

Meeting notes for reviewing Microsoft's comments on the Security 2.0 HLD. Part 1 held on 3/3/15 and part 2 held on 3/6/15

Review meeting part 1 begins

https://meetings.webex.com/collabs/url/EFt-NCcDNzn5E0OFE_4CUXcuQmjeNFSk4f5SasPmd_u00000

- Page 6
 - GUID- Should we use RFC 4122? If so, we need JIRA ticket
 - Replace Guild with more common terminology such as “security group”
 - Change to refer to app and not device
 - Update definition of security manager to be an app
 - The app may have AJ interfaces
 - Consider not using Security appliance as a terminology
 - Consider combining Cert authority and issuer definition.
 - Entity is Cert auth
- Page 7
 - Edit mutual auth sentence to be more specific
 - Clarify “...permissions can be installed directly into the application”
- Pages 8-10
 - Application and appld are too similar
 - Claiming – add “for AJ security”
 - Policy – add “any authorized peer”
 - Policy – Remove “delivered by admin”
 - Policy – An application may (add the word “Have”)...
 - Membership Certificate – Clarify last bullet
 - Guild equivalence certificate – Need to define notion of mapping
 - Can include definition sent on email thread with Dave Thaler (MSFT)
 - Update “access” to “the same access”
 - Identity certificate
 - Need to define “Identity data” separate from Identity certificate
 - Security manager – need to define “subject application”
- Page 11
 - Replace top of columns on drawings to be piece of code
 - Add identity cert on both sides
 - Table needs updating
 - ECDHE_NULL – needs response to Dave’s question on CoreWG mail list
 - Need JIRA ticket
 - Add additional explanation for the purpose of issuing an identity cert
- Page 12
 - Clarify guild name and what it is used for
 - Remove “typically”
 - Define “policy term” and “target policy term”
- Page 13
 - Phil will update all tables based on feedback
 - 2.3.5 maybe change to “add public key to guld”
 - 2.3.5 update description to include Dave’s comment

- Page 14
 - Text and diagram need to match
- Page 15
 - 2.3.7 update based on feedback
- Page 16
 - Potential JIRA ticket to use partial martial to put into one call for figure 2.8
- Page 18
 - 2.3.9 – Clarify requirements for how a revocation service works
 - If not specified then note it.
 - General comment – annotate the items that are proposed future features not fully designed.
- Page 19
 - 2.3.11 needs clarification based on Dave’s comment
 - Need more discussion on 2.3.11
- Page 22
 - 2.4.2 diagram – Type “Any User Policy” needs to be defined
 - 2.4.2 – enforcement needs to be clarified

Review meeting part 1 ends

Review meeting part 2 begins

<https://meetings.webex.com/collabs/url/FHeABKYj57sE27ifFF8XDTrANUzFNEwvcYtPgOJR9e00000>

- 2.12 diagram – Information disclosure vulnerability exposed
 - Should file JIRA ticket but not urgent for 15.08
- Page 25
 - 2.4.6 – need to clarify wording
- Page 27
 - May want to add info as to when serialNumber is used – this is a new definition
 - Admins is removed
- Page 28
 - Rename 2nd entry to not use GUID and instead call it public key
 - Clarify what it means when there is no star (*)
- Page 29
 - If data type is number values should specify the numbers
 - Clarify observe based on feedback - take observe out of modify
- Page 30
 - Clarify table titles
 - Update 2.5.2.4 first bullet to clarify based on feedback
- Page 33
 - Clarify the format the guild identifier is encoded – 16byte
- Page 35
 - Clarify not granted
- Page 39
 - Update table based on feedback
- Page 42
 - Why not a session signal?
 - Security manager will have to deal with about
 - Consider 2 interfaces – one with claim method
 - QEO to take action to determine impact on Security Manager

Action items:

- Plan to schedule a day long F2F (most likely at MSFT campus)
 - Dino and Chris to sync on location and proposed timing.
- Phil to file JIRA tickets as identified in the notes
- Gerrit to determine impact to Security Manager regarding not using sessionless signals as identified on page 42