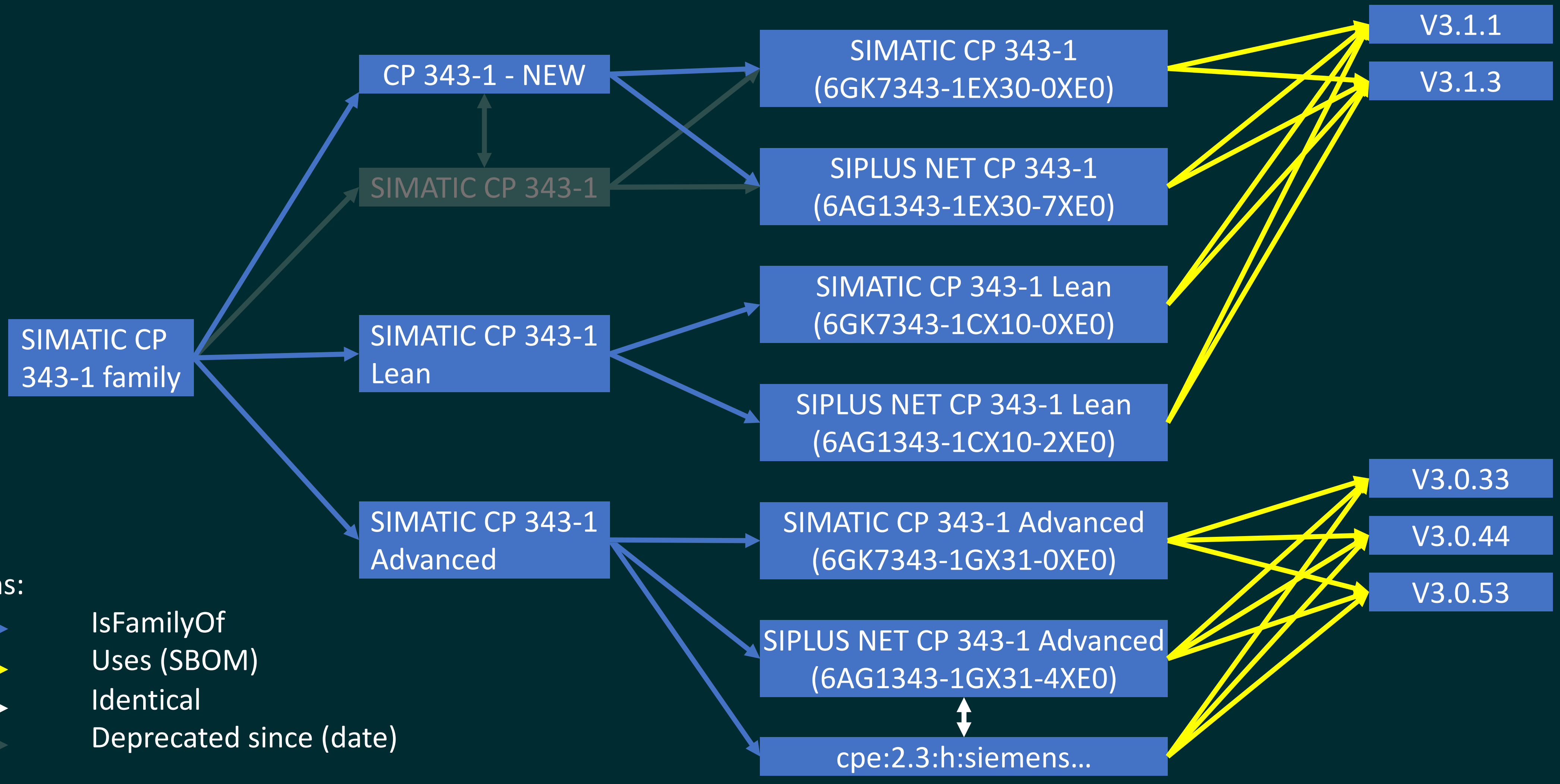

SIMATIC CP 343-1 family
SIMATIC CP 343-1
SIMATIC CP 343-1 Lean
SIMATIC CP 343-1 Advanced
SIMATIC CP 343-1 (6GK7343-1EX30-0XE0)
SIPLUS NET CP 343-1 (6AG1343-1EX30-7XE0)
SIMATIC CP 343-1 Lean (6GK7343-1CX10-0XE0)
SIPLUS NET CP 343-1 Lean (6AG1343-1CX10-2XE0)
SIMATIC CP 343-1 Advanced (6GK7343-1GX31-0XE0)
SIPLUS NET CP 343-1 Advanced (6AG1343-1GX31-4XE0)
V3.1.1
V3.1.3
V3.0.33
V3.0.44
V3.0.53
Relations:
IsFamilyOf
Uses (SBOM)

Vendor Graph – Managing Duplicates



CP 343-1 - NEW
SIMATIC CP 343-1
SIMATIC CP 343-1 family
SIMATIC CP 343-1 Lean
SIMATIC CP 343-1 Advanced
SIMATIC CP 343-1 (6GK7343-1EX30-0XE0)
SIPLUS NET CP 343-1 (6AG1343-1EX30-7XE0)
SIMATIC CP 343-1 Lean (6GK7343-1CX10-0XE0)
SIPLUS NET CP 343-1 Lean (6AG1343-1CX10-2XE0)
SIMATIC CP 343-1 Advanced (6GK7343-1GX31-0XE0)
SIPLUS NET CP 343-1 Advanced (6AG1343-1GX31-4XE0)
cpe:2.3:h:siemens...
V3.1.1
V3.1.3
V3.0.33
V3.0.44
V3.0.53
Relations:
IsFamilyOf
Uses (SBOM)
Identical
Deprecated since (date)

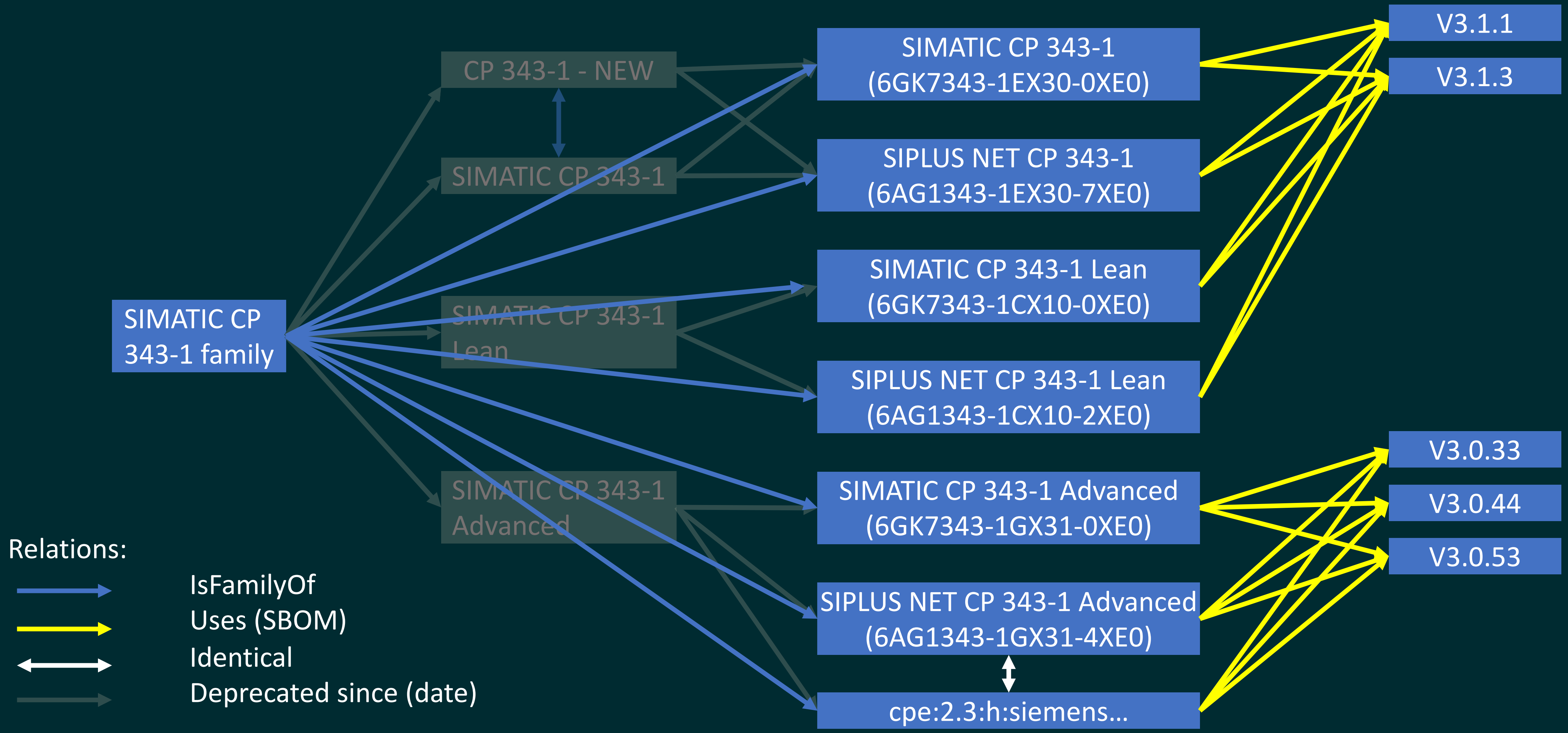
Vendor Graph – Renaming


SIMATIC CP 343-1 family
CP 343-1 - NEW
SIMATIC CP 343-1
SIMATIC CP 343-1 Lean
SIMATIC CP 343-1 Advanced
SIMATIC CP 343-1 (6GK7343-1EX30-0XE0)
SIPLUS NET CP 343-1 (6AG1343-1EX30-7XE0)
SIMATIC CP 343-1 Lean (6GK7343-1CX10-0XE0)
SIPLUS NET CP 343-1 Lean (6AG1343-1CX10-2XE0)
SIMATIC CP 343-1 Advanced (6GK7343-1GX31-0XE0)
SIPLUS NET CP 343-1 Advanced (6AG1343-1GX31-4XE0)
cpe:2.3:h:siemens…
V3.1.1
V3.1.3
V3.0.33
V3.0.44
V3.0.53

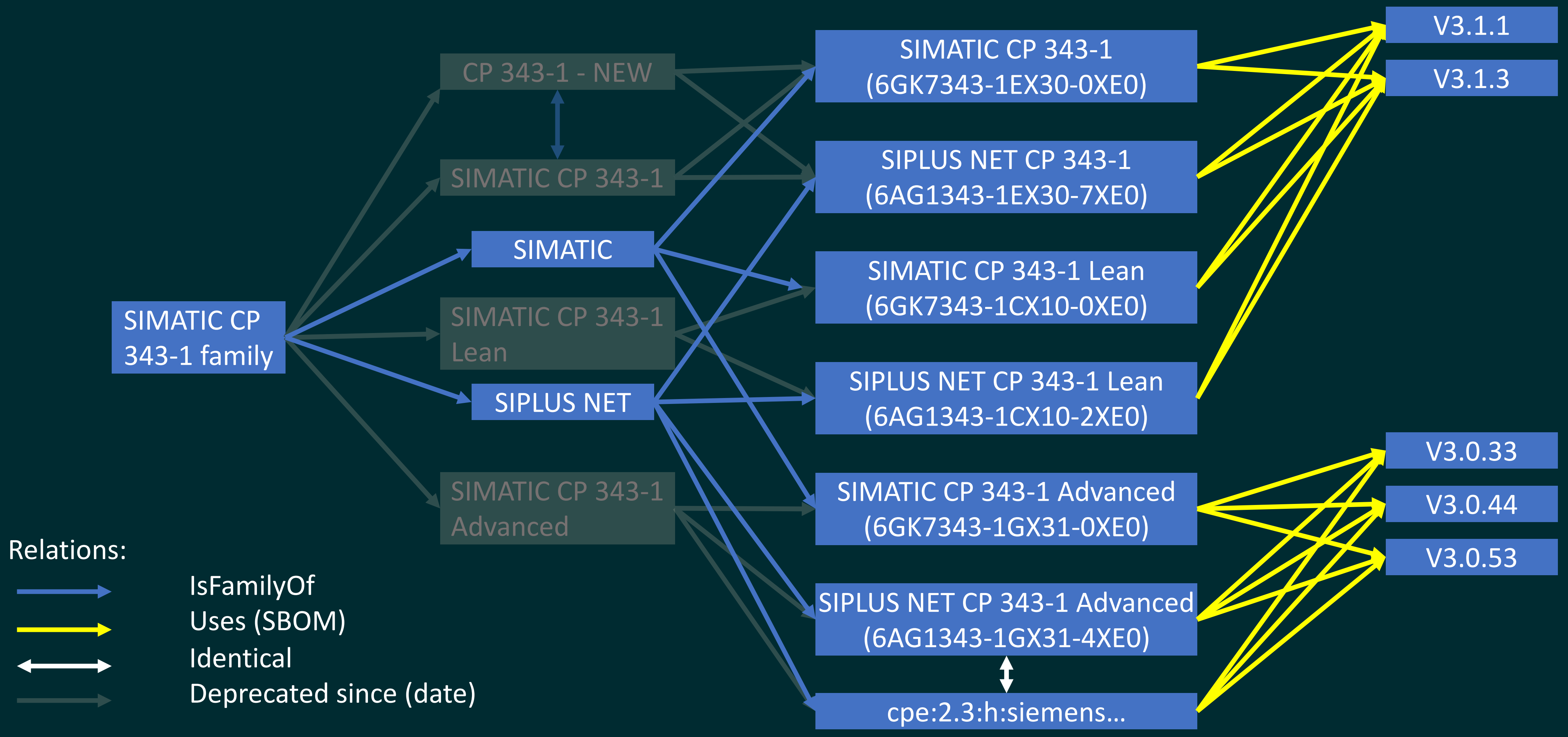
Relations:

→	IsFamilyOf
→	Uses (SBOM)
↔	Identical
→	Deprecated since (date)

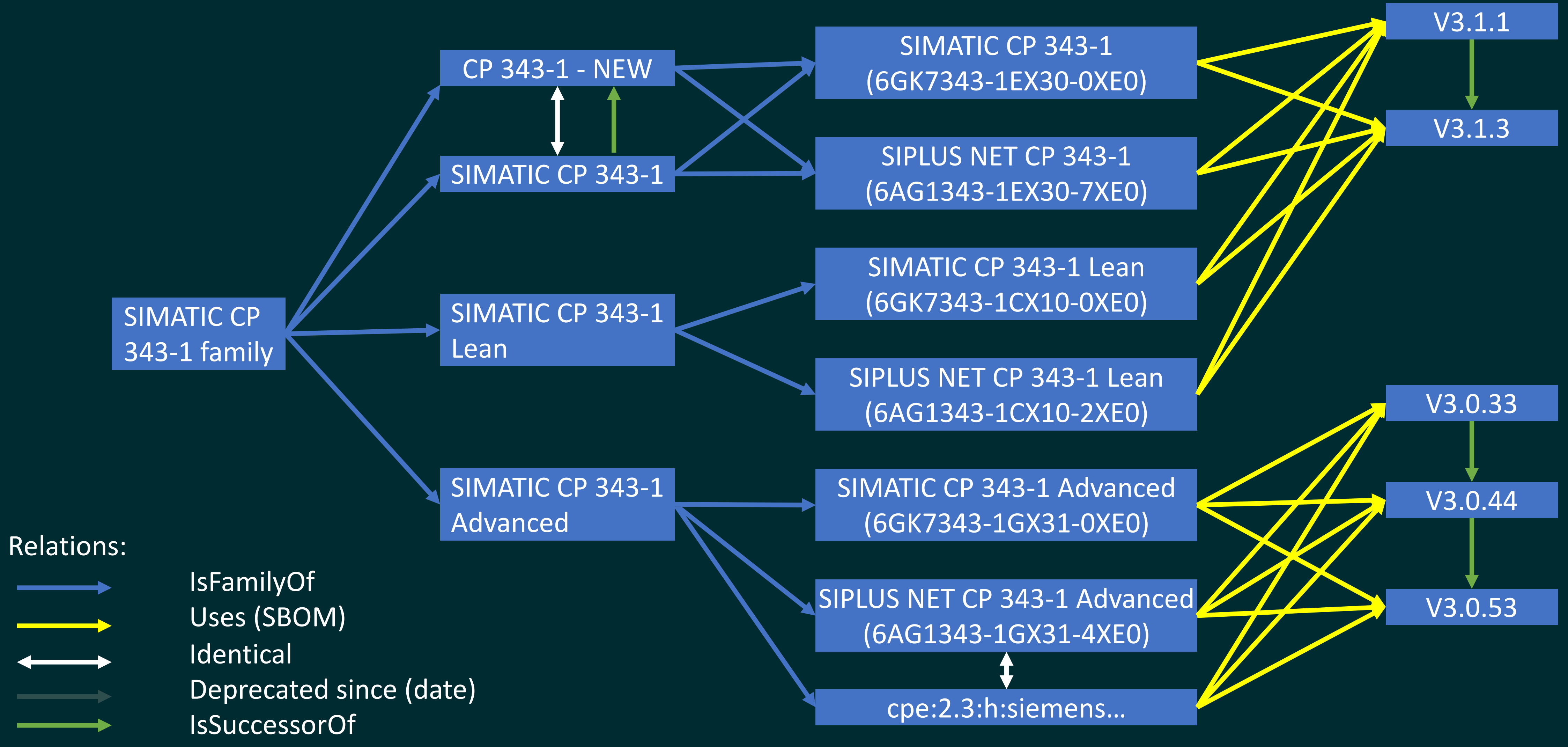
Vendor Graph – Deprecating Nodes


SIMATIC CP 343-1 family
CP 343-1 - NEW
SIMATIC CP 343-1
SIMATIC CP 343-1 Lean
SIMATIC CP 343-1 Advanced
SIMATIC CP 343-1 (6GK7343-1EX30-0XE0)
SIPLUS NET CP 343-1 (6AG1343-1EX30-7XE0)
SIMATIC CP 343-1 Lean (6GK7343-1CX10-0XE0)
SIPLUS NET CP 343-1 Lean (6AG1343-1CX10-2XE0)
SIMATIC CP 343-1 Advanced (6GK7343-1GX31-0XE0)
SIPLUS NET CP 343-1 Advanced (6AG1343-1GX31-4XE0)
cpe:2.3:h:siemens...
V3.1.1
V3.1.3
V3.0.33
V3.0.44
V3.0.53
Relations:
IsFamilyOf
Uses (SBOM)
Identical
Deprecated since (date)

Vendor Graph – Inserting Nodes


SIMATIC CP 343-1 family
CP 343-1 - NEW
SIMATIC CP 343-1
SIMATIC
SIMATIC CP 343-1 Lean
SIPLUS NET
SIMATIC CP 343-1 Advanced
SIMATIC CP 343-1 (6GK7343-1EX30-0XE0)
SIPLUS NET CP 343-1 (6AG1343-1EX30-7XE0)
SIMATIC CP 343-1 Lean (6GK7343-1CX10-0XE0)
SIPLUS NET CP 343-1 Lean (6AG1343-1CX10-2XE0)
SIMATIC CP 343-1 Advanced (6GK7343-1GX31-0XE0)
SIPLUS NET CP 343-1 Advanced (6AG1343-1GX31-4XE0)
cpe:2.3:h:siemens...
V3.1.1
V3.1.3
V3.0.33
V3.0.44
V3.0.53
Relations:
IsFamilyOf
Uses (SBOM)
Identical
Deprecated since (date)

Vendor Graph – Managing Duplicates



SIMATIC CP 343-1 family
CP 343-1 - NEW
SIMATIC CP 343-1
SIMATIC CP 343-1 Lean
SIMATIC CP 343-1 Advanced
SIMATIC CP 343-1 (6GK7343-1EX30-0XE0)
SIPLUS NET CP 343-1 (6AG1343-1EX30-7XE0)
SIMATIC CP 343-1 Lean (6GK7343-1CX10-0XE0)
SIPLUS NET CP 343-1 Lean (6AG1343-1CX10-2XE0)
SIMATIC CP 343-1 Advanced (6GK7343-1GX31-0XE0)
SIPLUS NET CP 343-1 Advanced (6AG1343-1GX31-4XE0)
cpe:2.3:h:siemens…
V3.1.1
V3.1.3
V3.0.33
V3.0.44
V3.0.53
Relations:
IsFamilyOf
Uses (SBOM)
Identical
Deprecated since (date)
IsSuccessorOf

Bottom line: Vendors

Only vendors can assign names to their products

- Every vendor creates own product graph and these names are authoritative

Every node and relationship has creation and deprecation dates

These names change constantly by mergers, marketing, carve-outs, restructurings

- Never delete nodes or relationships – deprecate them!
- Full flexibility – full backwad compatibility

The „identical“ relationship allows integration of other identifiers (CPE, PURL, ...)

The hardware part of the graph can be used as Bill of Materials (BOM)

The software part of the graph can be used as Software Bill of Materials (SBOM)

Maturity can be seen in the product graph

- See 2015 → 2018 → 2023 → future development

Bottom line: Consumers

Consumers find many identifiers on:

- Product label
- Orders
- Web sites
- Invoice
- SNMP scan

Each of these IDs can be part of the product graph

IDs that are not in the product graph are not genuine

Even low skilled user will find high level family names and can navigate deeper with help

#FIRSTCON23

35TH ANNUAL FIRST CONFERENCE
MONTRÉAL
JUNE 4–9, 2023

Questions welcome

#FIRSTCON23

35TH ANNUAL FIRST CONFERENCE

MONTRÉAL

JUNE 4-9, 2023

Merci, thanks, danke

Art Manion
zmanion@protonmail.com

Thomas Schmidt
thomas.schmidt@bsi.bund.de

Thomas Proell
thomas.proell@siemens.com