SIEMENS
Ingenuity for life

Version 1.0
April 2019

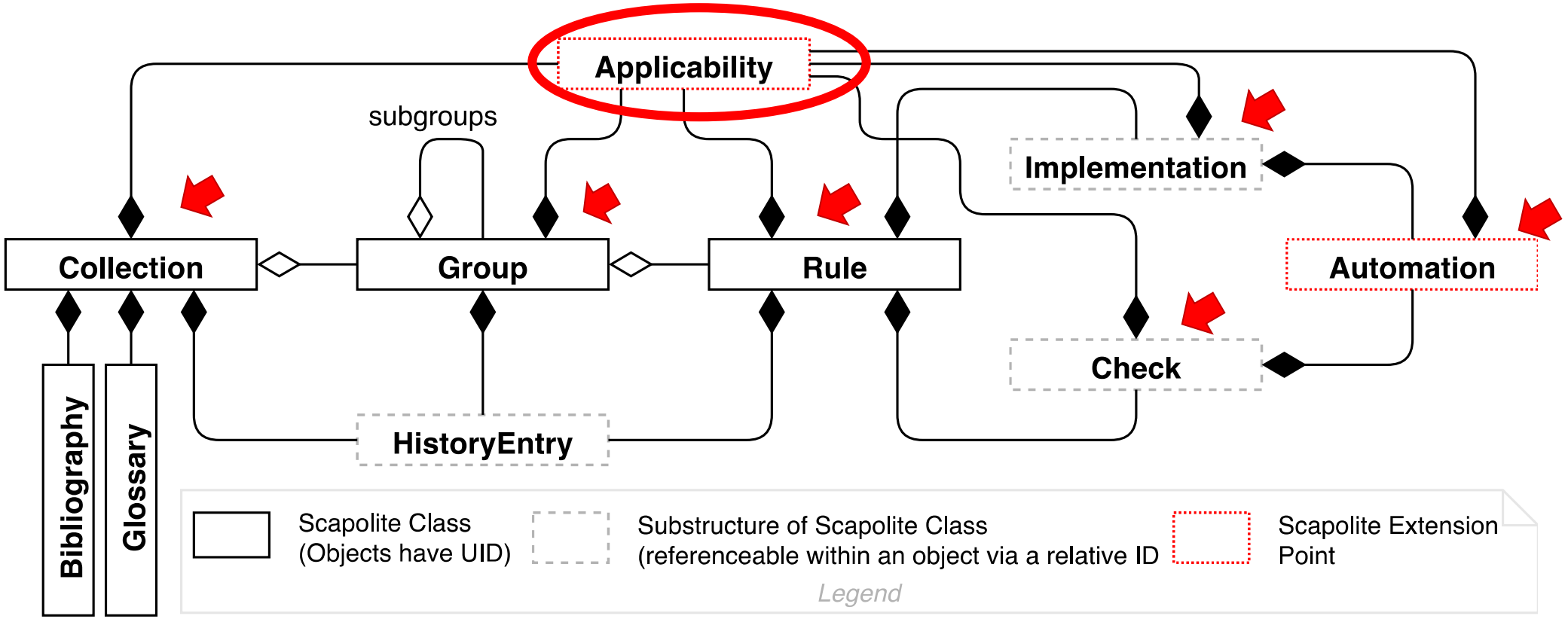
Toward a hierarchical and extensible applicability language

(presented @NIST SCAP v2 Workshop April 30th to May 2nd 2019)

Dr. Bernd Grobauer, Siemens CT RDA ITS

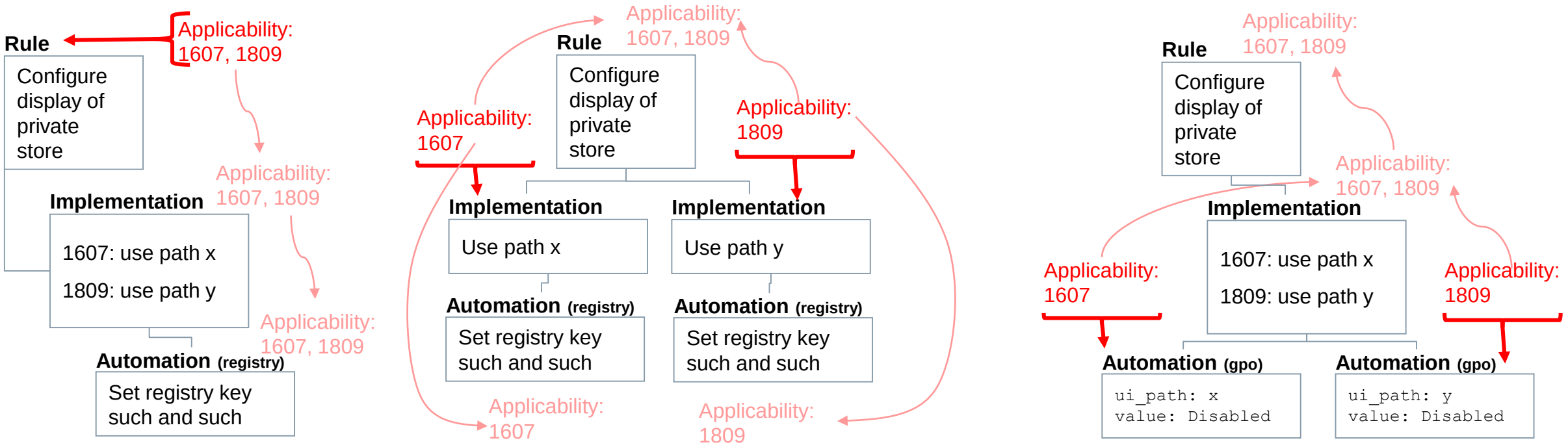
Depending on use-case and authoring style, applicability information may be used on one or more of several „levels“

SIEMENS
Ingenuity for life



Example: Handling a GPO path that changes between Windows releases

in 1607: `Windows Components\Store\Only display the private store within the Windows Store app`
In 1809: `Windows Components\Store\Only display the private store within the Microsoft Store`



Caution: Other applicability data may need a different semantics of how applicability information percolates to other levels; in some cases, having more than one item of applicability information within in a „path“ from top to bottom may not make sense.

Conclusion

SIEMENS
Ingenuity for life

- Applicability metadata is a prime candidate for format extensions
- Because of the hierarchical nature of security policies/baselines: the definition of an applicability extension must include the semantics of
  - How applicability information on one level transfers to other levels
  - How applicability information on different levels interacts with each other
    - Synthesis?
    - Possible contradiction, which leads to a semantic error?
    - …

5.1.3.3. Role-based definition of target audience

Siemens uses a roles to describe the target audience of an IS rule.

Figure 25 describe the contents of Siemens's role-based applicability-information entries.

```
system: com.siemens.cert.target_audience
roles: <SEQUENCE of role identifiers -- currently,
        the following identifiers are use:
        - employee
        - asset_owner
        - asset_manager
        - business_manager
        - bp_isec
        - ccso
        - gcso
        >
```

Figure 25: Example: Siemens use of applicability for defining target audience of a rule

Role-based applicability is used only for rules.

There are also simple cases ☺