

CS1/06-0236 Project Proposal – Enterprise Dynamic Access Control (EDAC) Model

1. Source of the Proposed Project

1.1. Title – Enterprise Dynamic Access Control (EDAC) Model

1.2. Date Submitted – January 4, 2006

1.3. Proposer: Richard Fernandez, U.S. Navy

2. Process Description for the Proposed Project

2.1. Project Type

D - this is a standard development project.

2.2. Type of Document

The project is expected to result in an American National Standard.

2.3. Definitions of Concepts and Special Terms

Reference EDAC Overview in NIST RBAC Roadmap web site.

<http://csrc.nist.gov/rbac/rbac-stds-roadmap.html>

2.4. Expected Relationship with Approved Reference Models, Architectures, etc.

None.

2.5. Recommended INCITS Development Technical Committee

INCITS CS1, Cyber Security

2.6. Anticipated Frequency and Duration of Meetings

It is anticipated that this project would require one-day meetings approximately quarterly.

2.7. Target Date for Initial Public Review

A standalone EDAC demonstration program is publicly available, which should be helpful in developing this standard. It is estimated

that the draft document would be ready for submission to INCITS for Milestone 4 processing in the last quarter of 2007.

2.8. Estimated Useful Life of Standard

There is no known limitation on the useful life of this proposed standard.

3. Business Case for Developing the Proposed Standard

3.1. Description

The proposed standard will specify a flexible access control model with standard tie-ins to customer assets, extending INCITS 359-2004 functionality. Customer assets include:

- Web-based resources
- Portal to display available resource and respective roles
- Customer meta-database
- Customer personnel databases - human resource data stores used in creating a user profile.

The proposed standard will specify the following interchangeable components in order to ensure communication with each other via web services and the interchangeability of standard operations:

- Rules Engine Service (RES) - XACML based evaluator that compares a policy with a user request and issues a response whether a resource is accessible by a user.
- Condition Management Service (CMS) – web-based interface used to establish policy.
- Object Profile Management Service (OPMS) – queries Customer Personnel Databases (CPD) or human resource databases to compile a user profile for selection by user.
- Structural Format Service (SFS) – formats the user profile into a structure found in the Customer Meta Database (CMD).
- Condition Status Service (CSS) – monitors any changes between conditions in a policy and the Customer Meta Database (CMD).

The proposed standard will furnish the resource manager salient features identified in the American National Standard INCITS 359-2004. The proposed standard could be used by civilian and military organizations to access resources.

3.2. Existing Practice and the Need for a Standard

Existing industry access control products currently require a proprietary commitment. A concern with access control proprietary solutions is the lack of standard tie-ins with customer assets. A standard less access control tie-in with customer assets leaves the customer at a disadvantage because proprietary solutions require some level of customization and maintenance. Customization also leaves the customer at risk if the servicing access control product can no longer be vendor supported. These unforeseen changes can quickly leave a customer's access control solution vulnerable. The consequences could be wide-ranging and significant since access control is tightly coupled with security. The only other alternative for the customer is to abandon the current access control infrastructure and replace it with another proprietary solution. This "fork-lift" approach leaves a customer with financial burdens and disruption of services. For these reasons, many customers end up funding in-house research and development initiatives to produce a customized but stovepipe access control solution that guarantees supportability.

Dynamic role assignments. Role assignments have to be dynamic and automated. Human intervention in assigning users to roles in an access control system is neither reliable nor manageable. There are important events involving user profile attribute changes, corporate re-structuring, environmental and workflow that can actually determine what role a user is assigned.

Comprehensive access control solution. Customers have to be presented a standard access control solution that offers a comprehensive solution capable of evaluating the following events in order to assign users to roles:

- User profile attribute changes
- User profile selections
- Corporate changes
- Environmental
- Questionnaire
- Workflow

Initially a customer may only require an access control system that can furnish them certain evaluations of events to assign users into roles. But as the customer IT requirements mature additional evaluations may spawn and thus render the existing access control

solution primitive and ineffective. This would require the customer to spend additional funds for an upgrade or a replacement.

A standard access control implementable model such as the EDAC would significantly reduce costs to customers. There are three cost associated in deploying an access control system: research and development, implementation and maintenance. If a standard EDAC model existed no research and development cost would be required because a comprehensive access control solution would already be part of the standard. Manufacturers would instead invest these funds in developing more efficient access control components that complied with the standard implementation and salient features. The implementation costs would be lower because customer assets such as: portal, human resources databases and resource would already have adopted standard tie-ins. Because the EDAC automates the assignments of users into roles, customers would significantly reduce the staff assigned to performing this task.

3.3. Implementation Impacts of the Proposed Standard

3.3.1. Development Costs

Currently COMPACFLT, Pearl Harbor Hawaii is furnishing development costs for the EDAC implementation. SPAWAR SSC will also market EDAC concept to commercial development companies.

3.3.2. Impact on Existing or Potential Markets

The proposed standard will serve as an implementation model of the INCITS 359-2004, RBAC standard. Many development vendors can participate in niche components of the proposed standard. Vendors would compete to offer added features in addition to complying with the proposed standard's minimum requirements for interoperability and salient features.

3.3.3. Costs and Methods for Conformity Assessment

No information is available on possible conformance costs.

3.3.4. Return on Investment

Standard based access control solutions are expected to be more economical than proprietary solutions. Customers will have confidence that a standards-based access control model will not disrupt their security policies.

3.4. Legal Considerations

3.4.1. Patent Assertions

The United States Government (USG) has three pending U.S. Government patents relevant to EDAC. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189

If these patents are issued and the proposed standard is approved, the USG plans to license on a reasonable and non-discriminatory basis, in accordance with the ANSI patent policy.

3.4.2. Dissemination of the Standard

Drafts of this standard will be distributed electronically. There may be distribution constraints as this document reaches different stages of development and processing within INCITS.

4. Related Standards Activities

4.1. Existing Standards

ANSI/INCITS 359-2004 – Role Based Access Control

4.2. Related Standards Activity

This proposed standard is expected to be compatible with the Core and Hierarchical Role Based Access Control (RBAC).

4.3. Recommendations for Close Liaison

OASIS XACML Technical Committee

5. Units of Measurement used in the Standard

Indicate units of measurement used in the Standard:

International Systems of Units (SI)

Inch/Pound

Both

Other

XX Not Measurement Sensitive

It is not anticipated that units from a physical dimensioning system will be needed for specifying the requirements of this standard. If necessary, the goal would be to use the International System of Units (SI).