ATOCA: The Plan
A voice from the past ...
Questions to the WG

Proposed milestones:
1. Architecture
2. Secure Alert Format
3. Distribution Protocol
4. Broadcast Protocol

- Is this generally the right direction?
- Do we need to work on a distribution protocol?
Questions to the WG

Proposed milestones:
1. Architecture
2. Secure Alert Format
3. Distribution Protocol
4. Broadcast Protocol

• Is this generally the right direction?
• Do we need to work on a distribution protocol?
The Documents

- draft-ietf-atoca-requirements
- draft-barnes-atoca-cap-mime
- draft-barnes-atoca-escape
- draft-barnes-atoca-meta
- draft-barnes-atoca-delivery

- How do these fit together into an overall solution for delivering alerts?
The Picture

- On each of these hops...
- How does the sender know where to send the alert?
- How does the sender send the alert?
- How does the recipient know whose alerts to accept?
Alert Targeting

• Two questions:
  – Who should receive the alert?
  – How should they receive it?

• Allow recipients to register information about themselves
  – Location, language, capabilities
  – Contact URIs

• Allow senders to advertise publication points
Alert Delivery

• Standard protocols apply: SMTP, XMPP, ...

• Also a desire for a simpler mechanism
  – Controllable ACKs, compatible with broadcast

• Define a simple, UDP-based fragmentation layer for delivering alerts
  – Sender divides full alert into small fragments
  – Retransmit to achieve some degree of reliability
Alert Delivery

• When a receiver gets an alert, how does it verify that it’s OK?
• Provision recipients with prior information about which alerts are good
  – Hash over a nonce (without publishing the nonce)
  – Alert sender information contact info, public keys
• Provide corresponding verifiers in alert
  – Hash pre-image (the nonce)
  – Signature over alert body
Historical Milestones

Jan 2011 - Submit 'Terminology and Framework' to the IESG for publication as Informational

Apr 2011 - Submit 'Addressing security, performance and congestion issues for alert distribution' to the IESG for publication as Informational

Apr 2011 - Submit conveying point-to-point Authority to Citizen Alerts to the IESG for publication as Proposed Standard

May 2011 - Submit 'Discovering alerting servers' to the IESG for publication as Proposed Standard

Jun 2011 - Submit conveying point-to-multipoint Authority to Citizen Alerts to the IESG for publication as Proposed Standard

Aug 2011 - Submit 'Considerations for interworking with currently deployed alert distribution systems' to the IESG for publication as Informational
For Discussion

**Apr 2012** - Submit 'Terminology and Framework' to the IESG for publication as Informational

**Apr 2011** - Submit 'Addressing security, performance and congestion issues for alert distribution' to the IESG for publication as Informational

**Nov 2012** - Submit 'Secure alert format for alert distribution' to the IESG for publication as Proposed Standard

**Dec 2012** - Submit 'Discovering alerting servers' to the IESG for publication as Proposed Standard

**Dec 2012** - Submit 'Lightweight conveyance of Authority to Citizen Alerts' to the IESG for publication as Proposed Standard

*Collapsed from “point-to-point” and “point-to-multipoint”*

**Jul 2013** - Submit 'Considerations for interworking with currently deployed alert distribution systems' to the IESG for publication as Informational
Omitted from the previous list

- Discuss the inclusion of items for:
  - A MIME media type for CAP
    - Why? Pre-requisite for other items
  - A SIP event package
    - Why? Enable registration for out-of-area alerts