Registry Lock - What’s The Standard?

Registration Operations Workshop #8 - 9 May 2019

James Galvin, Ph.D.,[Afilias] (Chair)
Justin Mack [MarkMonitor]
Jaromir Talir [CZ.NIC]
Tongfeng Zhang [CIRA]
Gavin Brown [CentralNic]

What is registry lock?

- Protocol element - Defined in EPP since 2004 (2001)
  - Use of 1 or more of the following registry domain, host, and contact statuses
    - serverDeleteProhibited
    - serverHold
    - serverRenewProhibited
    - serverTransferProhibited
    - serverUpdateProhibited
- Security Service
  - Bundle of 1 or more registry statuses for 1 or more of domain, host, or contact objects
  - Establishes a relationship between the registry and the registrant
- A popular response to DNSpionage
  - Root cause is a credential management problem
  - DNS and other registration data changes were the consequence

What Should Be Standardized?

- What problem are we trying to solve?
  - gTLD vs ccTLD
- Which protocol elements should be part of the “security” bundle?
  - serverTransferProhibited and serverUpdateProhibited are good candidates
  - Probably don’t want to include serverHold and serverRenewProhibited
- Should the registry interact with the registrant directly?
  - gTLD Policies today would suggest no
  - Credential management is an issue and security is enhanced with fewer actors
- Impact of automation
  - Credential management is an issue
  - Automated and Manual have different security characteristics, e.g., threat vectors