S/MIME v4 Updates

Jim Schaad

August Cellars

Last Issue Resolved

- What algorithm is used when the capabilities on the other side are unknown
- Document says:
  - SHOULD AES-GCM
  - Else SHOULD AES-CBC
- Russ Request for comment from implementers on 13 March
- Wei responded on 14 March – yes use AES-GCM
- Issue closed