Kerberos Reserved Names and Anonymity Support

Larry Zhu

IETF66

Microsoft

Reserved Principal Names

- New name type
  - KRB_NT_RESERVED TBA
- Name values
  - Two or more components
  - First component MUST be “RESERVED”
- Errors
  - KRB_AP_ERR_RESERVED_PRINCIPAL_NAME_UNKNOWN TBA

Reserved Kerberos Realms

- RFC4120 realms
  - domain: ATHENA.MIT.EDU
  - X500: C=US/O=OSF
  - other: NAMETYPE:rest/of.name=without-restrictions
- Reserved Realm Names:
  - RESERVED:realm-name
- Errors
  - KRB_AP_ERR_RESERVED_REALM_NAME_UNKNOWN TBA

Naming of Anonymity

- Anonymous principal name
  - Name type: KRB_NT_RESERVED
  - Value: “RESERVED”, “ANONYMOUS”
- Anonymous realm name
  - Value: “RESERVED:ANONYMOUS”
- Anonymous authentication path
  - NO-TRANSITED-INFO TBA

Issues for Anonymity Support

- authtime reset, preventing association
- Anonymity in cross-realm authentication
  - Client realm can be the real realm name or the anonymous realm name
  - Rules for preserving authentication paths
- Authorization data and client identity
  - AD-IF-RELEVANT is critical

GSS-API updates

- Single string representation for GSS_KRB5_NT_PRINCIPAL_NAME.
  - “RESERVED/ANONYMOUS”
  - “RESERVED/ANONYMOUS@RESERVED:ANONYMOUS”
  - “RESERVED/ANONYMOUS@<realm name>”
- GSS_C_NT_ANONYMOUS name type

Questions