A Distributed Security Announcement Authoring System with CAIF Support

Anselm R. Garbe, Oliver Goebel
IMF 2006

Oct 18 2006

Common Announcement Interchange Format (CAIF)

- Document-based format to describe security issues
- XML-based
- Designed to allow easy co-operation and
  - minimize multiplication of work
  - minimize introduction of errors
- Rendering independent

Paradigms

- Handle constituency specific information
- Minimal restrictions
- Normalized terminology
- Separation of policy and format

Design Goals

- Multiple problems in a single document
- Documents for multiple target groups
- Extensibility on a per-document basis

Co-operations/Adopters/Interested parties

- CERT-VW
- comCERT
- British Cabinet Office
- SAP AG

What is an Authoring System for Security Announcements?

Service Oriented Application (SOA) with following core functionality:

- Author management/administration
- Implements an authoring process (policy, version control)
- Persistation of Announcements
- Presentation of Announcements
- Import/Export of Announcements

Authoring Process (Participants)

Some definitions...

Author

Person, who creates/writes Security Announcements, e.g. /me.

Issuer

Organization, an author is working for, e.g. RUS-CERT.

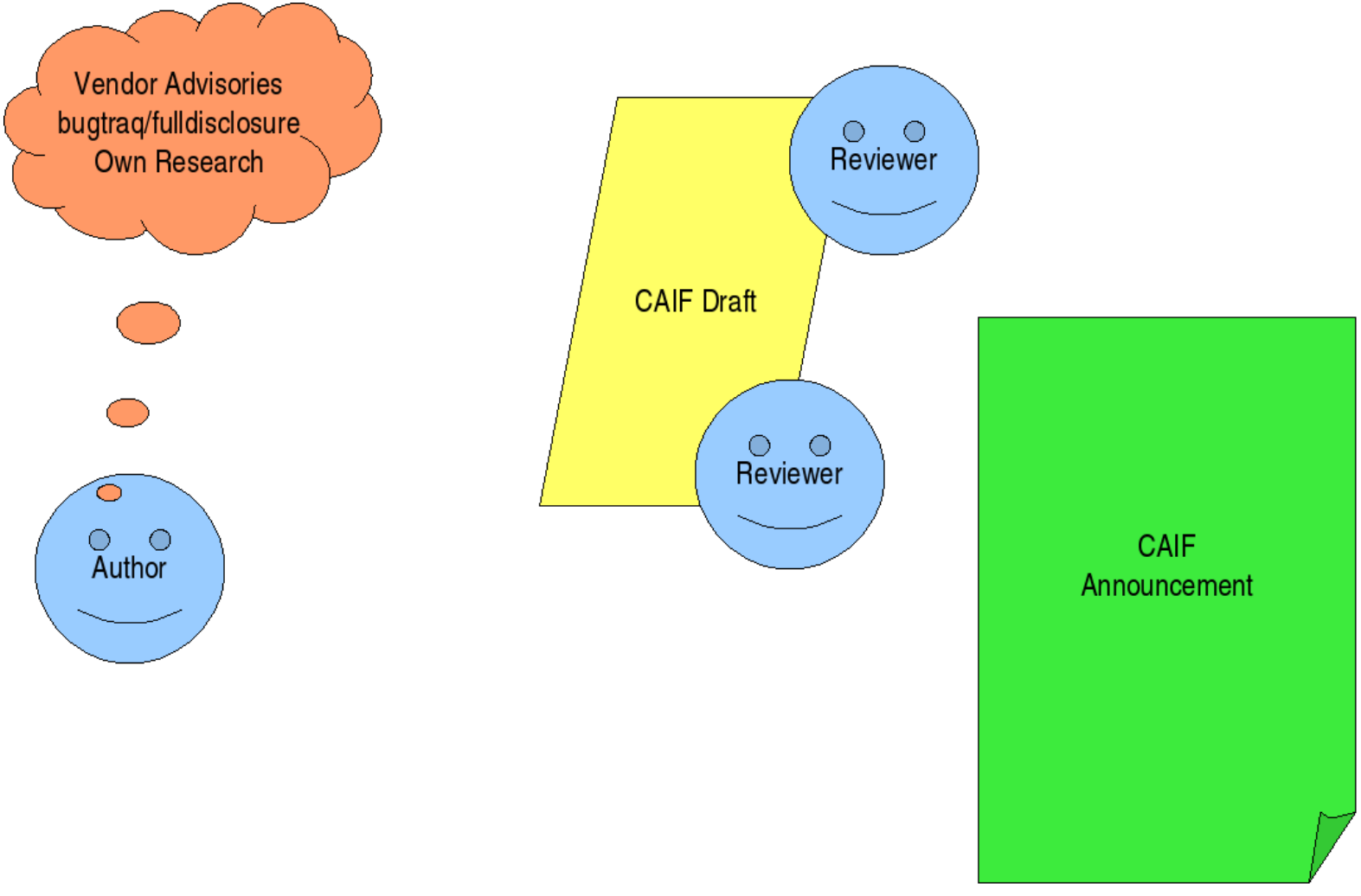
Constituency (zu dt. 'der Kundenkreis')

Users and IT infrastructure of organization(s), an issuer is working for, e.g. Uni-Stuttgart.

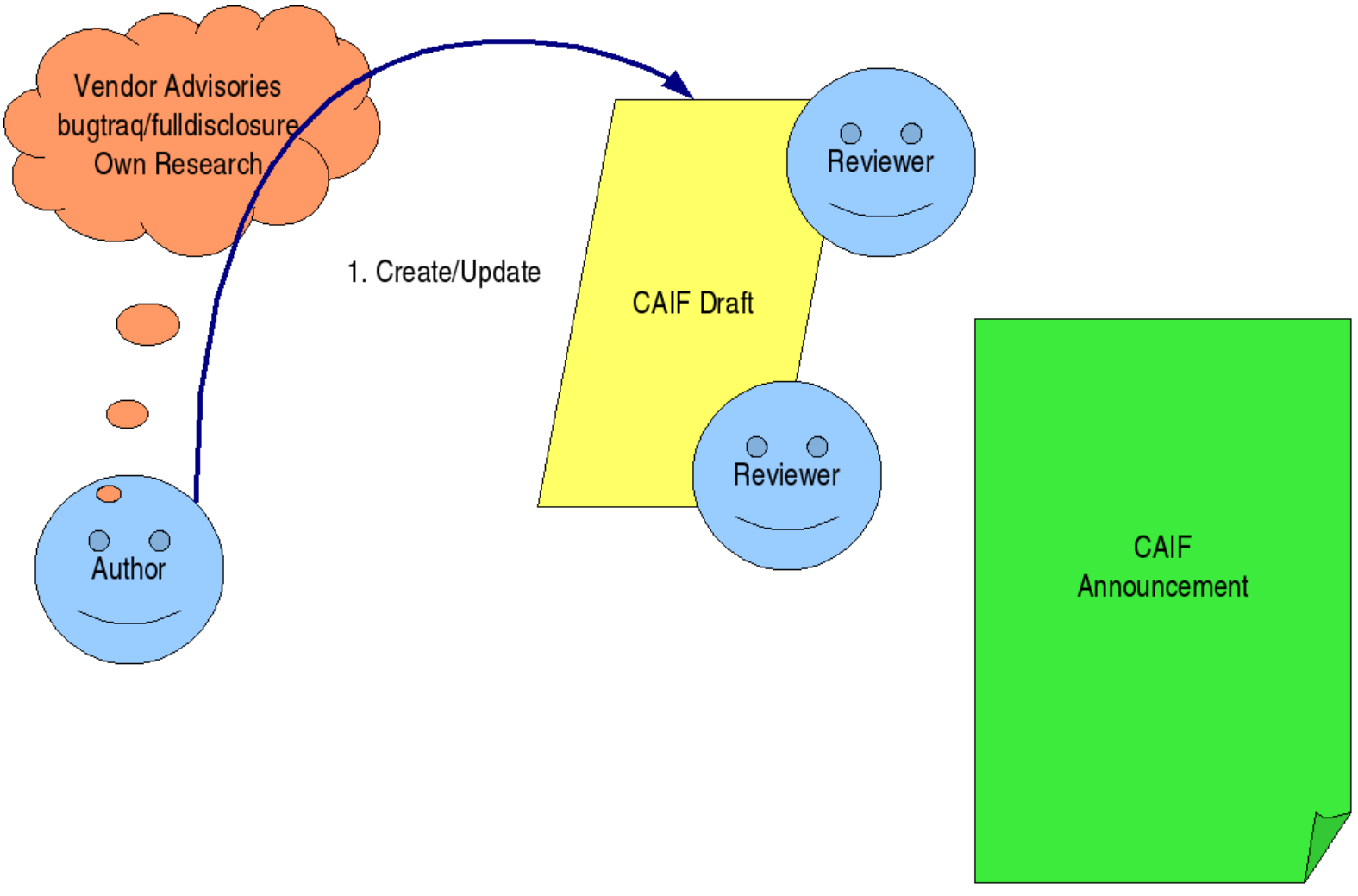
Target Group/Audience

Readers of Security Announcements, e.g. Administrators.

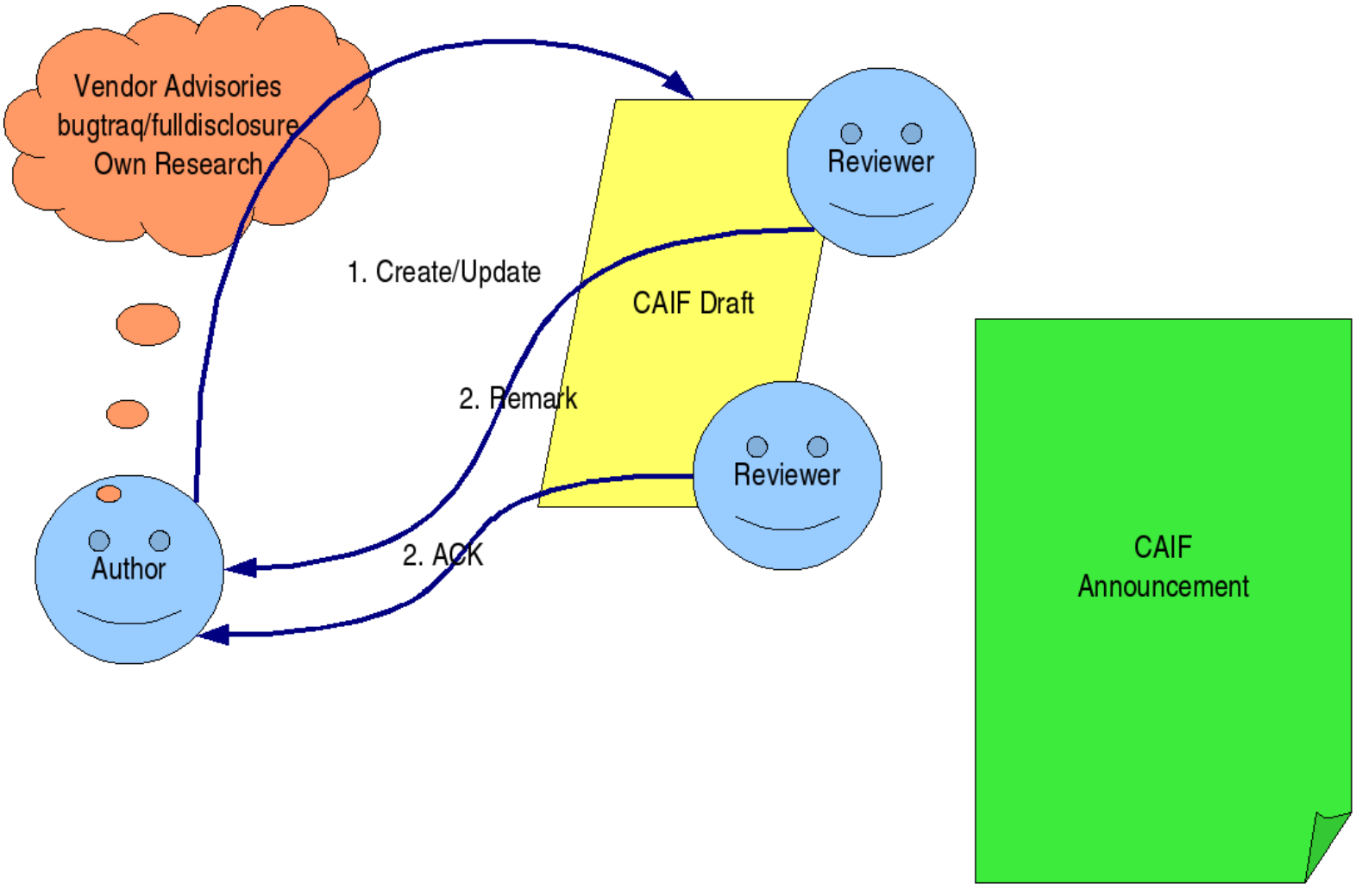
Example: Authoring Process at RUS-CERT



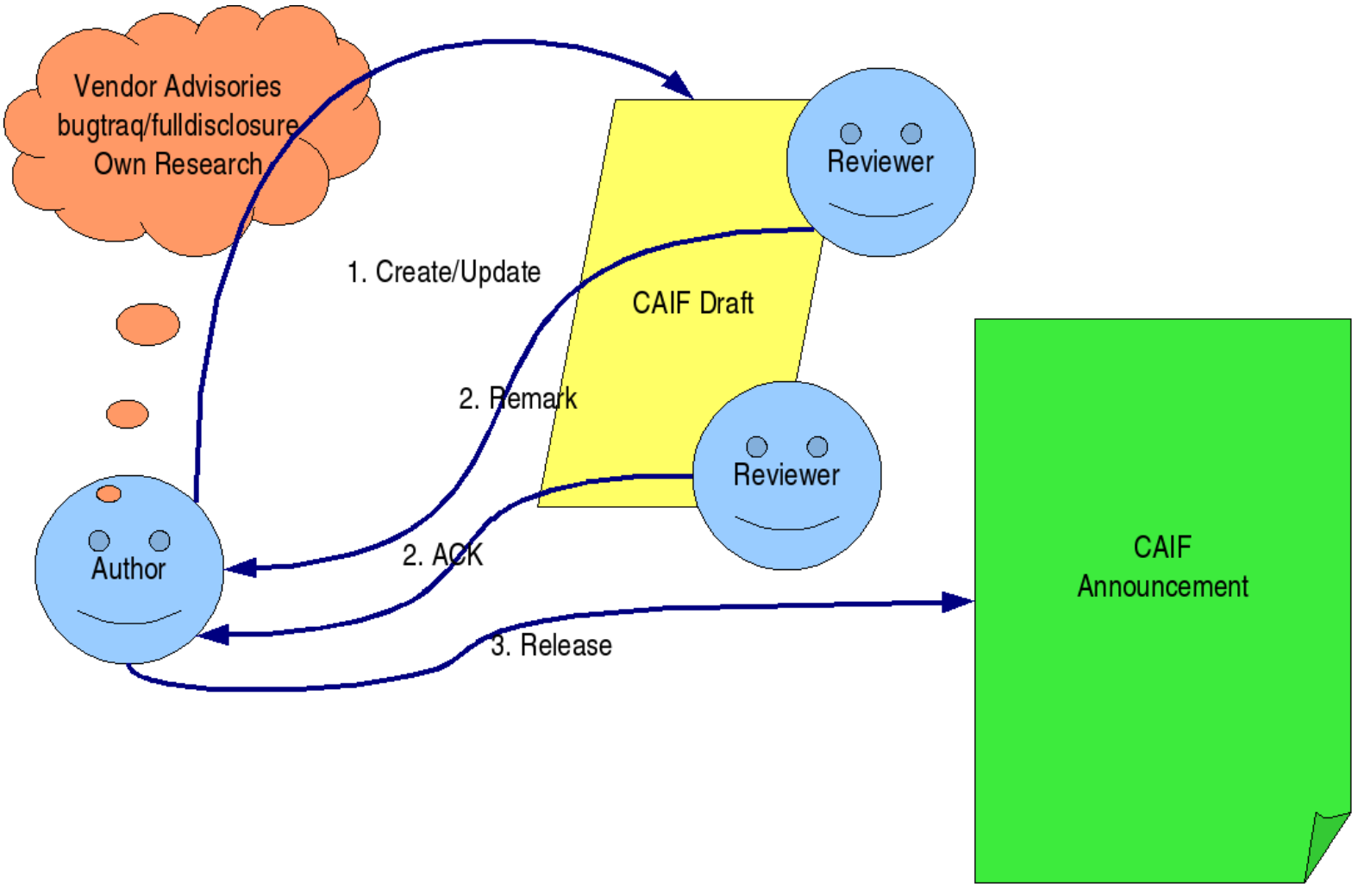
Example: Authoring Process at RUS-CERT



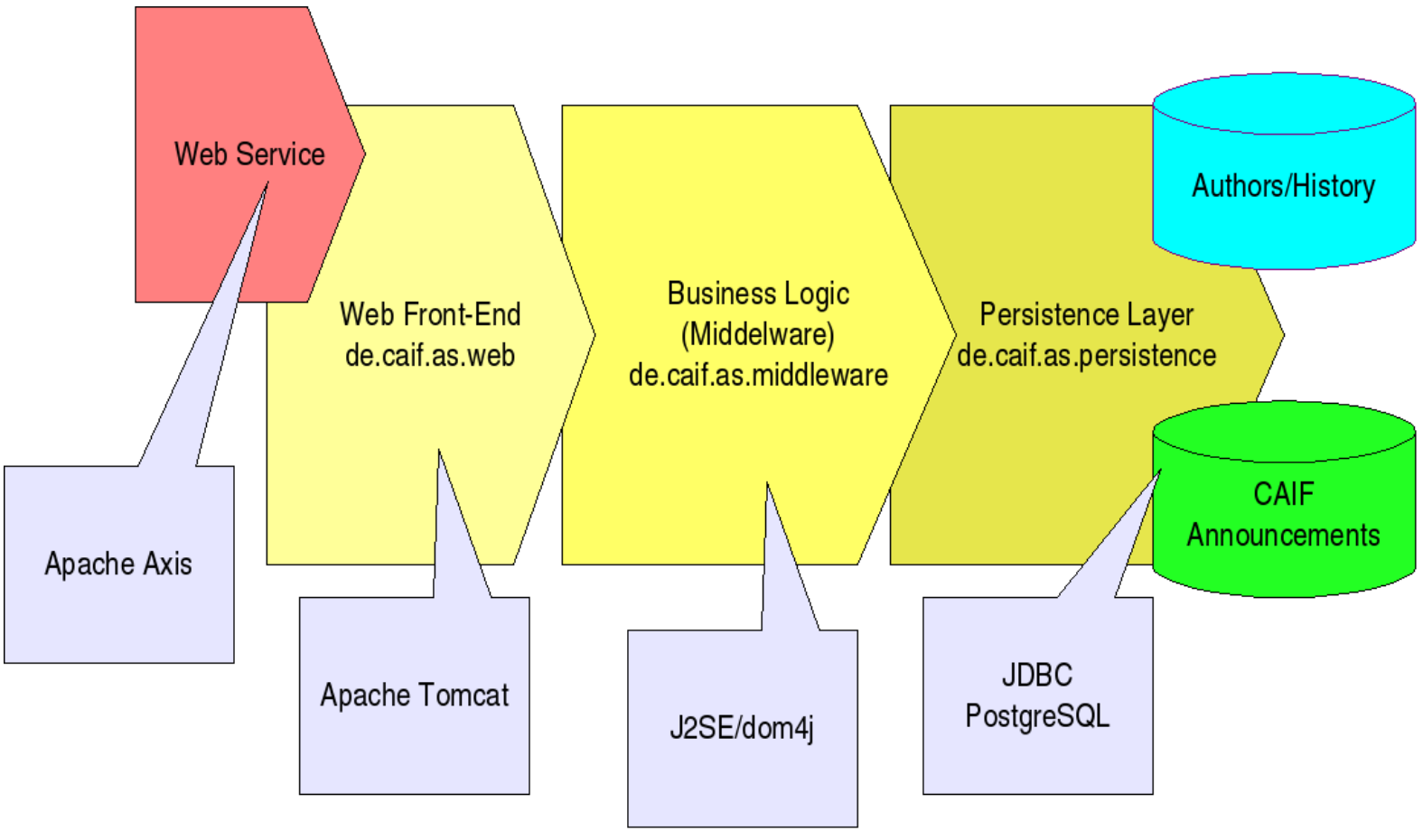
Example: Authoring Process at RUS-CERT



Example: Authoring Process at RUS-CERT



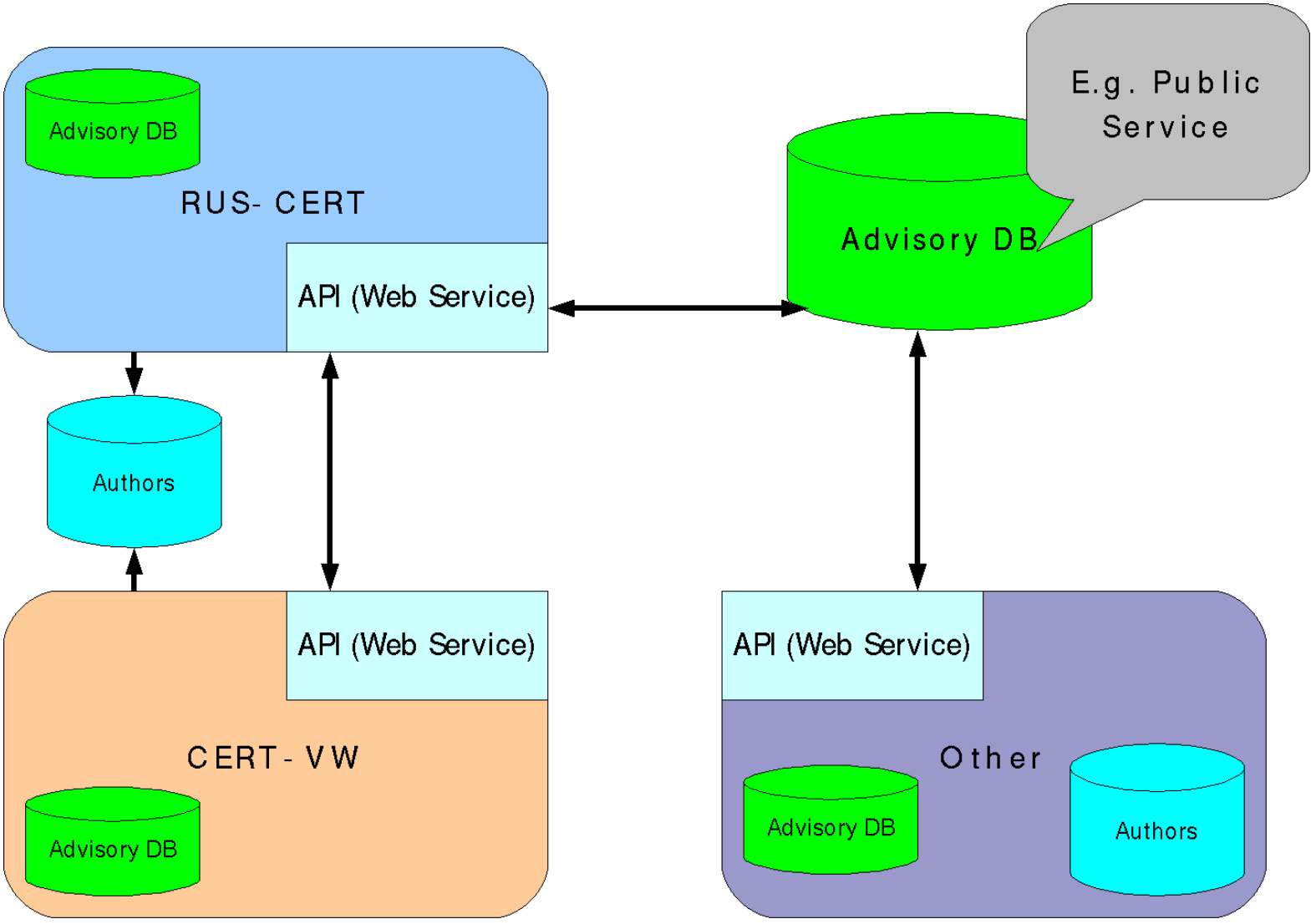
System Design



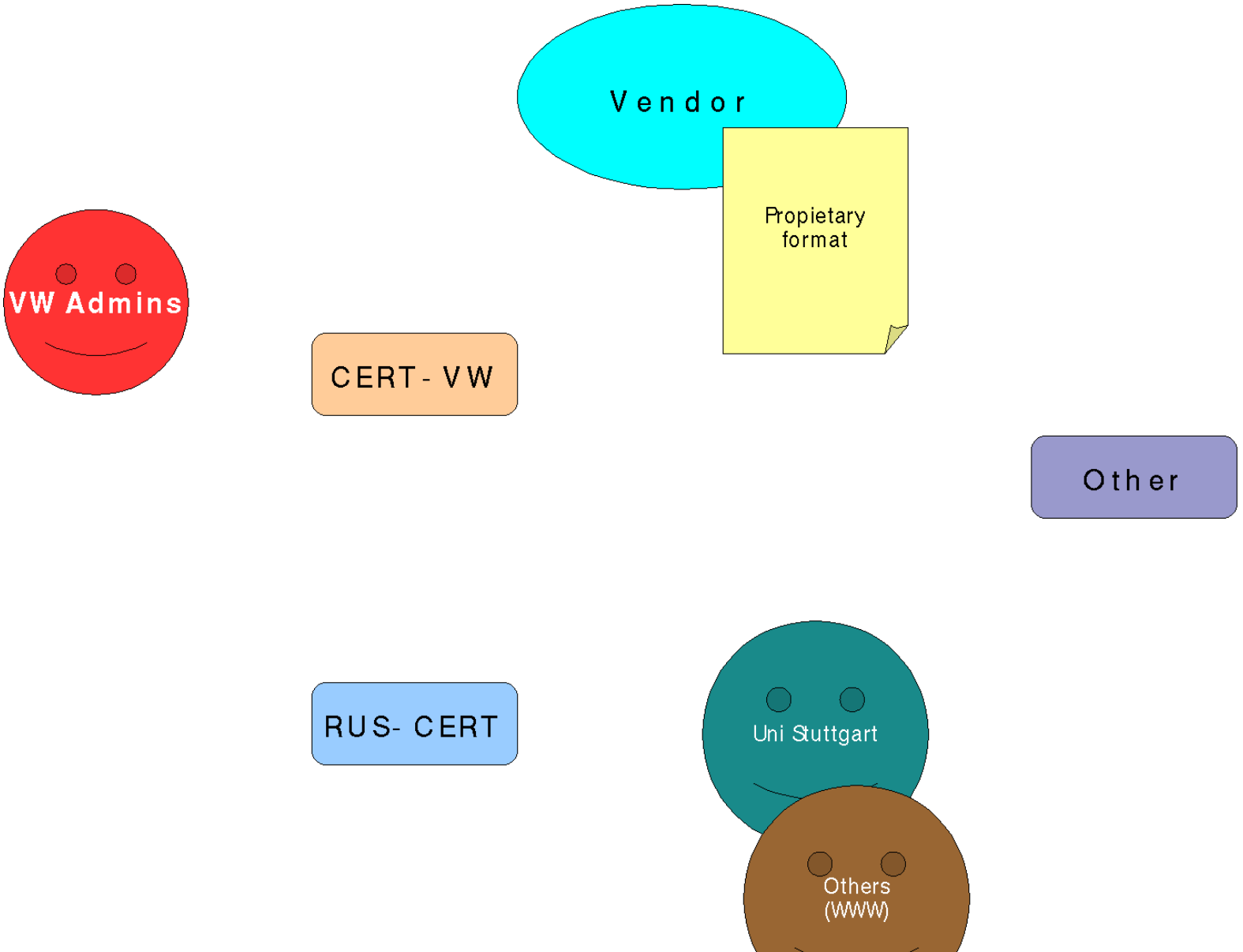
Service Interface of the Middleware

- Open Ticket (Authentication)
- Close Ticket (Authentication)
- Get Author Info
- Get Permission Info
- Get New Announcement
- Get Announcement
- Get Announcements
- Store Announcement
- Comment Announcement
- Change Announcement State (New, Review, Release, Revision)

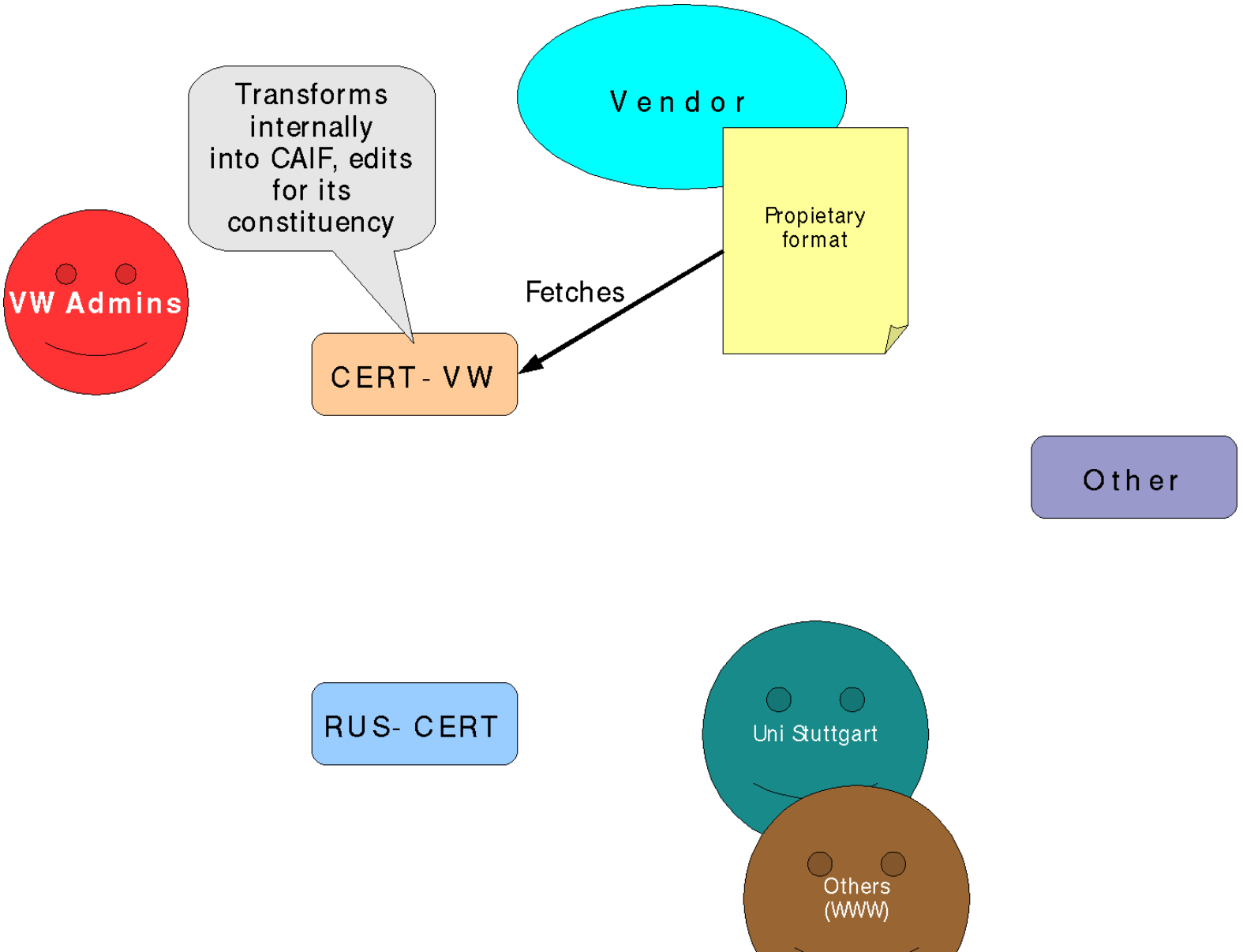
What makes an Authoring System *distributed*?



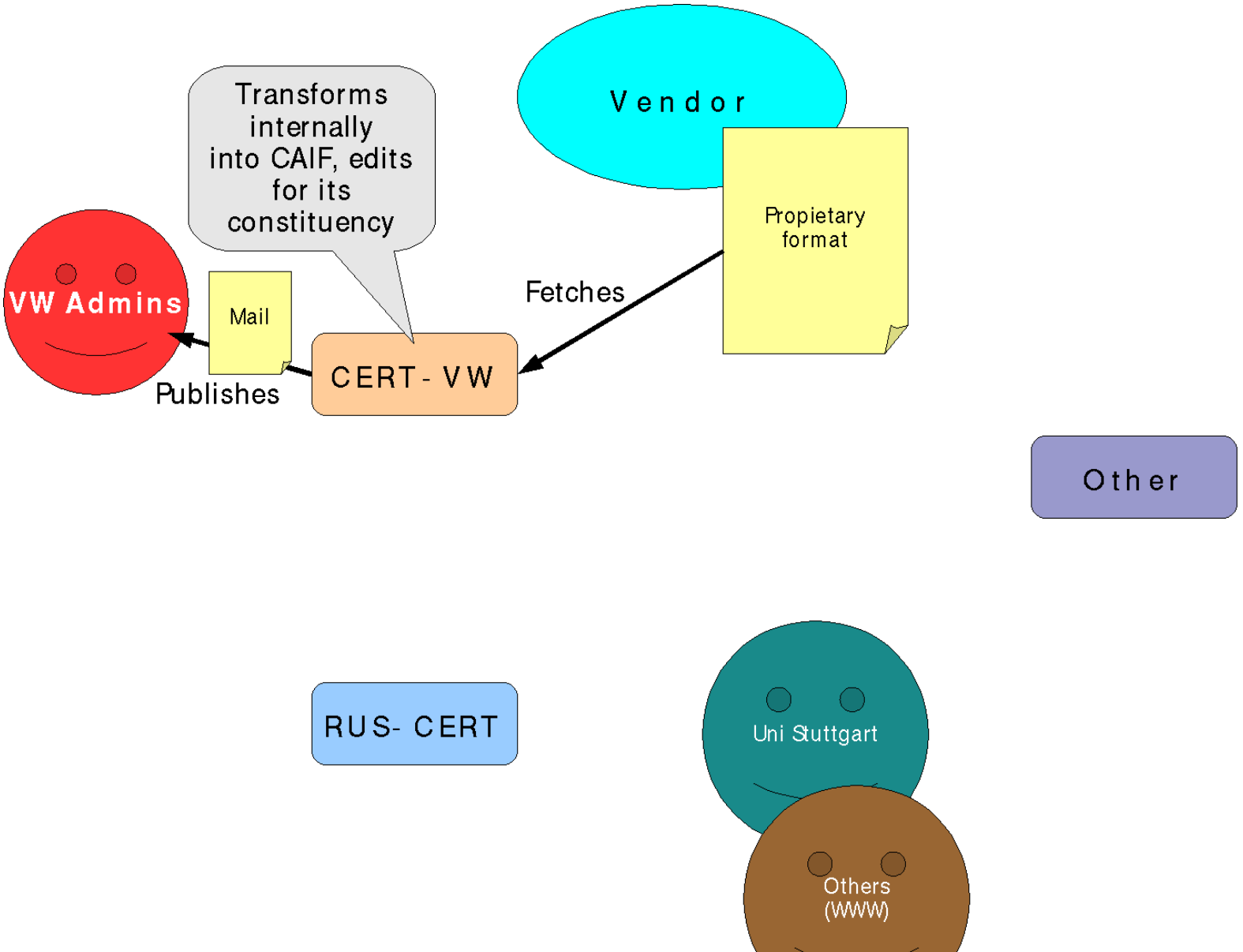
Example: Distributed Authoring Process



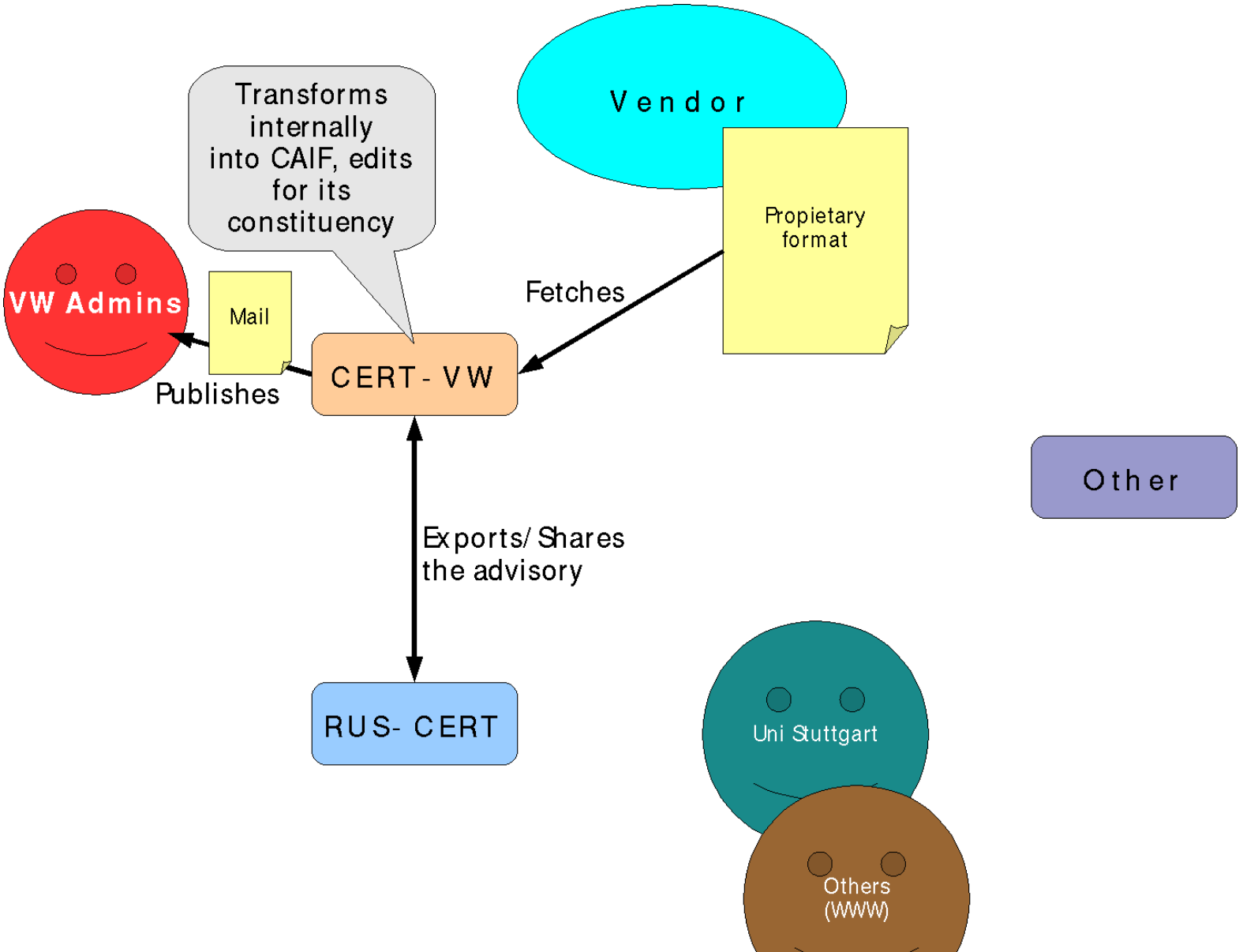
Example: Distributed Authoring Process



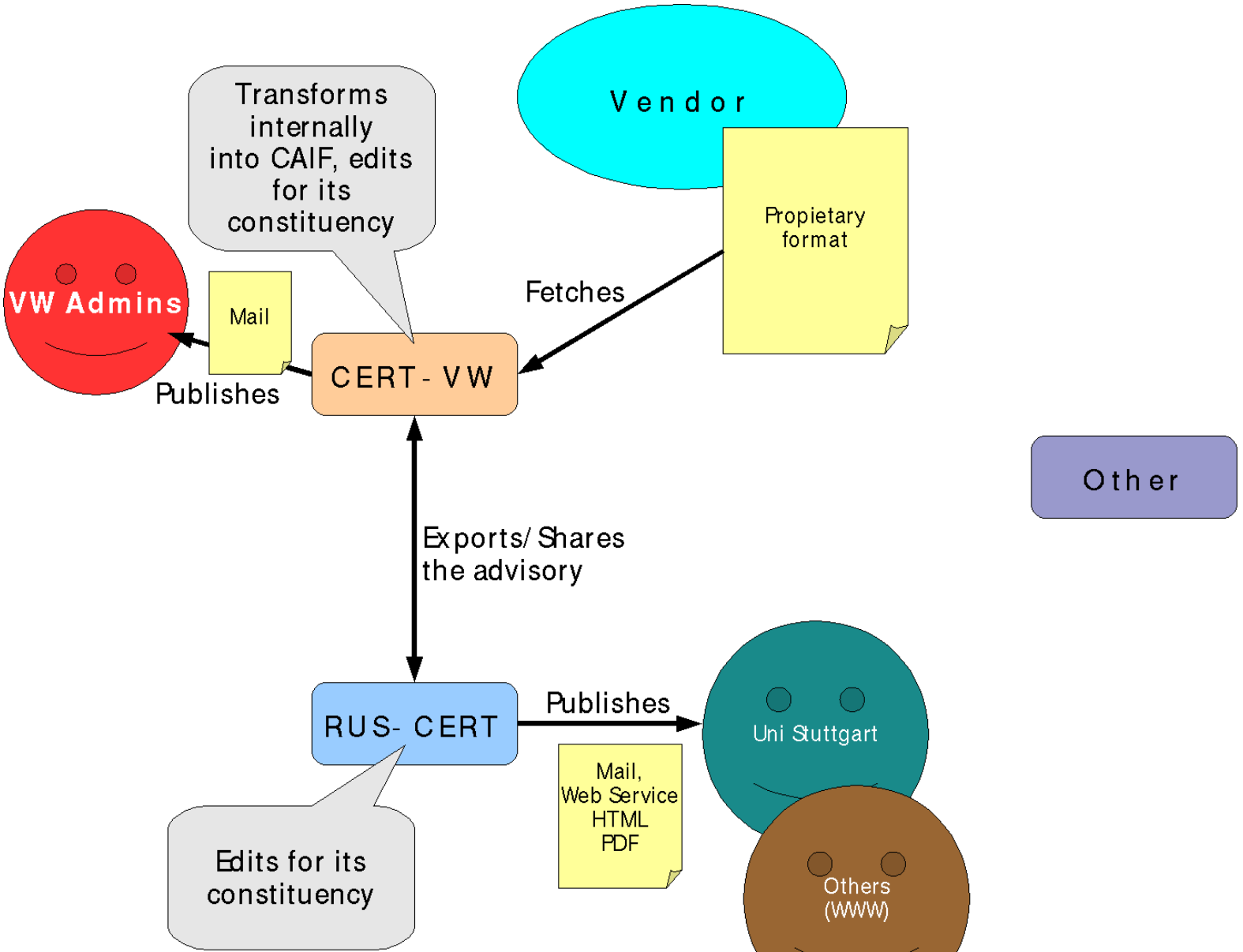
Example: Distributed Authoring Process



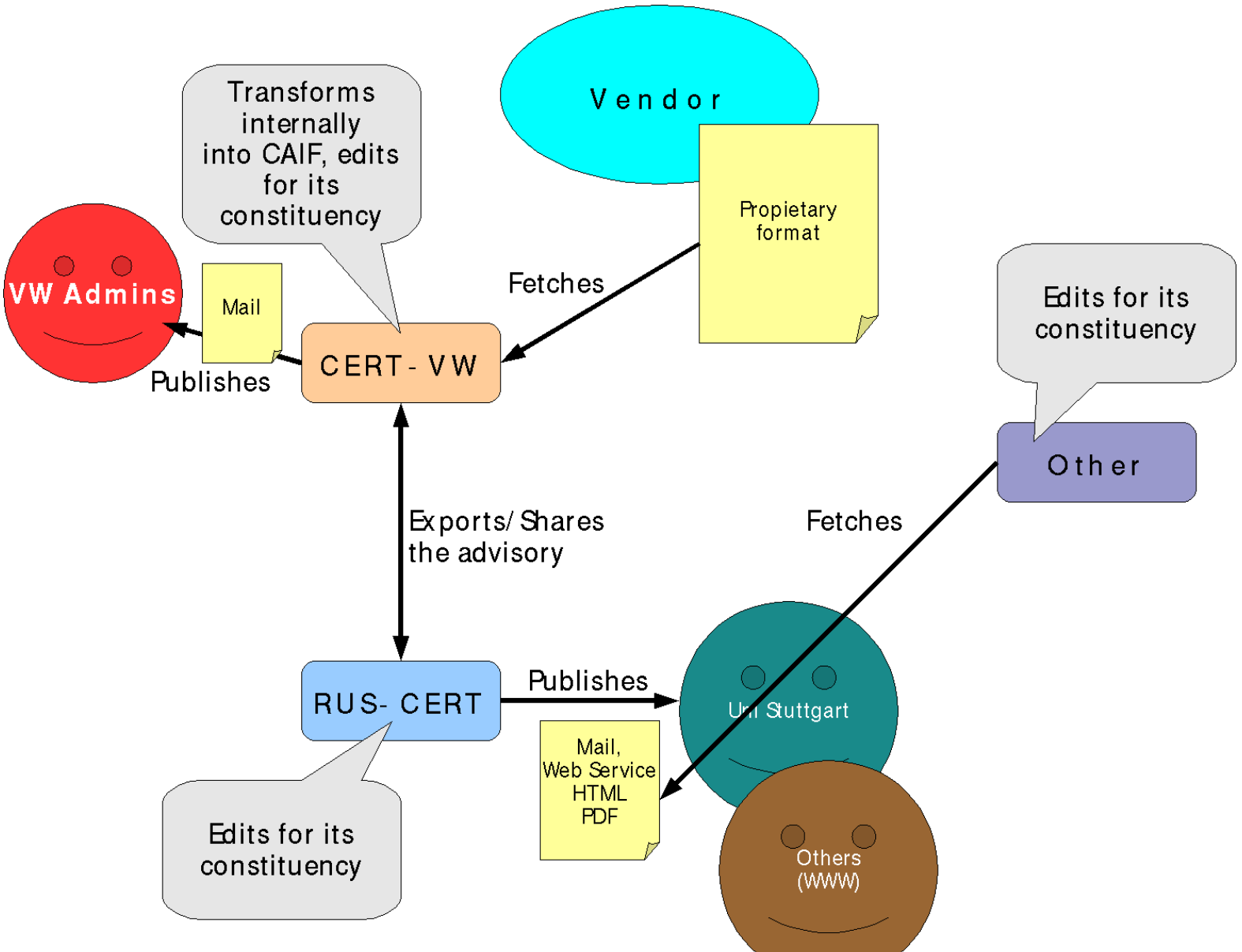
Example: Distributed Authoring Process



Example: Distributed Authoring Process



Example: Distributed Authoring Process



Apache Axis-based Web Service

- List of announcements via SOAP
- Announcement details via SOAP
- WSDL description

Application

RSS feed generator which accesses the service interface.

Current development

Support **all** functionality of service interface (authoring access).

Web-based Front-End *(ws-caif)*

- Apache Tomcat Web application
- Depends on persistence layer and middleware APIs
- Consists of a bunch of Servlets
- Some screenshots in the Proceedings..

Current Development

- OpenSource development of *ws-caif*
- CAIF 2.0 (XML Schema based)
- Integration of wxWidget-based CAIFed GUI
- Distributed Middleware (extending Web Service Interface)
- Administration front-end
- Public release of ws-caif

FIN

Questions?

Related information

- http://www.caif.info
- http://suckless.org/arg/
- garbeam@gmail.com