Step Up Protocol Requirements
references

• Please refer to
  http://www.surf.nl/binaries/content/assets/surf/en/knowledg
ebase/2012/rapport_step-up_authentication-as-a-
service_architecture_and_procedures_final.pdf

• Step-up Authentication Scenarios with AD FS 2.0 Part . see
  http://blog.auth360.net/2013/07/30/step-up-authentication-
  scenarios-with-ad-fs-2-0-part-ii/

• for examples of step up systems in use or development today
• Open
  – vendor neutral
  – Standards based
  – Build on standard based LOA for authentication
  – Clear definition of what LOA means
    • LoA is the combination of
      – Identity Assurance
      – Authentication assurance
  – Use Known methods for Step Up with auth tokens
  – Use well defined and standard based Meta data expression for LOA
    • IS LOA done in real time or off line or combination
  – Can work with an architecture that accommodate the ability of RP to determine how a step up LOA can be done.
• Can work with many possible federation architecture
  – Many to many Hubs
  – Gateway/Proxy
  – Delegated
  – Cloud (step-up as a service)
• Authentication Flow is flexible and can be bound to API, existing protocols or services
• Should be able to enable the RP and IdP to work together to contribute to an LoA increase
• Should be able to bind identity to an authentication step. Identity can be a collection of attributes.
• Can work with current password replacement solutions (FIDO, IBOPS, Browser etc)
• Should provide a foundation for a non-password authentication on the web
• Does need to work with or without point to point solutions
• Protocol need to be general enough (not tied to a specific identity system) and capable of plugging in specific solutions
• How can an RP know the Max LoA that can be achieved from a given device
• Can work with current password replacement solutions (FIDO, IBOPS, Browser etc)
• Should provide a foundation for a non-password authentication on the web
• Does need to work with or without point to point solutions
• Protocol need to be general enough (not tied to a specific identity system) and capable of plugging in specific solutions
• First cut should focus on the functions that need to be provided and can keep specific details to implementers.