Maryland's Emergency Geographic Information Network, a Technical Walkthrough

David Geeraerts
Systems Engineer

Joe Bizzell
Senior Web Programmer

Copyright © 2006 Towson University Center For Geographic Information Sciences
Overview

- MEGIN is a resource metadata system for the Emergency Management community, as well as a system for secure map services
- This is a discussion/demo presentation of the working MEGIN pilot system
  - MEGIN Functions
    - Portal
    - Map Service Security
  - MEGIN Technology
    - Security
    - Software
    - Network Concepts
Portal Security

• Public MEGIN Home Page
• Secure Site
  – IIS 6.0 (Web Server)
  – HTTPS [SSL] 128 bit encryption
  – Certificates
    • HTTP 1.1 Protocol for Certificate Authentication
    • X.509 v.3
    • Aladdin eTokens
  – Oracle COREID Access
    • ISAPI Filters
    • AAA
    • URI Registration for Applications
    • Passing user information to the Java Applications
Permissions System

• Directory (Active Directory)
  – Organized with roles and organization grouping
  – Used by Oracle CoreID Access for Authenticating and Authorizing users based on roles and group membership

Directory Harvesting

• Java Application harvesting the directory to populate the database in order to achieve record level security
  – Users
  – Groups
  – Roles

• Booze Allen Hamilton, a security consultant company has reviewed this architecture
Portal – “Publish”

• Upgraded system that was originally developed for the Maryland Mapping Resource Guide
  – Publishing to a ArcIMS Metadata Service
  – Adding extra data for searching, etc.
• The Data Provider is in control of its records and the permissions set on them
• User can belong to multiple organizations
Portal – “Publish” cont.

- Stored information used for simplified record creation
  - Map Services
    - Used for MEGIN secured mapservices
  - Contact Information
  - Preference Information (Project, organization, etc.)
- Easy to use publish System
  - Publish form utility to create FGDC level 1 metadata
  - Upload utility to upload FGDC metadata
  - Extra “EGIN” specific fields handled automatically
Portal – “Set Permissions”

• Security is record level at the record level and controlled by the data provider
  – Security is stored in the database for fast searching

• We have setup 3 primary roles for this system to be used for base permissions

• Easy one click option to set base permissions on a record
  – Overall role (Official Use, Sensitive, Restricted)
Portal – “Set Permissions” cont.

- Security level customization is granular
  - Access levels are used, where a user can be locked down to an unclassified part of a record (or just part of a record)
  - Role access can be customized
  - Group / Individual user access can be customized
    - Group based system allows drill down approach to select groups / users
    - Group based access can hierarchically populate down
    - Users/groups can be “explicitly denied”
Portal – “Search”

- Customized system that is part of ESRI’s Portal Toolkit 2.0 (PTK)
  - Only customized Search being used, all admin, publish, and channel management stripped
  - Portal Toolkit calls SQL stored procedures directly, for faster searches

- Complex query driven, but simple to use form
Portal – “Search” cont.

• Search results are limited to what you’re allowed to view
  – Unclassified access gives just an unclassified name and abstract, which are not part of the actual content of the record.
  – Users can be denied access altogether
  – Using separate XML style sheets for different permission levels

• Communities of interest provide information for different user groups (PTK 2.0 Channel System)
  – Highlighted records
  – Resource Links
MEGIN Software

- **Microsoft Network**
  - Windows Server 2003 Enterprise and Standard
  - IIS 6.0
  - DNS
  - Active Directory
  - PKI
- **Microsoft SQL Server 2000**
- **Apache Tomcat 5.0**
- **Sun Java SDK 1.4.2**
- **ESRI**
  - Portal Toolkit 2.0 (Customized)
    - (PTK used in geodata.gov)
  - ArcIMS 9.1
  - ArcSDE 9.1
- **Oracle COREID**
Map Service Security

- Client-MEGIN authentication / authorization system
  - MEGIN to log in
  - Service establishing communication

- Gateway System
  - Authentication
  - Authorization
  - Message Translation and Forwarding
    - ArcXML to SOAP
• RDP Side (Remote Data Provider)
  – IPSEC Security between Gateway and RDP secure site
  – Filter System
    • Reverse SOAP / AXL Translation
  – Combined Hosting Options
• Image Streaming / Image Servlet
  – Response with stream
    • Stored in database for specific user
    • Updated to URL
  – Image Servlet serves the image data for the client
    • Can require security