

# PWG -Imaging Device Security (IDS) Working Group

December 9, 2010

Irvine, CA

PWG F2F Meeting

Joe Murdock (Sharp)

Brian Smithson (Ricoh)

# Agenda

---



- 11:00 – 11:05 Administrative Tasks
- 11:15 – 12:00 Supporting Documents for Common Criteria Evaluation (NIAP conference call)
- 12:00 – 13:00 Lunch
- 13:00 – 13:30 Supporting Documents for Common Criteria Evaluation
- 13:30 – 13:45 Review action items
- 13:45 – 14:00 Document status and Review
- 14:00 – 14:15 MPSA Survey results
- 14:15 – 15:00 Identification, Authentication and Authorization
- 15:00 – 15:15 Break
- 15:15 – 16:14 IDS Security Ticket
- 16:15 – 16:30 Wrap up and adjournment

# Administrative Tasks

---



- Select minute-taker
- Introductions
- IP policy statement:  
*"This meeting is conducted under the rules of the PWG IP policy"*  
*If you don't agree, Disney Land needs the business*
- Approve Minutes from December 2 conference Call

# IDS WG Officers

---



- IDS WG Chairs
  - Joe Murdock (Sharp)
  - Brian Smithson (Ricoh)
- IDS WG Secretary:
  - Brian Smithson (Ricoh)
- IDS WG Document Editors:
  - HCD-ATR: Jerry Thrasher (Lexmark)
  - HCD-NAP: Joe Murdock (Sharp), Brian Smithson (Ricoh)
  - HCD-TNC: Ira McDonald (Samsung), Jerry Thrasher (Lexmark), Brian Smithson (Ricoh)
  - HCD NAC Business Case: Joe Murdock (Sharp)
  - HCD-Remediation: Joe Murdock (Sharp)
  - HCD-NAP-SCCM: Joe Murdock (Sharp)
  - HCD-Log: Mike Sweet (Apple)
  - IDS-IAA: Joe Murdock (Sharp)

# Supporting Documents for Common Criteria Evaluation

---



# Action Items



| Action Item # | Entry date | Assignee   | Type        | Action   | Status | Disposition   |
|---------------|------------|--|-------------|--|--------|---|
| 33            | 12/10/2009 | Randy Turner                                     | SHV         | Randy Turner will contact Symantec (when appropriate) to encourage discussion with the PWG about a SHV.      | H      | No longer blocked waiting for AI #32 so we can send market rationale to Symantec.   |
| 34            | 12/10/2009 | Randy Turner                                     | Remediation | Randy Turner will investigate Symantec's products and their method(s) to "remediate noncompliant endpoints." | H      | Symantec wants an NDA, but PWG cannot do an NDA; will do a generic version; should we invite Symantec to a PWG IDS teleconference?                                    |
| 44            | 3/11/2010  | Jerry Thrasher<br>Ira McDonald<br>Brian Smithson | NEA Binding | Recast the NEA Binding document as a TCG TNC Binding document  |        | Make it a TCG document, not an IETF NEA document  |
| 58            | 6/11/2010  | Joe Murdock<br>and Ira McDonald                  | SCCM        | Create a first draft SCCM binding spec based on the NAP binding spec   | H      | MS is releasing R3 of SCCM and also a beta of "R-next", while at the same time adding power management; WIMS group may also be interested. On hold due to priorities. |
| 66            | 10/20/2010 | Brian Smithson<br>Joe Murdock<br>Ira McDonald    | admin       | Create a project charter for creating IEEE 2600.1 Supporting Documents                                       |        | With no requirements specification  |
| 67            | 10/28/2010 | Joe Murdock<br>Ira McDonald                      | auth        | Write HCD-Authentication-and-Authorization-Framework specification   | P      |   |
| 68            | 12/2/2010  | Joe Murdock                                      | auth        | Define IAA Security Ticket (per October 2010 F2F)  | P      |   |
| 69            | 12/2/2010  | Michael Sweet                                    | log format  | Write HCD Logging specification  | P      |   |

# Document Status

---



- HCD-Assessment-Attributes

- <ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-idsattributes10-20100930.pdf>

- Stable (needs a binding prototype)

- HCD-NAP Binding

- <ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-napsoh10-20100930.pdf>

- Stable

- HCD-TNC Binding

- Initial Draft still under development

- HCD-NAC Business Case White Paper

- <ftp://ftp.pwg.org/pub/pwg/ids/white/tb-ids-hcd-nac-business-case-20100422.pdf>

- Final

# Document Status



- HCD-Remediation
  - <ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-remediation10-20100930.pdf>
    - Initial Draft
- HCD-NAP-SCCM Binding
  - Specification on hold
- HCD-Log
  - White Papers:
    - <ftp://ftp.pwg.org/pub/pwg/ids/white/ids-logging-20100608.pdf>
    - [ftp://ftp.pwg.org/pub/pwg/ids/white/IEEE2600.1\\_audit\\_events.pdf](ftp://ftp.pwg.org/pub/pwg/ids/white/IEEE2600.1_audit_events.pdf)
  - Specification:
    - <ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-log10-20101018.pdf>
  - Initial Draft
- IDS-Identification-Authentication-Authorization
  - White Papers:
    - <ftp://ftp.pwg.org/pub/pwg/ids/white/ids-authorize-20100608.pdf>
  - Mind Map:
    - <ftp://ftp.pwg.org/pub/pwg/ids/white/ids-iaa-framework-2010-12-03.xmind>
  - Specification (outline only):
    - <ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-iaa10-20101202.pdf>
    - <ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-iaa10-20101202.docx>



# NAC Attributes

---



- IDS-ATR Security Attributes
  - Do we need to add a security log destination attribute
    - Ensure location to archive logs
  - Any other attributes?

# MPSA Survey Results

---

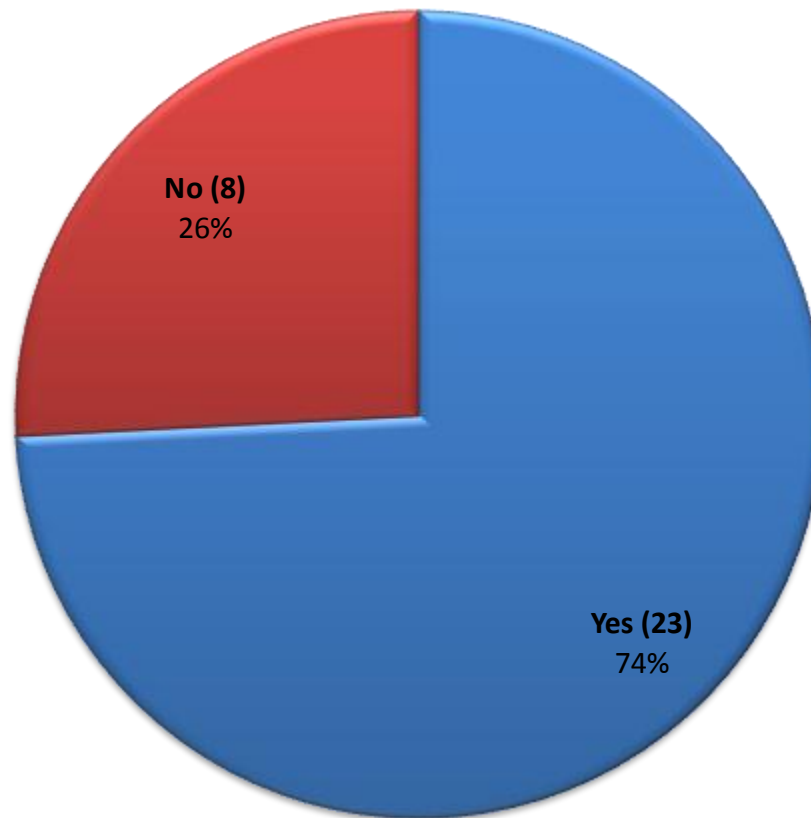


- Questionnaire and survey posted during November
- Good Survey response
  - 31 respondents
- Just received raw data
  - Need to analyze

# MPSA Survey Results

---

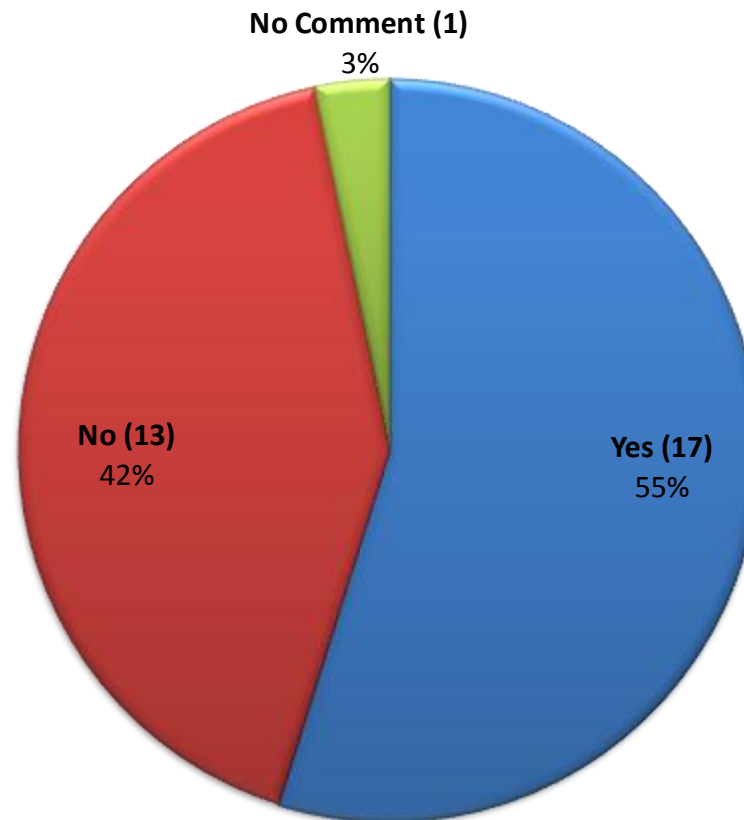
**Do your clients use NAC to manage network access?**



# MPSA Survey Results

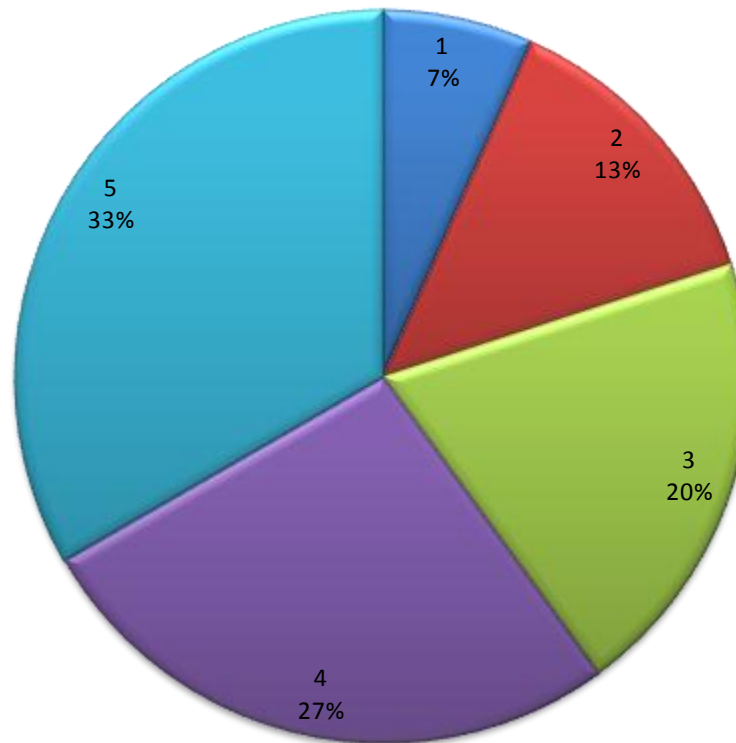
---

**Are your client's multifunction hardcopy devices manually configured in their NAC system?**



# MPSA Survey Results

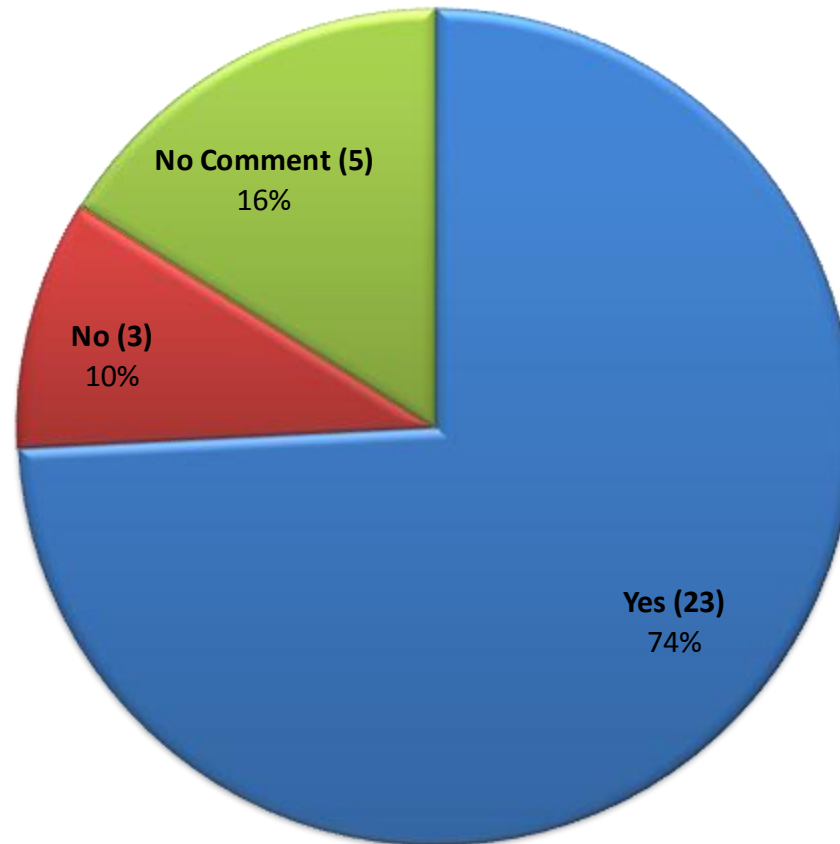
Rate how important that your client's multifunction  
hardcopy devices support NAC?  
1 = Low, 5 = High



# MPSA Survey Results

---

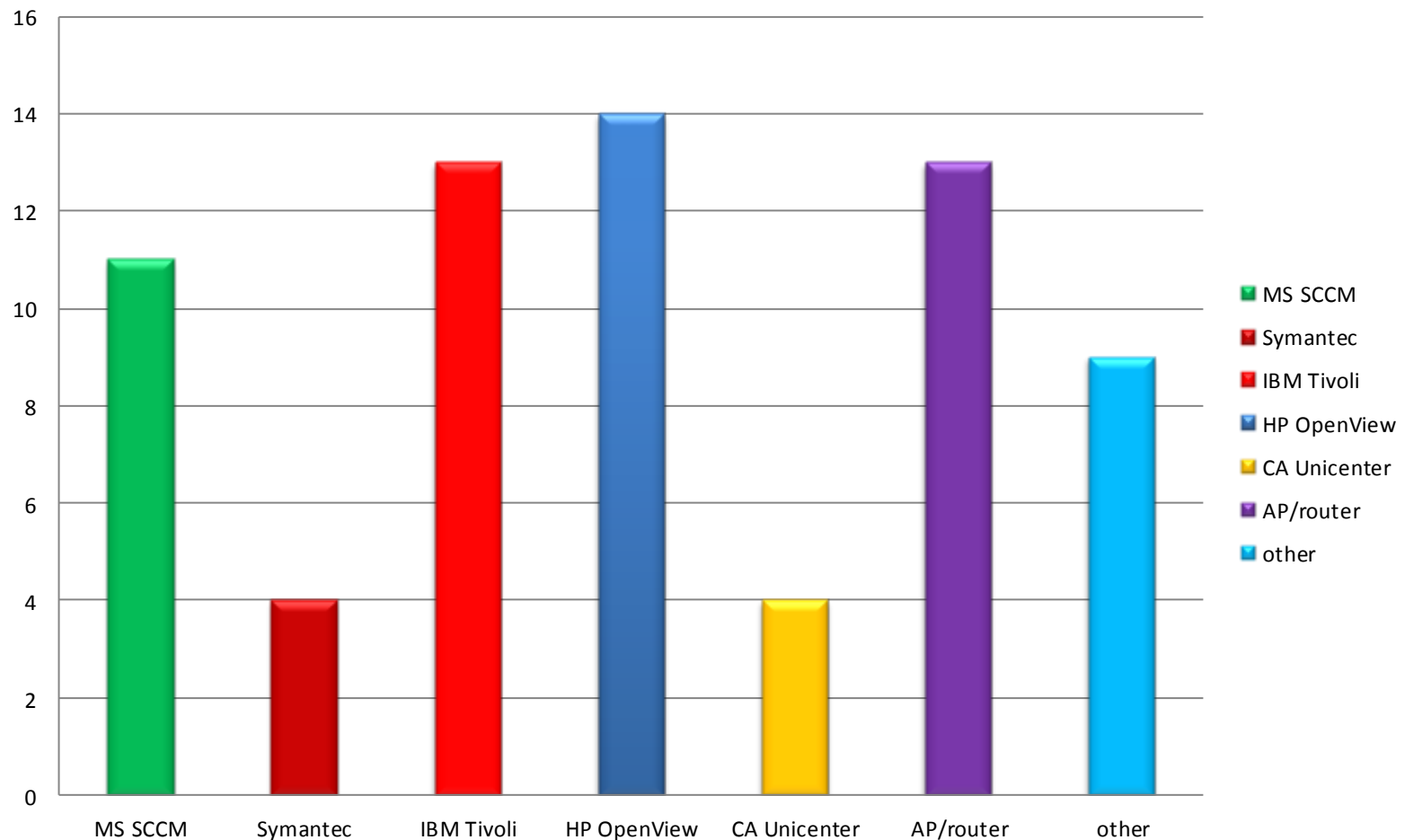
Do your clients use network asset management tools



# MPSA Survey Results



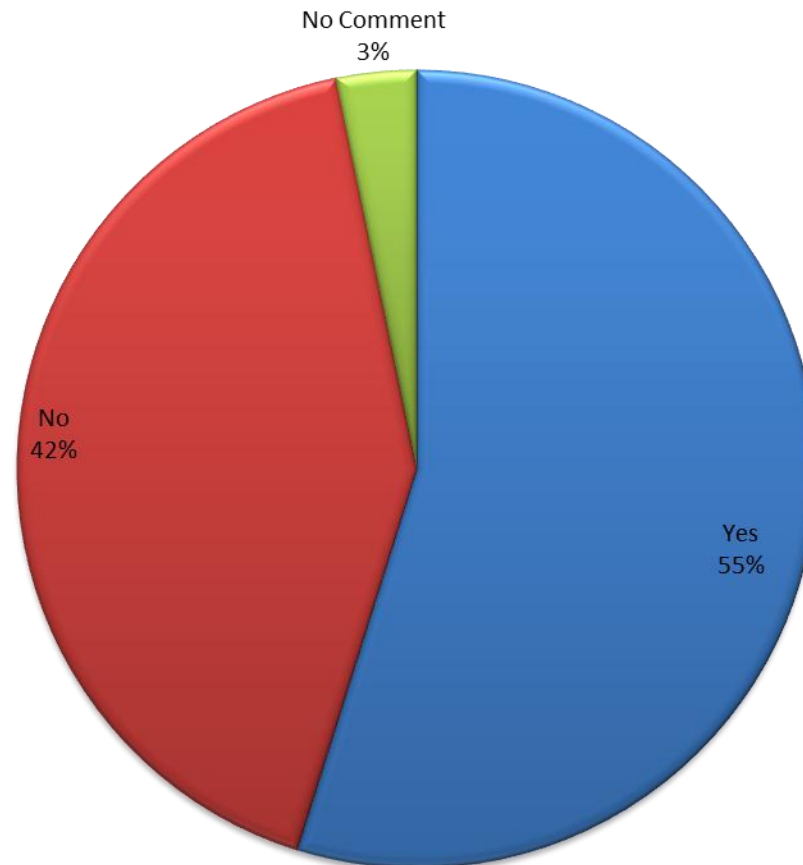
Which Network Management tools do you run across most commonly?



# MPSA Survey Results



**Would limited support for existing NAC tools such as Microsoft SCCM help your clients?**

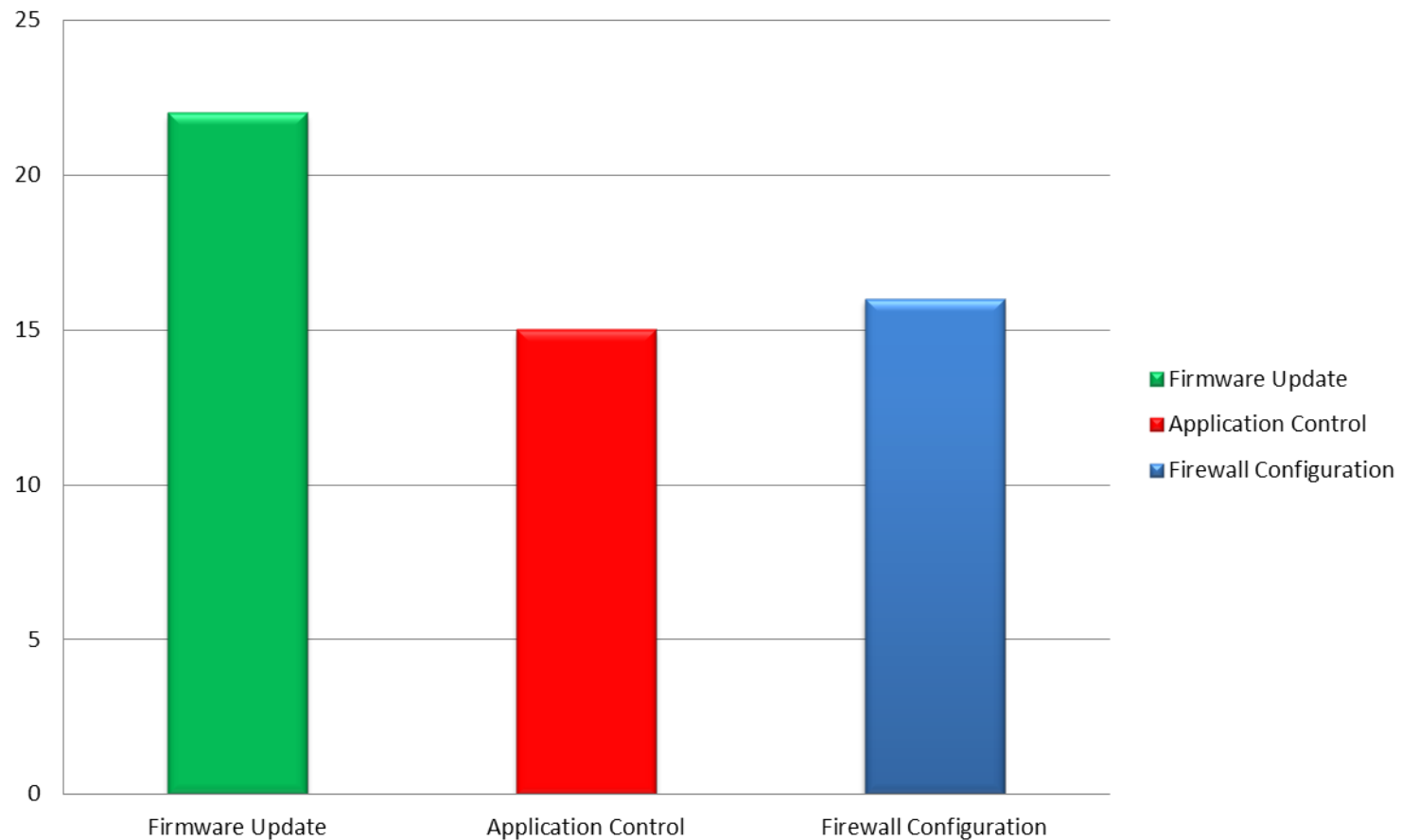




# MPSA Survey Results



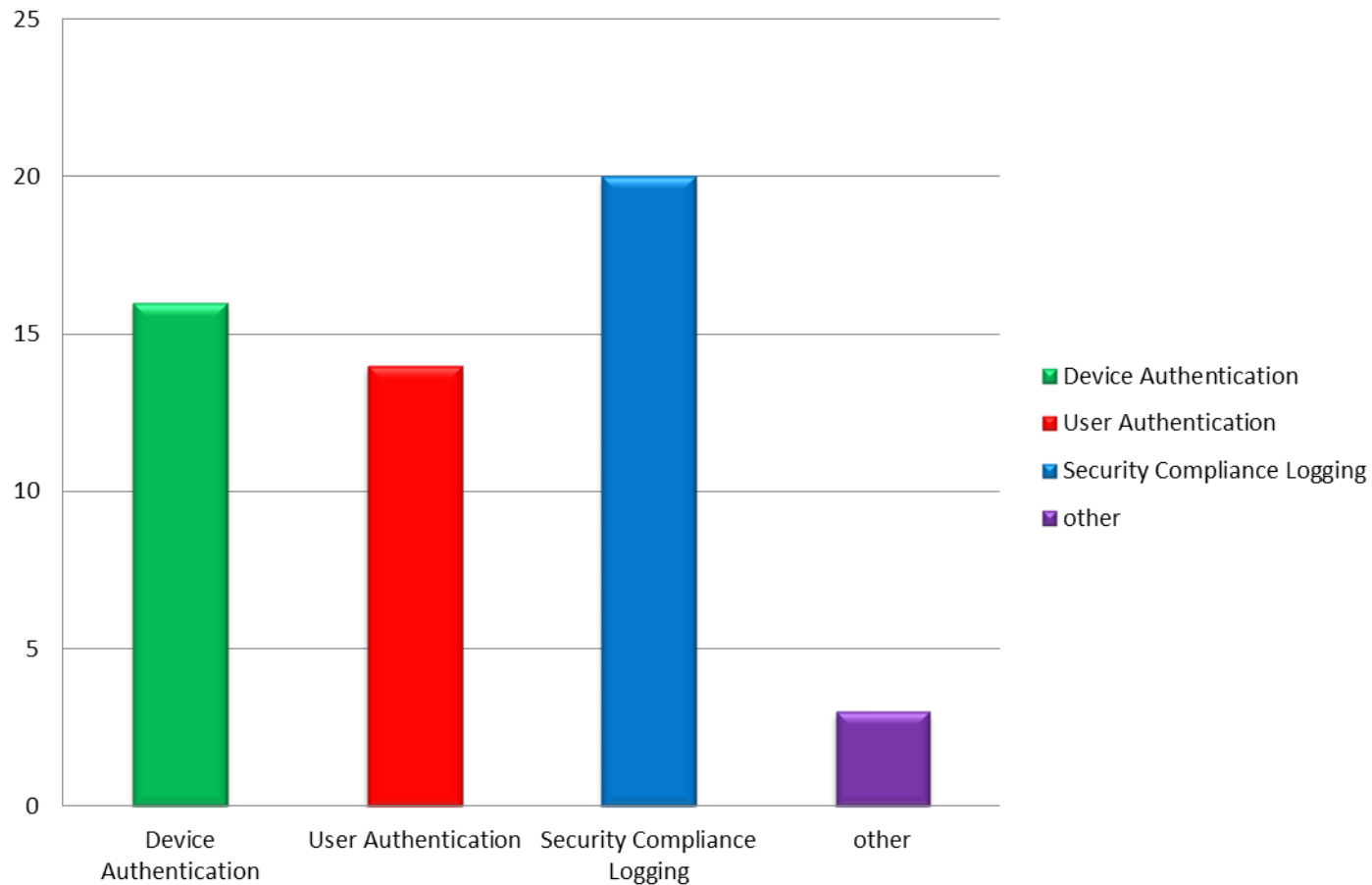
**Would automatic remediation of device security failures help your clients?**



# MPSA Survey Results



**What are other hardcopy security issues that your clients are concerned with?**

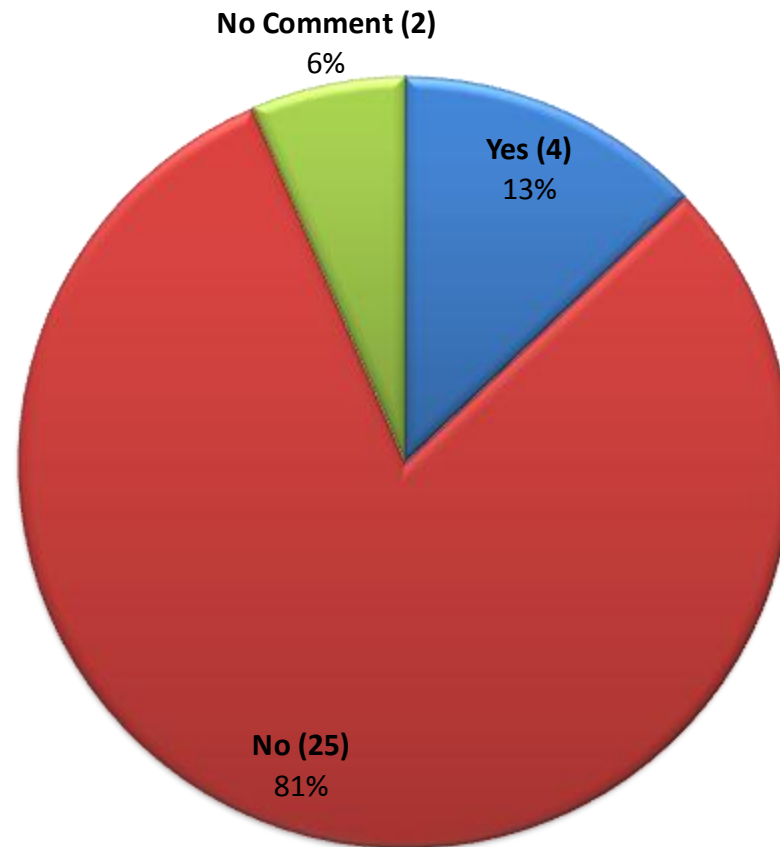


# MPSA Survey Results

---



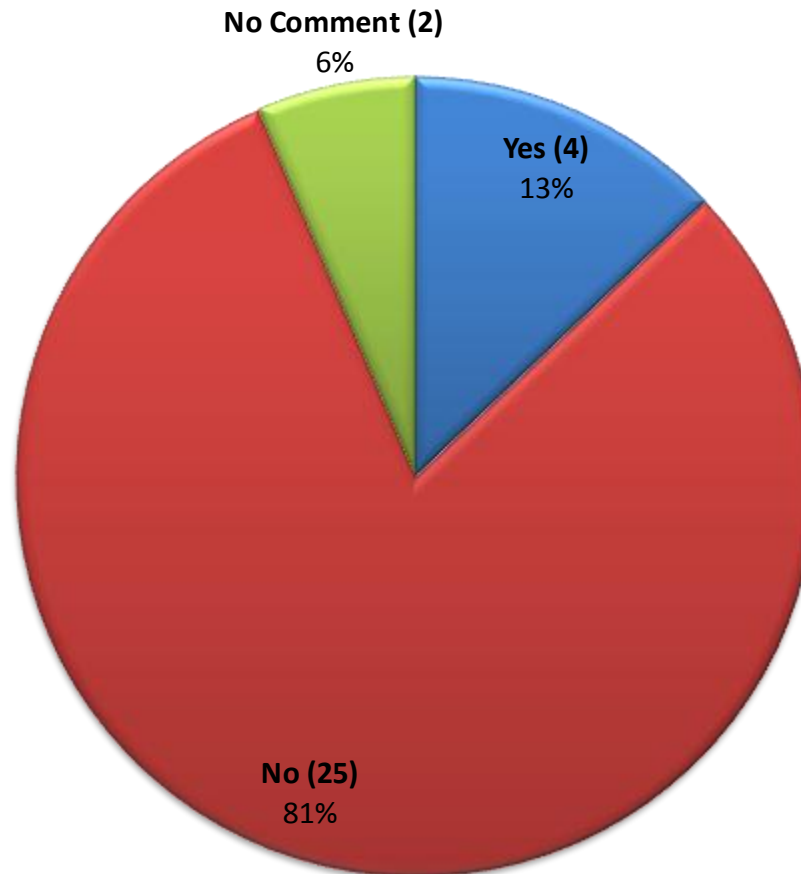
**Are you or your clients aware of the IEEE 2600 series of hardcopy security standards?**



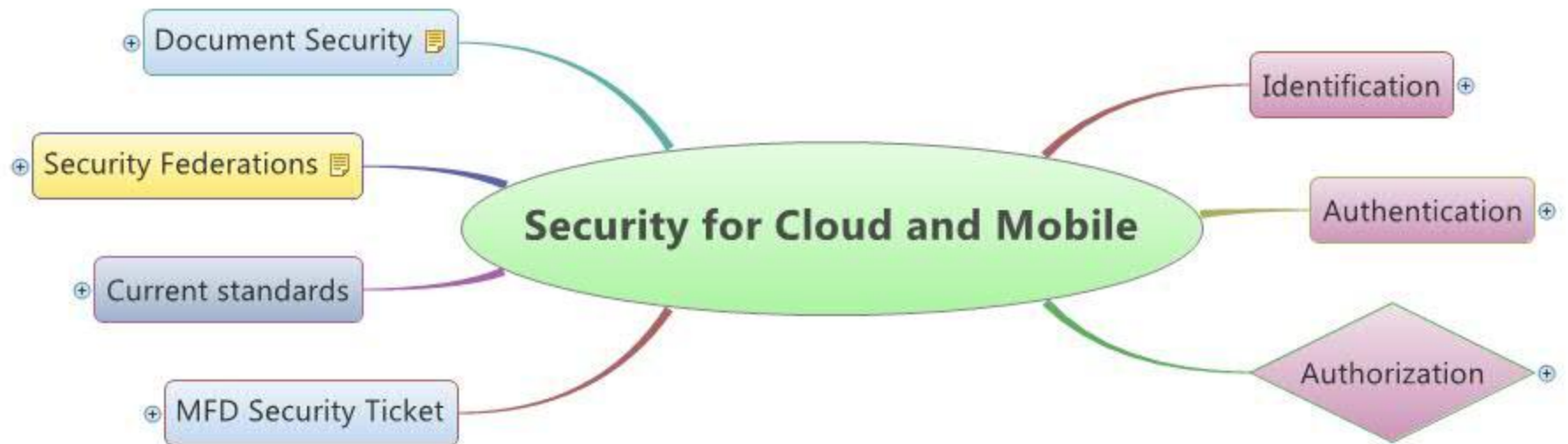
# MPSA Survey Results



**Are you or your clients aware of the PWG Imaging Device Security projects?**



# Mobile, Cloud and Device Security



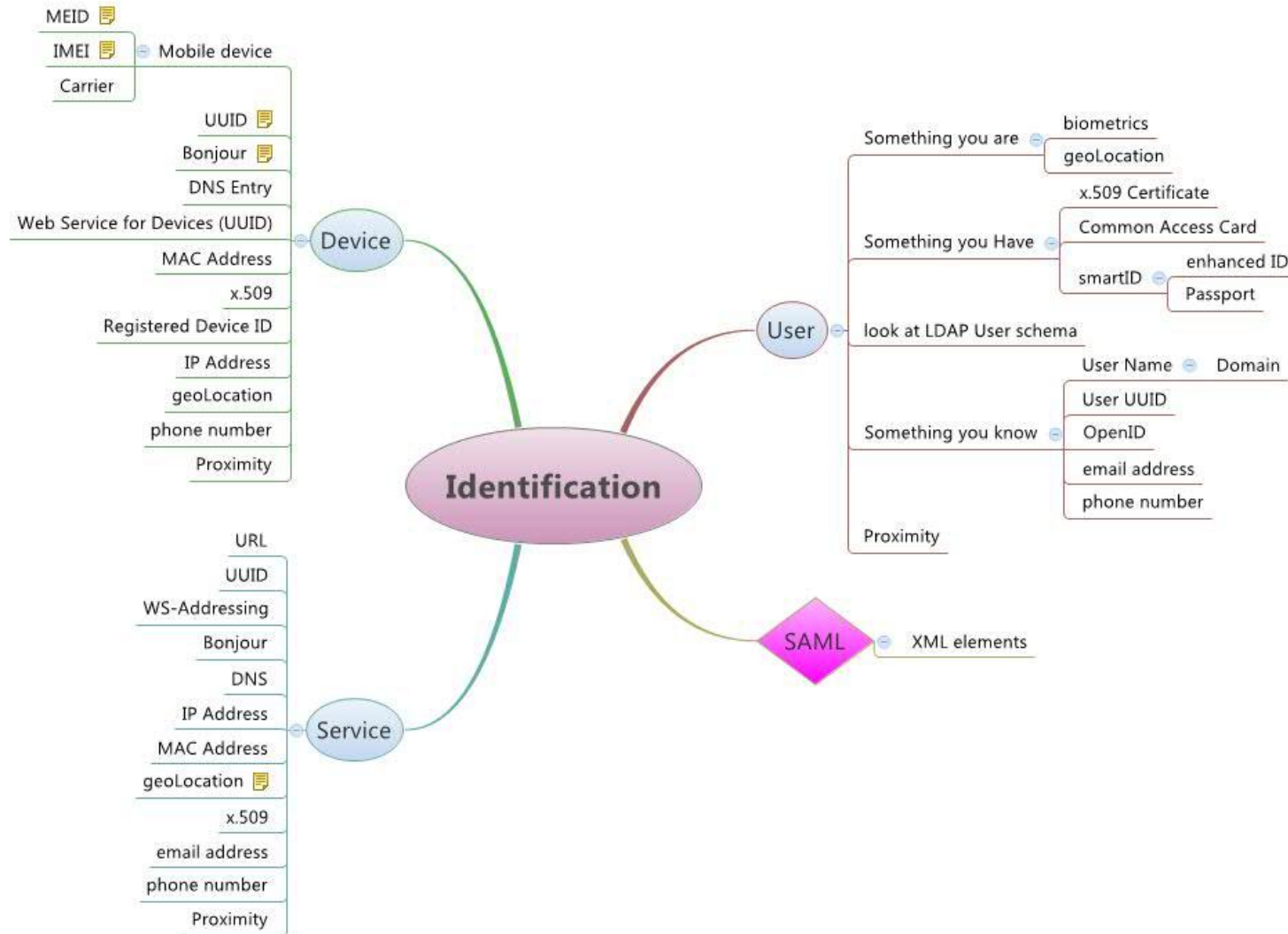
# Identification, Authentication and Authorization

---

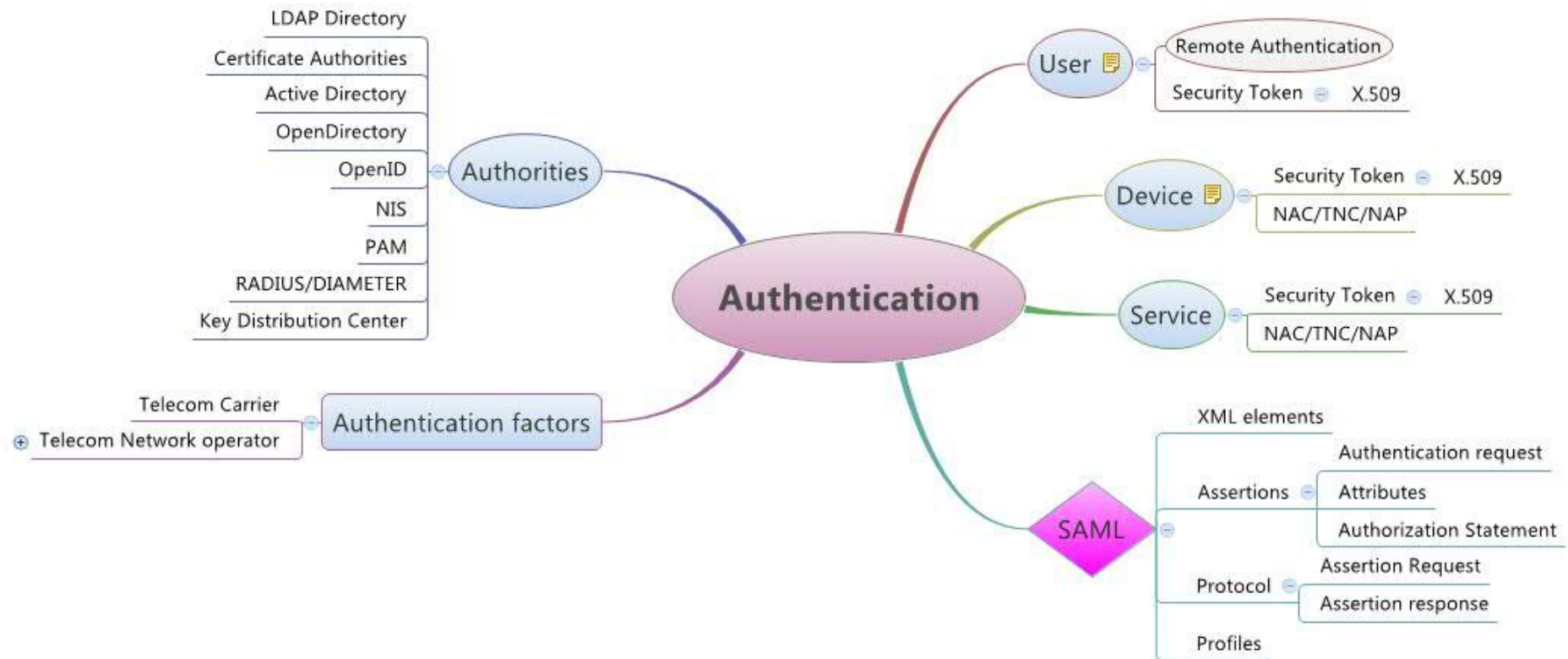


- Recommendations only
  - Recommendation of standards and methods for IPP Everywhere and cloud computing
  - No new protocols
    - Define PWG Security Ticket
- Use Current standards where applicable
  - SAML – widely used
  - WS-Federation – heavy Microsoft support, supports SAML assertions
  - WS-Security Extensions
  - XML Digital Signature
  - XACML
- Mindmap file:
  - <ftp://ftp.pwg.org/pub/pwg/ids/white/ids-iaa-framework-2010-12-03.xmind>
- Identification, Authentication, Authorization
  - Specification outline
    - <ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-iaa10-20101202.pdf>
    - <ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-iaa10-20101202.docx>
- Document Access Control
  - Not DRM

# Identification Framework

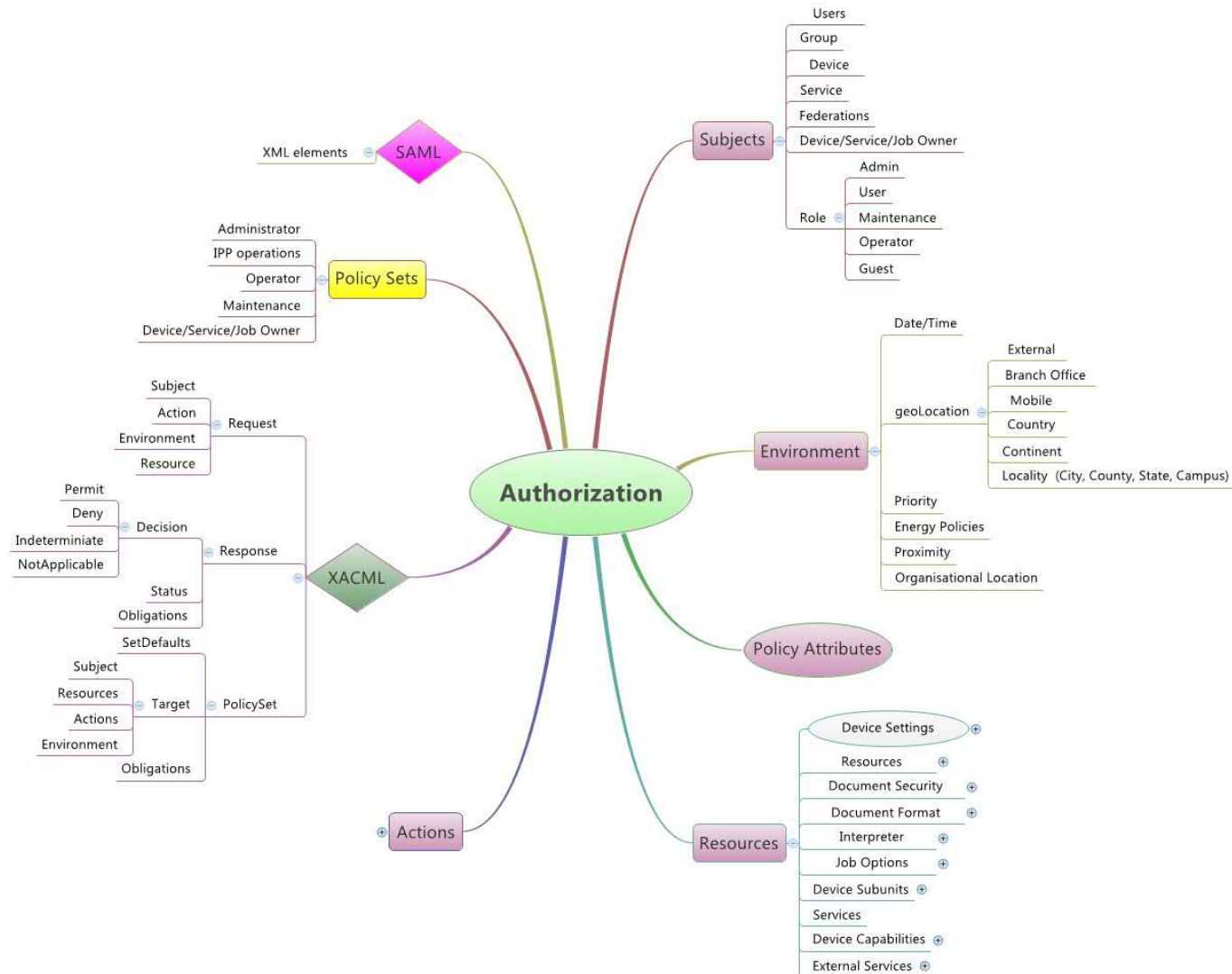


# Authentication Framework





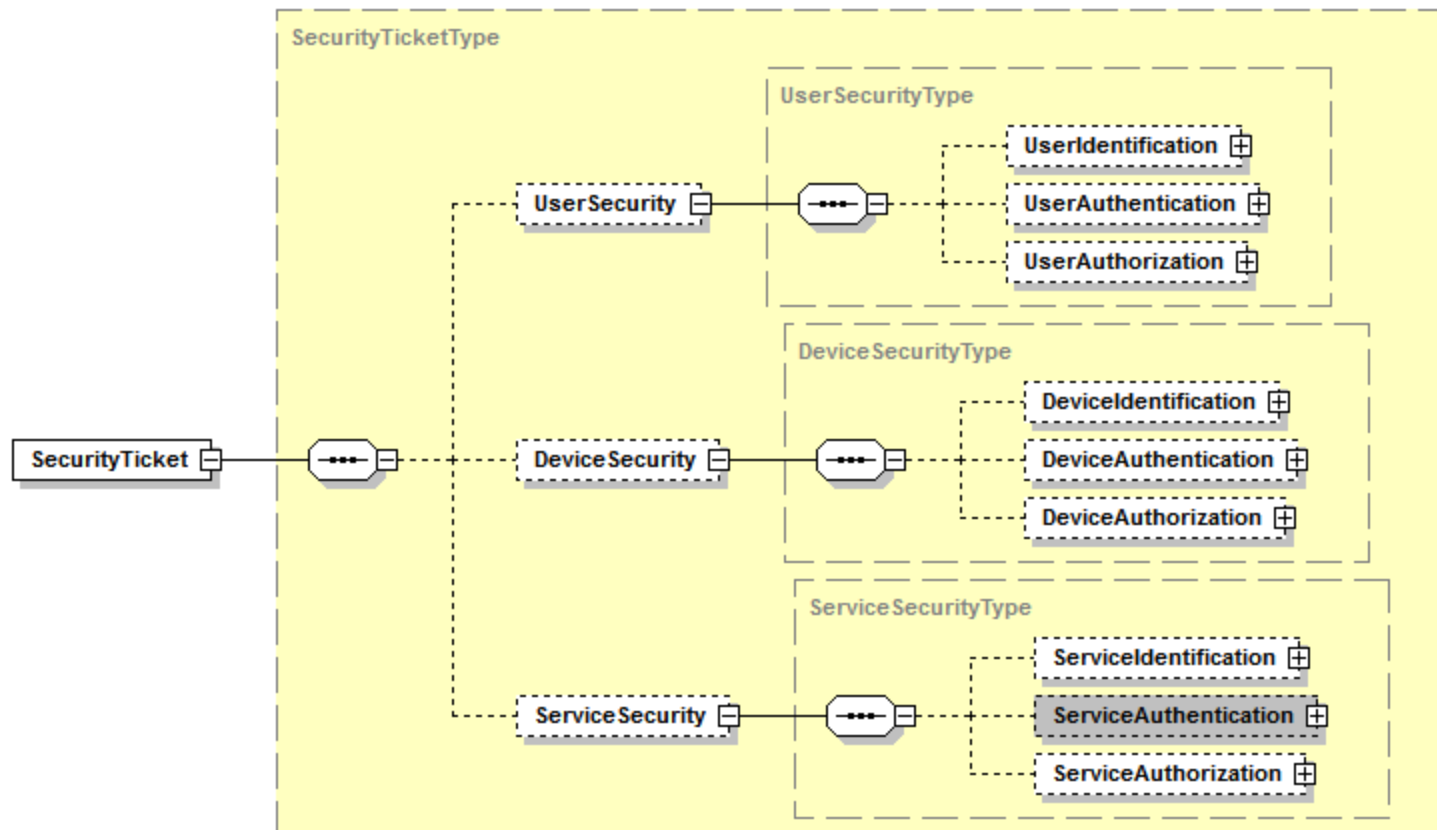
# Authorization Framework



# Security Ticket

- Review XML Schema Element

<ftp://ftp.pwg.org/pub/pwg/ids/white/ids-security-2010-12-08.xsd>



# Wrap up

---



- Review of new action items and open issues
- Conference call / F2F schedule
  - Next Conference call January 13, 2011
- Adjournment