
Requirements Assessment

MOBILE

TRANSACTION

GATEWAY

To

State of Ohio

Department of Administrative Services

Columbus, Ohio 43215

Battelle
The Business of Innovation



August 2004

This report is a work prepared for the State of Ohio Government by Battelle and Information Control Corporation. In no event shall the State of Ohio Government, Battelle, or Information Control Corporation have any responsibility or liability for any consequences of any use, misuse, inability to use, or reliance on the information contained herein, nor does either warrant or otherwise represent in any way the accuracy, adequacy, efficacy, or applicability of the contents hereof.

Acknowledgments

Special thanks to representatives of participating departments for giving their time to this effort.

Document History

Date of issue:	August 4, 2004
Status:	Original draft released for internal review
Name(s) of issuing organization(s):	Battelle Information, Science and Technology (Battelle) Information Control Corporation (ICC)
Change history	Draft for internal review, August 12, 2004 Draft for external review, August 16, 2004 State of Ohio OIT release, August 23, 2004 Last revision for distribution, October 12, 2004
Summary:	This document summarizes the requirements assessment for the Mobile Transaction Gateway (MTG) initiative and serves as an input to the conceptual architecture, business case, and pilot planning activities.

TABLE OF CONTENTS

	Page
ACKNOWLEDGMENTS	II
DOCUMENT HISTORY	III
TABLE OF CONTENTS	4
EXECUTIVE SUMMARY	9
Background	9
Method.....	9
Results	9
1.0 INTRODUCTION	12
1.1 Purpose	12
1.2 Scope	12
1.3 Document Organization	13
2.0 METHODS AND MATERIALS.....	14
2.1 Data Collection and Analysis	14
2.1.1 Instruments	14
2.1.2 Business Process Definition	15
2.1.3 Quantitative Analysis	15
2.2 Use Case Modeling	15
2.3 Analysis of Dependencies	15
2.4 Sources	15
2.5 Qualifications	16
3.0 ASSESSMENT	17
3.1 Data Collection and Analysis	17
3.1.1 Business Process Definition	17
3.1.2 Quantitative Analysis	18
3.2 Use Case Modeling	20
3.2.1 Variants	20
3.2.2 Packages	21
3.2.3 Common Requirements.....	23
3.3 Analysis of Dependencies	23
3.3.4 Special Requirements	24
4.0 REQUIREMENTS.....	26

4.1 Organization	26
4.1.1 Template Structure	28
4.1.1.1 Business Process Requirements	28
4.1.1.2 Requirements Mapping	28
4.2 Application	29
4.3 Assumptions	29
4.4 Functional Requirements.....	30
1.0 Internet Access	30
2.0 Communication Services.....	33
3.0 Electronic Data Collection	39
4.0 Document Management	47
4.5. Requirements Mapping	50
APPENDICES	1
APPENDIX A. ACRONYMS	2
APPENDIX B. PROCESS DEFINITIONS.....	3
APPENDIX C. SCENARIOS.....	0
APPENDIX D. USE CASE MODELS.....	8
USE CASE MODELS	9
MTG Use Cases.....	9
1.0 Internet Access	9
1.2 Information Access.....	11
Identify Device Type.....	12
Render Content.....	12
Request Web Content.....	12
Search	12
Serve Documents.....	12
Serve Forms.....	12
Serve Web Pages	12
Transform Content	12
1.3 Application Access.....	12
Execute Application	13
Mobile Data Applications	13
Serve Mobile Data Application.....	13
Terminal Services Applications	14
Serve Terminal Services Application.....	14
Web Applications.....	14
Serve Web Applications.....	14
Web Services.....	14
Provide Web Service	14
2.0 Communication	15
2.1 Alerting.....	16

1.1 DPS/EMA Alerting	17
Alerts	17
Audit	18
Broadcast Alerts	18
Delete Alerts.....	18
Forward Alerts.....	18
Manage Alerts	18
Originate Alert.....	18
Read Alerts	19
Receive Alerts	19
Reference Supplements	19
Repudiate False Alarm	19
Save Alerts	19
Target Alert	19
Validate Alert	19
1.2 Public Alerting	20
Format alerts.....	20
Location-Based Services	20
Number portability	20
Repudiate Alert.....	21
Target Clients	21
Map to IX Carriers	21
2.2 Instant Messaging.....	22
Manage Messages.....	22
Manage Presence	22
2.3 Notifications	23
Notifications Integration Example	23
Citizens	24
myOhio.gov	24
Build Job Profile.....	24
Portal Log-in.....	24
Portal Log-out.....	24
Manage My Account/Profile	25
Manage My Notifications.....	25
State of Ohio Job Search	25
Find Job Description	25
Send Email	25
Send Message.....	25
Send Notification.....	25
Subscribe	25
Unsubscribe	25
2.4 Mail & Schedules	25
Mail Services	26
3.0 Electronic Data Collection	26
3.1 Customer Service Request.....	28
3.2 Inspections & Audits	29

Complete Form.....	29
Design Forms	30
Download Data.....	30
Extract Data.....	30
Find Form.....	30
Forms Management.....	30
Generate Compliance Acknowledgement.....	30
Generate Forms	30
Generate Receipt	30
Mail Forms	31
Obtain Form	31
Populate Form	31
Receive	31
Route the Ticket	31
Save Form.....	31
Select Form.....	31
Sign Form.....	31
Store Forms	32
Submit Form.....	32
Track Ticket Disposition.....	32
Update Form.....	32
Upload Data.....	32
Upload forms templates.....	32
3.3 Inventory Management.....	32
3.4 Remote Sensing.....	32
Aggregate Data.....	33
Analyze Data	33
Forward Alerts.....	33
Report Data.....	33
Transmit Data	34
3.5 Surveys	34
4.0 Document Management	35
APPENDIX E. PARTICIPANTS	0
APPENDIX F. GLOSSARY	1
APPENDIX G. REFERENCES.....	2

LIST OF TABLES

Table 1. Process Type Frequency	20
Table 2. Categories, Types, and Sub-types.....	27

LIST OF FIGURES

Figure 1 : Distribution of Scenarios by ProcessType by Department	19
Figure 2 : Dependencies: High-Level Business & System Requirements.....	24
Figure 3 : Context - Internet Access	10
Figure 4 : Information Access.....	11
Figure 5 : Application Access.....	13
Figure 6 : Situation: Communication Dependencies	15
Figure 7 : Alerts Context.....	16
Figure 8 : DPS/EMA Alerting	17
Figure 9 : Public Alerting	20
Figure 10 : Notifications Context	23
Figure 11 : Notifications.Example.Jobs.Ideal.....	24
Figure 12 : Dependency Diagram-EDC.....	27
Figure 13 : Off-line forms completion.....	29
Figure 14 : Remote Sensing.....	33
Figure 15 : Dependencies Diagram-DM.....	35

EXECUTIVE SUMMARY

Background

This report provides a requirements assessment of the State of Ohio, Mobile Transaction Gateway (MTG) initiative based on information collected from two “joint application definition” (JAD) sessions, government standards, industry solutions, and follow-up interviews with stakeholders.

Battelle and Information Control Corporation (ICC) received a request from the Ohio Department of Administrative Services (OIT) for a requirements assessment and proof-of-concept that would determine the scope and cost of a mobile transaction gateway pilot. Forced to do more with less, state governments like Ohio are pursuing ways to improve the efficiency of delivering services to citizens. MTG, a common services solution centered on support for the mobile workforce, business partners and citizenry, is seen as one way to deliver such value.

Method

The JAD sessions enjoined twenty-five (25) stakeholders and knowledge-workers from six (6) departments with resources from Battelle and ICC to collaborate on an inventory of State-of-Ohio mobile user needs and business requirements. The sixty-seven (67) scenarios describing various mobile applications that had been collected in these sessions were then analyzed for similarities and differences and clustered into ten (10) different process types.¹ The process types were modeled via use case analysis and included an enumeration of pertinent business rules and constraints. Use cases were then placed into context to identify dependencies. The resulting functional requirements and quality attributes (non-functional requirements) were then mapped to government standards and industry solutions, with supplemental qualifications being provided through subsequent interviews with stakeholders to arrive at a requirements set.

Results

The resulting requirements set addresses twelve (12) business process types which can be summarized as high-level business need as follows:

1.1 Information Access

Provide web content to the mobile workforce, business partners and citizenry as appropriate to the user/customers’ role, device, and configuration via the shared services of identity management and security, personalization and **content transformation**.

¹ The ten (10) business-process types subsequently became (N), where functional and dependency analyses identified two (2) of these to be a variants of more fundamental patterns, capabilities were already delivered, or the process was deemed to be out-of-scope for lack of information.

1.2 Application Access

Provide on-line services to the mobile workforce, business partners and citizenry as appropriate to the user/customers' role, device, and configuration via the shared services of identity management and security, personalization, content transformation, and **remote application access delivery mechanisms**.

2.0 Communication Services

Provide communication services to the mobile workforce, business partners and citizenry as appropriate to the user/customers' role, device, and configuration via the shared services of identity management and security, personalization, and content transformation with access to the following capabilities:

- Provide secure and reliable **alerts** including origination, propagation, and control capabilities to public safety and emergency management first and second responders and support organizations both within and across jurisdictions with possible extension of one-way alerting capability to citizens via wired and wirelessly enabled devices.
- Provide secure and reliable **instant messaging** and **chat conference** capabilities to public safety and emergency management first and second responders and support organizations both within and across jurisdictions.
- Provide **electronic mail and schedule** access to the State mobile workforce as appropriate to role.
- Provide timely **notifications** of impending State business to business partners and citizenry on a subscription basis appropriate to the user/customers' device and configuration.

3.0 Electronic Data Collection

Provide **roundtrip electronic data collection** capabilities to the mobile workforce, business partners and citizenry as appropriate to the user/customers' role, device, and configuration via the shared services of identity management and security, personalization, content transformation, document and workflow management. Specifically:

- Provide constituents with the ability to **request services** from a provider organization, via the elicitation and submission of structured data (and payments), with the issuance of receipts and/or tracking information for access to processing status.
- Provide the mobile workforce of inspectors, auditors, and caseworkers with the ability to **conduct round-trip electronic data collection and management for the range of compliance targets** such as mechanical systems, building or construction sites, service agencies, and grant applicants/recipients, including support for workflow for process management.
- Provide state employees with ability to do **systems-based**

inventory management both on- and off-line (with synchronization capabilities) as required by context of application (availability of network connectivity).

- Provide **automated data collection capabilities from remote field sensors**, specifically for field and stream gauges.
- Support collection of **field survey data on- or off-line** with synchronization capabilities.

4.0 Document Management

Provide **document portability and management solutions** to the mobile workforce, business partners, and citizenry as appropriate to the user/customers' role, device, and configuration via the shared services of identity management and security, personalization, content transformation (where appropriate²), and workflow to render the following:

- Provide the ability to obtain, consult, and manage (voluminous) state, federal, and proprietary codes, manuals, operational guidelines, and procedures in electronic formats on- or off-line.
- Support customer service through ready access to public documents, directions, instructions, and resources.
- Support the document lifecycle from inception through creation, review, redaction, storage, dissemination and destruction.

The requirements set for MTG has been defined as functional requirements and quality attributes in recognition of these diverse business needs, rapid technological change, and evolving government standards and industry practices.

The objectives of this requirements assessment have been fourfold:

- To define the business requirements of Ohio mobile workforce, business partners and citizenry based on the input of participating departments and agencies
- To provide a basis for the definition of a “conceptual architecture” to meet the needs of a business case and pilot implementation of MTG.
- To provide a set of criteria for evaluating competing solutions.
- To provide an input into the business case for a pilot implementation.

² “Where appropriate” is an acknowledgement that the limitations of bandwidth, memory, and form factor may simply be insufficient to download and manage certain types of documents (i.e., cell phones do have limitations).

1.0 INTRODUCTION

1.1 Purpose

Battelle and Information Control Corporation (ICC) received a request from the Ohio Department of Administrative Services (OIT) for a requirements document and proof-of-concept that will assist in determining the scope and cost of a wireless transaction gateway pilot. State governments are being forced to do more with less, and are pursuing ways to improve the efficiency of delivering services to citizens. The recent improvements in mobile/wireless technologies present just such an opportunity.

Battelle and ICC understand the State's need to improve workforce efficiency and to deliver key information to its citizens. The State believes that mobile applications, coupled with seamless integration to backend systems, will increase worker productivity and reduce the cost of delivering service. Additionally, mobile capabilities hold the promise of more tightly coupled customer relationship management (CRM) and enterprise resource planning (ERP). Such improvements in the value chain typically yield improved customer satisfaction, faster more reliable service, and better resource utilization and cost management.

The business requirements contained herein have been written and mapped to various standards (as applicable) to document the combined findings of the MTG interview sessions. The principal objective of these sessions and follow-up interviews was to obtain descriptions of scenarios and requirements for tasks and business processes which could benefit their stakeholders if enabled via a Mobile Transaction Gateway (MTG). MTG is defined as a set of system services and supporting infrastructure that enable "mobile" information access and task accomplishment.

The analysis identifies twelve (12) principal business processes distilled from more than sixty (60) scenarios described in the interview sessions. Use case and dependency analysis have been used to further categorize and map business process into seven (7) major service areas providing a basis for the MTG conceptual architecture. The appendices of this assessment include the model used in these analyses as well as traditional requirements provided in structured text.

This document is, then, the requirements assessment for the Mobile Transaction Gateway (MTG) initiative, and serves as a principal input to the conceptual architecture, business case, and pilot planning activities.

1.2 Scope

Mobile capabilities of the MTG are not exclusively defined as wireless implementations/extensions, but rather, as the systems infrastructure that enables the mobile citizenry and workforce. This translates into infrastructure that supports reliable, and consistent, and secure access to state services for citizens, business clients and partners, and state employees. It includes the following cases:

- Mobile/roaming users attempting to access services remotely from different locations at different times from private and public machines via the Internet

- Mobile/Roaming users with properly equipped wireless devices needing to access services via the Internet as extended by wireless wide-area network services (TDMA, GPRS, CDMA, etc.)
- Remote users for properly equipped wireless devices via WLAN network services in well-defined physical environments connected to the State network
- Intermittently via data synchronization capabilities that leverage wireless or wired capabilities when and where available as WWAN, WLAN, WAN, LAN.

1.3 Document Organization

This document is organized into the following sections:

- **Section 1 – Introduction:** Summarizes the purpose and scope of the MTG requirements assessment and outlines the document organization.
- **Section 2 – Method and Materials:** Summary of the tools and techniques used in the requirements collection and analysis including data instruments, collection, aggregation, functional and dependency analysis, mapping, and sources.
- **Section 3 – Assessment:** Outlines assumptions and presents the findings of the data collection, and functional and dependency analysis, with their implications for MTG.
- **Section 4 – Requirements:** Defines the template and application of requirements. Catalogues both functional and nonfunctional requirements according to business process type, requirement type and class of service.
- **Appendix:** Provides a series of supplements including use case models, a catalogue of scenarios forming the basis of the analysis, participants, process-type definitions, acronyms, and a glossary.

2.0 METHODS AND MATERIALS

2.1 Data Collection and Analysis

In the first session on June 3, two groups were formed of two departments each (DOC with OIT and DPS with DNR). The two teams each worked collaboratively with an analyst to complete the questionnaires, or were interviewed for a description of applicable scenarios.

The second smaller session of June 10 allowed participants to work as a single group consisting of representatives from OIT/MARCS, DOD, and ODH.

The method enjoined stakeholders and knowledge-workers to collaborate on the identification and definition of mobile user needs via a three-step process:

1. Inventory organizational scenarios
2. Analyze those scenarios to define business requirements
3. Inventory supporting information systems and technical owners for subsequent analysis

2.1.1 Instruments

Two questionnaires and examples were used to guide the data-collection effort:

- a. The *Organizational Needs Questionnaire* was used to inventory scenarios and business processes with mobile workforce requirements including existing or planned mobile applications, but also prospective needs of citizens such as alerts, and services for special interest groups. One such questionnaire was completed for each participating organization.
- b. A *Process Analysis Questionnaire* was used to catalogue business requirements for key scenarios including goals, resources, and business rules. One process questionnaire was completed per scenario, time permitting.

The number and representation of agencies and interests suggested a change in questionnaire format for the second session:

1. The *Organizational Needs Questionnaire* was simplified for cataloging actual, planned, and envisioned deployments via an attribute assignment. Additional white space was added.
2. The *Process Analysis Questionnaire* was augmented with a choice of templates to capture workflow, process, or context models.

For further information see: *State of Ohio, Mobile Transaction Gate: JAD Summary*.

2.1.2 Business Process Definition

The sixty-seven (67) scenarios identified in the inventory could be categorized according to similarities and differences in inputs and outputs, resources and workflows, and goals. Common patterns were used to define a preliminary typology of ten (10) business process-types summarized in *Appendix B, Process Types*.

2.1.3 Quantitative Analysis

Individual scenarios were evaluated for frequency on status and priority. They were then aggregated by process type and cross-tabulated to determine the distribution across departments. These measures provided an estimate of relative importance, need, and commonality.

2.2 Use Case Modeling

The ten (10) preliminary business process types became the inputs to a use case analysis resulting in high-level functional requirements, and providing the basis for an analysis of dependencies, and for refinement of the types, themselves.

Use case analysis provides a description of system behavior in terms of its uses, the sequences of actions between a system and an actor, a role that may be fulfilled by users or other systems. The set of all use cases is a description of a system's complete functionality, where a given use case represents a functional requirement.

The set of all interacting users and systems is identified for any given processes type. The uses to which these actors may put the system are, then, enumerated. The nature of relationships between the use cases is then modeled as either necessary (an “includes” stereotype) or conditional (an “extends” stereotype) according to UML 2.0 standards.

2.3 Analysis of Dependencies

The use case analysis yields a catalogue of functional requirements for MTG. Completeness and coherency requirements of the model help to identify dependencies including quality attributes and system interfaces. These can be grouped and cross-referenced to identify end-to-end dependencies of the system. The analysis is realized via use case situation diagrams³ and results in the identification of downstream and upstream systems, including infrastructure support systems.

2.4 Sources

The fiduciary and structural role of the customer, the state of Ohio OIT; the evolving nature of mobile/wireless technology; and the complexity of information technology are three key factors driving the mapping to, and incorporation of, external sources into this document. Specifically, these include standards and requirements defined by Federal and State agencies (DHS, NIST, DPS etc.) and standards bodies (OMA, W3C, WFMC, IETF, OASIS, etc.).

³ Also known as context diagrams.

It is also prudent to re-use requirement definitions that have been previously validated by standards organizations.

The following standards have been referenced or mapped:

- *Statement of Requirements for Public Safety Wireless Communications and Inter-Operability*, The SAFECOM Program, Department of Homeland Security, Version 1.0, March 2004.
- *Criminal Justice Information Services Security Addendum to the Code of Federal Regulations Title 28, Part 20, Subpart C and the National Crime and Information center (NCIC) Policy Paper approved Dec. 6, 1982*, Federal Bureau of Investigation, March 2003.
- *LEADS Security Policy*, Ohio State Highway Patrol, Revised May, 7, 2003.

2.5 Qualifications

- While interpretations may be readily applied to the data collected from these two interview sessions, and seem intuitive, caution must be exercised in generalizing conclusions. Because scenarios were collected through a convenience sampling of participants (not a census or probabilistic sample), the validity of interpretations is limited.
- The process types and their related requirements described in this document are/may not be exhaustive or representative of all State mobile needs. They are based on the limited participation of six (6) State departments in two joint application definition sessions, follow-up interviews, and federal, state, and academic reference materials.
- Because of the number of perceived needs, viz., the number of processes inventoried in these two sessions, process drill-down on any one process was limited, and while pursued in a number of follow-up interviews, support or depth of respondent knowledge was not always forthcoming.

3.0 ASSESSMENT

3.1 Data Collection and Analysis

3.1.1 Business Process Definition

Stakeholders readily recognized candidate scenarios for MTG. The number of participating agencies and potential applications forced some changes in data collection format resulting in more enumeration than drill-down. However, this had the benefit of providing a larger and more representative inventory of needs. Some patterns were readily apparent.

Activities and needs identified through the inventory could be grouped according to similarities and differences in inputs and outputs, workflow and resources, and goals. These patterns were used to define a preliminary typology of ten (10) business process types summarized in *Appendix B, Process Type Definitions* and enumerated here:

- Alerts
- Application Access
- Access to Reference Documents
- Inspections & Audits
- Instant Messaging
- Inventory Management
- Mail & Schedule Access
- Notifications
- Access to “Remote Field Sensing” Data
- Surveys

This list was subsequently extended to include two (2) additional categories, *Information Access* and *Service Requests* as a result of the use case and dependency analysis. Additionally, some process titles were renamed and regrouped (see below).

3.1.2 Quantitative Analysis⁴

The following section summarizes results of a quantitative analysis of session participation, scenario status, priority, and departmental distribution of needs.

3.1.2.1 Participation

Twenty-five (25) individuals participated in the two different sessions, twenty (20) representing State of Ohio Departments. The first session was roughly twice as large as the second and justified the division into two separate working groups.

Participating departments were well-represented with a range of internal agencies and working groups (e.g., IT) as was the case for OIT, DOC, DPS, or by sending fewer but very knowledgeable parties as did ODH, DOD, and DNR.

3.1.2.2 Status

Participants readily identified a range of mobile/wireless applications for a total of sixty-seven (67) such processes or activities. Of these, the majority (76%) were envisioned, while a minority (15%) were planned, or in some current state of deployment (10%). DPS cited the greatest number of potential applications (20), followed by DNR (14), ODH (13), OIT (11), DOC (6), and DOD (3).

3.1.2.3 Priority

Priority was slightly skewed from high (27%) to intermediate (36%) and low (37%) priority. Priority was an assignment relative to each department. Where this measure was in question or not explicitly defined by department representatives, priority was assigned according to a rule proposed by DNR:

- High priority to activities involving public safety
- Intermediate priority to those enabling communication and scheduling
- Low priority for enabling processes currently supported via paper processes

⁴ This is a summary of material released earlier, entitled *State of Ohio, Mobile Transaction Gate: JAD Summary*.

3.1.2.4 Distribution

Figure 1 provides a tabular break-down of scenarios by process type by department. The chart depicts the relative prominence of each process type or category, as well as the degree to which that process type is pertinent to a given department and the set of all participating departments.

Figure 1 Distribution of Scenarios by ProcessType by Department

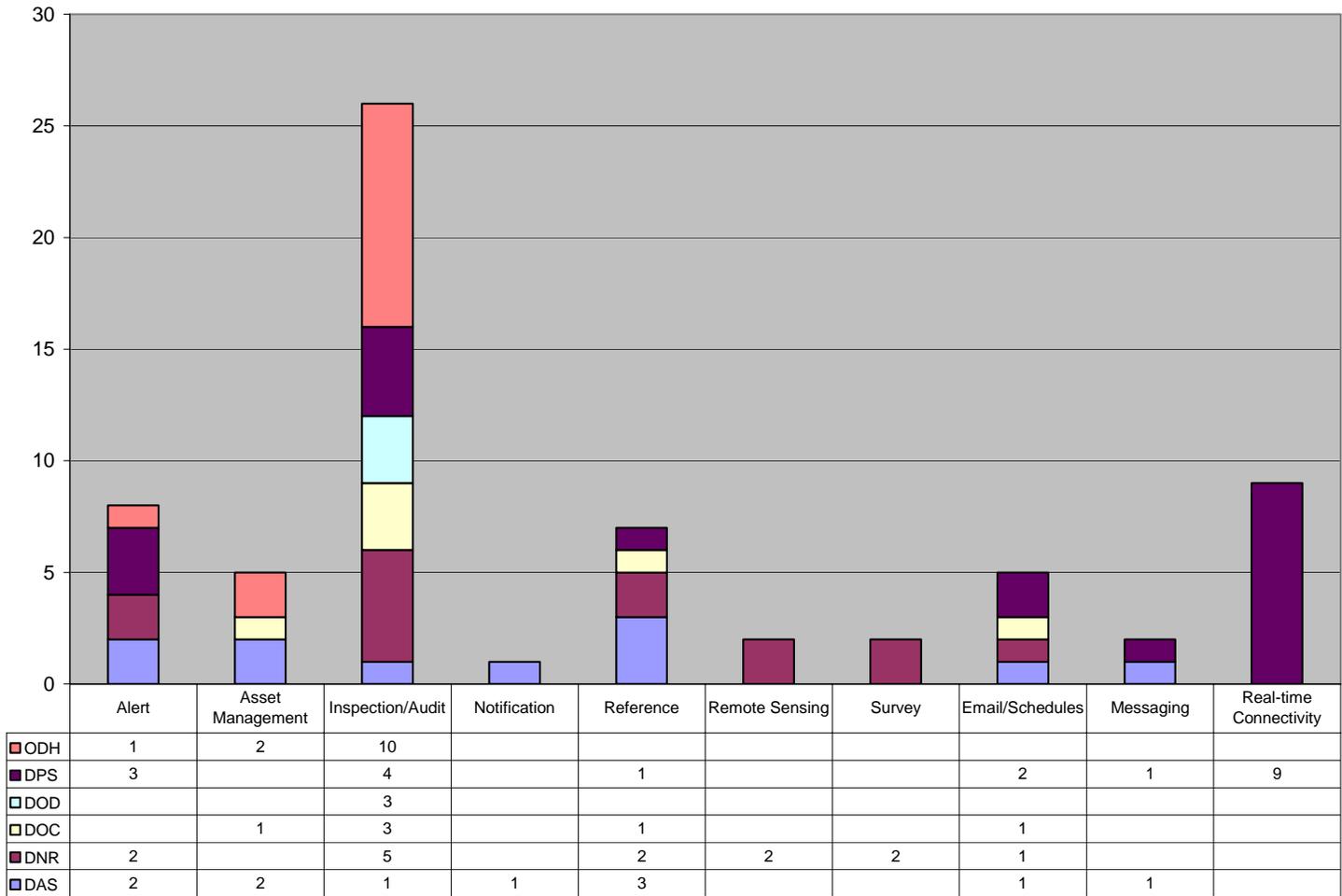


Table 1. Process Type Frequency	
Type	Total
Inspection/Audit	38.81%
Real-time Connectivity	13.43%
Alerts	11.94%
Reference	10.45%
Asset Management	7.46%
Email/Schedules	7.46%
Remote Sensing	2.99%
Survey	2.99%
Messaging	2.99%
Notification	1.49%
Grand Total	100.00%

- *Inspection/Audit* is the most prominent process type (38%), and the most common. It is an activity that cuts across all departments, accounting for as many as ten applications (ODH). There was an average of 4.3 inspection/audit processes identified per department during these sessions.⁵
- *Real-time connectivity* is the next most prominent category (13%), but based on the information collected in these sessions, and this preliminary analysis, it applies chiefly to DPS.⁶
- *Alerts* account for 12% of the total and were mentioned by 4 of 6 departments in the context of public safety or the support of DPS infrastructure.
- *Reference*, or information access, accounts for 10% of mentions by four departments and was frequently cited as an adjunct to *Inspection/Audit* processes.
- *Asset Management* and *Email/Schedules*, two adjunct mobile work enablers, have next most frequent mention (both approx. 7%).
- The more specialized requirements and limited (but critical) applications for *Remote Sensing*, *Surveys*, and *Messaging* follow (all at 3%).

- The *Notification* class was least mentioned, but this is likely due to the minimal representation of citizen-consumer representation in these meetings, and the fact that, the strong representation of the mobile workforce allocated such communication to *Email* or *Messaging*.

3.2 Use Case Modeling

Use case models were built for each of the ten (10) preliminary business process types. The modeling procedures of identifying the actors and enumerating system uses resulted in refinement and extension of the types and packaging of common functionality for dependency analysis.

3.2.1 Variants

Additional variants of the preliminary business process types were identified or reorganized as follows:

⁵ In other words, this was the information obtained in these sessions, and we don't have the sampling power to generalize beyond our data set. See 2.5, *Qualifications*.

⁶ Viewed at an infrastructure level, *Alerts* and *Messaging* assume real-time connectivity as well, but our categories are also distinguished by requirements such as synchronous vs. asynchronous communication.

- *Information Access*, defined as the need to transform Web content to be suitable for the processing capabilities, form-factors, and protocols of wireless handheld devices was identified as a necessary adjunct to application access for the same devices.
- *Service Requests*, a variant of Electronic Data Collection round-trip forms completion and submission, was identified after inspection of the Ohio.gov web portal and interviews with Digital Ohio.
- *Inventory Management, Surveys, and Field-Sensing* were recognized to be variants of *Electronic Data Collection*.
- *Alerts, Instant Messaging, Mail & Schedules, and Notifications* were grouped and categorized as *Communication Services*.
- The need for soft-copy reference material in the line of work, both on and off-line, was re-labeled *Document Portability and Management*.

3.2.2 Packages

This revised set of thirteen (13) different process types was assigned to five (5) logical groupings or packages with definitions and breakdowns expressed as high-level business needs as follows:

1.1 Information Access

Provide web content via the Internet, enterprise network, and their wireless extensions to the mobile workforce, business partners and citizenry as appropriate to the user/customers' role, device, and configuration via the shared services of identity management and security, personalization and **content transformation**.

1.2 Application Access

Provide on-line services via the Internet, enterprise network, and their wireless extensions to the mobile workforce, business partners and citizenry as appropriate to the user/customers' role, device, and configuration via the shared services of identity management and security, personalization, content transformation, and **remote application access delivery mechanisms**.

2.0 Communication Services

Provide communication services via the Internet, enterprise network, and their wireless extensions to the mobile workforce, business partners and citizenry as appropriate to the user/customers' role, device, and configuration via the shared services of identity management and security, personalization, content transformation with access to the following capabilities:

- Provide secure and reliable **alerts** including origination, propagation, and control capabilities to public safety and emergency management first and second responders and support organizations both within and across jurisdictions with possible extension of one-way alerting capability to citizens via wired and wirelessly enabled devices.
- Provide secure and reliable **instant messaging and chat conference** capabilities to public safety and emergency

management first and second responders and support organizations both within and across jurisdictions.

- Provide **electronic mail and schedule** access to the State mobile workforce as appropriate to role.
- Provide timely **notifications** of impending State business to business partners and citizenry on a subscription basis appropriate to the user/customers' device and configuration.

3.0 Electronic Data Collection Provide **roundtrip electronic data collection** capabilities to the mobile workforce, business partners and citizenry as appropriate to the user/customers' role, device, and configuration via the shared services of identity management and security, personalization, content transformation, document and workflow management. Specifically:

- Provide constituents with the ability to **request services** from a provider organization, via the elicitation and submission of structured data (and payments), with the issuance of receipts and/or tracking information for access to processing status.
- Provide the mobile workforce of inspectors, auditors, and caseworkers with the ability to **conduct round-trip electronic data collection and management for the range of compliance targets** such as mechanical systems, building or construction sites, service agencies, grant applicants/recipients, including support for workflow for process management.
- Provide state employees with ability to do **systems-based inventory management both on- and off-line** (with synchronization capabilities) as required by context of application (availability of network connectivity).
- Provide **automated data collection capabilities from remote field sensors**, specifically for field and stream gauges.
- Support collection of **field survey data on- or off-line** with synchronization capabilities.

4.0 Document Management Provide **document portability and management solutions** via the Internet, enterprise network, and their wireless extensions to the mobile workforce, business partners, and citizenry as appropriate to the user/customers' role, device, and configuration via the shared services of identity management and security, personalization, content transformation (where appropriate⁷), and workflow to render the following:

⁷ "Where appropriate" is an acknowledgement that the limitations of bandwidth, memory, and form factor may

- Provide the ability to obtain, consult, and manage (voluminous) state, federal, and proprietary codes, manuals, operational guidelines, and procedures in electronic formats on- or off-line.
- Support customer service through ready access to public documents, directions, instructions, and resources.
- Support the document lifecycle from inception through creation, review, redaction, storage, dissemination and destruction.

For more information, see the models and use case descriptions in *Appendix D. Use Case Models*.

3.2.3 Common Requirements

The MTG use case analysis also identified the need for various system support capabilities that can be mapped to the industry-standard domains of document management, workflow management, security services, and data transport/enterprise application integration (EAI). Requirements for these systems can similarly be grouped into packages of system requirements as follows:

5.0 Workflow	Provide capability to define, create and manage the execution of workflows through the use of software, running on one or more workflow engines, which are able to interpret process definitions, interact with workflow participants, and, where required, invoke the use of IT tools and applications [WFMC].
6.0 Security	Provide authentication and role-based access control, user administration, and policy management, auditing and reporting for privileged resources within the domain of state responsibility and control. Provide single-sign-on capabilities where appropriate and practical, and delegated administration where required.
7.0 Data Transport	Provide data staging and transport capabilities between distributed repositories for Enterprise Application Integration (EAI).

These nine (9) packages of related functionality become key inputs to the analysis of dependencies and the conceptual architecture.

3.3 Analysis of Dependencies

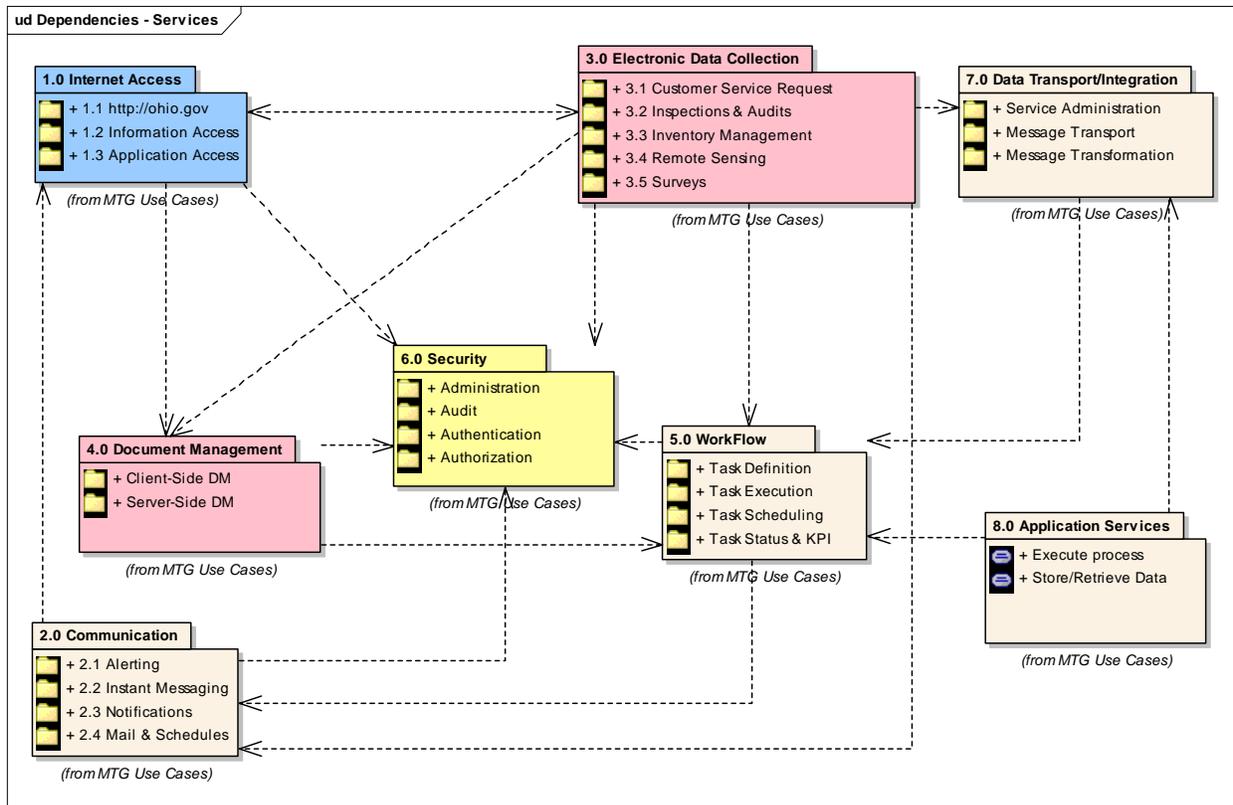
MTG business and system requirements can be put into context via use-case situation diagrams. Such diagrams capture the high-level functional dependencies between packages of MTG business needs and system support capabilities. Context diagrams and analyses of domain-specific requirements can be found in *Appendix D, Use Case Models*.

A summary of dependencies can be found in Figure 2. This is a rather coarse analysis but sufficient to indicate relationships between packages. A more granular mapping of business process requirements to

simply be insufficient to download and manage certain types of documents (i.e., cell phones do have limitations).

functional and quality requirements is available via the relationship matrix, and provided as a spreadsheet supplement.

Figure 2 – Dependencies: High-Level Business & System Requirements



3.3.4 Special Requirements

While many requirements are well-distributed and common across the range of mobile business processes, there are domains that require special consideration because of the nature of their operations and the confidentiality of their data. DPS, EMA, possibly DNR, and some ODH operations are such domains.

These are handled as variants of the use cases. Detailed requirements addressing quality attributes are cross-listed in the relationship matrix referenced in Section 4.5 as the Excel spreadsheet supplement. At a high-level, these special requirements can be summarized as follows:

1.2 Application Access

In addition to specific policy/process conformance for personnel and vendor management, and incident response, access to the DPS system, LEADS, and related law-enforcement systems, must be conformant with CJIS Security Policies including the following technical requirements:

- Anti-virus detection and protection on ALL clients
- Strong encryption

- Client-side firewalls and standardized configurations
- Limitations on Internet and third-party access
- Stringent logging
- Auditable documentation to a standard
- Federal identity management
- Password and account Management
- Auditable network monitoring

2.1 Alerts

2.2 Instant Messaging

Public safety and emergency management alerts and instant messaging capabilities require similarly stringent requirements along the following lines:

- Private networks
- Two-factor authentication
- Role-based access controls (RBAC)
- Message Integrity
- DHS conformant audit trails

4.0 REQUIREMENTS

4.1 Organization

Requirements in the following sections describe the range of functionality for the process types identified from the interview sessions, as supplemented with government and industry requirements, necessarily or typically applied in standards-based solutions.

Section 4.4, Business Process Requirements -- provides an enumeration by process type and variant. These are grouped by package (see *Packages 3.2.2*), and identify the business purpose, constituency, business and high-level requirements, and input scenarios for the following:

1. Internet Access

- 1.1. Information Access
 - 1.1.1. Deliver web content (provided today)
 - 1.1.1.1. Via Wireless Extension
 - 1.1.2. Deliver secure web content (provided today)
 - 1.1.2.1. Via Secure Wireless Extension
- 1.2. Application Access
 - 1.2.1. Deliver Native Wireless Applications
 - 1.2.2. Deliver Terminal Services Applications

2. Communication Services

- 2.1. Alerts
 - 2.1.1. Provide Alerts for Emergency Management and Public Safety
 - 2.1.2. Forward Alerts to Citizens
- 2.2. Secure Instant Messaging
- 2.3. Notifications (subscription-based)
 - 2.3.1. Via Email
 - 2.3.2. Via Text Messaging
- 2.4. Mail and Schedule Services

3. Electronic Data Collection

- 3.1. Service Requests
- 3.2. Inspections & Audits
- 3.3. Inventory Management
- 3.4. Remote Sensing
- 3.5. Surveys

4. Document Portability and Management

- 4.1. On-line
- 4.2. Off-line

Section 4.5, Relationship Matrix -- Cross-lists the business process requirements against a range of system requirements and quality attributes derived from applicable industry, federal, and state standards (with references) arranged by category, type, and sub-type. This taxonomy has been inherited from the SAFECOM, Version 1.0, March 2004 as follows:

Table 2. Categories, Types, and Sub-types

Category	Type	Sub-type
Features	Backwards Compatibility	
	Call-Types	Multi-cast Communication Streams
	Device	Form Factor Function Hardware Mobility Network Interface Protocol Software Type
	CCMO	Maintenance and Operations CC Provisioning Communication Prioritization
	COTS Based Products	
	Extensibility	System-wide revision and enhancement
	Migration Path	
	Mobility	User Motion
	Modularity	Component Feature Add-on
	Scalability	Vertical Scaling Horizontal Scaling
	Security	Access Control Privacy Integrity

		Monitoring
		Attack Detection and Prevention
	Spectrum and Network	Allow for greater extensibility and scalability
	Standards-based design	
Performance	QoS	
	Restorability	
	Survivability	
Service	Data	Interactive
		Non-Interactive

4.1.1 Template Structure

4.1.1.1 Business Process Requirements

High-level requirements of Section 4.4 are organized according to business process types as listed in *Section 4.1, Organization*, and are structured by the following template:

Purpose:	Describes the purpose of the business process type.
Constituents:	Identifies users
Business Requirements:	Summarizes overarching business requirement and high-level functional requirements.
Functional Specification:	References use cases as defined in the appendix.
Scenarios:	Identifies scenarios that map to the generalized business process requirements.
Issues/Notes:	Enumerates notes and issues.

4.1.1.2 Requirements Mapping

A mapping between business functional and system requirements, especially quality attributes (“-ilities”), is provided as a supplemental spreadsheet.

The workbook provides a cross-listing between requirements (e.g., functional vs. security) in a format that supports filtering by attribute. This format was chosen to make an unwieldy amount of data more usable, and is structured using the following layout.

- ID - Each requirement is given a unique identification number in the form #####.

- Types - System requirements and quality attributes are arranged by various categories, super- and sub-types per Section 4.1.
- Source and Source ID - Many of the requirements were derived from documented sources as discussed in section 1.5, Sources. The Source column shows an ID for the source document. The Source ID column shows the requirement number used for the requirement in that source document. Requirements that were derived from MTG interviews have no entries in these columns.
- Requirement Description - This is a statement of the requirement/capability/constraint to be applied.
- Additional Notes – Are appended as required for clarification or where supplied in an original reference.
- Business Process Mapping – These columns list the business process requirements in a series of columns. An “R” is placed in the column for each capability or constraint that applies. An “O” is used where the requirement is optional. A cell is left blank where the requirement is inapplicable.

4.2 Application

The requirements in this document describe a range of business process needs of mobile Ohio. In such a broadly defined context, specific agencies and offices will have varying requirements based on their mandates and compliance issues. The breakdown of process types into variants addresses this in part. The mapping to system requirements and quality attributes as required or optional provides additional flexibility in determining the scope of requirements for a given application.

Not all requirements will be mandatory for every department or agency process. This document describes the range of capabilities to be supported and does not discuss their application on per instance/scenario. The spreadsheet tool does assist in such applications, however, and can be applied as a template to such cases. The requirements can be filtered on any of the listed criteria to form a template to be applied to the evaluation of any additional process types, individual scenarios, or vendor solutions.

4.3 Assumptions

The following general assumptions have been made for the definition of the MTG requirements assessment and architecture:

1. Wireless networking capability is provided through a network-of-networks including both commercial and proprietary implementations managed through OIT (directly or indirectly).
2. Wireless network services, per se, are beyond the scope of this deliverable, and are being addressed through ongoing activities of OIT Service Delivery to select vendors and negotiate contractual agreements.
3. The requirements must provide guidance for these processes which can be used by the sponsor when evaluating wireless capabilities.
4. Common services and infrastructure will provide greater scalability, flexibility, reliability, disaster-recovery, re-usability, and cost savings for customers
5. In line with various State initiatives, MTG recommendations assume a consolidated and centralized computing infrastructure for enterprise shared services.

6. As patterned activities generalized from the data set of sixty-seven processes identified in the JAD sessions, the process-types are sufficiently representative to provide a valid (though not necessarily exhaustive) set of requirements
7. In the case of MTG, the focus is limited to data transmission/management capabilities. Voice requirements have been excluded from the analysis.

4.4 Functional Requirements

1.0 Internet Access

This section describes the generalized functional variants to deliver web-content and on-line services with extensions for wireless and mobile access. See 4.5, Requirements Mapping for details.

1.1 Information Access

Purpose: Supports the State's commitment to deliver information and services to citizens, business partners and employees in line with e-government initiatives.

Constituents:

- Citizens
- Business Partners and clients
- State Employees
- Special Interest Groups

Business Requirements:

Provide web content via the Internet, enterprise network, and their wireless extensions to the mobile workforce, business partners, and citizenry as appropriate to the user/customers' role, device, and configuration via the shared services of identity management and security, personalization and **content transformation**.

This high-level business requirement has the following functional variants:

1.1.1 Deliver Web Content (provided today)

Provide web content via the Internet or enterprise network to the mobile workforce, business partners, and citizenry.

1.1.1.1 Deliver Web Content to Wireless Devices

Extends the delivery of web content to wireless devices adjusting display formats for client device form factors.

1.1.2 Deliver Secured Web Content

Deliver web content securely as appropriate to the user/customers role, device, and configuration via

the shared services of identity management and security, personalization, requiring authentication, role-based access control, and encryption of content.

1.1.2.1 Deliver Secured Web Content to Wireless Devices

Extends the delivery of web content to wireless devices securely as appropriate to the user/customers role, device, and configuration via the shared services of identity management and security, personalization, requiring authentication, role-based access control, and encryption of content.

Functional Specification: See *Appendix D, Use Case Models*.

Scenarios: ▪ Access to portal/portal content

Issues/Notes: 1. While access to web content and secure web content is delivered today, wireless access in a form amenable to wireless devices is only available in limited ways.

1.2 Application Access

Purpose: Supports the State's commitment to deliver on-line services to citizens, business partners and employees in line with e-government initiatives, and the needs of public safety and emergency management via real-time network connectivity.

Constituents: ▪ Citizens

 ▪ Business Partners and clients

 ▪ State Employees

 ▪ Special Interest Groups

Business Requirements:

Provide on-line services via the Internet, enterprise network, and their wireless extensions to the mobile workforce, business partners and citizenry as appropriate to the user/customers role, device, and configuration via the shared services of identity management and security, personalization, **content transformation** or **suitable mark-up language**, and **remote application access delivery mechanisms**.

This high-level business requirement has the following functional variants:

1.2.1 Deliver On-line Services

Provide on-line services via the Internet and enterprise network to the mobile workforce, business partners and citizenry via **remote application access delivery mechanisms appropriate to the application architecture (web applications, WTS, web-to-host, etc.)**.

1.2.1.1 Deliver On-line Services to Wireless Devices

Extend the delivery of on-line services to wireless devices adjusting display formats for client device form factors, device and protocol capabilities.

1.2.2 Deliver Secured On-line Services

Deliver on-line services securely as appropriate to the user/customers role, device, and configuration via the shared services of identity management and security, personalization, requiring authentication, role-based access control, and encryption of content.

N.B. -- In particular, enable DPS/EMA users to maintain persistent connections for synchronous communication with critical applications from the field via strongly encrypted virtual private networks. See 4.5. Requirements Mapping.

1.2.2.1 Deliver Secured On-line Services to Wireless Devices

Extend the delivery of on-line services to wireless devices securely as appropriate to the user/customers role, device, and configuration via the shared services of identity management and security, personalization, requiring authentication, role-based access control, and encryption of content

Functional Specification: See *Appendix D, Use Case Models.*

- Scenarios:**
- Access to Crash Reporting
 - Access to LEADS Application
 - Access to LRMS
 - Camp reservation System Access
 - Digital image Upload Capability
 - Disaster Damage Assessment
 - Disaster Incident Response
 - Field Device Software Maintenance
 - Mobile Disaster Field Office Connectivity
 - Upload Traffic Citations

- Issues/Notes:**
1. While the request to support mobile access to web came specifically from DPS/EMA to support dispatchers, first responders, law enforcement access to LEADS and related web-based applications, the capability to provide mobile access to web content, applications, electronic documents and forms, and web services is one that can be put to use for all constituents, albeit, with different security requirements (e.g., DPS requires AES compliant VPN for access).

2.0 Communication Services

This section describes the generalized functional variants for requested communication services with extensions for wireless and mobile access. See 4.5, Requirements Mapping for details. In general:

Provide communication services via the Internet, enterprise network, and their wireless extensions to the mobile workforce, business partners and citizenry as appropriate to the user/customers' role, device, and configuration via the shared services of identity management and security, personalization, content transformation with access to the following capabilities.

This high-level business requirement has the following functional variants:

2.1 Alerts

2.1.1 Alerts for Emergency Management and Public Safety

Purpose: Supports the Federal and State government's commitment to public safety and emergency management by facilitating awareness of alerts to agency first-responders, second-responders, support groups. Includes the ability to broadcast or multicast event-driven, time-sensitive, information of an emergency nature (Alerts). Examples include DHS and EMA alerts.

- Constituents:**
- First Responders
 - Secondary Responders
 - Support Organizations
 - Upstream Alerting Systems (e.g., EAS)
 - Downstream Alerting Systems (e.g., public broadcast channels)

Business Requirements: **2.1.1.1 Provide secure alerts to first, and second responders and supporting organizations**

Provide the capability to securely and reliably originate, propagate, and control alerts for public safety and emergency management first and second responders and support organizations within and across jurisdictions via a digital format that is standards-compliant.

Functional Specification: See *Appendix D, Use Case Models*.

Constraints: See 4.5, *Requirements Mapping*

Issues/Notes:

1. As defined by the customer, the scope of “Alerts” has been limited to:
 - a. Alert origination, propagation, and management
 - b. An adjunct need for collaborative messaging in the context of incident management

N.B. -- The reality of vendor offerings typically incorporates (usually as a suite) a broader range of capabilities including:

- c. Computer-Aided Dispatch (CAD),
 - d. Overlay of GIS data, incident and
 - e. Resource plotting and status
2. The majority of these capabilities at the State level in Ohio are provided by a combination of LEADS, JREIS, and ATIXS. Since specifying a comprehensive DPS incident/emergency management package was not part of the charter, MTG requirements are limited to (a) and (b).
3. Note that the process-type, *Notifications* addresses the sending of non-emergency notices to users on a subscription basis.
4. What restrictions need to be imposed on the forwarding of messages?
5. Possibility of more comprehensive changes in tool suite motivated by DNR.

Scenarios:

- Amber Alerts
- Bio-Terrorism Response System
- Emergency Notification
- Homeland Security Alerts
- Lost Visitor/Child Locator/Information Service
- Public Safety Alert
- Stream-Gauge Alert System
- Weather Alerts

2.1.1 Forward Alerts to Citizens

Purpose:

Provide the capability to send and manage alerts to citizens via a digital format that is standards-compliant and deliverable to wired and wirelessly enabled devices.

Constituents:	<ul style="list-style-type: none"> ▪ Citizens
Business Requirements:	<ol style="list-style-type: none"> 1. Extend one-way alerting capabilities to citizens via wired and wirelessly enabled devices. Must include security controls and recall of false alarms.
Functional Specification:	See <i>Appendix D, Use Case Models</i> .
Constraints:	See 4.5, <i>Requirements Mapping</i>
Issues/Notes:	<ol style="list-style-type: none"> 1. Alerts for citizens are defined as an optional extension of public safety/emergency management alerting capabilities. 2. Digital Ohio representatives have expressed concerns regarding public broadcasting of un-requested alerts and ensuing disruption, irritation, and panic in daily life. 3. The process-type, <i>Notifications</i> addresses the sending of non-emergency notices to users on a subscription basis. 4. Propagation of alerts to citizens via mobile and wireless capability is limited to the penetration of mobile and wireless infrastructure in the general population, (the point being that broadcasting through traditional channels may be more effective). 5. In the event of a real disaster, encryption of true alerts is a mute point (though one would say that of incident management messaging), so no encryption is required for broadcast alerts from distributors to citizens.
Scenarios:	<p>Alerts and subscriptions for the general public remain to be differentiated with the following list providing some examples:</p> <ul style="list-style-type: none"> ▪ Amber Alerts ▪ School Closures ▪ NOAA Alerts ▪ FEMA Alerts ▪ Rolling Blackouts ▪ Road Closures ▪ DHS/Security Alerts

2.2 Instant Messaging

Purpose: Supports intra- and inter-jurisdictional public safety and emergency management agency collaboration via presence and instant messaging protocol with extensions for wireless text messaging capabilities, particularly via enabled MCTs or handheld devices as an adjunct to real-time alerts (DHS, flood, and Amber alerts).

Constituents:

- First Responders
- Secondary Responders
- Support Organizations

Business Requirements:

2.2.1 Provide secure instant messaging

Provide secure and reliable **instant messaging** capabilities to public safety and emergency management first and second responders and members of support organizations to communicate with each other individually in real-time both within and across jurisdictions.

2.2.2 Provide secure group conference capabilities

Extend secure and reliable instant messaging capabilities to public safety and emergency management first and second responders and members of support organizations to communicate with multiple individuals in real-time (chat) both within and across jurisdictions.

2.2.3 Provide a presence service

Provide the ability to detect whether other users are online and whether or not they are available (presence).

Functional Specification:

See *Appendix D, Use Case Models*.

Constraints:

See 4.5, *Requirements Mapping*

Issues/Notes:

1. EMA currently uses ATIXS for chat conferencing
2. This request for collaborative messaging is limited to the domain of emergency and incident management. The scope of architectural recommendations is therefore limited to this domain. Recommendations do NOT include those for the enterprise as a whole.
3. Given this limited scope, the shared (and more stringent) operational and security requirements of this domain, and the bundling of alerting and instant messaging capabilities in vendor offerings, the architectural recommendations for Alerts and Instant Messaging will be addressed jointly.

- Scenarios:**
- Real-time Conferencing
 - Suspicious Activity Report

2.3 Notifications

Purpose: Supports a public service where employees/citizens may be notified of pending business obligations or opportunities with the State via email or mobile messaging on a subscription basis. Distinguished from an alert as non-emergency in nature.

- Constituents:**
- Citizens
 - Business Partners
 - Employees

Business Requirements:

2.3.1 Provide subscription based notifications

Provide a service where citizens, business partners, and employees may subscribe to and manage notifications of pending business obligations or opportunities with the State.

2.3.1.1 Provide subscription based notifications via email

Provide these notifications as an email to a customer's email account.

N.B. -- The notification may be sent via email where the subscriber provides an email account.

2.3.1.2 Provide subscription based notifications via messaging

Provide these notifications as a text message to a customer's wireless account.

N.B. The notification may be sent via messaging where the subscriber is properly enabled with an appropriate mobile device and wireless service, or desktop messaging client and the subscriber provides a forwarding address.

Functional Specification: See *Appendix D, Use Case Models*.

Constraints: See 4.5, *Requirements Mapping*

- Issues/Notes:**
1. Support non-emergency notifications only.
 2. Network and mail services of the client are supplied by the end-user.
 3. This is assumed to be a Web-based service as no requirements were

specified for support of Interactive Voice Response (IVR).

4. Communications are one-way unicast via email or text messaging by subscription. No confirmation of delivery to the host is required.
5. Client applications will be (re)tooled to create a mail with supporting links/attachments to fulfill the notification process and leverage the common service.
6. N. B. -- Notifications are distinguished from “alerts”, by their non-emergency nature, and the fact that, they are subscription services. Digital Ohio representatives have expressed concerns regarding public broadcasting of un-requested messages and possible ensuing disruption, irritation, and panic in daily life. A subscription list remains to be determined (see Issues).
7. Can we assume that a better way to do this is to consolidate services on the portal under user profile?
8. What services other than license and registration renewal should be targeted?

Scenarios: ▪ License/Registration Renewals

2.4 Mail and Schedule Services

Purpose: In support of efficient workforce management, provide email and schedule access/capabilities as an adjunct service to support the work-distribution requirements and schedule adjustments for inspections, audits, and other field-based work activities.

Constituents: ▪ State Employees

Business Requirements: **2.4 Provide remote access to electronic mail and schedules for State Employees**

Provide the state mobile workforce with mobile access **to electronic mail and schedules** as appropriate to role.

Functional Specification: See *Appendix D, Use Case Models*.

Constraints: See 4.5, *Requirements Mapping*

Issues/Notes: 1. Respondent’s mention of mail and scheduling services in the JAD sessions for work-distribution requirements and schedule adjustments for inspections, audits, and other field-based work activities indicates a more fundamental need for workflow in these areas. This need is addressed under in 6.0, Electronic Document Collection.

2. Services should be standardized based on email consolidation project.

Scenarios:

- Facilitate DNR work processes.
- Facilitate DOC work processing and scheduling.
- Adjunct support for MCTs.
- Alternate route to mail for under-served BMV offices.
- Outlook Mobile Access

3.0 Electronic Data Collection

This section describes the generalized functional variants for electronic data collection services with extensions for wireless and mobile access. See 4.5, Requirements Mapping for details. The high-level requirement is to:

Provide **roundtrip electronic data collection** capabilities via the Internet, enterprise network, and their wireless extensions to the mobile workforce, business partners and citizenry as appropriate to the user/customers' role, device, and configuration via the shared services of identity management and security, personalization, content transformation, document and workflow management.

This category includes five (5) variants described in the sections below, all of which involve a general model of locating and obtaining a template, optionally provisioned with data of record, which is then completed in either on-line or off-line mode, and then submitted for further processing and fulfillment of a task request by a service or human resources.

This high-level business requirement has the following functional variants:

3.1 Service Requests

Purpose: As part of the State's offering of "Service to Citizens" provide "round-trip" electronically enabled service requests to meet the needs of citizen and business constituents.

Constituents:

- Citizens
- Business Clients and Partners

Business Requirements: **3.1 Request Services**

Provide users with the capability to request services from a provider organization, via the submission of forms data (and payments), with the issuance of receipts and tracking information as required.

Functional Specification: See *Appendix D, Use Case Models*.

- Constraints:** See 4.5, *Requirements Mapping*
- Issues/Notes:**
1. This is a candidate for support via a document management solution as forms, whether templates or completed instances, must be searched, managed, and archived.
 2. This is a ready candidate for workflow as completed and submitted forms must be routed, tracked and managed through service fulfillment process from start to finish.
- Scenarios:**
- Any ohio.gov forms based service request (dozens).

3.2 Inspections & Audits

Purpose: Supports the State’s responsibility to monitor environmental, workplace, building, vehicle, and industrial device compliance to safety and other operational or fiduciary standards such as program or grant service via field inspection activities that have been identified as necessary, numerous, and geographically distributed.

- Constituents:**
- State employee mobile field service personnel
 - Mobile field service support staff

Business Requirements: **3.2 Inspections and Audits**

Provide the mobile workforce of inspectors, auditors, and caseworkers with the ability to conduct round-trip electronic data collection and management for the range of compliance targets such as mechanical systems, building or construction sites, service agencies, grant applicants/recipients, including support for workflow for process management.

Enable a mobile field staff employee to be able to:

3.2.1 (Securely) obtain an inspection form or ticket that is generated according to a schedule including vital data (identifier, location, evaluation criteria, inspection history, etc.) for a specific inspection, audit, or compliance target.

3.2.3 Collect inspection/audit/compliance data electronically via a mobile device, including the ability to modify and save both closed and open-ended data via a standard template and/or procedure, either on or off-line.

3.2.3 Manage the incomplete and complete forms for correctness, efficiency, and convenience, both on and off-line including the ability to find a form, search the form, navigate among and within forms, and save or delete forms.

3.2.4 Where required, provide the customer with a receipt of completion, either:

3.2.4.1 Electronically, where a network connection enables a receipt to be routed to the email address of a responsible party of the client organization, (possibly upon submission of the completed report)

3.2.4.2 Via a pre-printed acknowledgement that is signed and dated by the inspector upon completion of the site visit

3.2.4.3 Via dynamically generated receipt that is printed on-demand, via a printing facility that generates such acknowledgements for U.S. mail to the client

Additionally, the system must support:

3.2.5 Routing the inspection/audit/compliance through the proper chain of supervision for the capture of approvals/disapprovals and the chain of rework.

3.2.6 Tracking of the workflow (processing status)

3.2.7 Generating a compliance certificates for completed and approved inspections/audits as softcopy for email to the client and/or paper certificate format for U.S. Mail delivery to the client as required for legal compliance.

Functional Specification:

See *Appendix D, Use Case Models*.

Constraints:

See 4.5, *Requirements Mapping*

Issues/Notes:

1. DOC has expressed a preference for tablet PCs. Work-styles require a larger format, store and forward device, for field deployment. Tablets offer the ideal footprint, however, such devices are currently costly (\$1300 to \$3400).
2. Many inspectors work from their homes throughout the state and only periodically check into regional offices limiting the cost savings of pooled devices.

Scenarios:

- Asbestos Inspection
- Blood-alcohol Testing
- Dam Safety Inspection
- Elevator Inspection
- Fire Code Enforcement

- Gas and Oil-Well Safety Inspection
- Grant Compliance Enforcement
- Grant Compliance Enforcement (Via SPESS)
- Grant Eligibility
- Ground-Water and Well Safety Inspection
- Household Energy Inspection
- Labor and Safety Inspection
- Lead Inspection
- Liquor License Enforcement
- MARCS Trouble/Service Management
- Mine Safety Inspection
- Mobile Driver Examinations
- Nuclear Inspection
- Nursing Home Complaints
- Nursing Home Inspection
- Pollution Incident Reporting & Assessment
- Radon Inspection
- STD Monitoring
- Title Inspections
- Vehicle Safety Inspections
- X-Ray Inspection Program

3.3 Inventory Management

Purpose: Supports the State's responsibility to analyze current and projected asset conditions and to evaluate economic trade-offs among alternative investment options for cost-effective investment decisions and public service/safety through the collection or verification of the existence, type, number and condition of assets in a place of storage or deployment. Examples include inventory, fleet, and vaccine management.

- Constituents:**
- Field service technicians
 - Warehouseman
 - Facility administrator
 - Fleet administrator

Business Requirements:

3.3 Inventory Management

Provide state employees with ability to do systems-based inventory management -- to collect or verify the existence, type, number and condition of an asset from a place of storage or deployment (e.g., warehouse or field) for a predefined set of attributes (via a template) -- both on- and off-line (with synchronization capabilities) as required by context (availability of network connectivity).

3.3.1 On-line via remote applications access

Must support real-time assessment of inventory stockpiles.

N.B. May be completed on-line via thin-client application access where network connectivity is available.

3.3.2 Off-line applications with synchronization capabilities

Must support off-line capabilities for certain variants via electronic data collection due to network (un)availability.

N.B. May be completed off-line using the electronic data collection.

Functional Specification:

See *Appendix D, Use Case Models*.

Constraints:

See 4.5, *Requirements Mapping*

Issues/Notes:

1. The inventory processes can be supported by three different architectures depending on context of application and the nature of the inventory application:
 - a. This is another form of electronic data collection, but with the difference that the context of application is more likely to support access to (near) real-time inventory tools and repositories via the state network as extended by wireless access points deployed to data centers, and other sites that warehouse state assets such as lots, garages, and yards. The principal driver here is the device used in the data collection, and whether it can support the native application client, or some intermediary such as an ICA thin- or thick-clients, or RDP clients.
 - b. Where locations are not linked to the state network directly, but

are within the range of wireless internet access, thin- or thick-clients could be used to connect to the web-enabled interfaces of inventory applications, or client server applications enabled via web-to-host or Windows Terminal Services solutions across HTTP/S as required. The recommendation for this variant, then, is for portal-based application access (for centralization of control) via WTS and similar tools depending on the nature of the application.

- c. A third variant is similar to that of inspection and audits, where no network connectivity can be assumed and all information may need to be connected in off-line mode. Data is synchronized between the device and the repository when connectivity can be established. The architecture in these cases is similar to that of electronic forms, where previous inventory data can be populated into inventory check lists, and downloaded to the client prior to the site visit.
1. Per Dan Orr, the State is currently in the process of defining requirements for the “mother-of-all inventory systems.” Any solution probably needs to be commensurate with this initiative.
 2. MARCS has stated the intention to extend their existing trouble management implementation, a Remedy application, to handle MARCS inventory requirements. This could be a good candidate for WTS via commercial wireless.

Scenarios:

- Communication Equipment Inventory
- Expense Reimbursement
- Hardware Inventory
- Inventory Synchronization
- SNS Stockpile Management

3.4 Remote Sensing

Purpose:

In support of public safety, emergency forecasting and management, requires remote sensing capabilities to obtain data collected by devices deployed in the field on a periodic or ad hoc basis, where such data is a necessary input to downstream processes used in event and disaster prediction, notification, and control. Applications include stream and rain gauges.

Constituents:

- DNR
- EMA
- Downstream alerting systems

Business Requirements:

3.4 Remote Sensing

Provide the capability to transmit rain and stream gauge data to aggregation and analysis systems over existing proprietary or commercial wireless networks as available

Functional Specification:

See *Appendix D, Use Case Models*.

Constraints:

See 4.5, *Requirements Mapping*

Issues/Notes:

1. Existing networks leverage a patchwork of RF, microwave, and satellite communication systems, both public and private.
2. Given the existence of IFLOWS/AFWS (<http://www.afws.net/>), and USGA (<http://waterdata.usgs.gov/oh/nwis/rt>) field sensor networks, data aggregation and analysis, and presentation capabilities today, a clarification of the requirement was sought from both DNR and EMA contacts without response. The following questions were posed:
 1. Is the present deployment of rain and flood gauges sufficient in number and distribution to support relevant data collection for emergency management purposes (flood prediction and control)? If number and distribution are inadequate, how so? [Client Distribution and Coverage]
 2. Is the present deployment of rain and flood gauges sufficient in kind, that is, to what degree (a percentage) are these capable of real-time data transmission? What percent are based on manual data collection? [Client Suitability]
 3. To what extent is the need for real-time reporting from rain and flood gauges a result of inadequacies in wireless/radio network capabilities? How can we characterize the existing network of real-time enabled devices? [Network Capability]
 4. To what extent (if any) does the Ohio EMA utilize IFLOWS/AFWS (or other) flood forecasting service and software? [Application Services] Is the real-time station reporting on their portal utilized in any systemic way?
 5. What issues are preventing or delaying further integration and federation with a NWS model for flood alerting and disaster prevention in Ohio?
 6. Are AFWS and STORMS adequate to the needs of weather condition/flood alerting and disaster prevention in Ohio? What suggestions would be made for their improvement?

Scenarios:

- Rain-Gauge Notification System

- Stream-Gauge Notification System

3.5 Surveys

Purpose: In support of natural resources management and the delivery of social and transportation services, facilitates the data collection of physical or population characteristics of natural or built environments according to coordinate location, correlated features, cartographic or collateral data. Examples include geological, wildlife, and environmental surveys and transportation studies.

- Constituents:**
- DNR
 - USGS
 - ODOT

Business Requirements: **3.5 Surveys**

Enable a surveyor to collect field data, down-load, or up-load data for mapping overlays including GIS data.

3.5.1 On-line

Support collection of **field survey data on-line via remote applications access.**

3.5.2 Off-line

Support collection of **field survey data off-line** with data synchronization capabilities.

Functional Specification: See *Appendix D, Use Case Models.*

Constraints: See 4.5, *Requirements Mapping*

Issues/Notes: 1. Insufficient requirements from the client. DNR has proposed a vendor solution.

- Scenarios:**
- Field and Stream Data Collection
 - Land Surveys

4.0 Document Management

Definition/Purpose: Supports citizen, business, and state-employee needs to obtain, consult, and manage (sometimes voluminous) state, federal, and proprietary codes, manuals, operational guidelines, and procedures in electronic formats.

Supports customer service through ready access to public documents, directions, instructions, and resources.

- Constituents:**
- Citizens
 - Business Partners and clients
 - State Employees
 - Special Interest Groups

Business Requirements:

4.0 Document Management

Provide **document portability and management solutions** via the Internet, enterprise network, and their wireless extensions to the mobile workforce, business partners, and citizenry as appropriate to the user/customers' role, device, and configuration via the shared services of identity management and security, personalization, content transformation (where appropriate⁸), and workflow.

This high-level business requirement has the following functional variants:

4.1 Provide Access to Documents

Provide the ability to locate and obtain (download), state, federal, and proprietary codes, manuals, operational guidelines, and procedures in electronic formats.

4.1.1 Provide Secure Access to Documents

Limit the ability to locate and obtain, state, federal, and proprietary documents of sensitive nature via appropriate access control, authentication of requestors, and (appropriate levels) of encryption in transit.

4.2 Provide Document Management

Provide the ability to consult and manage (voluminous) state, federal, and proprietary codes, manuals, operational guidelines, and procedures in

⁸ Where appropriate is an acknowledgement that the limitations of bandwidth, memory, and form-factor may simply be insufficient to download and manage certain types of documents (i.e., cell-phones do have limitations).

electronic formats.

4.2.1 On-line

Documents may be read directly from websites via browser, or where properly enabled, a micro-browser on a handheld device, and book-marked for future reference.

4.2.2 Locally

Documents may be downloaded from a site to a local document cache, viewed, navigated, and book-marked, or even annotated with a locally installed electronic document reader. Optionally support automatic updating of locally stored documents.

4.3 Support the Document Management Lifecycle

Provide capabilities to support, creation, review, redaction, storage, dissemination, archiving and destruction of documents including document tagging and metadata and indexing

Functional Specification:

See Appendix D, Use Case Models.

Constraints:

- Consultation of reference documentation must be supported in the field where a user may be un-tethered with no connectivity via wireless or wire-line connection during some (critical) working time.
- System must support restricted access to some documents for some groups requiring authentication of some type (single or multi-factor).
- System must support strong encryption for transfer of confidential documents.
- *See 4.5, Requirements Mapping*

Issues/Notes:

Scenarios:

- Facility Information
- Job Postings
- Organ Donor Look-up
- OSHA Reference Volume Access
- Site Information
- All Forms Management

- All portal procedures, codes, manuals

4.5. Requirements Mapping

See the Requirements Relationship Matrix provided as a spreadsheet supplement to this document.

APPENDICES

Appendix A. Acronyms

CAP	Common Alerting Protocol
CRM	Customer Relationship Management
DAS	Department of Administrative Services
DHS	Department of Homeland Security
DNR	Department of Natural Resources
DOC	Departments of Commerce
DOD	Department of Development
DPS	Department of Public Safety
EMA	Emergency Management Agency
ERP	Enterprise Resource Planning
GPS	global positioning system
IC	The Industrial Compliance Division of the Department of Commerce
ICC	Information Control Corporation
JAD	Joint Application Definition/Development
JFS	Job and Family Services
MTG	Mobile Transaction Gateway
ODH	Ohio Department of Health
OIT	Office of Information Technology
PDA	Personal Digital Assistant
RIM	Research in Motion

Appendix B. Process Definitions

<u>Category</u>	<u>Definition</u>
Process type maps to/includes those mobile activities with the following characteristics or needs:
Alerts	Supports the Federal and State government's commitment to public safety and emergency management by facilitating inter-agency awareness and communication. Includes the advertisement, subscription, and acyclic broadcast of notifications and information that are event-driven and of emergency nature. Examples include DHS and EMA alerts.
Inventory Management	Supports the State's responsibility to analyze current and projected asset conditions and to evaluate economic trade-offs among alternative investment options for cost-effective investment decisions and public service/safety through the collection or verification of the existence, type, number and condition of assets in a place of storage or deployment. Examples include inventory, fleet, and vaccine management.
Mail & Schedule Services	In support of efficient workforce management, email and schedules provide adjunct communication channels that support inspections and intra-agency communication work-distribution requirements.
Inspection/Audit	Supports the State's responsibility to monitor environmental, workplace, building, vehicle, and industrial device compliance to safety and other operational or fiduciary standards such as program or grant service via field inspection activities that have been identified as necessary, numerous, and geographically distributed.
Instant Messaging	Supports public safety and emergency management response via two-way wireless text messaging capabilities, particularly via Research in Motion (RIM) devices or enabled MCTs and as an adjunct to real-time alerts (flood alerts, Amber alerts).
Notifications	Supports a public service where employees/citizens may be notified of pending business obligations or opportunities with the State via mobile messaging on a subscription basis. Distinguished from an alert as non-emergency in nature. It is assumed to be one-way multicast communication via subscription pending further inquiry.
Application Access	Supports the State's commitment to insure public safety and manage emergencies via field-based activities that predominantly cite the need for real-time network connectivity for application access, including bandwidth requirements for effective two-way synchronous data communication.
Document Portability and Management	Supports public and work-force safety and mobile-field-force efficiency via timely access to both dynamic and static data and informational resources. Examples include state and federal repositories of law-enforcement information, safety codes, manuals, and operational guidelines and procedures. Supports public/customer service through ready access to public information.

Remote Sensing

In support of public safety, emergency forecasting and management, requires remote sensing capabilities to obtain data collected by devices deployed in the field on a periodic or ad hoc basis, where such data is a necessary input to downstream processes used in event and disaster prediction, notification, or control. Applications include stream and rain gauges.

Surveys

In support of natural resources management and the delivery of social and transportation services, facilitates the data collection of physical or population characteristics of natural or built environments according to coordinate location, correlated features, cartographic or collateral data. Examples include geological, wildlife, and environmental surveys and transportation studies.

Appendix C. Scenarios

Table N Processes Described by JAD Session Participants

<u>Type</u>	<u>Process</u>	<u>Description</u>	<u>Dept.</u>
Alert	Amber Alerts	Distribute/provide access to Amber Alert information.	OIT
Alert	Bio-Terrorism Response System	A.k.a. Virtual Alert System. Local health alert system currently in testing provides emergency notification to essential staff via pager, cell-phone, PDA phone. Includes instructions as to where to report. Management interface for personnel to update profiles, calendars, and identify backup personnel.	ODH
Alert	Emergency Notification	Provide wireless enablement of facilities-based accident and event notification (e.g., drowning in the park).	DNR
Alert	Homeland Security Alerts	Provide access to DHS Alerts information via InfoPush.	OIT
Alert	Lost Visitor/Child Locator/Information Service	Provide access to a service which enables the finding/pinpointing of lost visitors and missing children.	DNR
Alert	Public Safety Alert	Provide Director of Ohio DHS with capability to view and cascade DHS alerts/messages to direct reports and responsible organizations (EMA, EMS).	DPS
Alert	Stream-Gauge Alert System	This is an extension to item (20) where stream gauge alerts can be pushed to mobile/wireless subscribers of state agencies or via email.	DPS
Alert	Weather Alerts	Provide Wireless access to severe weather alerts via Internet subscription by group for warnings and watches. Alerts should be deliverable to pages, cell phones and email.	DPS

Asset Management	Communication Equipment Inventory	Provide a means for field-based personnel to update asset management system with changes from the field to maintain data integrity of field-based equipment and database of record. E.g., cards/components on MCTs are frequently changed in the field resulting in difficult tracking of these components. This must support technicians w/o immediate access to a vehicle and requisite communications equipment. Such techs may frequently be on foot. Maintains data integrity. A convenient means to update the asset tracking system with respect to changes to devices in the field results in a more accurate basis of information from which subsequent service calls and procurements are driven. It improves service time and saves waste.	OIT
Asset Management	Expense Reimbursement	Traveler is an application used by field inspectors to submit expenses while on the road and is a component of the re-imburement/vendor management workflow process. In the current scenario, the field inspector completes a form and sends as an attachment to the MA who does an upload of data to the expense mgmt. system.	ODH
Asset Management	Hardware Inventory	As part of its asset management workflow, OIT would like to extend an (incipient) inventory management system with mobile/wireless access. This would allow field support staff to inventory deployments of servers, routers, switches, etc. during site service and work visits.	OIT
Asset Management	Inventory Synchronization	Currently handle via Lotus Notes on-demand via dial-up connections.	DOC
Asset Management	SNS Stockpile Management	Specifically, require a mechanism to provide real-time monitoring of the inventory of antidote and inoculation stockpile under field administration constraints.	ODH
Email/Schedules	Email/Schedule Access	Provide mobile/wireless access to email and schedules for DNR employees to facilitate general work processes. Possibly from watercraft.	DNR
Email/Schedules	Email/Schedule Access	Provide email access as adjunct support to a work process.	DOC
Email/Schedules	Email/Schedule Access	Provide outgoing email access as adjunct support for vehicles equipped with MCTs. Current bandwidth issues.	DPS
Email/Schedules	Email/Schedule Access	Provide alternative connectivity channel to many of the 217 BMV offices state-wide which currently use principal phone lines for dial-up access when needed.	DPS
Email/Schedules	Outlook Mobile Access	Provide access to mobile mail (via InfoPush?).	OIT

Inspection/Audit	Asbestos Inspection	To support asbestos abatement efforts, Ohio certifies and licenses independent contractors who must complete a 1 page inspection report which must be filed 10 days in advance of an upcoming job (to qualify for State funds). The form is currently faxed to State. Data entry is done manually to a VAX system. 100-200 contractors performing 100+ jobs per annum. Contractors pay the State \$65.00/transaction. A check is mailed in and workflow is stopped until the check can be synchronized with the faxed form. Moving to a website accepting form inputs and payments via credit card.	ODH
Inspection/Audit	Blood-alcohol Testing	Another opportunity mentioned. Require specifics.	ODH
Inspection/Audit	Dam Safety Inspection	Provide mobile/wireless capabilities to facilitate DNR dam safety inspections.	DNR
Inspection/Audit	Elevator Inspection	A prototype as part of Phase 1 MTG. business processes in the Division of Industrial Compliance (IC). State inspectors certify elevators using a manual, repetitive data entry process. The State believes that a mobile application, coupled with seamless integration to backend systems, will increase worker productivity and reduce the cost of delivering service.	DOC
Inspection/Audit	Fire Code Enforcement	Provide a means to enable Fire Marshal with audit materials and upload of information post audit; reporting.	DOC
Inspection/Audit	Gas and Oil-Well Safety Inspection	Provide mobile/wireless capabilities to facilitate DNR gas and oil-well safety inspections.	DNR
Inspection/Audit	Grant Compliance Enforcement	As a grant-giving agency, ODOD does auditing of grantees. Cycle-time depends on loan service window (LE 15 Yrs.) or tax credit (LE 10 Yrs.). Auditors do site visits to inspect payroll records of grantees, or verify that training grants have been used to certify trainees. Currently these are all paper processes with separate data-entry to central system. Most questions in these audits are discrete, yes/no with some fill-in the blanks. Enablement could provide standardization and accuracy of reporting. Having a device that supports information look-up from soft copy could speed up the process and make it less cumbersome.	DOD
Inspection/Audit	Grant Compliance Enforcement (Via SPESS)	Some \$8-10M is provided annually by way of grants for preventative medicine programs and public education. Such grantees must be evaluated periodically to insure compliance with grant terms. Dept. would like to move from current laptop collection and in-office network synchronization process to wireless POIT deployed in field with an objective of speeding the grant-approval process.	ODH

Inspection/Audit	Grant Eligibility	The Office of Economic Development evaluates business for grant eligibility for development opportunities including retooling, expansion, re-training. Field representatives visit potential grantees throughout the state to interview applicants and assess businesses for investments. Qualifications are delivered with a turn-around of 3-5 days ave. currently. This is a paper process today with @24 inspectors and N data-entry clerks supporting. A total of 200-300 projects are effected per annum. Cycle time is 3-6 months ave. for initiation to authorization.	DOD
Inspection/Audit	Ground-Water and Well Safety Inspection	Provide mobile/wireless capabilities to facilitate ground-water and well safety inspections.	DNR
Inspection/Audit	Household Energy Inspection	The Office of Energy Efficiency currently offers energy inspections and grants to low-income households for the improvement of dwelling energy efficiency. Where approved by DOD, grants are provided for vendor supplied site/dwelling improvement. Filed force of 6-N inspectors is employed today using Windows CE devices. Several hundreds of grants issued per annum. CE based data is currently cradled and synched upon return to office.	DOD
Inspection/Audit	Labor and Safety Inspection	On-demand and voluntary labor and safety inspections that are supported via an application called "Consultant" that simplifies report writing.	DOC
Inspection/Audit	Lead Inspection	Part of lead abatement program. See Asbestos. Different constituents -- inspectors, supervisors.	ODH
Inspection/Audit	Liquor License Enforcement	Support bar, festival, and college audit requirements.	DPS
Inspection/Audit	MARCS Trouble/Service Management	In support of MARCS, the OIT team noted that trouble tickets are currently "physically" dispatched to field support via a call from the help desk. This support can include anything from changing damaged/failed components to fueling gas-powered generators at any one of 200 towers supply voice (and data) services that are situated through-out the state. Field support requires both a trouble-ticket and site information to complete its service call. CRM - Remedy system is not currently web-enabled, but having a thin-client interface could facilitate trouble-management/service calls. Improve service response times for critical infrastructure.	OIT
Inspection/Audit	Mine Safety Inspection	Provide mobile/wireless capabilities to facilitate DNR mine safety inspections.	DNR

Inspection/Audit	Mobile Driver Examinations	Provide connectivity to vehicle registration and driver examination application and scheduling from mobile BMV unit.	DPS
Inspection/Audit	Nuclear Inspection	Another opportunity mentioned. Require specifics.	ODH
Inspection/Audit	Nursing Home Complaints	A variant of Nursing Home Inspection requires an inspector to investigate a complaint or other emergency within 24 hrs. or 10 days according to Attorney General rules (see website).	ODH
Inspection/Audit	Nursing Home Inspection	Today 150+ inspectors conduct week-long recurring audits and emergency/complaint initiated inspections of nursing home and similar health care facilities around the state. "Shell" inspection form and soft copy of code are supplied on a notebook PC today for field use of inspectors who work out of their homes. Client application for completion of forms is part of C/S application which is federally mandated and supplied. Data is exported from client to a file, file is attached to mailer which is sent to ODH for upload to Oracle repository at central office by an "MA", or administrative assistant who supports the inspection teams. Inspectors check-in to regional offices every two weeks, so are paid for time used to dial-in to central office and upload their data. Sometimes dial-in is provided from nursing home. Weeklong visit of 3-5 inspector team typically results in update of data on Friday afternoons. Inspectors may be called off of these teams to respond/document complaints. Some small workflow involved.	ODH
Inspection/Audit	Pollution Incident Reporting & Assessment	Provide mobile/wireless capabilities to facilitate pollution incident reporting and inspection.	DNR
Inspection/Audit	Radon Inspection	Part of radon abatement program. See asbestos.	ODH
Inspection/Audit	STD Monitoring	Inspectors are required to do periodic monitoring/assessment of known carriers of socially-transmitted diseases. Tracking and reporting requirements. Tracking is typically problematic.	ODH
Inspection/Audit	Title Inspections	Provide field support for blue title inspections during lot visits and auto-auctions. Access to title database required. Variant on this applies to DNR which must be able to inspect titles for watercraft in the field. Key issue pertains to file output and print capabilities.	DPS

Inspection/Audit	Vehicle Safety Inspections	Provide field access to information in ASPEN (truck safety compliance application) for use in field at weigh-stations, school bus lots, and for roadside vehicle safety inspections.	DPS
Inspection/Audit	X-Ray Inspection Program	This was described as similar to nursing home inspections. See ICC documentation in this regard.	ODH
Messaging	Real-time Conferencing	Provide sufficient bandwidth to support real-time conference voice/chat. Current capability is dial-up at 56kbps. Provide access to JRES (Joint Response Emergency System) and support ATIXS, an EMS discussion group.	DPS
Messaging	Suspicious Activity Report	Provide access a service which allows reporting of suspicious persons' activities in or around MARCS towers/installations.	OIT
Notification	License/Registration Notification	Provide license/registration renewal notification to citizens/licensee holders via InfoPush.	OIT
Real-time Connectivity	Access to Crash Reporting	Provide access to crash reporting application (HP7) via MCTs.	DPS
Real-time Connectivity	Access to LEADS Application	Provide secure access of sufficient bandwidth to allow mobile/field access to LEADS. LEADS provides access to repackaged intranet/internet content, include road, weather, and traffic conditions (via redirects). Constituents are State correctional officers, sheriff's dept., criminal justice system, county courts, DNR, prisons and jails.	DPS
Real-time Connectivity	Access to RIMS	Provide field access to information in RIMS (case investigation tool) currently used at OSHP posts today.	DPS
Real-time Connectivity	Digital image Upload Capability	Provide sufficient bandwidth to support attachment/upload of digital images for incident reporting/site investigation (accident scene, crime scene, informant stop). Longer-term vision is real-time transmission.	DPS
Real-time Connectivity	Disaster Damage Assessment	Enable field liaisons with access to damage assessment reporting systems. Inspectors are typically in the field a week or more delaying assessments and claims. No infrastructure currently.	DPS

Real-time Connectivity	Disaster Incident Response	Enable field access to back-office systems for reporting flood, weather, radiological or biohazard emergency/disasters. Require access to incident registry, sufficient bandwidth to upload digital imagery. Access to DMIS, JRES, ATIKS.	DPS
Real-time Connectivity	Field Device Software Maintenance	Provide connectivity of sufficient throughput to allow the push of operating system and virus updates to mobile devices in the field. This is currently a big problem (1400 MCTs in vehicles throughout the state, up to 2 updates per week).	DPS
Real-time Connectivity	Mobile Disaster Field Office Connectivity	Enable disaster field offices with access to back-office systems. Currently State EMA co-locates with FEMA. In emergency situations, there are agreements in place for T1 drops in 24 hr. window from regional bell operating company (RBOC).	DPS
Real-time Connectivity	Upload Traffic Citations	Provide ability to upload traffic citation data to central repository in real-time.	DPS
Reference	Access to Portal	Provide access to myOhio.gov personalized portal pages via wireless/mobile.	OIT
Reference	Camp Reservation System Access	Give the park ranger wireless access to the camp reservation system at the campsite in the field (to verify reservations, adjudicate, conflicts, etc.).	DNR
Reference	Facility Information	Provide information access to support "first responders" who are called to a DNR facility in the event of fire, or burglary, or other alarm. A record of key information regarding the facility such, as drop location, would be available via mobile/wireless-enabled device for reference. More timely assessment and correction of real and false alarms. Reduced hazard to first responders.	DNR
Reference	Job Postings	Provide wireless/mobile access to State job postings to employees/citizens via InfoPush.	OIT
Reference	Organ Donor Look-up	Provide capability to access organ-donor information from field locations such as crash sites. Verify donor.	DPS
Reference	Reference Volume Access	Access to statutory documents and codebooks needs to be electronically enabled. Inspectors carry as many as 11 volumes in their cars to be consulted as needed.	DOC

Reference	Site Information	MARCS field service technicians would find access to reference information for each of the 200+ service sites helpful. E.g., some sites require 24 advance notifications to schedule a site service visit.	OIT
Remote Sensing	Rain-Gauge Notification System	Provide an infrastructure to assess information from remote field-sensors -- in this case from rain-level gauges -- that provide data to alert authorities to flood threats. Eliminate manual reads.	DNR
Remote Sensing	Stream-Gauge Notification System	Provide an infrastructure to assess information from remote field-sensors -- in this case from stream-level gauges -- that provide data to alert authorities to flood threats.	DNR
Survey	Field and Stream Data Collection	Provide DNR with mobile capabilities to facilitate field-based data gathering and upload with respect to field and stream wildlife audits.	DNR
Survey	Land Surveys	Provide mobile/wireless capabilities to facilitate geological surveys including access to GPS coordinates, and the ability to up/download digital photos of land and rockslides, etc.	DNR

Appendix D. Use Case Models

Use Case Models

Use cases are a means for specifying required usages of a system. Typically, they are used to capture the requirements of a system, that is, what a system is supposed to do. The key concepts associated with use cases are actors, use cases, and the subject. The subject is the system under consideration to which the use cases apply. The users and any other systems that may interact with the subject are represented as actors. Actors always model entities that are outside the system. The required behavior of the subject is specified by one or more use cases, which are defined according to the needs of actors.

Strictly speaking, the term "use case" refers to a use case type. An instance of a use case refers to an occurrence of the emergent behavior that conforms to the corresponding use case type. Such instances are often described by interaction specifications.

Use cases, actors, and systems are described using use case diagrams.

Actor:

An actor specifies a role played by a user or any other system that interacts with the subject. (The term "role" is used informally here and does not necessarily imply the technical definition of that term found elsewhere in this specification.)

Extend:

A relationship from an extending use case to an extended use case that specifies how and when the behavior defined in the extending use case can be inserted into the behavior defined in the extended use case.

Include:

An include relationship defines that a use case contains the behavior defined in another use case.

Use Case:

A use case is the specification of a set of actions performed by a system, which yields an observable result that is, typically, of value for one or more actors or other stakeholders of the system.

[OMG Adopted Specification - ptc/03-08-02]

MTG Use Cases

1.0 Internet Access

Provide access to Web content and on-line services of various types via the public Internet in support of various users and circumstances via a range of compatible devices.

Where privacy, access control, and authenticity of users and data are required, assure such content and services are delivered via secure means (encryption), to authorized users, whose identity can be validated (via one or more means), without tampering, for the transaction of State, commercial, of personal business.

The Internet Access Context Diagram identifies packages of functionality and their key dependencies to support this business requirement.

The State-of-Ohio portal enables Information and Application access through the aggregation of Web Content and On-line Services via a single point of access. Web Content, On-line Services, and Personalization extend the presentation capabilities of the portal. End-users may customize the presentation of content and services under a single user account and profile.

These capabilities are provided today (albeit not uniformly), but must be extended for MTG support of mobile/wireless devices and protocols via Content Transformation and Wireless Telephony Applications (WTA).

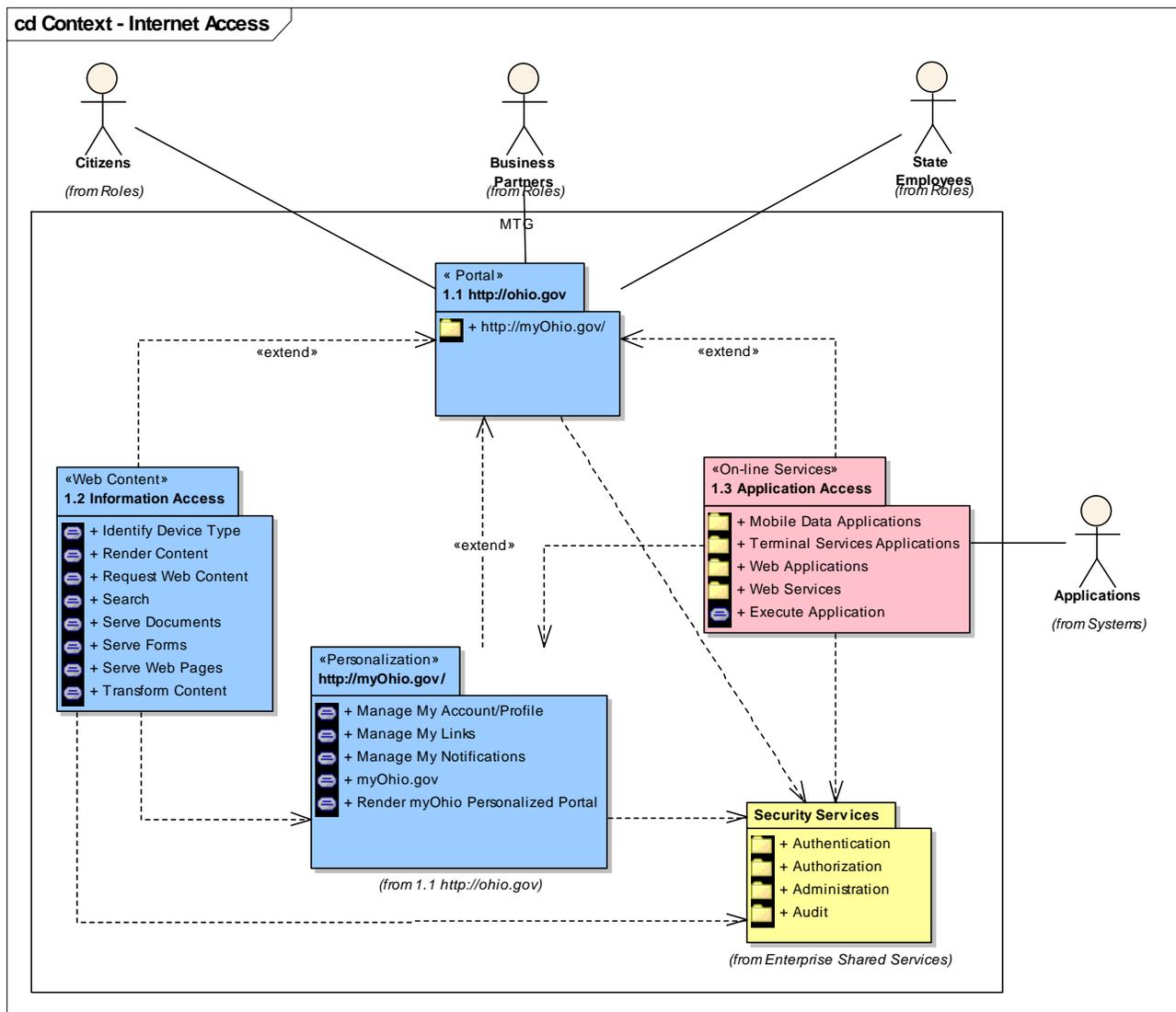


Figure 3 : Context - Internet Access

1.2 Information Access

Provides a collection of files accessed through a Web address managed by a particular person or organization. Its opening page is called a home page. A Web site resides on servers connected to the Internet and is able to format and send information requested by worldwide users 24 hours a day, seven days a week. Static Web sites typically use HTML to format and present information and to provide navigational facilities. Static Web sites lack the interactivity of web applications.

This use case diagram identifies the minimal additional functionality that must be added to web content delivery systems to support wireless handheld devices such as WAP 2.0 compatible phones and PDAs.

The "Identify Device Type" and "Transform Content" use cases highlight these new requirements, where Content Transformation reformats content for compatibility with a range of devices including Wireless Application Protocol (WAP) phones and personal digital assistants (PDAs) by converting HTML and XML data for devices with unique display requirements. Identify Device Type recognizes specific Web-enabled wireless devices such as (PDA's and mobile phones, and customizes the delivery of information to give users the right form of data, to optimize their Internet experience.

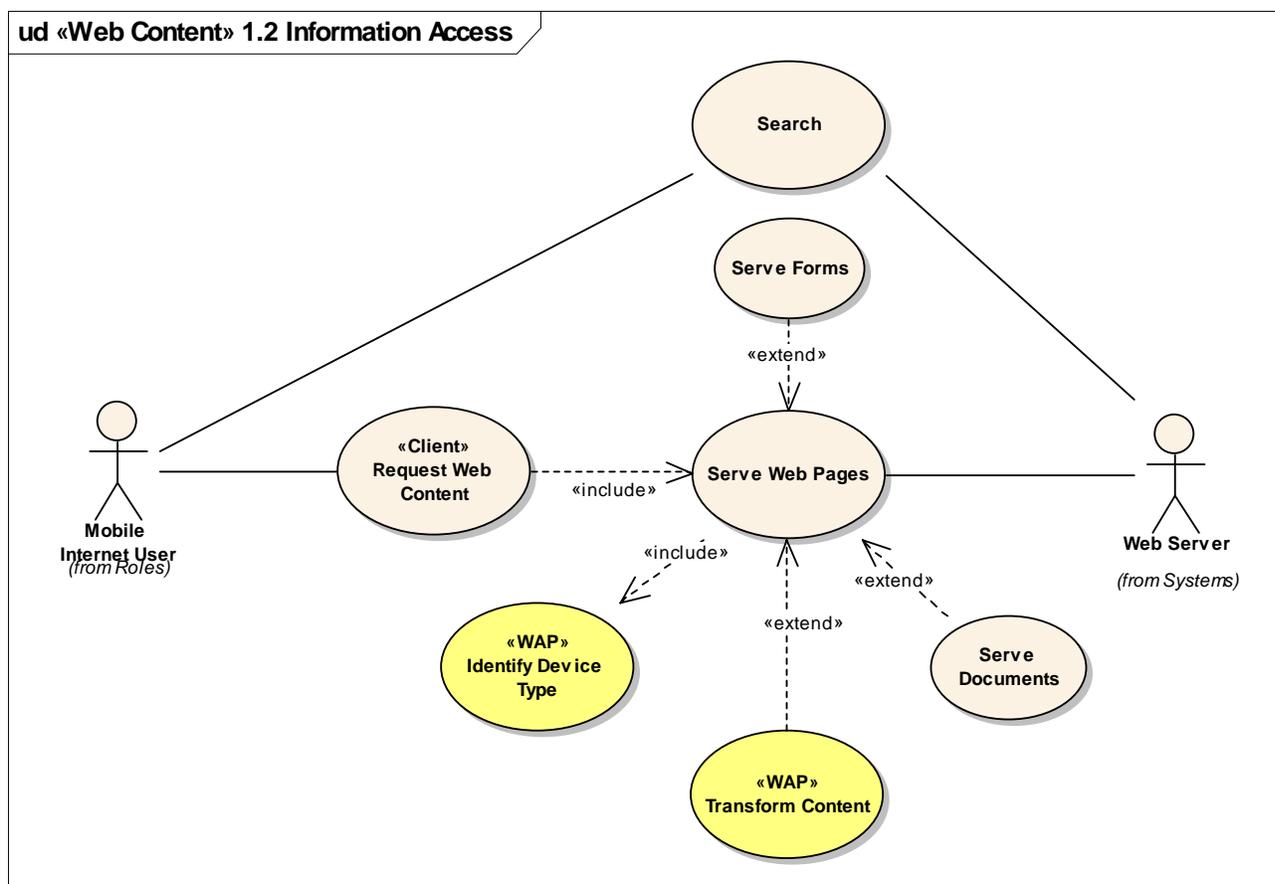


Figure 4 : 1.2 Information Access

Identify Device Type

public «WAP» UseCase: Provides the capability to identify WAP clients for the rendering of content compatible with the device and micro-browser types to account for form-factor and processing capabilities.

Internal Requirements

- WAP 2.0 Compliant Device.

Render Content

public «Web Client» UseCase: Provide the capability to render web content in conformance with HTML 4.1, XHTML 1.0, or WML, cHTML, etc.

Request Web Content

public «Client» UseCase:

Search

public UseCase: Provides the ability to locate content and documents on the site.

Serve Documents

public UseCase: Provides the ability to serve non-HTML based content.

Serve Forms

public UseCase: Provides the ability to render templates for the ordered collection and submission of data on-line.

Serve Web Pages

public UseCase: Provides the ability to render web content from a variety of formats (HTML, XML, XHTML, WML, etc.).

Transform Content

public «WAP» UseCase: Transform the requested content for compatibility with the requesting device and micro-browser (client) types.

1.3 Application Access

Application access describes methods used to run desktop applications remotely. The applications may live on a single user's desktop, or on a server used by many users. The applications may be accessed via a thick client application or via a web browser plug-in.

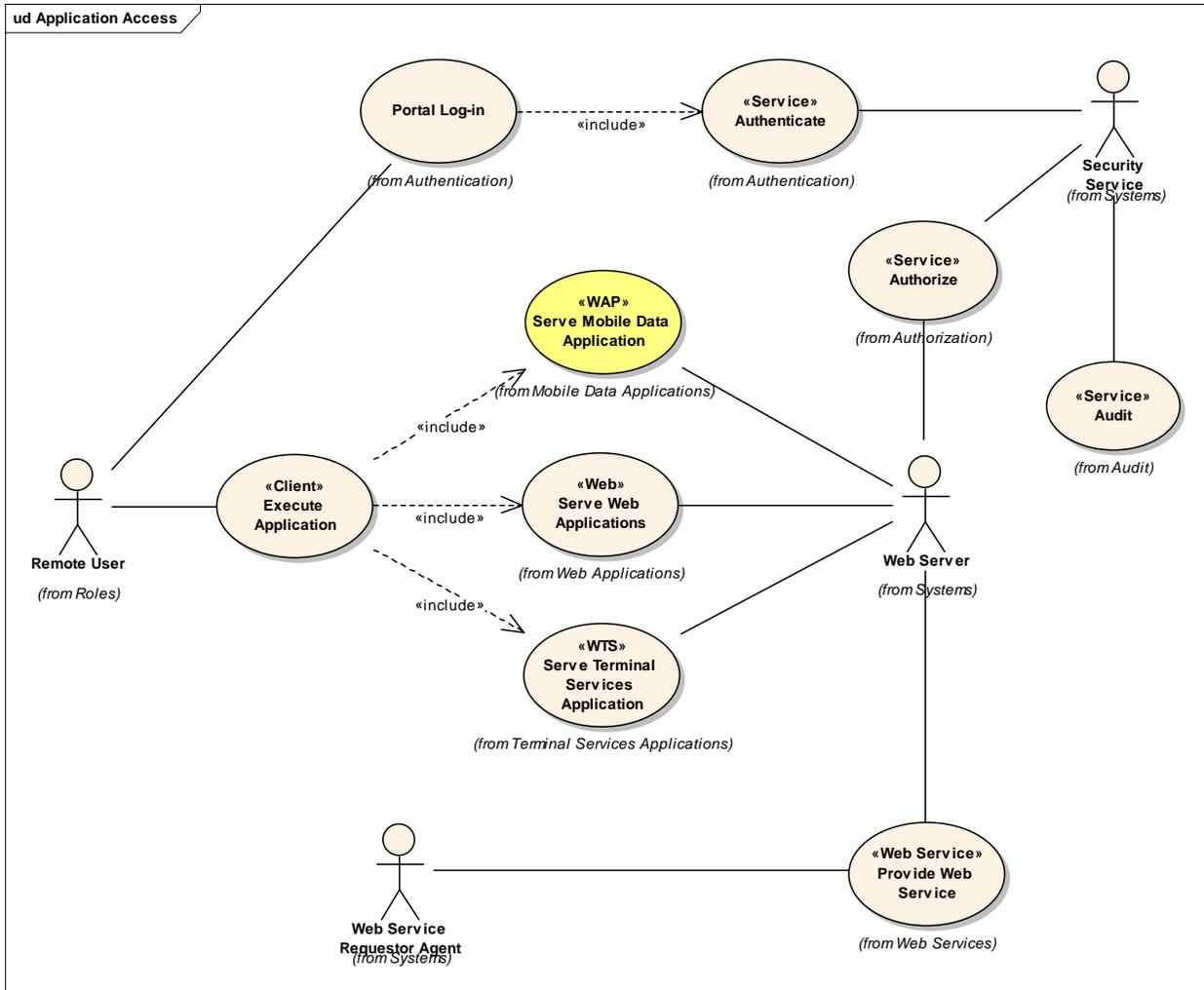


Figure 5 : Application Access

Execute Application

public «Client» UseCase: Provide the ability to execute application functionality using appropriate client and protocol.

Mobile Data Applications

Enables mobile users with applications designed specifically for wireless and hand-held devices via compatible mark-up languages (WML, XHTML), scripts (WMLscript), and protocols (WAP, WTLS).

Serve Mobile Data Application

public «WAP» UseCase:

Terminal Services Applications

Enable mobile and off-site workers with secure, reliable, real-time access to enterprise applications and services from centralized hosting facilities to any device, anywhere, over any connection with minimum client-side requirements.

Reduce network bandwidth requirements by limiting traffic between the client and server.

Increase the number of users able to share a network connection, as well as improve the response time on low-bandwidth connections.

Serve Terminal Services Application

public «WTS» UseCase: Provide the capability to access a WTS deployed application via a secure Internet connection using a thin or thick client per application specific requirements.

Web Applications

Enables on-line services directly from a web page as either:

A web-based thin-client application using HTTP/S for its core communication protocol having minimal client-side requirements and leveraging server-side processing for presentation, application, and data services.

Web-deployed applications installed directly from a web page where applications are designed to run within a secure context on the user's desktop, with access to local resources explicitly given to the application by the user. Updates to the application are made on the web site and automatically installed during the next application invocation.

Serve Web Applications

public «Web» UseCase:

Web Services

A Web service is a software application identified by a URI [RFC 2396], whose interfaces and bindings are capable of being defined, described, and discovered as XML artifacts. A Web service supports direct interactions with other software agents using XML based messages exchanged via Internet-based protocols.

Web Services are stateless and support both synchronous and asynchronous operations.

Provide Web Service

public «Web Service» UseCase: Deliver the capabilities of the provider service based on the contract on the contract of the service description.

2.0 Communication

The context of collaborations identifies the dependencies of notifications on both mail serves and wireless messaging as these are the two options for subscriptions-based notifications. Instant messaging is noted as an adjunct to alerting via dependency for collaborative emergency management.

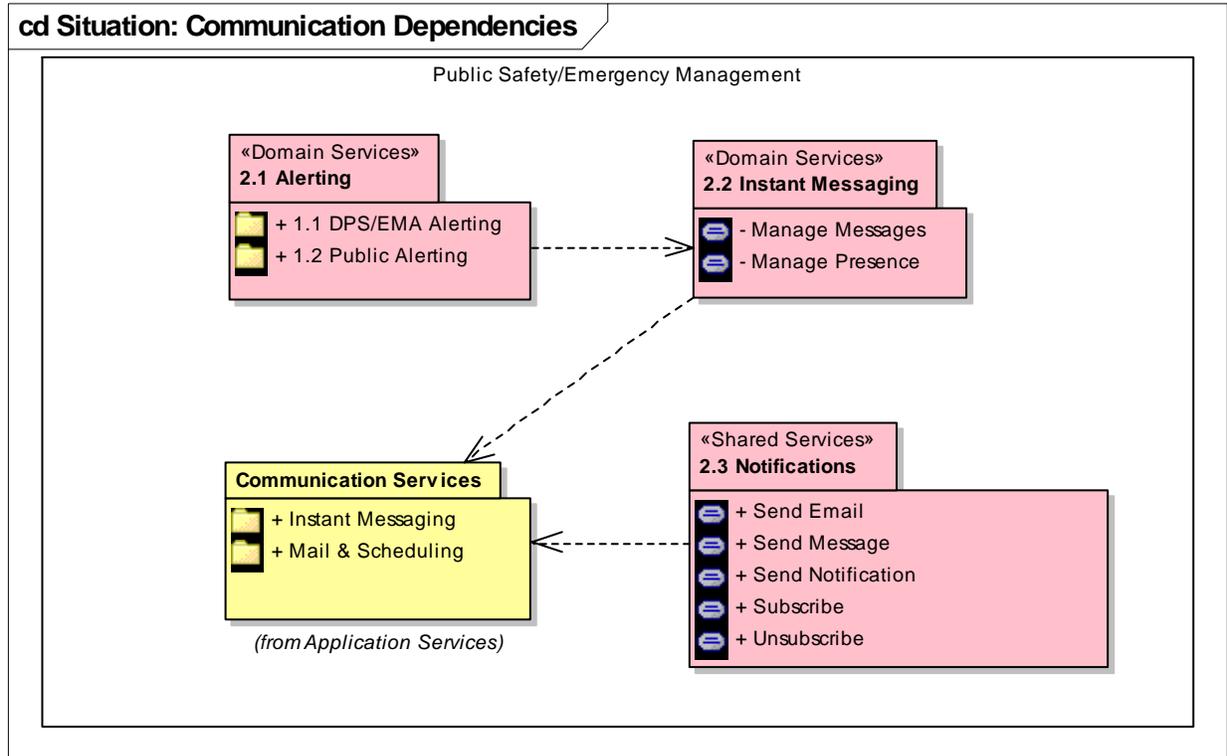


Figure 6 : Situation: Communication Dependencies

2.1 Alerting

Alert capabilities supports the Federal and State governments' commitment to public safety and emergency management by facilitating inter-agency awareness and communication. Includes the advertisement, subscription, and acyclic broadcast of notifications and information that are event-driven and of emergency nature. Examples include DHS and EMA alerts.

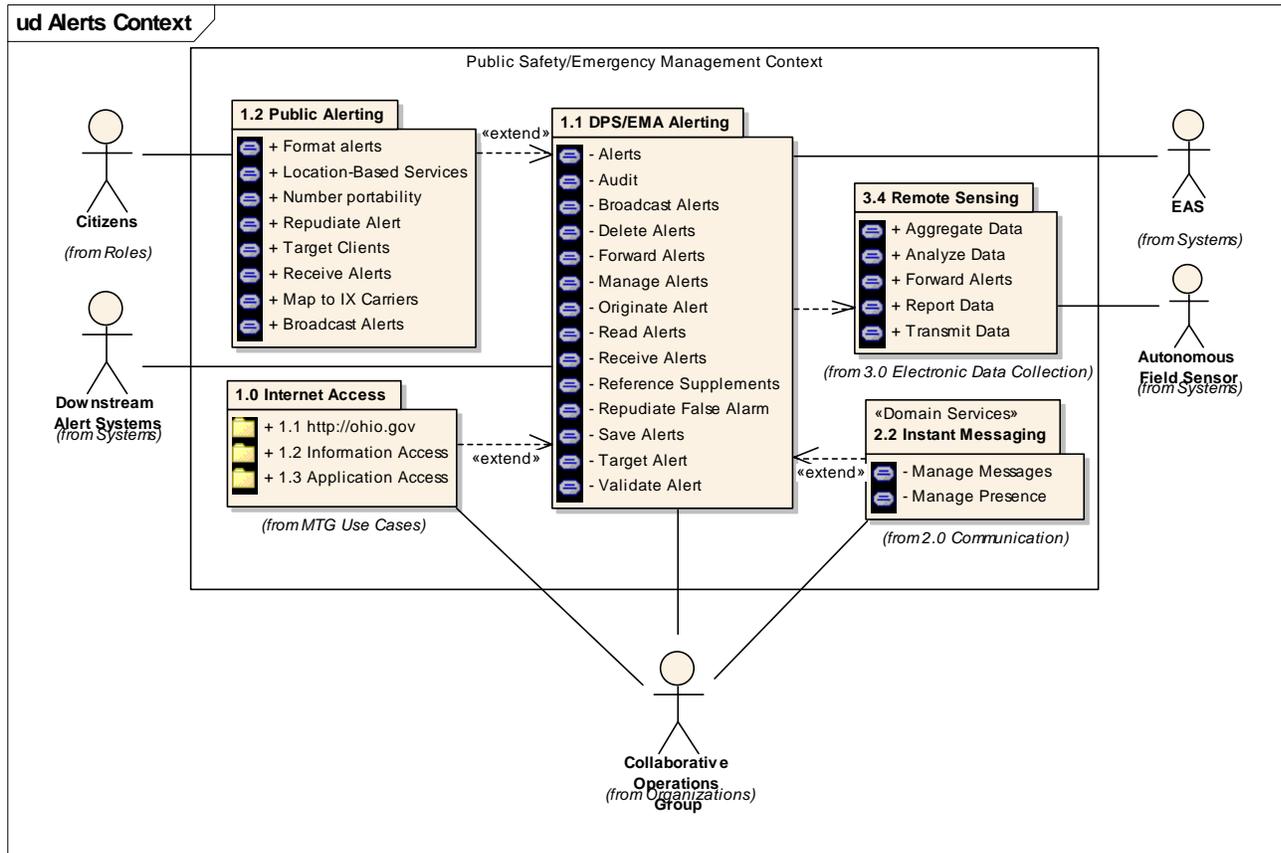


Figure 7 : Alerts Context

1.1 DPS/EMA Alerting

Enables an authoritative body to push an alert to a target or a specified address on an ad hoc basis. Membership in the list may be voluntaristic by subscription, or as required. Assumption is text messages or XML. Depending on device, adjunct access to wireless web content may be invoked.

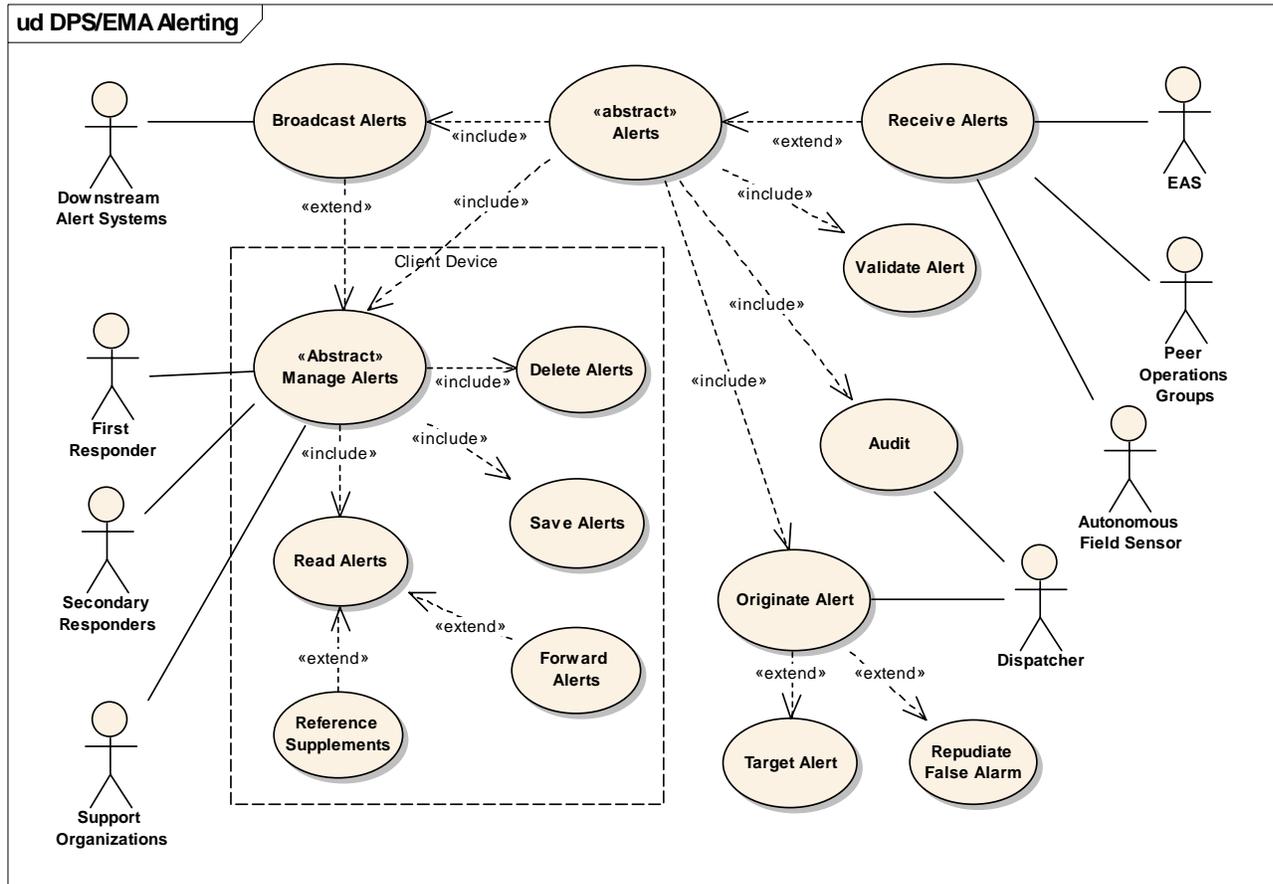


Figure 8 : DPS/EMA Alerting

Alerts

private <abstract> UseCase: Provide the capability to send and manage event-driven, time-sensitive information of an emergency nature (alerts) to agency first-responders, secondary-responders, support groups, and citizens via a digital format that is standards-compliant and deliverable to wired and wirelessly enabled devices. Types of alerts could include:

- Amber Alerts
- School Closures
- NOAA Alerts
- FEMA Alerts
- Rolling Blackouts
- Road Closures
- DHS/Security Alerts

Audit

private UseCase: Provide reporting for alert disposition, system and administrative message logging.

Broadcast Alerts

private UseCase: Provide the capability to distribute such alerts via TCP/IP based networks and one-way channels as:

- a. Broadcast alerts to 2:N client addresses based on geographic areas.
- b. Multicast alerts to predefined groups on a need-to-know basis.
- c. Possibly on a subscription basis according to event-type and priority (TBD).

Provide the capability to propagate such alerts to similarly (CAP) enabled downstream public-address systems (broadcast and cable TV, POTS, Radio).

Delete Alerts

private UseCase: Enable the user to delete alerts from the local data store.

Forward Alerts

private UseCase: Enable users to forward alerts.

Manage Alerts

private «Abstract» UseCase: Must support wired or wirelessly-enabled desktop, notebook, and wireless mobile computer terminals (MCT), PDA's, phone, and paging devices that are capable of receiving text messaging.

Multi-vendor environment and coverage limitations of any one network require that the solution be compatible with all vendor networks, in short the common solution must be suited to running over a network of networks and provide a mechanism to do so.

Must support additional transformations as required for downstream networks and devices.

Originate Alert

private UseCase: 1. Provide the capability to originate manual alerts specified according to the Common Alerting Protocol (CAP) including:

- a. Unique identifiers for each message and message originator
- b. Multiple messages types including:
 - i. Warnings
 - ii. Acknowledgements
 - iii. Expirations and cancellations
 - iv. Updates and amendments
 - v. Reports of results from dissemination systems

- vi. Administrative and system messages
- c. Flexible descriptions of each warning for:
 - i. Geographic targeting
 - ii. Level of urgency
 - iii. Level of certainty
 - iv. Level of threat severity
- d. A mechanism for referencing supplemental information such as digital audio, image files, supplemental text.

Read Alerts

private UseCase: Enables the the user to read and scroll alerts.

Receive Alerts

private UseCase: Provide a standards compliant (CAP) application programming interface (API) for receipt of compliant messages from upstream applications, including:

- a. Alerts from the Emergency Alert System (EAS) and other federal, state, and local systems.
- b. Autonomous sensor systems deployed in the field

Reference Supplements

private UseCase: Enables a user to navigate to supplemental text, digital audio or video via a URI.

Repudiate False Alarm

private UseCase: Support repudiation of false alarms.

Save Alerts

private UseCase: Allows a user to save alerts to a local store.

Target Alert

private UseCase: Enables originator to target alerts to downstream responders and alert systems by geography.

Validate Alert

private UseCase: Support credible authentication and validation of all messages.

1.2 Public Alerting

Public alerting systems extend the state's capability to broadcast relevant alerts to citizens via wireless devices.

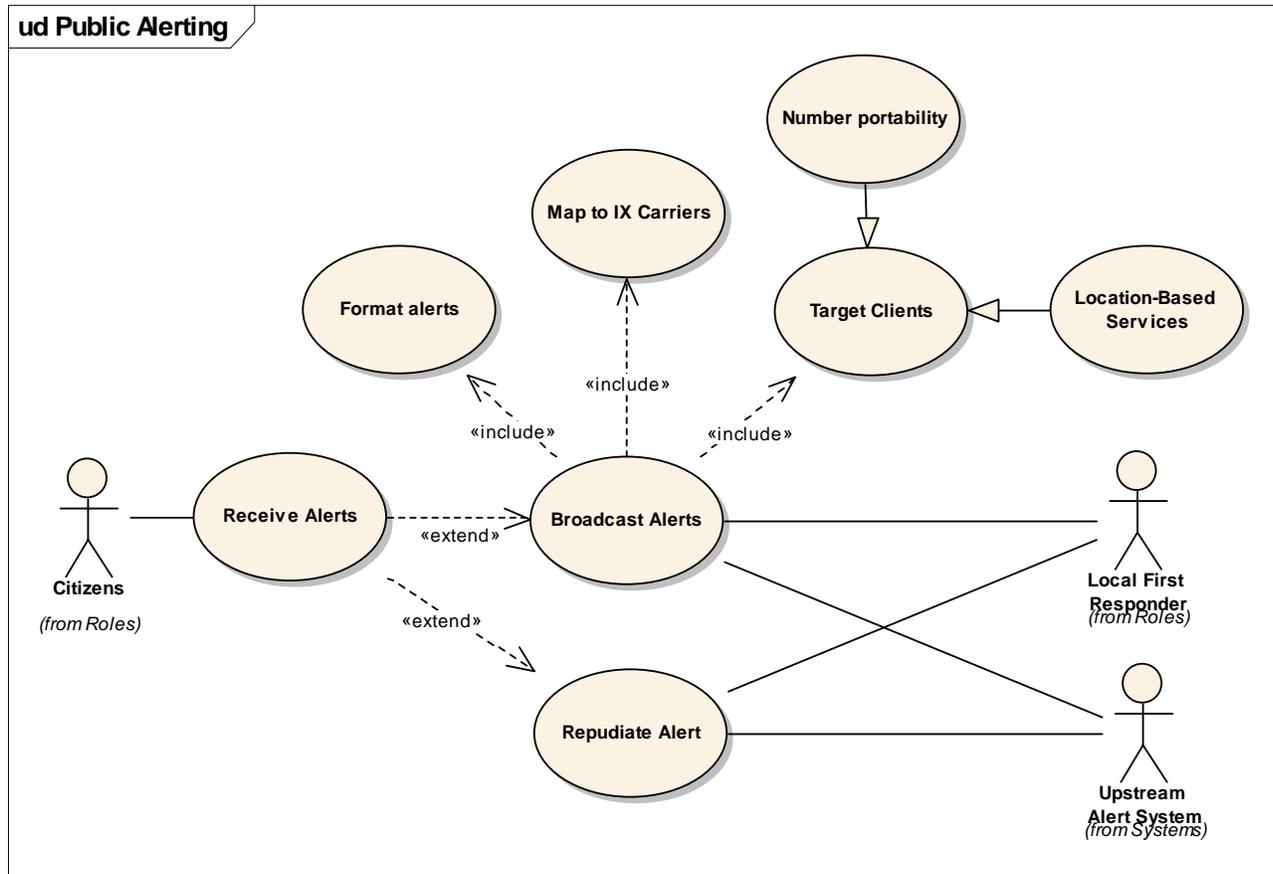


Figure 9 : Public Alerting

Format alerts

public UseCase: Reformat alerts according to requirements of network and protocol of downstream user wireless services.

Location-Based Services

public UseCase: Targeting subscribers according to location-based services (LBS) as relevant to the current emergency.

Number portability

public UseCase: Targeting subscribers based on their place of residence regardless of their current location.

Repudiate Alert

public UseCase:

Target Clients

public UseCase: Enable an operator or upstream standards compliant alerting system to define alert content, choose targeted localities, and specify delivery times for broadcast alerts.
Receive Alerts

public UseCase: Permits the ability to receive and view text messages.

Map to IX Carriers

public UseCase: Provide the ability to send text messages to recipients across two or more inter-exchange carriers using a 10-digit telephone number.
Broadcast Alerts

public UseCase: Proactively deliver local alerts such as Amber alerts, school closures, severe weather, road conditions, blackouts and others to every cell phone and pager within a specified city, county or state without regard to the variety of mobile carriers operating in the targeted geographical area.

2.2 Instant Messaging

In this context, instant messaging (IM) Supports intra- and inter-jurisdictional public safety and emergency management agency collaboration via presence and instant messaging protocol. Stakeholders had requested extension to wireless text messaging capabilities, particularly via enabled MCTs or handheld devices as an adjunct to real-time alerts (DHS, flood, and Amber alerts).

Manage Messages

private UseCase:

Manage Presence

private UseCase:

2.3 Notifications

Supports a public service where employees/citizens may be notified of pending business obligations or opportunities with the State via email or mobile messaging on a subscription basis. Notifications are distinguished from alerts as non-emergency in nature.

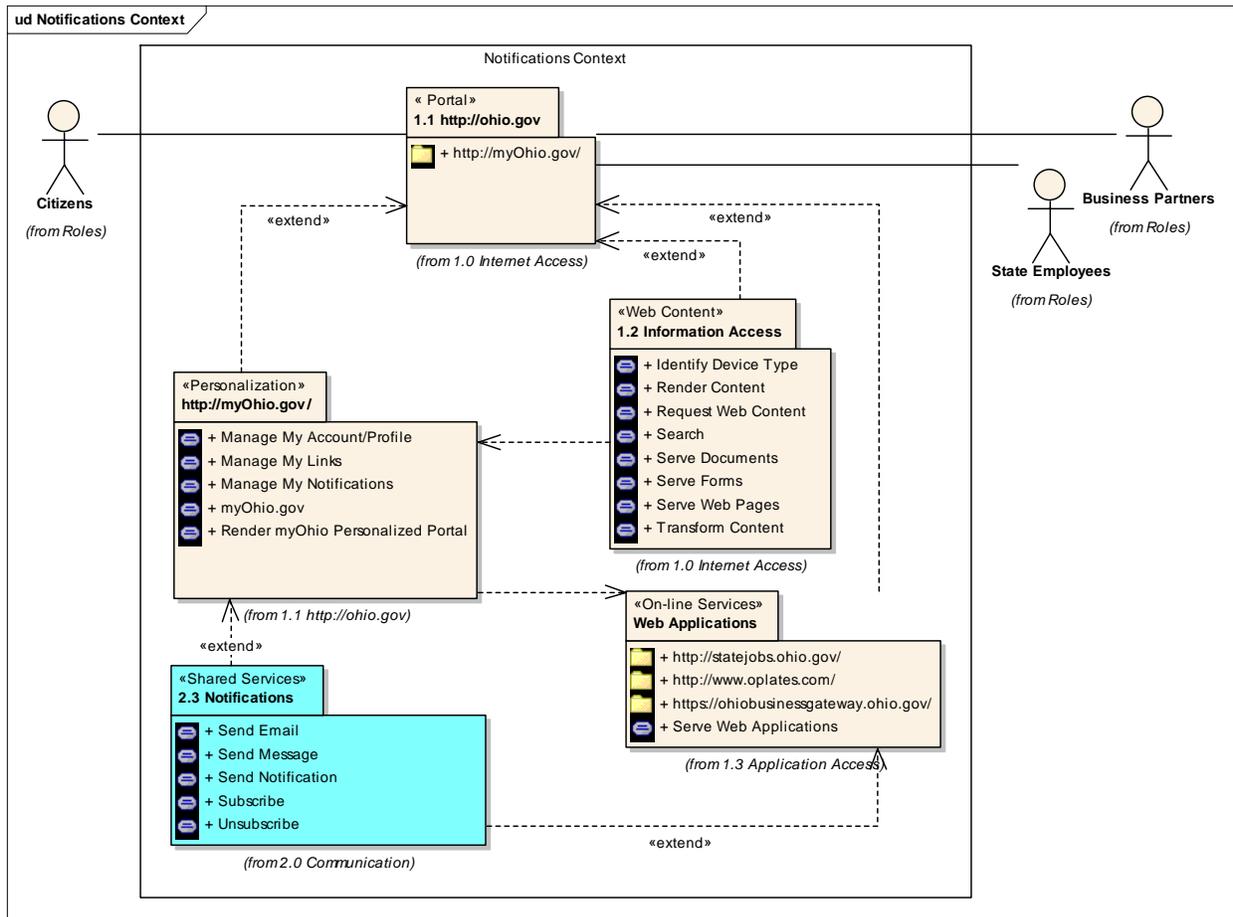


Figure 10 : Notifications Context

Notifications Integration Example

The following diagram represents the idealized case of SSO where user identity management and authentication is to a common subsystem. In this case, user email and notifications can be managed as part of the same, not independent profiles. Note that this is NOT currently the case today, as job profile and myOhio portal profiles are separately stored and managed. In the ideal case, a user could subscribe to notifications offered through various systems (job opportunities, license and registration renewal, legislative notifications, etc.), these subscriptions would be aggregated into a common profile, and these notifications and target email addresses could be managed from a single myOhio account profile. Note also the simplification of user /administrative credential management through consolidation on a single identity management service.

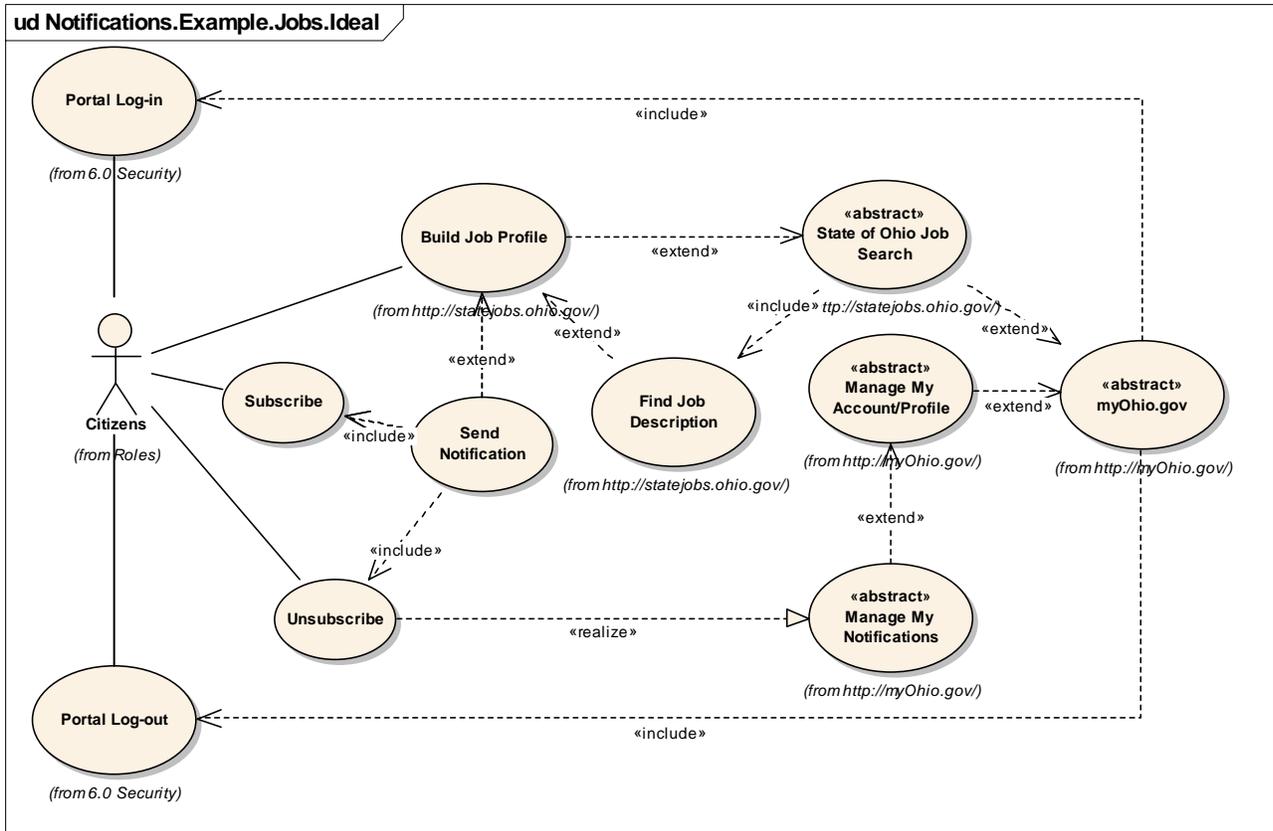


Figure 11 : Notifications.Example.Jobs.Ideal

Citizens

public Actor: Citizens of the State of Ohio.

myOhio.gov

public «abstract» UseCase:

Build Job Profile

public UseCase: Allows a job-seeker to build a personalized applicant profile and schedule a civil-service exam.

Portal Log-in

public UseCase:

Portal Log-out

public UseCase:

Manage My Account/Profile

public «*abstract*» UseCase: An abstract use case aggregating the CRUD scenarios associated with user account management.

Manage My Notifications

public «*abstract*» UseCase:

State of Ohio Job Search

public «*abstract*» UseCase: An abstraction of job search capabilities.

Find Job Description

public UseCase: Enables a job-seeker to search and list entries in the State job bank according to one or more criteria.

Send Email

public UseCase:

Send Message

public UseCase:

Send Notification

public UseCase: An extension of a service which provides an event-based notification to a subscriber via email. Destination is the email address (POP/IMAP) specified by the subscriber.

Subscribe

public UseCase: Enables a user to subscribe to email notifications associated with a service.

Unsubscribe

public UseCase: Enables a user to unsubscribe to email notifications with respect to the associated service.

2.4 Mail & Schedules

In support of efficient workforce management provide email and schedule access/capabilities as an adjunct service to support the work-distribution requirements and schedule adjustments for inspections, audits, and other field-based work activities.

Mail Services

E-mail is electronic messaging that uses standard conventions for addressing and delivering content across the Internet. An e-mail message has three parts: a header, a message, and attachments (documents or computer readable files). The header contains much technical information about the source and the route the message took from sender to recipient. The content contains the text of the actual message. Attachments contain any files sent with the message.

3.0 Electronic Data Collection

This category encompasses four variants described in the sections below, all of which involve a general model of locating and obtaining a template-based data collection tool which is then completed in either on-line or off-line mode and then submitted for further processing and fulfillment of a task request by a service or human resources.

Store and forward refers to technologies that allow message data to be stored locally until a connection is made with the remote computer that lets the message be forwarded to the designated recipient. This allows applications to be used offline, with needed data cached locally, or uploaded later when the client is again online.

ud Dependency Diagram-EDC

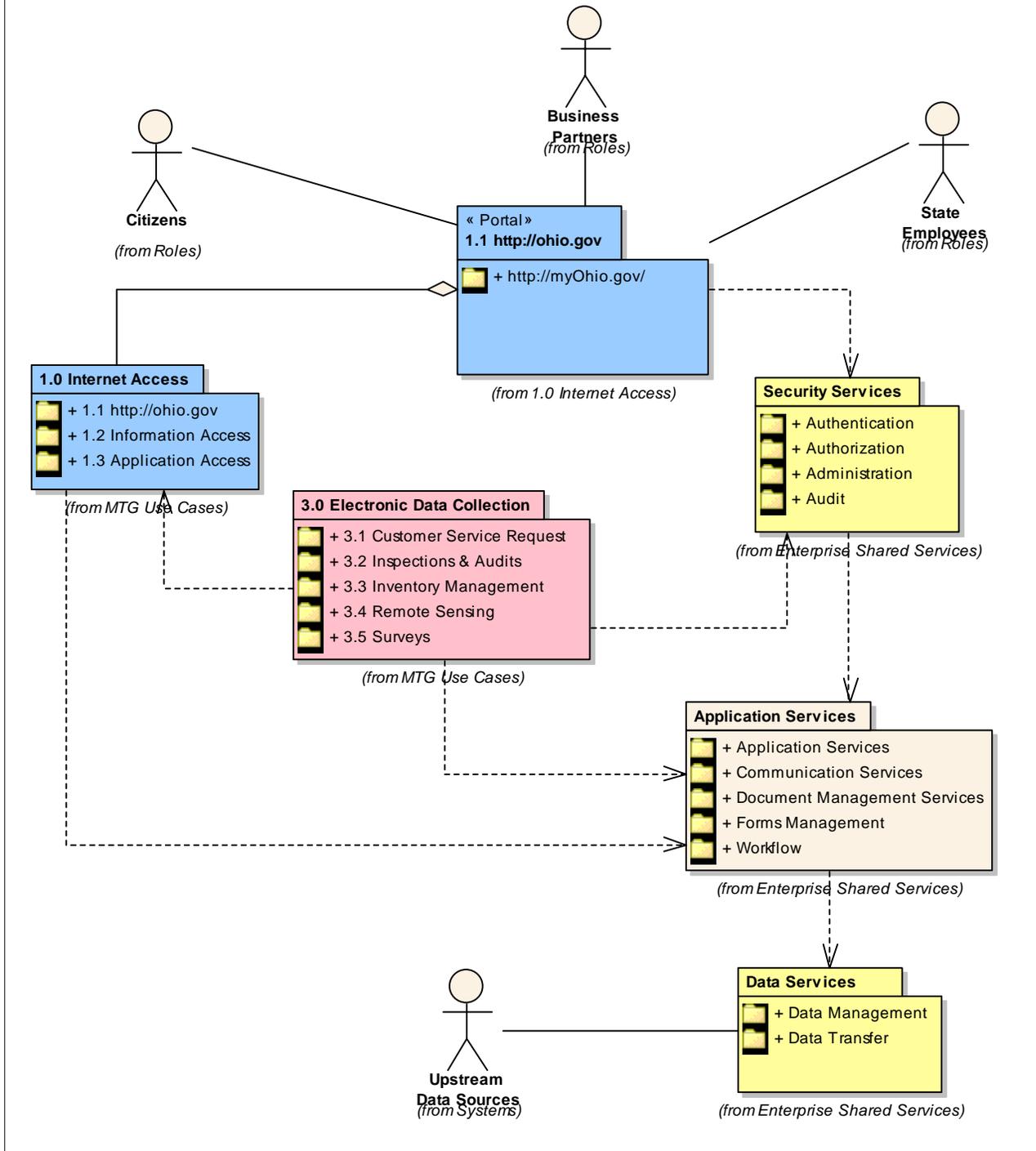


Figure 12 : Dependency Diagram-EDC

3.1 Customer Service Request

Provide the capability to collect or verify the existence, type, number and condition of an asset from a place of storage or deployment (e.g., warehouse or field) with respect to a predefined set of attributes (via a template). Add or update the information to a database of record. Applicable, but not limited to machinery, vehicles, real-estate, soft-goods, software, and financial instruments. Items that must be recorded, valued, and managed. Distinguishing features: the need to enumerate and describe instances of a kind/class in the field for a record to be used for purposes of valuation and control.

The user needs to:

1. Determine what information needs to be provided.
2. Assemble the necessary information into the correct format and submit it, typically via one of two modes:
 - Via a static template (form) that can be submitted to the service provider in batch format either on or off-line
 - Via a dynamic (web-based) wizard or form that can be completed and submitted on-line.
3. Ideally a receipt is provided.

The request may entail subsequent processing and information to the client.

3.2 Inspections & Audits

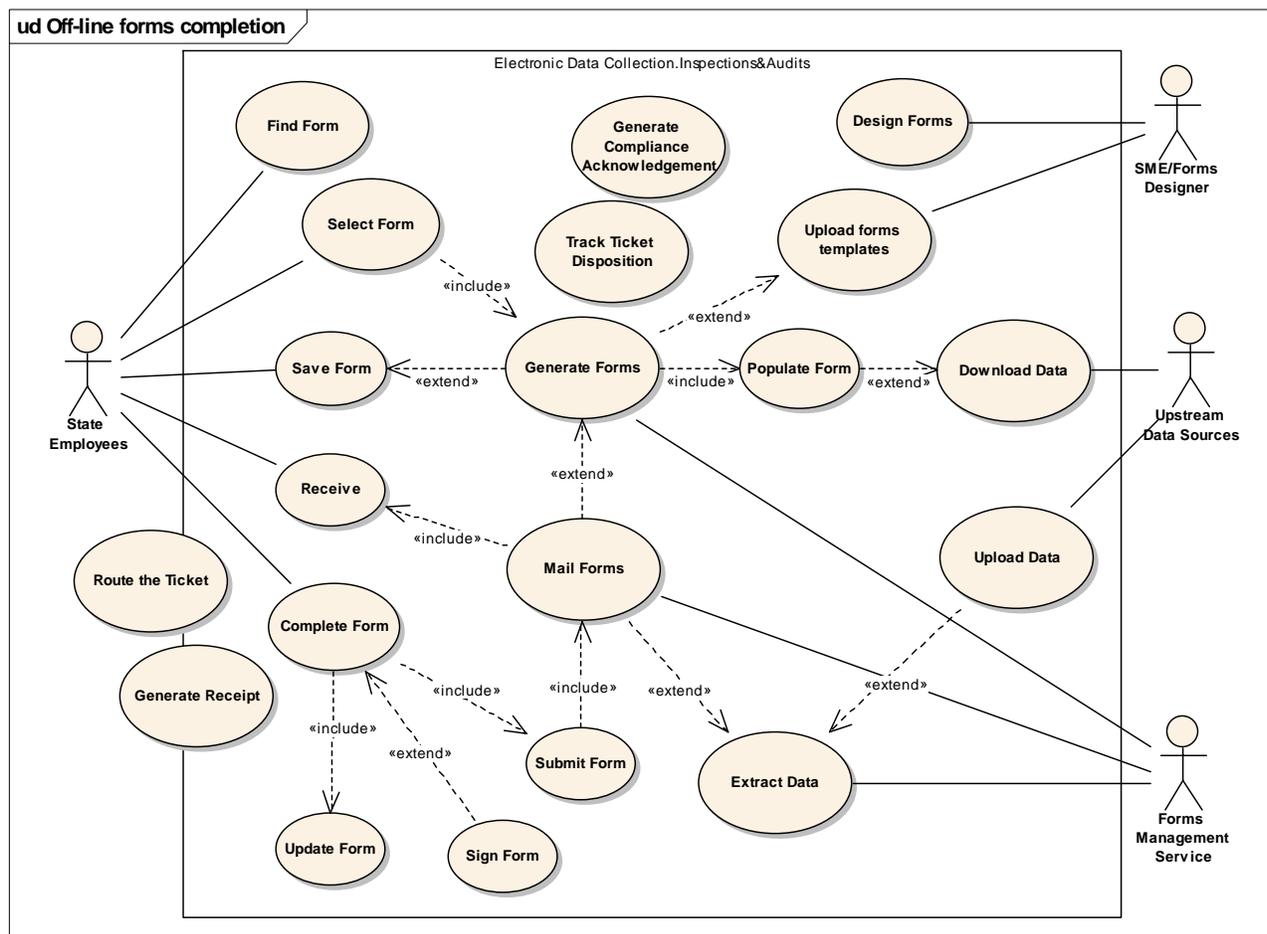


Figure 13 : Off-line forms completion

Complete Form

public UseCase: Collect inspection/audit/compliance data electronically via a mobile device, including the ability to modify and save both closed and open-ended data via a standard template and/or procedure, either on or off-line.

Notes:

- Saving the data off-line implies storage to the local device and the ability to synchronize the data with the repository of record via some service at a future date via a wired or wireless connection that allows batch transfer of the payload.
- Saving the data on-line implies continuous connectivity and session persistence.

Design Forms

public UseCase:

Download Data

public UseCase:

Extract Data

public UseCase:

Find Form

public UseCase:

Forms Management

public «abstract» UseCase:

Generate Compliance Acknowledgement

public UseCase: Generating:

- a. Compliance certificates for completed and approved inspections/audits as:
 - i. Softcopy for email to the client.
 - ii. Paper certificate format for U.S. Mail delivery to the client as required for legal compliance.

Generate Forms

public UseCase:

Generate Receipt

- public UseCase:* 4. Where required, provide the customer with a receipt of completion, either:
- a. Electronically, where a network connection enables a receipt to be routed to the email address of a responsible party of the client organization, (possibly upon submission of the completed report).
 - b. On paper via any of the following means:
 - i. Via a pre-printed acknowledgement that is signed and dated by the inspector upon completion of the site visit.
 - ii. Via a dynamically generated receipt that is printed by the inspector via a portable printer upon completion of the site visit.
 - iii. Via a printing facility that generates such acknowledgements for U.S. mail to the client.

Mail Forms

public UseCase: Populated forms can be sent directly to designated field inspectors via email with routing enabled via a workflow system. This raises issues with respect to data confidentiality and integrity in the event that the forms/data need to be secure, that is, mail must be submitted via secure channel, or form/document must be password word protected and possibly encrypted.

Obtain Form

public UseCase: Supports the end-users access to forms.

Populate Form

public UseCase: A function of the system responsible for populating form-fields with instance specific data as required.

Receive

public UseCase: Denotes the subtype where a form may be routed to the recipient via email.

Route the Ticket

public UseCase: Routing the inspection/audit/compliance through the proper chain of supervision for the capture of approvals/disapprovals and the chain of rework.

Save Form

public UseCase: Denotes the case (subtype) where a user downloads the appropriate form from a forms portal.

Select Form

public UseCase: Enable a mobile field staff employee to be able to (securely) obtain an inspection form or ticket that is generated according to a schedule including vital data (identifier, location, evaluation criteria, inspection history, etc.) for a specific inspection, audit, or compliance target such as:

- a mechanical system (elevator, boiler, underground fuel storage)
- a building or construction site (public, commercial, residential)
- a service agency (childcare facility, nursing home, etc.)
- a grant applicant/recipient

Data may be delivered to the end-user via log-in to an employee accessible portal (or sub-site of the existing State portal) where forms may be selected by date or evaluation target and downloaded to his/her local device, assuming a wired or wireless connection (of sufficient data transfer rate, but NLT 56kbps).

Sign Form

public UseCase:

Store Forms

public UseCase:

Submit Form

public UseCase:

Track Ticket Disposition

public UseCase: Tracking of the workflow (processing status)

Update Form

public UseCase: Manage the incomplete and complete forms for correctness, efficiency, and convenience, both on and off-line including the ability to find a form, search the form, navigate among and within forms, and save or delete forms.

Upload Data

public UseCase:

Upload forms templates

public UseCase: Provides the designer with the ability to upload completed form templates.

3.3 Inventory Management

See 1.2, *Application Access*, or 3.2, *Inspections and Audits*.

3.4 Remote Sensing

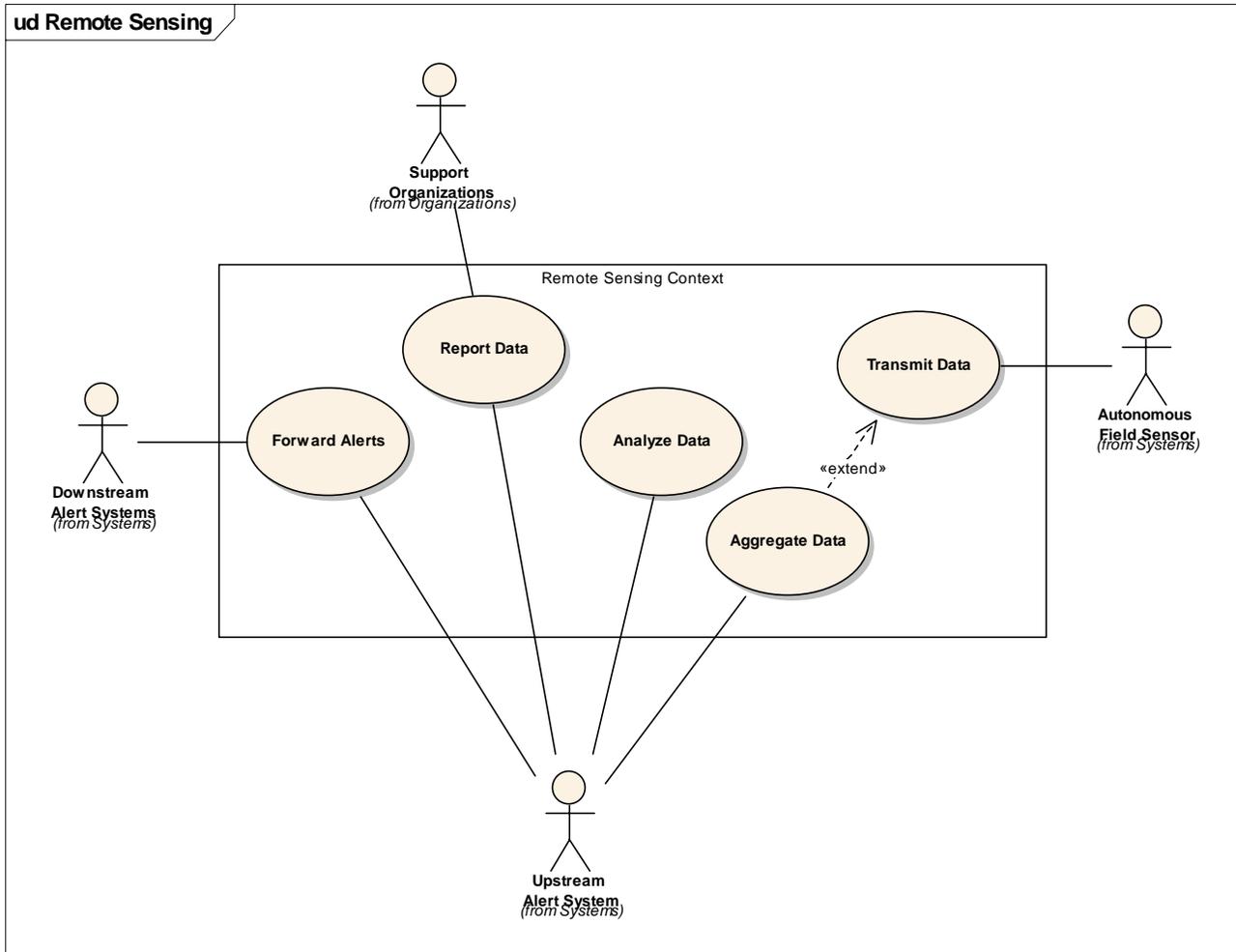


Figure 14 : Remote Sensing

Aggregate Data

public UseCase:

Analyze Data

public UseCase:

Forward Alerts

public UseCase:

Report Data

public UseCase:

Transmit Data

public UseCase:

3.5 Surveys

4.0 Document Management

Defines the capability to locate and display informational and reference materials on-line or off-line. Basic functional requirements include the ability to find, view, navigate, and bookmark or even annotate the information/document. Off-line, locally stored documents need to be updateable when a connection does exist, and previously unsaved documents need to be able to be obtained from a source and stored locally as an option. The ability to reference supporting documentation in the field -- whether on- or off-line -- is critical to inspections and audits, and various first-responder and field survey tasks. While on-line wireless access is not an absolute requirement in many cases, some means of provisioning end-user devices with soft-documentation must be provided.

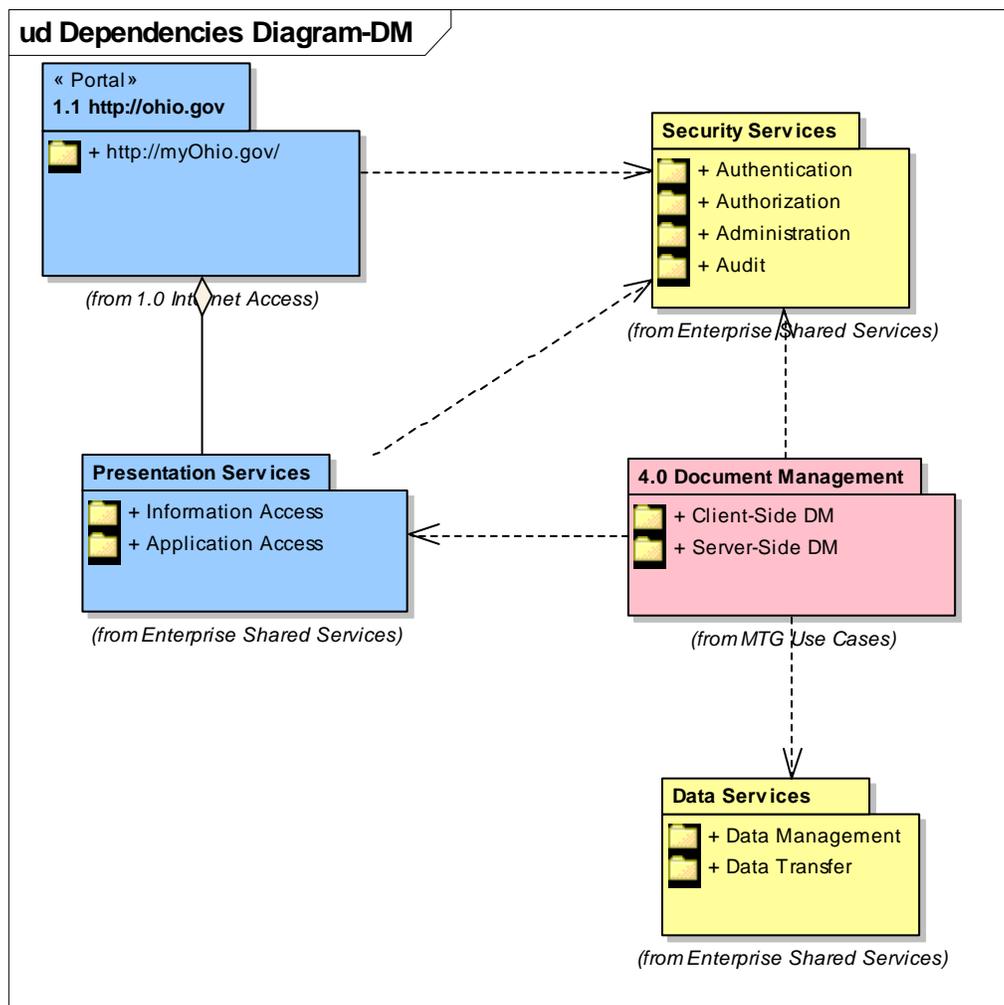


Figure 15 : Dependencies Diagram-DM

Appendix E. Participants

<u>Dept.</u>	<u>Name</u>	<u>Email</u>	<u>Phone</u>
Battelle	Krippendorff, Mike	krippendorffM@battelle.org	614-424-4857
OIT	Davis, Stu	stu.davis@ohio.gov	614-644-3923
OIT	Johnson, Mark	mark.johnson@ohio.gov	614-644-5797
OIT	Knecht, Brad	brad.knecht@ohio.gov	614-995-0059
OIT	Orr, Dan	dan.orr@ohio.gov	614-728-4701
OIT	Polinsky, Stephen	stephen.polinsky@ohio.gov	614-466-4618
OIT (ICC)	Sesfovic, Mensur	msesfovic@iccohio.com	614-286-9964
DNR	Mountz, Greg	greg.mountz@dnr.state.oh.us	614-265-6785
DOC	Ashenhurst, Jim	jashenhurst@com.state.oh.us	614-752-7160
DOC	Cairney, Dick	rcairne@com.state.oh.us	614-728-0054
DOC	Collins, Greg S.	greg.collins@perrp.com.state.oh.us	614-644-2527
DOC	Gibbs, Tony	tjibbs@com.state.oh.us	614-507-4174
DOC	Hart, Tom	tom.hart@com.state.oh.us	614-995-9914
DPS	Brown, David	dabrown@dps.state.oh.us	614-995-5031
DPS	Groghan, Michele	mgroghan@dps.state.oh.us	614-466-3816
DPS	Markowski, R.W.	rmarkowski@dps.state.oh.us	614-466-5933
DPS	Morrill, Mark	mmorrill@dps.state.oh.us	614-889-7157
ICC	Webb, Steve	swebb@iccohio.com	614-523-3070
ICC	Hamilton, Joe	jhamilton@iccohio.com	614-523-3070
DPS	White, D.E.	dewhite@dps.state.oh.us	614-466-0713
ODH	Darling, Steve	sdarling@odh.ohio.gov	614-466-5499
ODH	Gallant, Jim	jgallant@odh.ohio.gov	614-752-4794
ODH	Swan, Jeff	jswan@odh.ohio.gov	614-752-5998
ODOD	Phillips, Myron	mphillips@odod.state.oh.us	614-466-9667
OSHP	Perira, Mauro	mperira@dps.state.oh.us	614-752-3001

Appendix F. Glossary

Actor	An actor specifies a role played by a user or any other system that interacts with the subject. (The term "role" is used informally here and does not necessarily imply the technical definition of that term found elsewhere in this specification.)
Business Process	A high-level process or business level use case of low granularity. Examples might include, "Conduct a boiler inspection" or "File a traffic incident", where these high-level business processes could be further decomposed into smaller steps, such as, "log-in to building mechanical's inspection system", "Download inspection calendar/forms", etc.
Cost Management	All the procedures, tasks and deliverables that are needed to fulfill an organization's costing and charging requirements
Document Management	The process of managing documents through their lifecycle. From inception through creation, review, storage and dissemination all the way to their destruction.
Value Chain	The sequential set of primary and support activities that an enterprise performs to turn inputs into value-added outputs for its external customers. An IT value chain is that subset of enterprise activities that pertain to IT operations, both to add value directly for external customers and to add indirect value by supporting other enterprise operations. www.ichnet.org/glossary.htm

Appendix G. References

[FCC94] <http://www.fcc.gov/eb/eas/>

[OAS03] OASIS [1] Common Alerting Protocol, v. 1.0; Committee Specification, 12 August 2003

[RFC2119] RFC Key Words, Best Current Practice, May 1997.

[SAF04] SAFECOM, Statement of Requirements, Department of Homeland Security, 2004.

[RFC2026] The Internet Standards Process -- Revision 3, IETF, October, 1996.

[WFMC] Workflow Management Coalition, Terminology & Glossary, Document Number WFMC-TC-1011, Issue 3.0, Feb 99 (http://www.wfmc.org/standards/docs/TC-1011_term_glossary_v3.pdf).