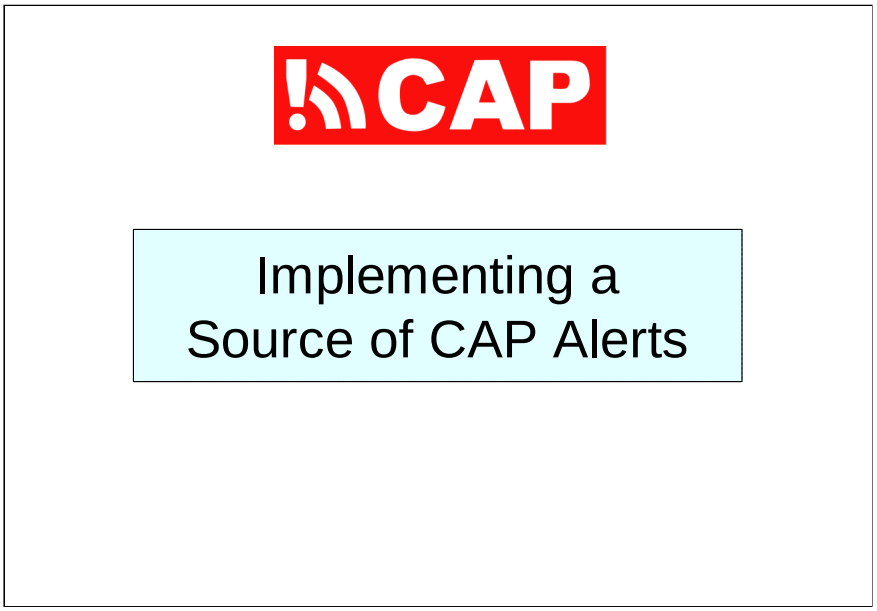
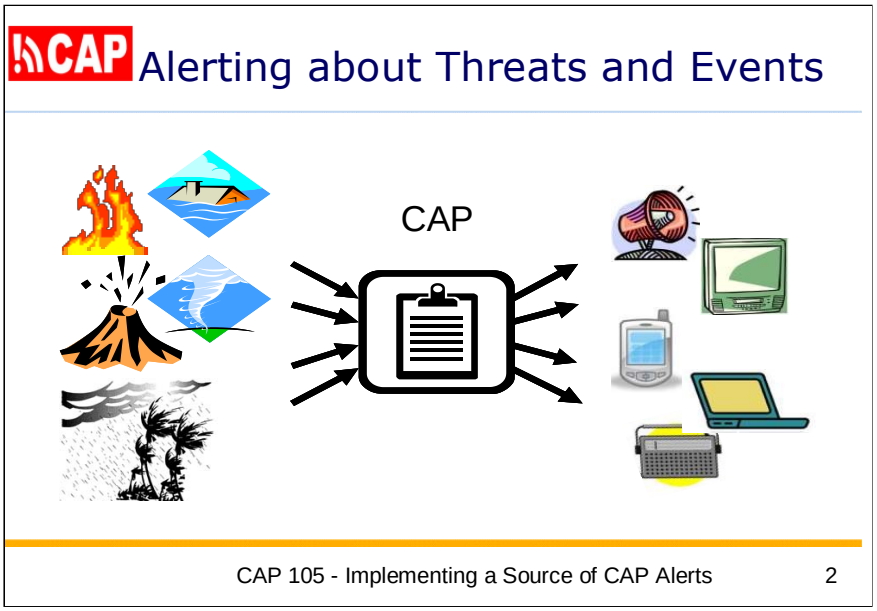
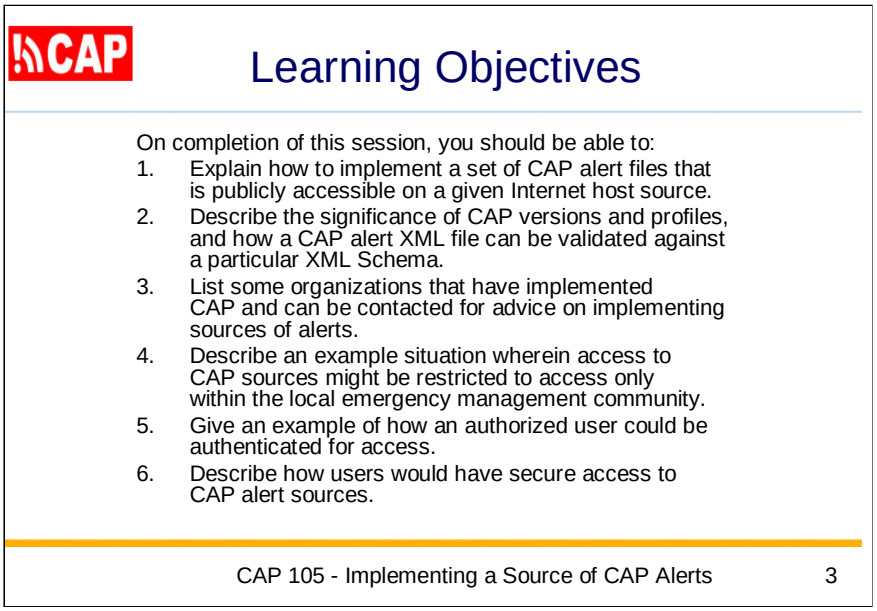


The title of this presentation is “Implementing a Source of CAP Alerts”.

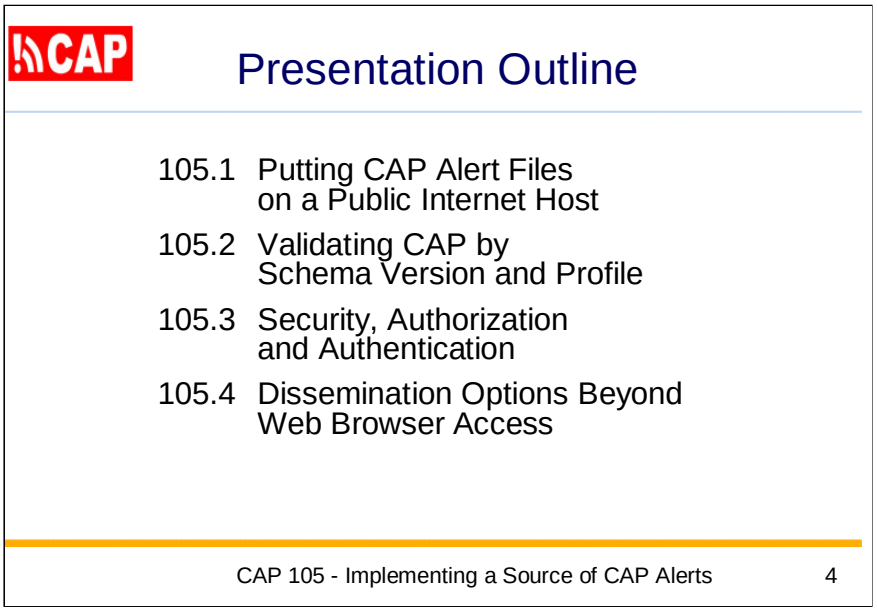


Remember this diagram—it shows CAP as a standard form for certain information on just about any kind of hazard threat or event.

The key requirement of CAP-enabled alerting is that alerting authorities disseminate alerting information in CAP format.



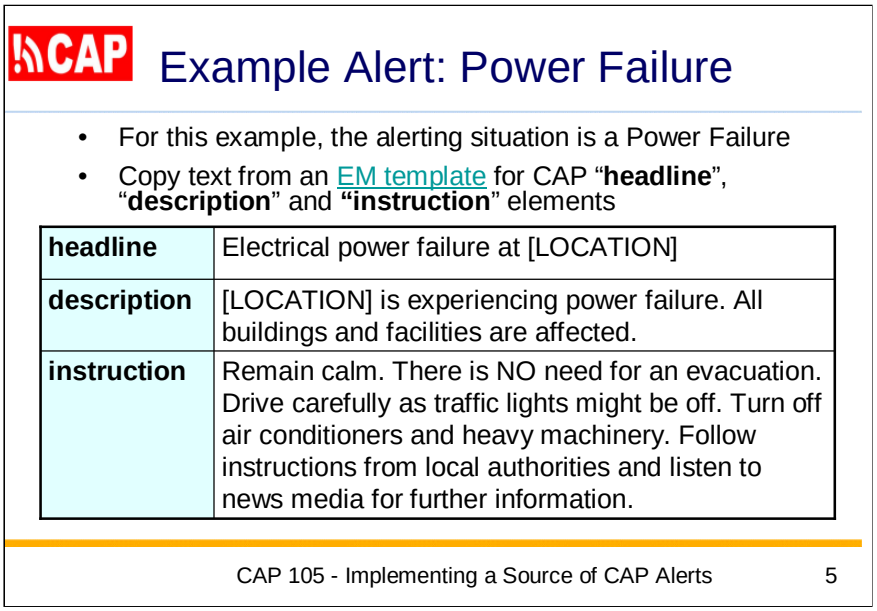
Here are the Learning Objectives for this session.



Here is an outline of this presentation.

The first topic is titled: Putting CAP Alert Files on a Public Internet Host

We'll start by making a CAP alert by simply editing a text file.



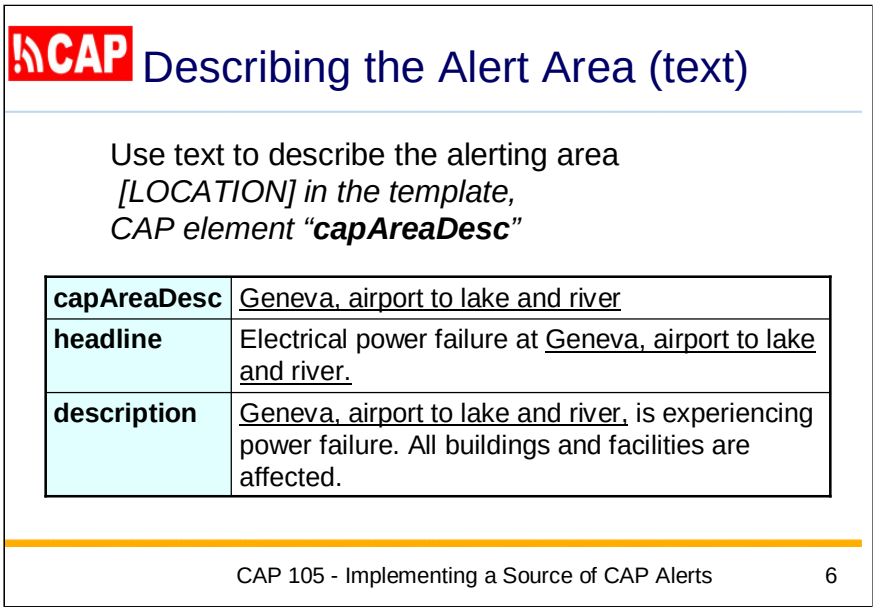
For this example, we'll assume the alerting situation is a power failure.

We have a collection of templates giving text to be used in three of the CAP alert elements.

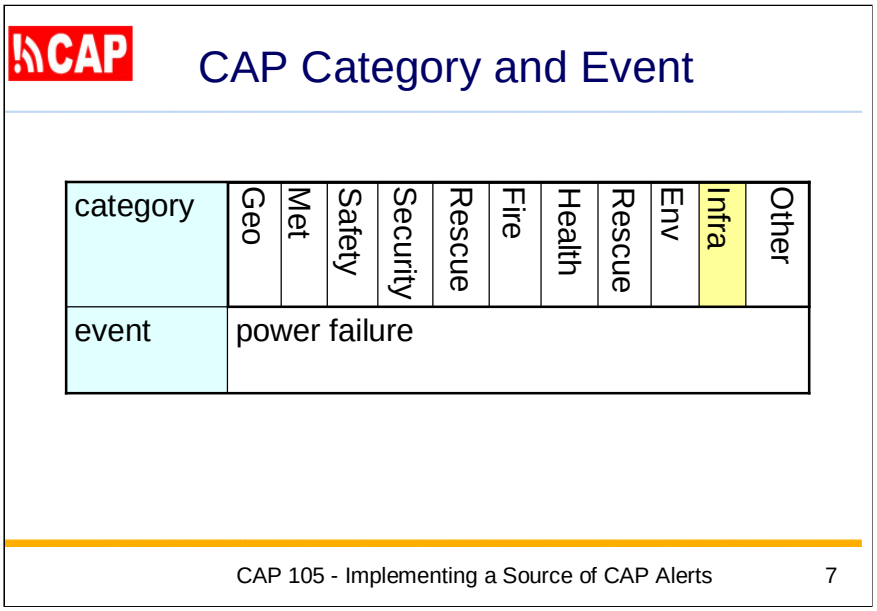
Here, we need to insert the Location applicable to the alert.

headline: Electrical power failure at [LOCATION]

description: [LOCATION] is experiencing power failure. All buildings and facilities are affected.



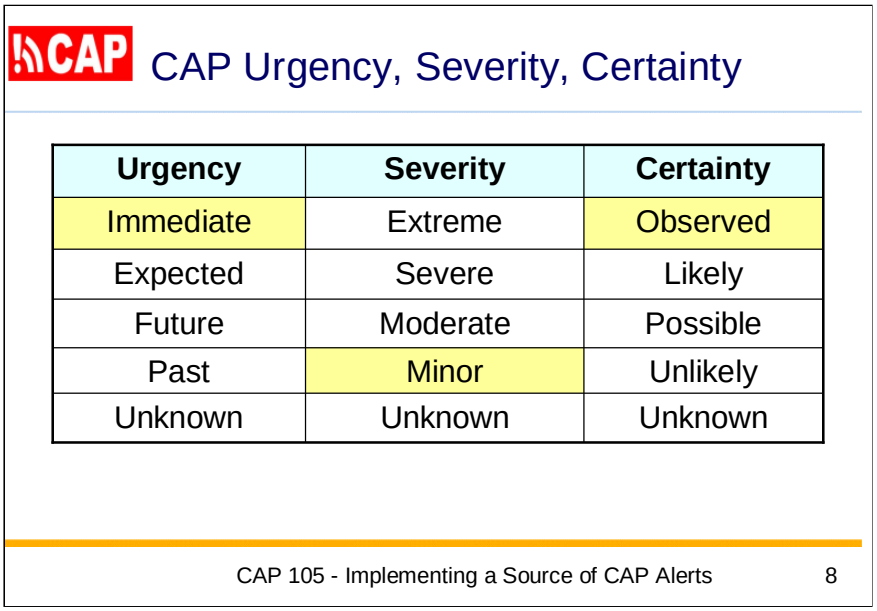
In my example, the power failure has affected a part of Geneva. Here is descriptive text for that area: "Geneva, airport to the lake and river".



There are 11 values we can select for the CAP “category” element, and we can select multiple values if desired.

Here I have highlighted in yellow the “Infra” (infrastructure) category, which is appropriate for a power failure event.

In the CAP “event” element, we will just enter the words “power failure”.



Now we also need to select values for each these three elements:
- urgency (time available to prepare)
- severity (intensity of impact)
- certainty (confidence in the observation or prediction)

From the CAP Data Dictionary, the values for urgency are:

"Immediate" - Responsive action should be taken immediately
"Expected" - Responsive action should be taken within the next hour
"Future" - Responsive action should be taken in the near future
"Past" - Responsive action is no longer required

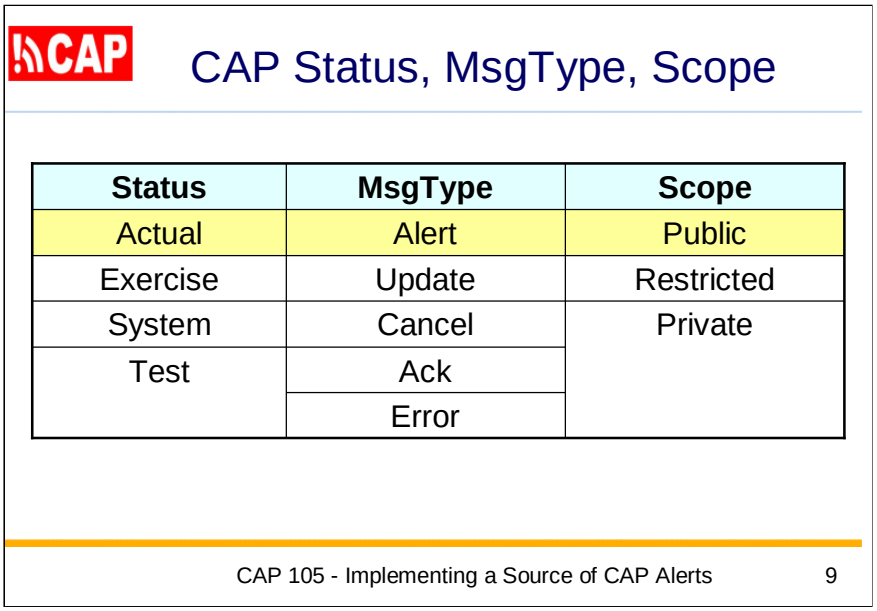
The values for severity are:

"Extreme" - Extraordinary threat to life or property
"Severe" - Significant threat to life or property
"Moderate" - Possible threat to life or property
"Minor" – Minimal to no known threat to life or property

The values for certainty are:

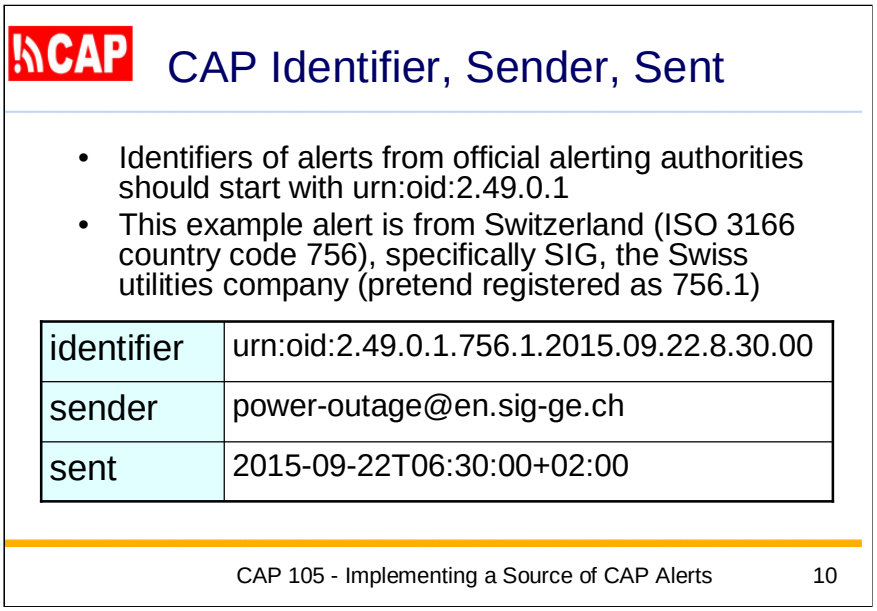
"Observed" – Determined to have occurred or to be ongoing
"Likely" - Likely (p > ~50%)
"Possible" - Possible but not likely (p <= ~50%)
"Unlikely" - Not expected to occur (p ~ 0)

In my example, the power failure has already begun, so we select "immediate" for urgency. The power failure is expected to be minimally disruptive, so we select "minor" for severity. And, for certainty we select "observed" because this is not a prediction but a report of an observed situation.



These next three elements will usually be set the same way.

- for status we select “actual” because we assume our example message is not an exercise, part of the system reporting, or a test.
- for msgType we select “alert” because this alert is not modifying any previous alert
- for scope we select “public” as distinct from restricted to a particular audience or private to a particular individual.



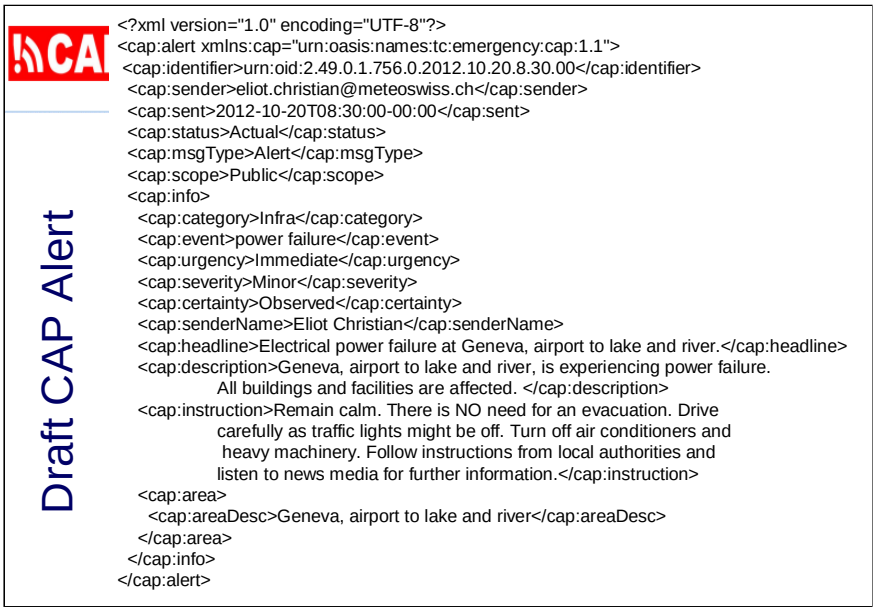
Identifiers of alerts from official alerting authorities should start with "urn:oid:2.49.0.1", followed by the specific identifier of the registered alerting authority.

This example alert is from Switzerland, country code "756", and it is issued by SIG (the Swiss utilities company), which we pretend is registered as "756.1".

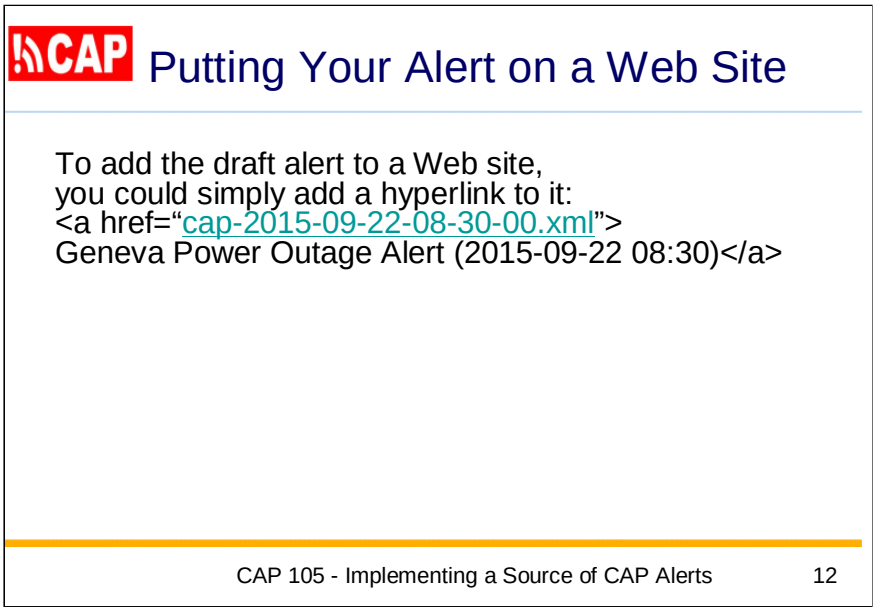
Appended to the unique identifier, here we have the date and time the alert is issued: September 22, 2015, at 8:30 am local time.

For the **sender** element, we use an e-mail address.

For the **sent** element, we provide the date and time issued, here in UTC (2 hours earlier than Geneva).

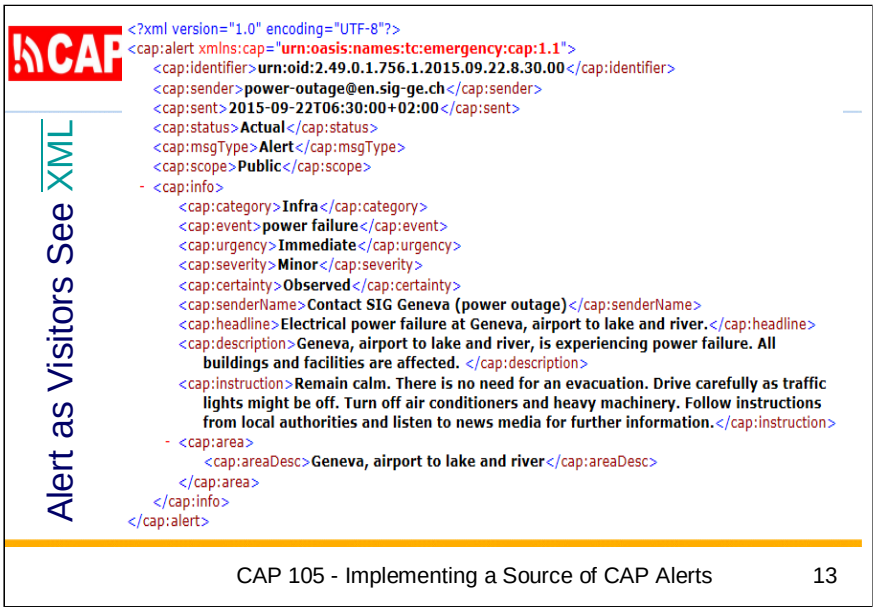


Putting together these values we selected, here is the CAP alert in its XML format. This can be just entered with any text editor and then saved with a file extension of ".xml".



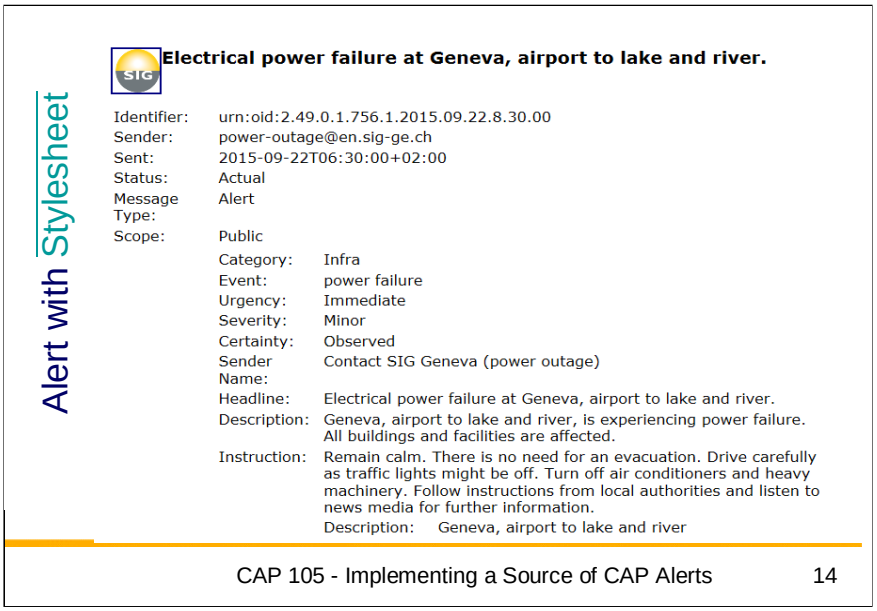
To add this draft alert to a Web site, you could just add a hyperlink to that file.

Here I'll click on the link to show what your users would see.



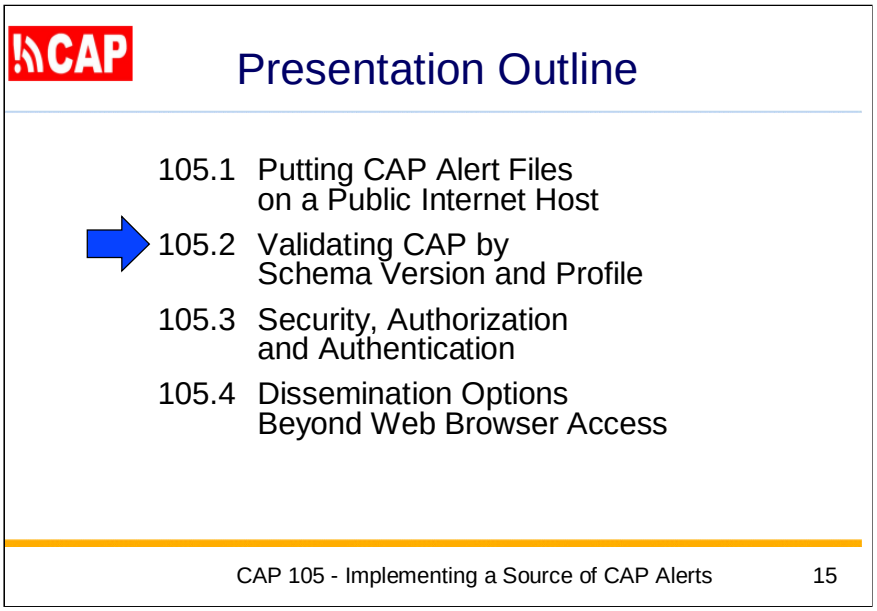
Here is the CAP alert as visitors would see it.

Although this does have all of the information and is important from a processing perspective, you do not want visitors to see raw XML.



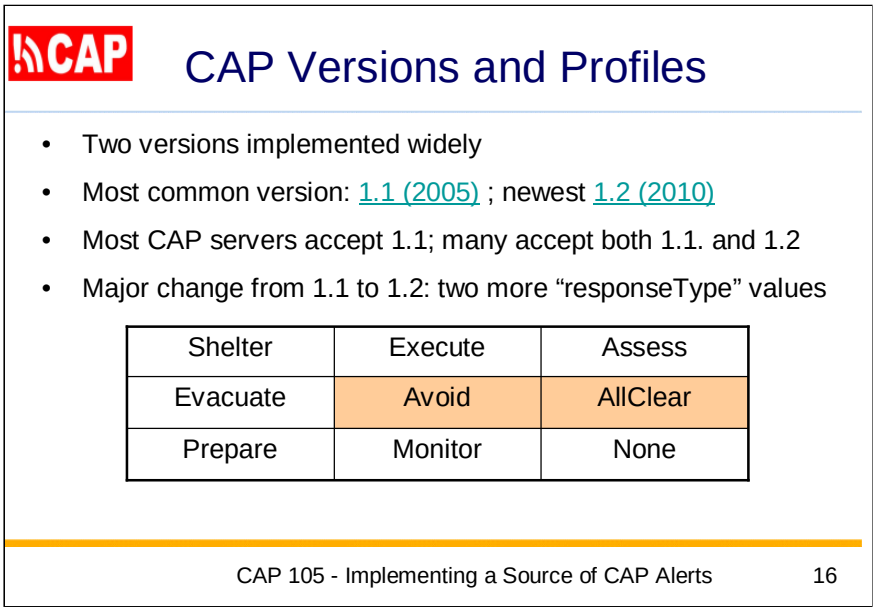
To make a CAP alert easier to read by a human visitor, we can add a line to the CAP alert to reference an XML Stylesheet.

You may find it's not too hard to use an example stylesheet and customize it for your own site.

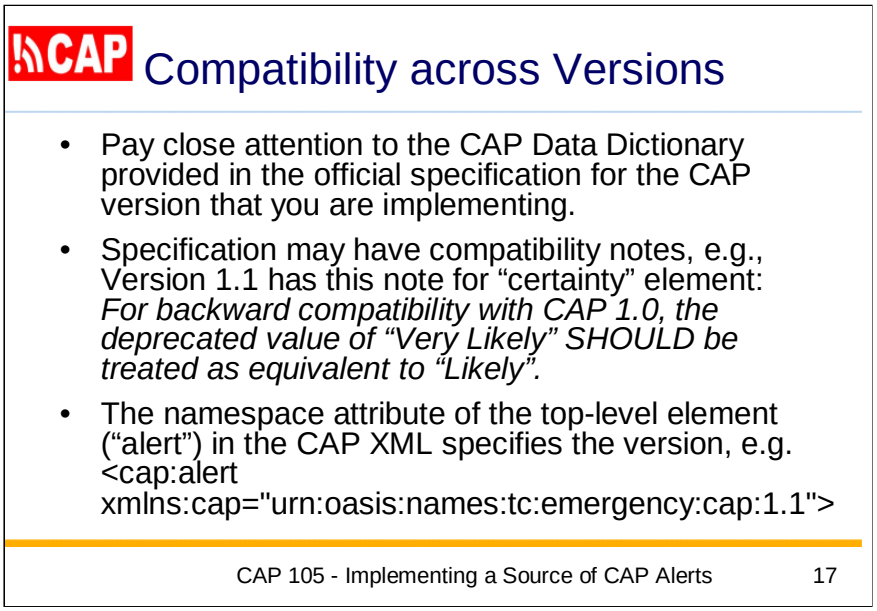


The next topic is:

Validating CAP by Schema Version and Profile

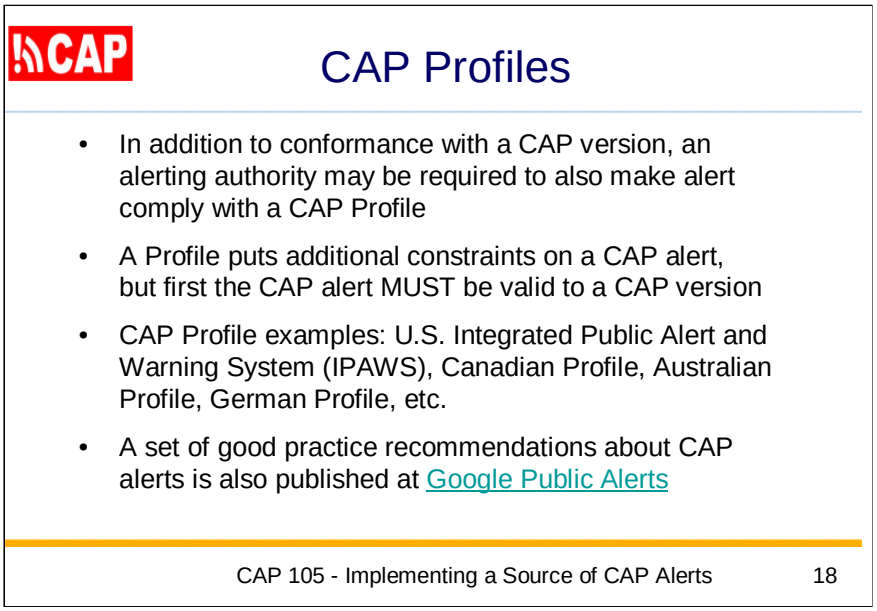


Most CAP servers accept version 1.1; many accept both 1.1. and 1.2. The major change from version 1.1 to 1.2 was the addition of two more “responseType” values: “avoid” and “allClear”.



Pay close attention to the CAP Data Dictionary provided in the official specification for the CAP version that you are implementing.

The version of CAP being used is given in the namespace attribute of the top-level element (“alert”) in the CAP XML.

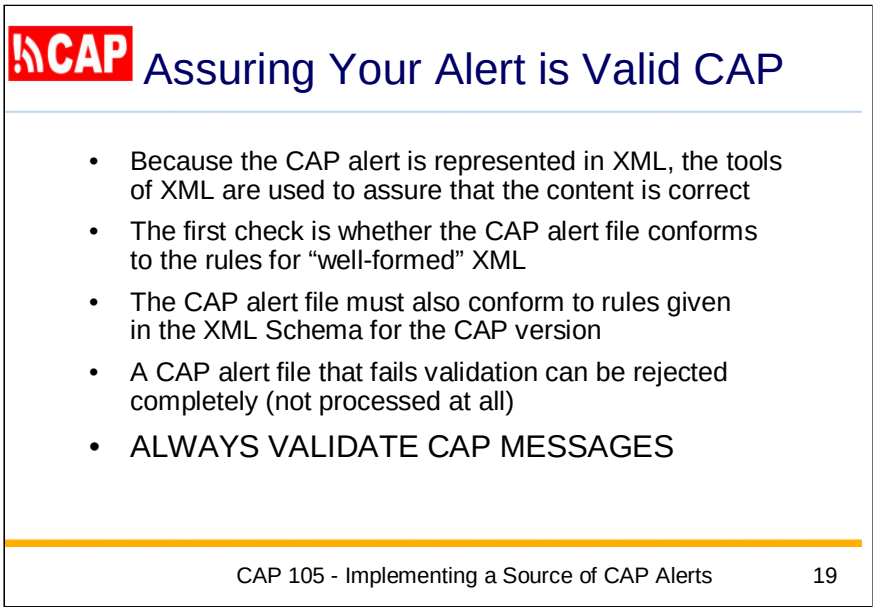


In addition to complying with a CAP version, an alerting authority may be required to also make its alert comply with a CAP Profile.

In the case of Canada, for instance, the CAP Profile addresses the requirement for alerts to be in French as well as English.

A Profile puts additional constraints on a CAP alert, but first the CAP alert MUST be valid to a CAP version.

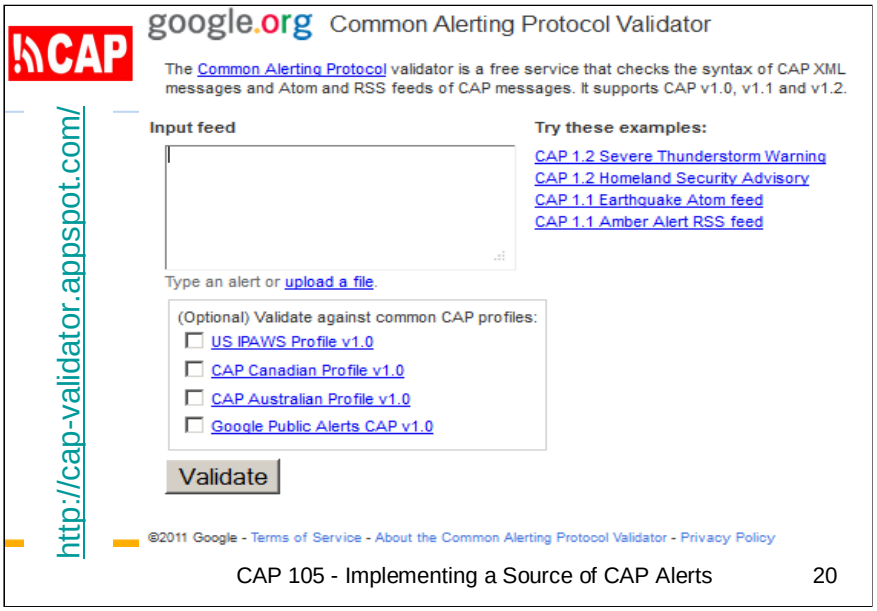
A set of good practice recommendations about CAP alerts is also published at Google Public Alerts.



Because the CAP alert is represented in XML, the tools of XML are used to assure that the content is correct.

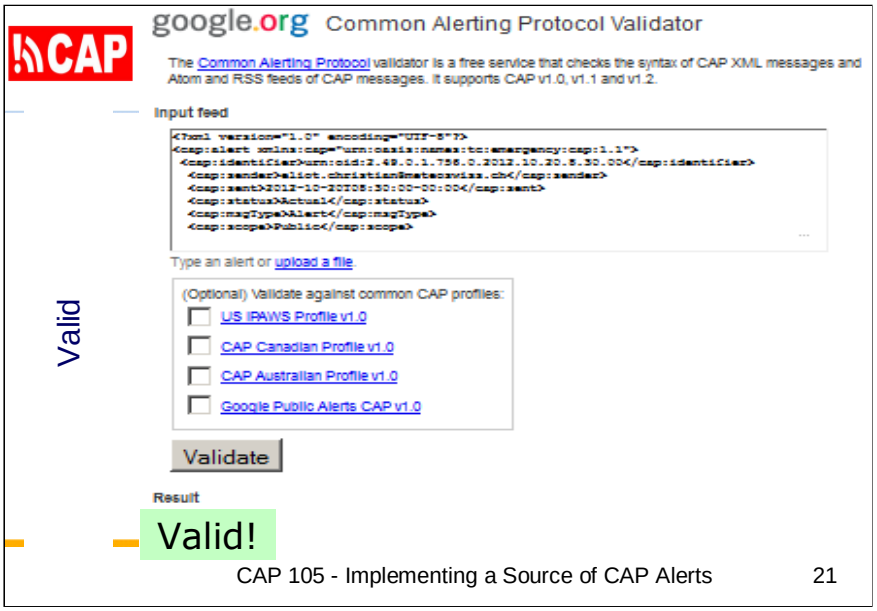
The CAP alert file must also conform to rules given in the XML Schema for the CAP version.

A CAP alert file that fails validation results in an alert NOT sent to many people who should have been alerted, so it is **very important** to always validate CAP messages!

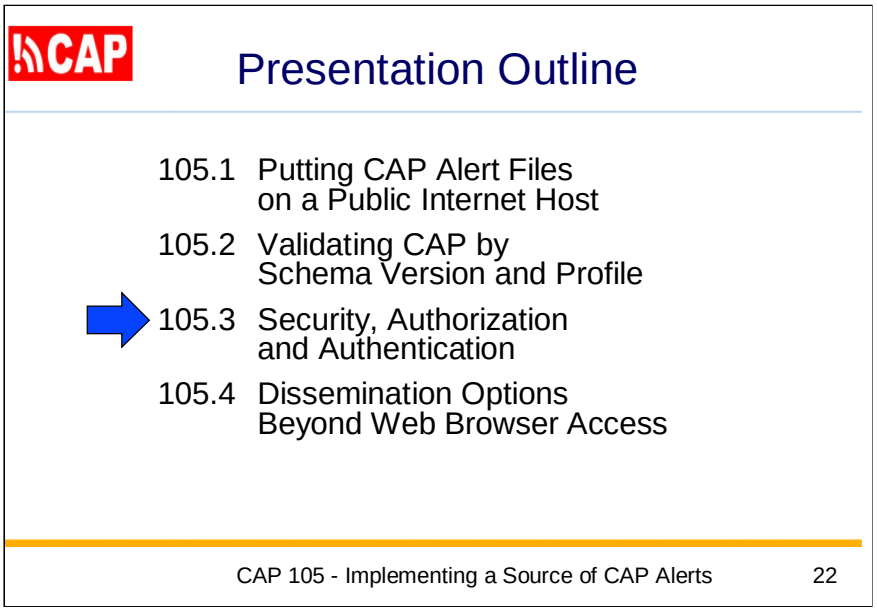


Here is an online validator from Google that supports CAP versions 1.0, 1.1, and 1.2.

The Google CAP validator prompts for you to either paste the CAP XML directly into the text box or to use the upload link. So, let's go ahead and run this using the CAP alert we just created.

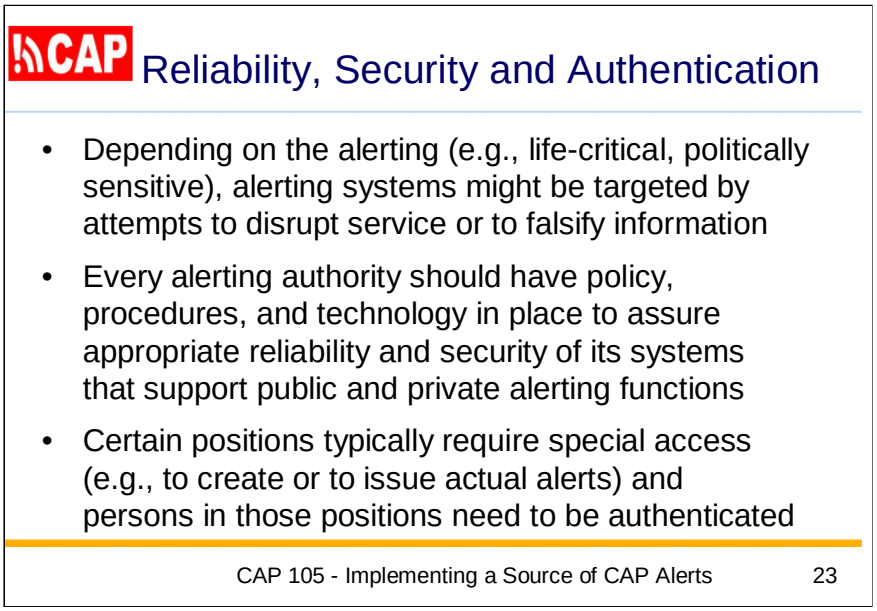


This CAP alert is well-formed XML and valid as CAP version 1.1.



The next topic is:
Security, Authorization and Authentication

Now we are shifting our focus: from a specific alert to more general features of the whole alerting system.

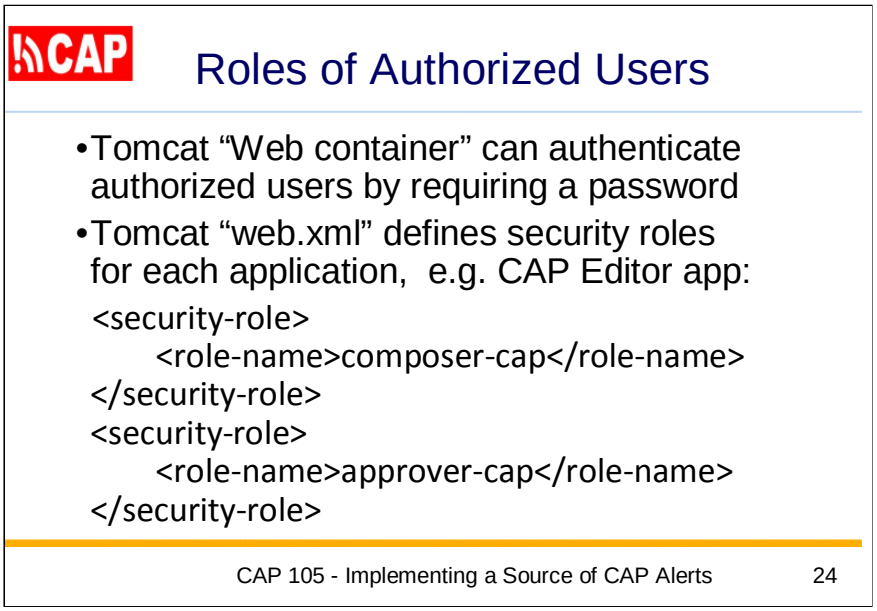


Not all alerting systems are life-critical or politically sensitive, but there certainly are cases where alerting systems might be targeted by attempts to disrupt service or to falsify information. And, all Internet hosts are targeted by malware that probes randomly.

A separate issue concerns alerting systems being overwhelmed even without harmful intent. This can occur when a threat or event generate broad interest and the alerting host receives a flood of traffic--the same effect as a distributed-denial-of-service attack.

Every alerting authority should have policy, procedures, and technology in place to assure appropriate reliability and security of all systems that support its alerting functions.

We will look at the usual situation where certain positions require special access, such as the authority to create or to issue actual alerts. Persons who are in those positions need to be authenticated before they are given access to restricted functions.



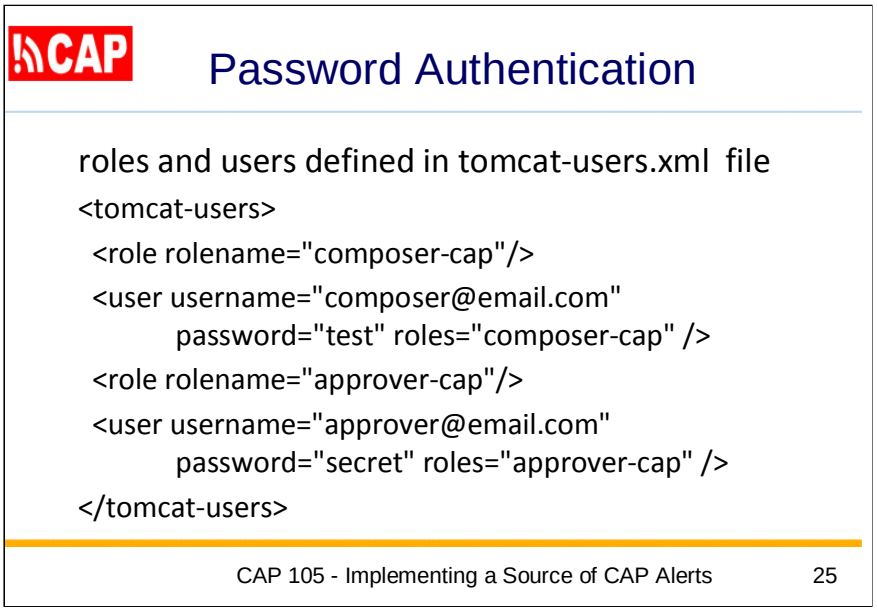
There are many mechanisms to implement security and it is likely that your Internet hosting service has particular procedures that must be followed.

A commonly used security mechanism is "container-managed security" and the most common Web container is Apache Tomcat.

Tomcat has configuration parameters for each application in a "web.xml" file. This file also defines security roles.

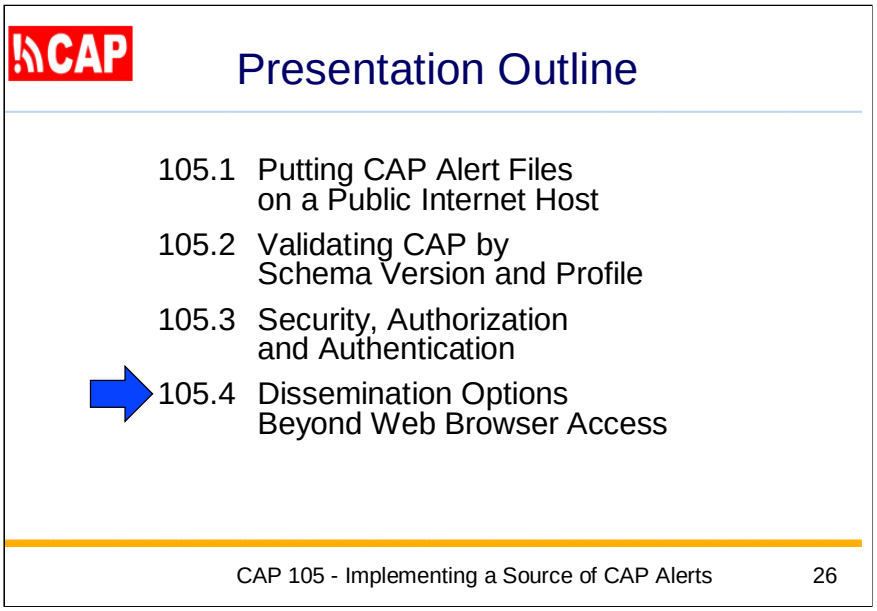
Here the user must be authenticated as a member in the authorized role. That authentication could require a fingerprint scan, a card key, or other credentials.

In my example, we're assuming that Tomcat is set to perform a password challenge.



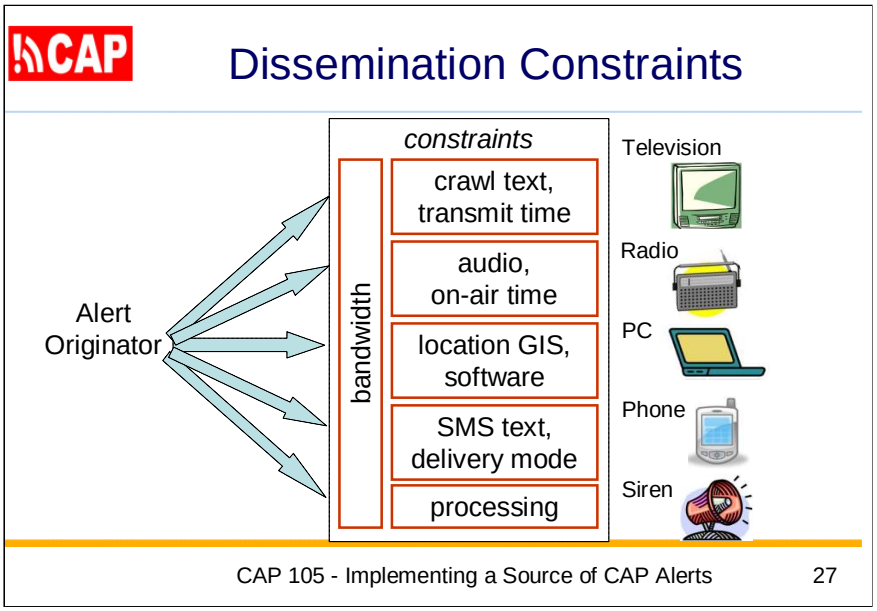
Because the password mechanism is built into the Tomcat Web container, the system administrator of the Internet hosting service manages the actual list of authorized users in a file known as “tomcat-users.xml”.

Using this mechanism, whenever someone tries to access the application associated with the web.xml file, the host system will produce a dialog box with the password challenge .



Of course, putting a CAP alert on a Web page is only one among many ways that people can be alerted.

In the next part of this training session, we'll take a quick look at some of these dissemination mechanisms.



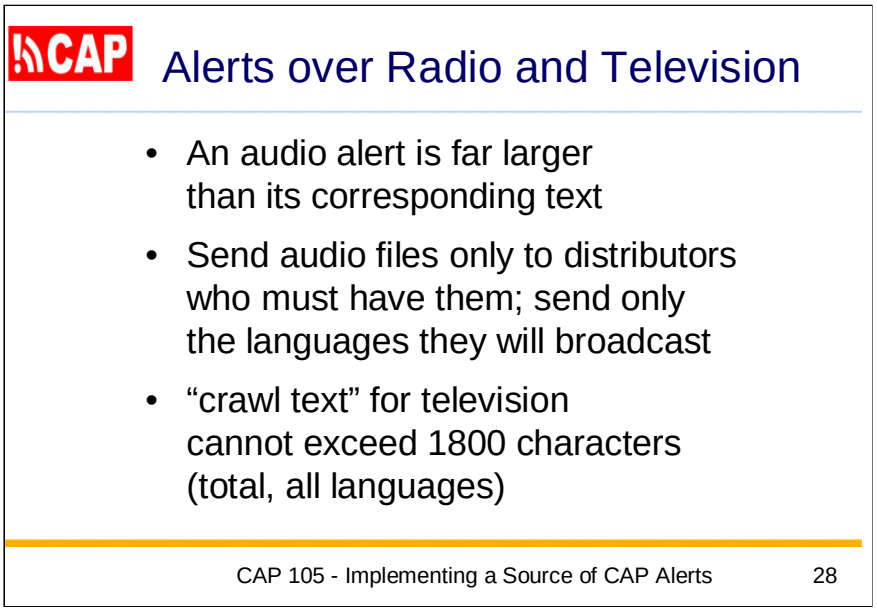
A local “last mile distributor” receiving alert information in CAP format needs to convert it for presentation to the public:

Here we want to keep in mind a distinction between "interactive media“ and "non-interactive media“.

With interactive media, message recipients are able to access referenced information sources external to the message. With non-interactive media, recipients have very limited or no ability to access referenced information sources that are external to the message.

Traditional radio, television, and Fax transmissions are typical of non-interactive media,

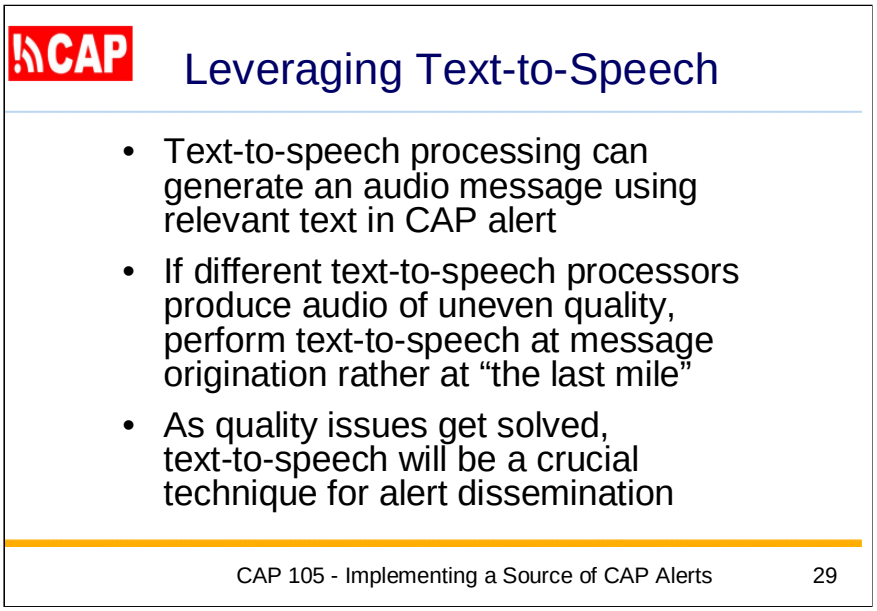
E-mail and Internet communications are typical of interactive media.



If the alert message must be audio, size is important because audio is vastly larger than the corresponding text. For instance, the U.S. Emergency Alert System requires that an audio alert message cannot be longer than two minutes. This long-standing constraint is built into the existing hardware.

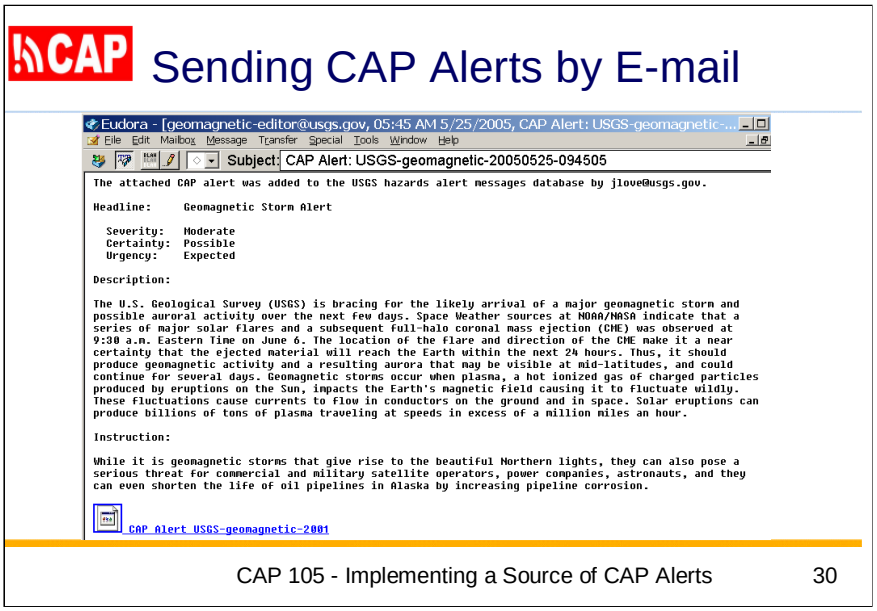
Given that the audio alert message must be of a quality to assure intelligibility, such audio files can be megabytes in size, even with compression. Accordingly, audio files ought to be transmitted only to those distributors who must have them. When alerts are in multiple languages, audio files should be packaged so that distributors get only those audio files they actually need to broadcast.

In the case of television, it is common to display an emergency alert as “crawl text” that scrolls across the television screen as an overlay to the program being broadcast. Receiving devices constrain the crawl text for public alert messages to not exceed 1800 characters.



Alerting equipment and software should be able to generate a quality audio message by picking out relevant text in the CAP alert.

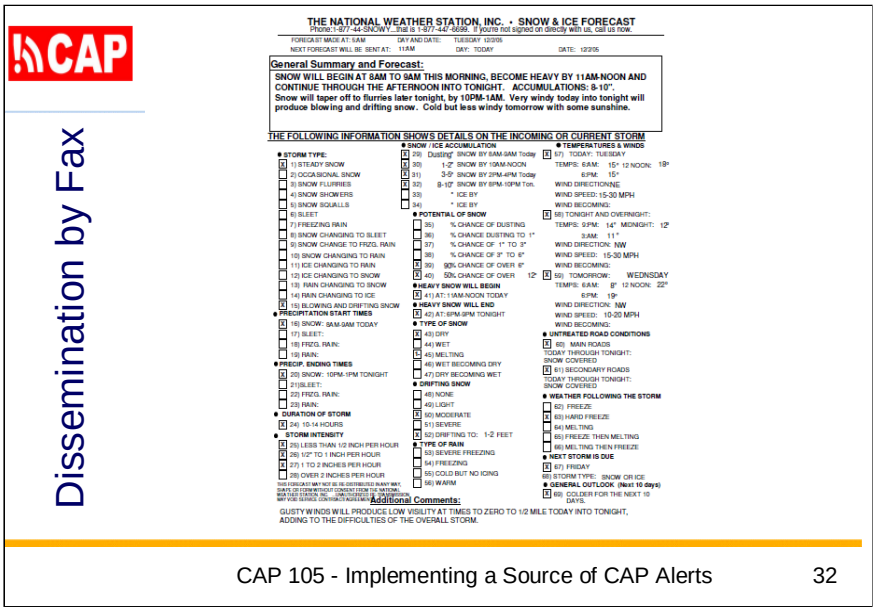
However, different text-to-speech processors produce audio of uneven quality. Once the text-to-speech quality issues are solved, text-to-speech will become an even more crucial technique to minimize the sizes of alert messages and reach everyone at risk.



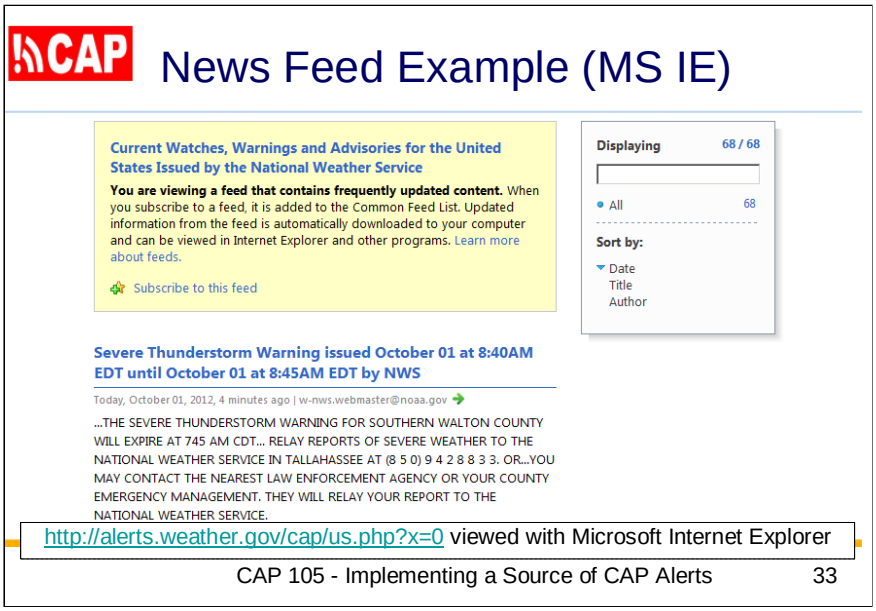
Here we see a CAP alert being provided as an attachment to an email message.

“Smart phones” can receive full CAP alerts. For other cellular telephones, the Short Message Service (SMS) provides a way to receive text alerts that originated as CAP. The CAP “headline” element is specifically designed to be sent over SMS.

Here we see an alert for a tornado warning, giving the place and time frame, plus a Web reference for additional information.



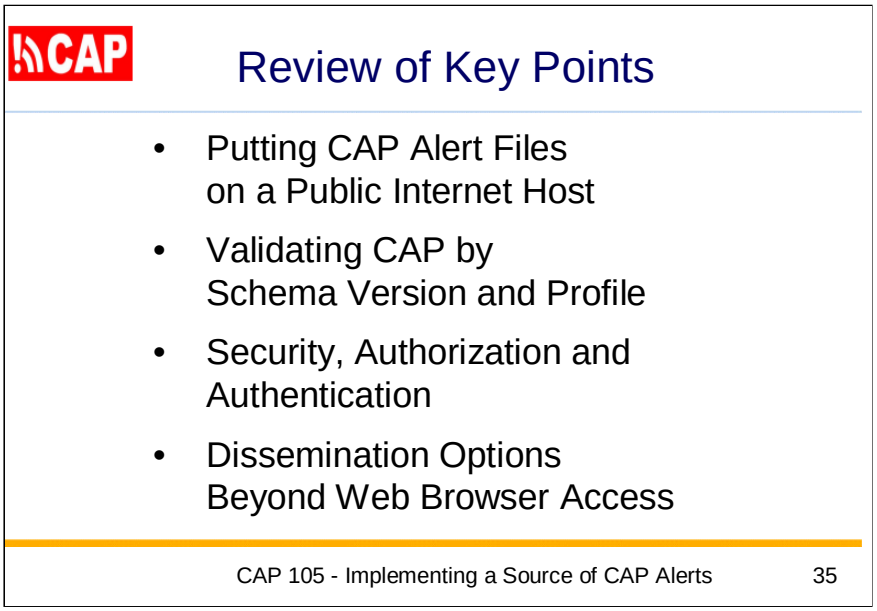
Here we see a service that sends out FAX pages for weather alerts.



For those who have access to the Web, news feeds are the preferred dissemination mechanism.

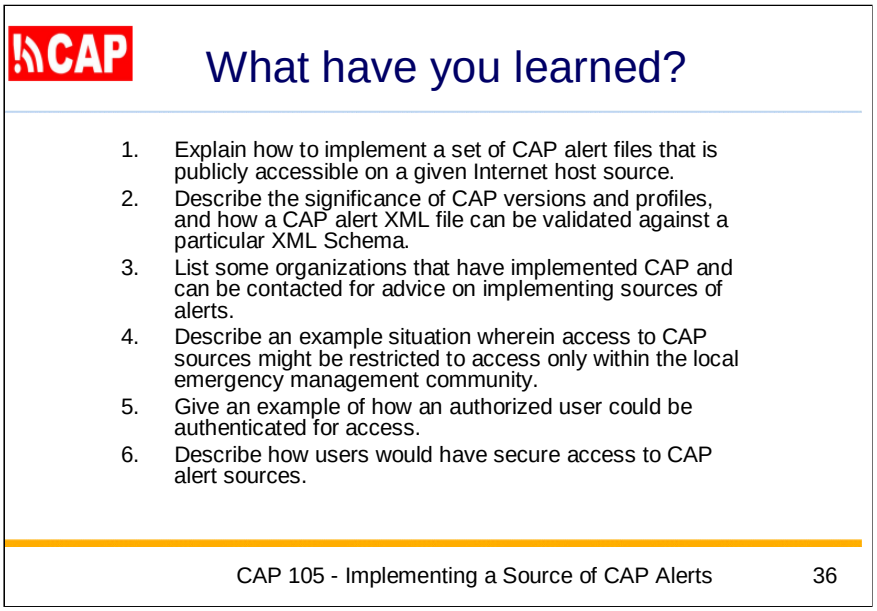
Here we see a CAP news feed offered by the U.S. National Weather Service, as it appears to a Web visitor with Microsoft Internet Explorer.

And here we see the same CAP news feed with the Firefox browser.



These are the Key Points of this presentation:

- Putting CAP Alert Files on a Public Internet Host
- Validating CAP by Schema Version and Profile
- Authorization and Authentication of Users and Editors
- Example of CAP Alert Sources
- Dissemination Options Beyond Web Browser Access



Now that you have completed this session, you should be able to perform the objective tasks.

Here are some key reference links concerning CAP.