Security Incident Response Contact Repository Implementation

Luis Diego Espinoza (Chair)
Antoinette Johnson, .vi
Isak Jacobsen, .fo
Hitoshi Saito, .jp
Mohamed Ibrahim, .so
Wim Degezelle, CENTR (observer)

http://ccnso.icann.org/workinggroups/iriwg.htm

Computer Incident Response Team

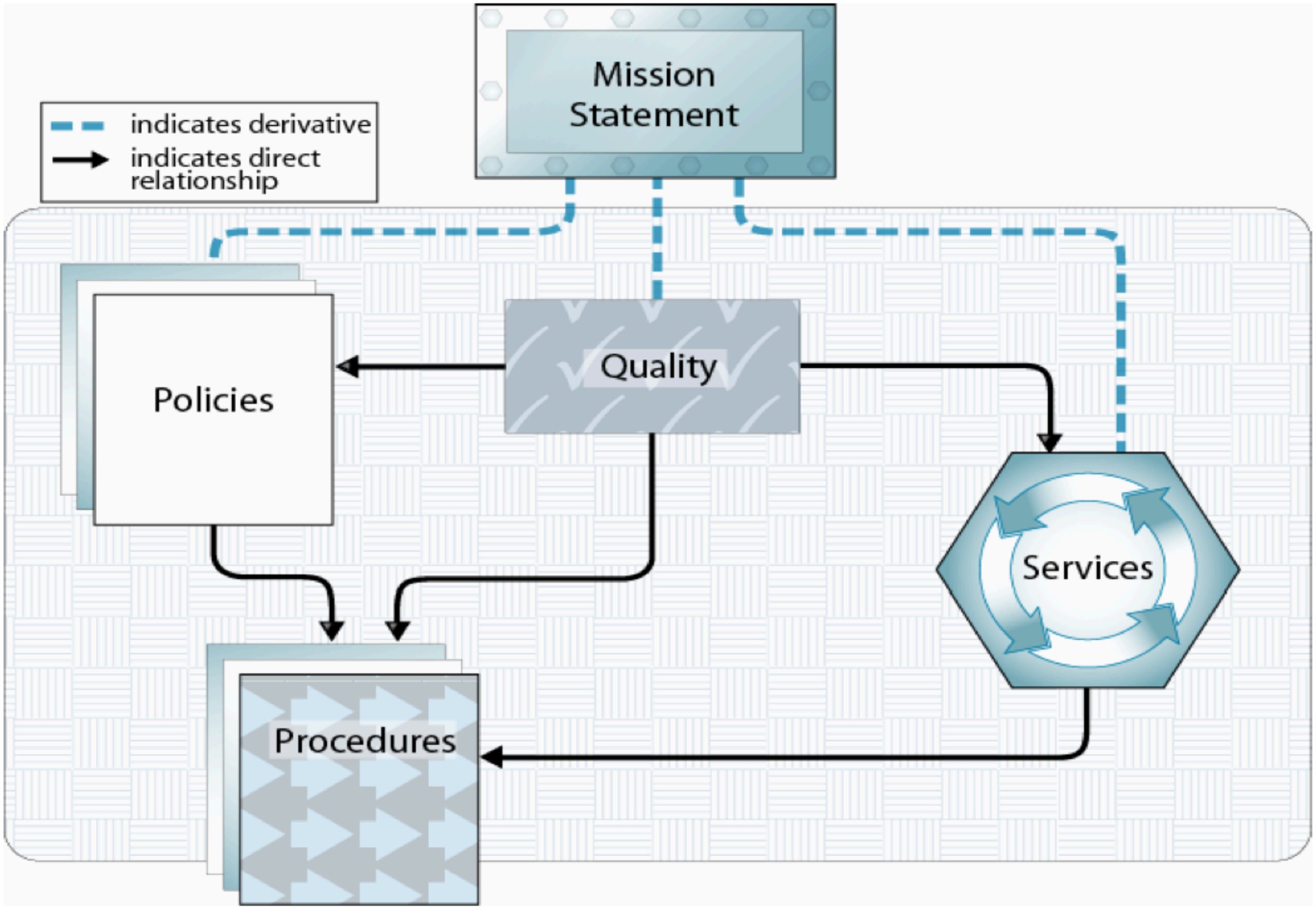


Figure 3: Service and Quality Framework as Derived from Mission Statement

West-Brown, Moira J. et al. (2003). Handbook for Computer Security Incident Response Teams (CSIRTs)

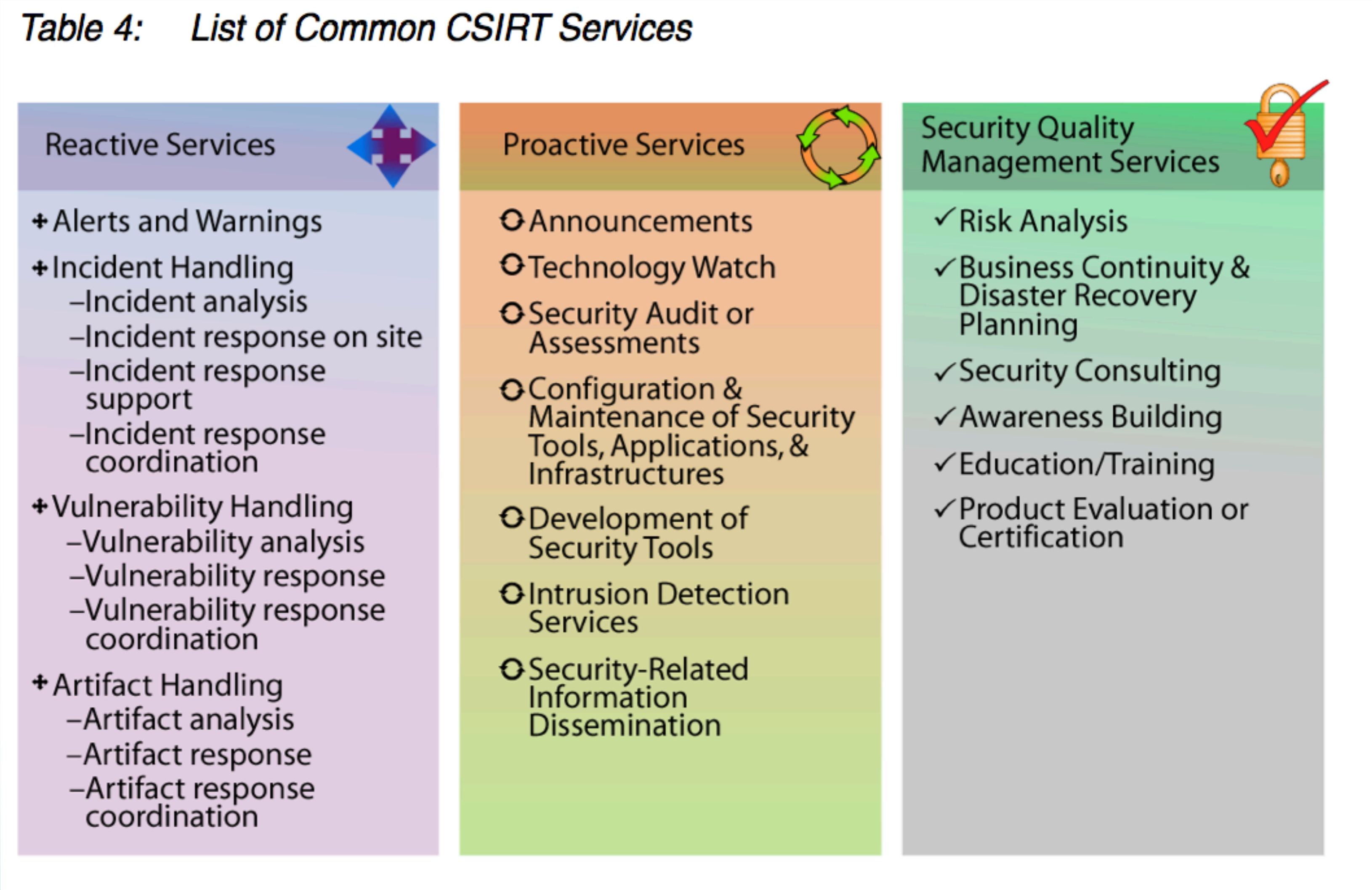


Table 4: List of Common CSIRT Services

Reactive Services

- ✚ Alerts and Warnings
- ✚ Incident Handling
  - –Incident analysis
  - –Incident response on site
  - –Incident response support
  - –Incident response coordination
- ✚ Vulnerability Handling
  - –Vulnerability analysis
  - –Vulnerability response
  - –Vulnerability response coordination
- ✚ Artifact Handling
  - –Artifact analysis
  - –Artifact response
  - –Artifact response coordination

Proactive Services

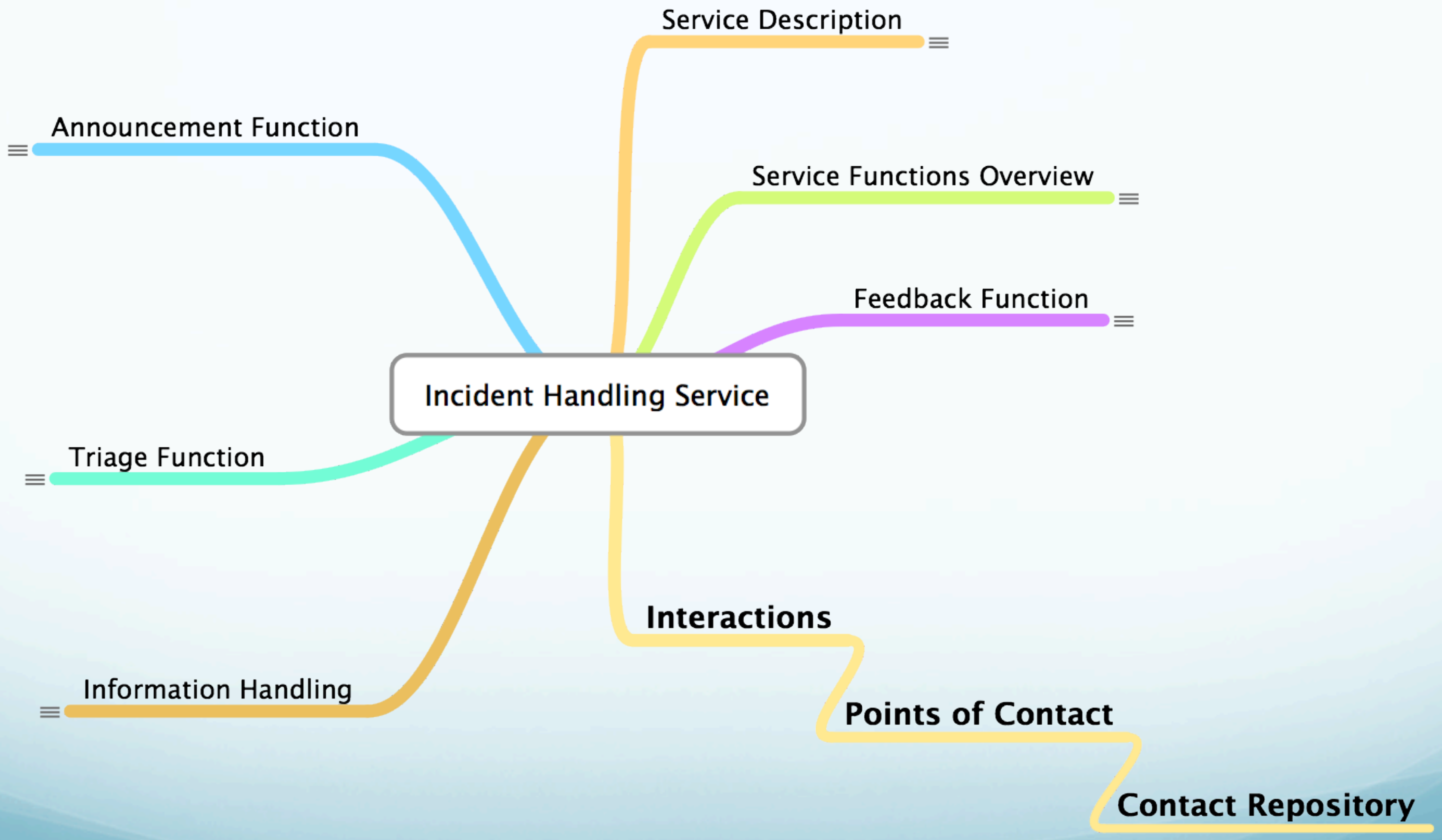
- ↻ Announcements
- ↻ Technology Watch
- ↻ Security Audit or Assessments
- ↻ Configuration & Maintenance of Security Tools, Applications, & Infrastructures
- ↻ Development of Security Tools
- ↻ Intrusion Detection Services
- ↻ Security-Related Information Dissemination

Security Quality Management Services

- ✓ Risk Analysis
- ✓ Business Continuity & Disaster Recovery Planning
- ✓ Security Consulting
- ✓ Awareness Building
- ✓ Education/Training
- ✓ Product Evaluation or Certification

West-Brown, Moira J. et al. (2003). Handbook for Computer Security Incident Response Teams (CSIRTs)

Contact Repository within CSIRT



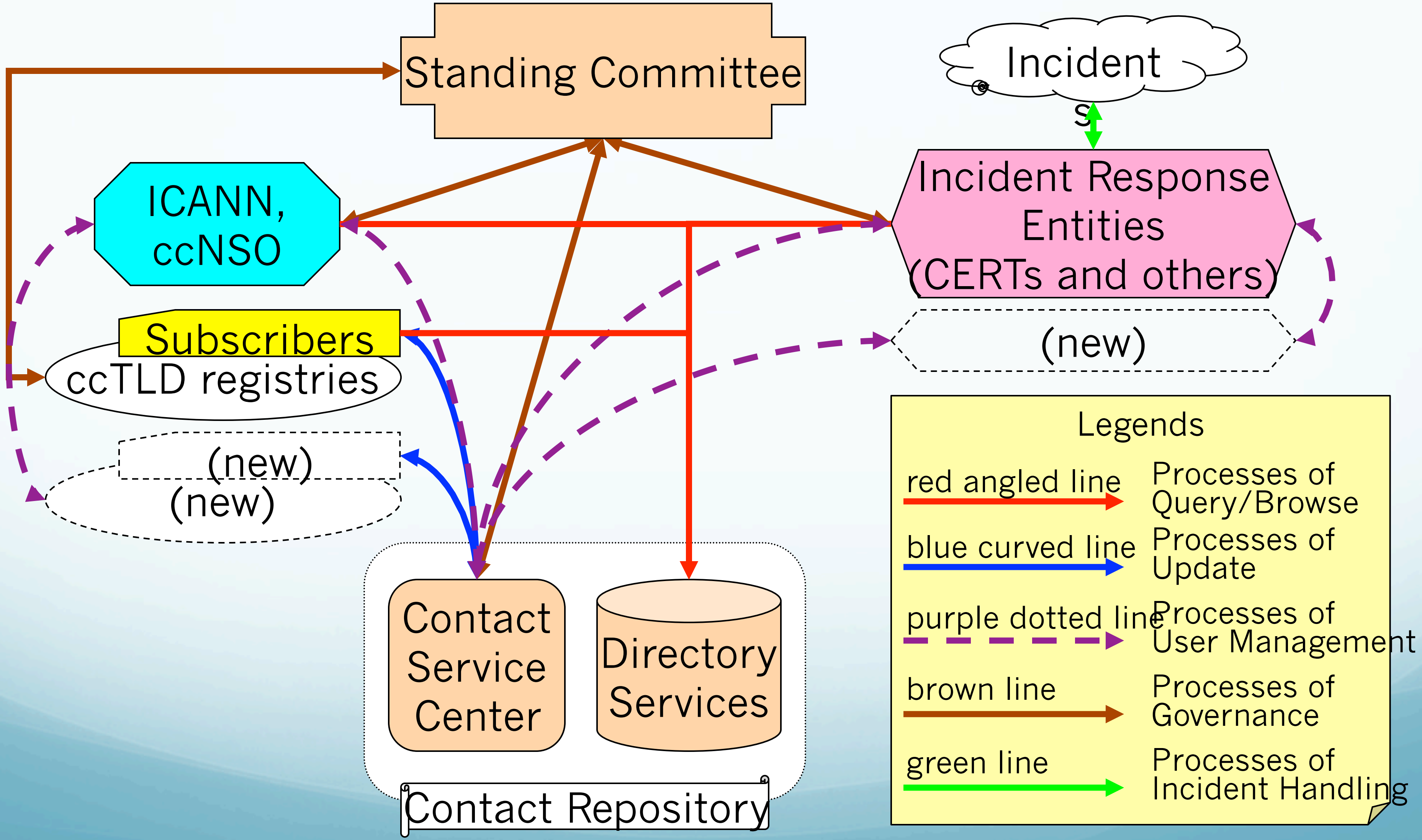
ccTLD Point of Contacts for Incident Response Services

- Contact Repository Implementation Working Group
- Explore factors to implement, maintain and operate the repository.
- Funding models
- Governance models

Repository Operation

- Database: Directory Service System
- Maintain and Operate: Contact Management Services

Relationship of Major Components



Standing Committee

Incident
s

ICANN,
ccNSO

Incident Response
Entities
(CERTs and others)

Subscribers

ccTLD registries

(new)

(new)

(new)

Contact
Service
Center

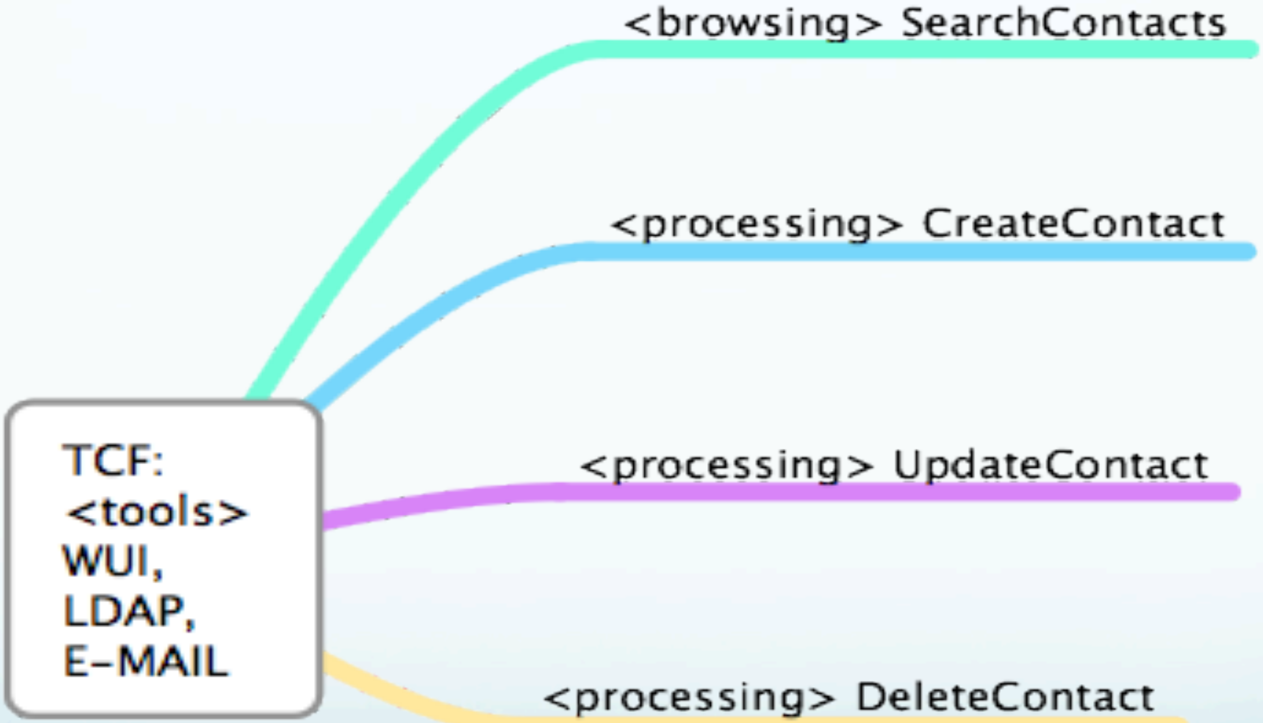
Directory
Services

Contact Repository

Legends

red angled line	Processes of Query/Browse
blue curved line	Processes of Update
purple dotted line	Processes of User Management
brown line	Processes of Governance
green line	Processes of Incident Handling

Directory Service System

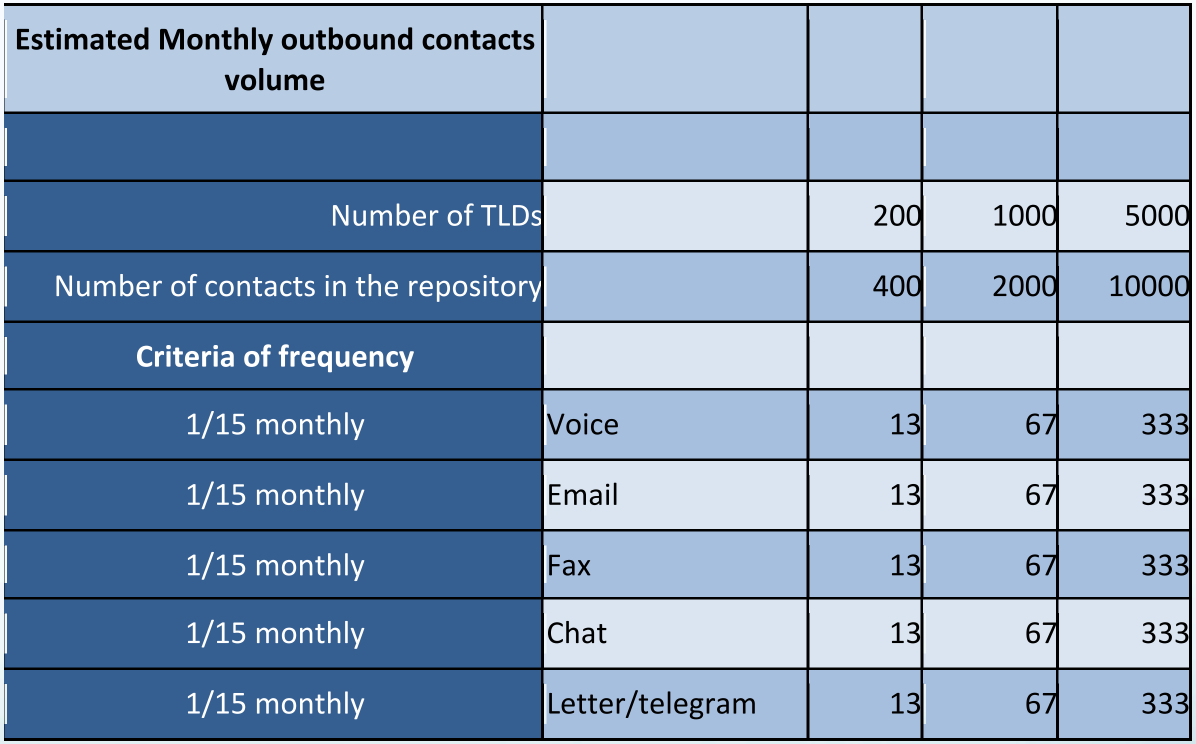

TCF:
<tools>
WUI,
LDAP,
E-MAIL
<browsing> SearchContacts
<processing> CreateContact
<processing> UpdateContact
<processing> DeleteContact

Maintain and Operate
Keep contacts updated

- 24/7/365 Operation
- E-mail response management
- Web Chat
- Session recording and transcript mailing
- Self-service Knowledge-base
- Analytics and Quality System
- Telephony infrastructure
- Interactive Voice Response (IVR) technology

Frequency and rotation of communication methods

- Complete update every 3 months.



Estimated Monthly outbound contacts volume				
Number of TLDs		200	1000	5000
Number of contacts in the repository		400	2000	10000
Criteria of frequency				
1/15 monthly	Voice	13	67	333
1/15 monthly	Email	13	67	333
1/15 monthly	Fax	13	67	333
1/15 monthly	Chat	13	67	333
1/15 monthly	Letter/telegram	13	67	333

Proposed Standing Committee to govern the repository

- ccNSO establishes Standing Committee
- Standing Committee reports to ccNSO Council and users.
- Standing Committee is supported by ccNSO Secretariat and with experts assistant from SSR department.
- Manage Service provider (Agreement compliance)
- Relation with subscribers.
- Maintain use cases of the repository.

Proposed Funding Models

- Uniform subscription and set-up fee.
- Cross-ccTLD funding
- ICANN funding (using part of the financial contribution).
- Mixed funding (additional support by more affluent ccTLDs combined with ICANN funding)

Next steps

- Send the Request of Information (ROI) to potential providers
  - To adjust specifications and ideas of possible costs.
- With the feedback of ROI, convert the document in a Request for Proposal for the ccNSO Council.
- Sent the Request For Proposal (RFP), approved by the ccNSO Council to potential bidders.
- Analyze and recommend the best offer to the ccNSO Council.

Questions?