

802.1AR task group
meeting notes
Mar. 2006 plenary – Denver

Managed objects

| function | managed object | administrator |
|----------------|-----------------------------|---------------|
| | user | |
| | if (IDevID_private == true) | |
| IDevID | { no access } else { RO } | RO |
| LDevID | RO | RW |
| IDevID_private | RO | RW |
| LDprivKey | n/a | n/a* |
| IDprivKey | n/a | n/a |

* confirm

Notes arising out of managed objects discussion

- auth protocols using .1AR run at “user” privilege level
- enabling IDevID_private results in IDevID being unavailable in user mode always (i.e. regardless the existence of LDevID)
- corollary: to use DevID with privacy set, assign a LDevID first then enable privacy
 - without LDevID, attempt to use DevID will fail, i.e. DevID functionality not available

- suggest viable keywrap mechanism(s) in non-normative text for wrapping keys off of DevID module
 - require disclosure of keywrapping methods (if any) in compliance statement
- find right spot in draft to define standard mechanism to create/insert key pairs for LDevID creation
- (check out RMON reuse for transportable MIB objects)

.1AR - .1af discussion

- Proposal: define a X509 certificate format and profile for DevID for use in an EAP exchange for .1af
- describe an enrollment protocol for introducing and bringing a device from IDevID to fully instantiated LDevID
- compare DevID format to what's used in 802.16, .21, .11i, .11s, DOCSIS, look for commonality
- Action: Max & Mike to capture into text and circulate to task group for TG ballot prior to interim