

# Architectural Checklist



## Real Time Communications (RTC) Next Generation Communications for Internet2 Campuses

The Real Time Communications Architectural Checklist is a tool that can help campuses assess how closely their systems and services comply with the recommendations of Internet2's Real Time Communications Reference Architecture.

### Who Should Use This Tool ?

#### **Campus CIOs**

Campus CIOs are responsible for developing comprehensive and strategic plans for campus IT infrastructure, including RTC services. Campus CIOs who want to measure their organization's readiness to support real time communications can administer this instrument internally for a view of RTC strengths and weaknesses in their institutions.

#### **IT Managers**

IT Managers are responsible for deploying, operating, and maintaining production services for their campuses. IT Managers may use this checklist to assess the ability of vendor products to comply with standards and practices being implemented at other Internet2 campuses and to ensure interoperability. The checklist can be copied into RFPs for equipment, systems and services.

#### **Vendors**

Vendors should be building support for RTC into their products. As part of their efforts to promote their standards-based products to the research and education community and demonstrate their strategic and technical leadership, vendors can share this completed instrument with potential clients at Internet2 universities.

#### **RTC Technical Professionals**

Campus technical professionals who are already engaged in RTC activities and want to share information about system performance can complete this instrument for a particular product that they have used to share their experiences within an Internet2 Working Group or more broadly across Internet2's membership.

#### **Internet2 Staff**

Internet2 executives, managers and technical staff can use this tool to assess how on-going and proposed Working Group activities align with the over-arching strategic direction for RTC.

# Architectural Checklist



## Real Time Communications (RTC) Next Generation Communications for Internet2 Campuses

<b>System or Product Under Evaluation (include version)</b>	
<b>Date of Evaluation</b>	
<b>Name of Individual Responsible for this Evaluation</b>	
<b>Role of Individual Responsible for this Evaluation</b>	
<b>Contact Information</b>	
<b>Organization</b>	
<b>Address</b>	
<b>Telephone</b>	
<b>Email</b>	
<b>Comments</b>	

### 1. Call Signaling

- a. Describe how SIP is supported.
- b. Describe how H.323 is supported.
- c. Describe how XMPP is supported.
- d. Describe efforts underway to develop next-generation call signaling protocols.

### 2. Middleware

- a. Describe interfaces for connecting to directories.
- b. Describe interfaces for connecting network management tools.
- c. Describe the use of DNS for address resolution and failover.

- d. Describe interfaces for interfacing with external authentication and authorization services.
- e. Describe interfaces for connecting to external accounting services.
- f. Describe interfaces to allow external location services and QoS events to be triggered in real time based upon call state.
- g. Describe the skill sets necessary to administer the systems.

### **3. Addressing**

- a. Describe alphanumeric SIP URI support.
- b. Describe alphanumeric H.323 URL support.
- c. Describe alphanumeric XMPP URI support.
- d. Describe ENUM support.
- e. Can the system operate with both E164 and alphanumeric addresses?

### **4. Authentication and Authorization**

- a. Does the system support SIP digest authentication?
- b. Does the system support H.235? Which Annexes?
- c. Does the system support TLS?
- d. Does the system support end to end authentication?
- e. Describe efforts underway to support end to end authentication and authorization across network domains?

### **5. Directory Services and Identity Management**

- a. Describe how H.350 is supported.
- b. Describe how users can be managed by a central, external directory rather than a built-in database of users.

### **6. Security: Encryption and Privacy**

- a. Describe support for encryption of media streams.
- b. Describe support for encryption of call signaling streams.
- c. Describe key management schemes.
- d. Does the system support wiretapping? How?

### **7. Security: DoS and SPAM Prevention**

- a. Describe white list / black list and other filtering capabilities.
- b. Describe how systems are managed and patched in emergency situations, i.e. when under attack that is exploiting vulnerabilities.
- c. Describe how you prevent source domain spoofing (e.g. does your product support RFC4474?).

### **8. Disaster Recover and Business Continuity**

- a. Describe system redundancy capabilities.
- b. Describe how public safety and emergency responders interact with the system.
- c. Describe alternative paths if primary directions fail.

### **9. Multipoint conferencing**

- a. Describe capabilities for large scale, central conferencing.

- b. Describe capabilities for small scale conferencing hosted on user endpoint equipment.

#### **10. Data Collaboration Tools**

- a. Describe how data collaboration tools integrate with voice, video and IM protocols and applications.
- b. Describe how user provisioning is integrated with other RTC applications.
- c. Describe how archived data can be served through other applications and migrated to third party tools.

#### **11. Presence**

- a. Indicate what standards and protocols are supported for publishing user presence online.
- b. Describe how external state information can be incorporated into the presence system, for example from a campus directory or location services system.
- c. Does the system support both server-based presence and peer-to-peer presence? If server based, describe any external server requirements for the handling of presence data.

#### **12. Location Services and Mobility**

- a. Describe how physical location of users and devices is tracked in real time.
- b. Describe support for IETF GEOPRIV standards.
- c. Describe support for NENA 911 standards.

#### **13. Firewall / NAT Traversal**

- a. Describe support for H.460.18/19
- b. Describe supported firewall / NAT traversal solutions.

#### **14. Media**

- a. List all media types (audio, video, text, etc.) and codecs supported and any limitations on their interoperability with third party systems.

#### **15. Finding People and Services**

- a. Describe support for users outside of the core community of authenticated users.
- b. Describe how non-human entities such as conference rooms and virtual organizations are supported.

#### **16. Communications Plan (for campuses)**

- a. Describe how end users learn about RTC applications on campus that conform to the Internet2 Reference Architecture.
- b. Describe how user needs are translated into participation in various Internet2 RTC application areas.