



## Increment 2 of the AAA Design Pattern Public Forum Office of Technology Strategies August 14, 2014

### Meeting Summary

**Purpose:** The purpose of this Public Forum was to provide an opportunity for VA and external experts and stakeholders to learn about the Authentication, Authorization and Audit (AAA) Design Pattern Increment 2 – External User Authentication, and provide feedback prior to the Design Pattern’s finalization, publication and implementation

**Background:** The Technology Strategies (TS) Design Patterns Team has been soliciting input for the development of Increment 2 of the AAA Design Pattern. This involved collaboration efforts with a variety of stakeholders, including internal VA subject matter experts (SMEs), external government SMEs, industry vendors, and members of academia. This Public Forum represented the final stage of stakeholder engagement in the Design Pattern development process.

**Overview:** The TS Design Pattern Team presented the final draft of their updated Design Pattern Increment 2. An introduction of the department was provided by Caitlin Ellsworth followed by an overview presented by Dusty Jackson of the Office of Technology Strategies. Steven Lang of the Design Patterns Team then presented the draft increment of the Design Pattern and covered the details of its content and development. Stakeholders from various OI&T offices and organizations, both internal and external to VA, shared their questions, comments, and insights related to the content covered in the presentation. The presentation and Q&A session lasted roughly 1.5 hours.

#### Key Discussion Points:

The presentation content can be found in Appendix B.

Key items discussed during the Q&A portion of the public forum are paraphrased and summarized below.

- ***External Credential Service Providers (CSPs) and VA***
  - All externally facing applications that want to leverage FICAM compliant CSPs have to do so through IAM’s SSOe infrastructure. The IAM team is working to migrate a number of applications to the use of SSOe.
  - IAM will also be managing VA’s integration with the Federal Credential Community Exchange (FCCX) which will allow VA to leverage credentials from a potentially larger number of CSPs.
  
- ***Tokens shared through mobile applications***
  - SAML tokens will continue to be the primary format for authentication for user information exchange. SAML tokens can be carried across both REST and SOAP.

- While JSON is gaining attention, no formal standards or vetting have been finalized. New tokens can be supported once their standards are formalized and VA has agreed to a standard format for their use.
  - Various CSPs and their interfaces must be adaptable to mobile. IAM has solutions that work for both native client and HTML.
  - All of the current IAM solutions are workable in REST environment and are already supported through the current infrastructure.
  - Not all CSPs that IAM has on-boarded have provided a user log in page that is designed to support a mobile environment. IAM can work with application designers to help mitigate this issue.
  - Project Management Accountability System (PMAS) milestones and Enterprise Technology Architecture (ETA) compliance, reviewed by the Architecture and Engineering Review Board (AERB) check adherence to IAM compliance criteria.
  - A number of groups in the VA are working in the mobile space with mobile applications and authentication, and IAM is trying to meet those needs in the absence of overarching mobile guidance or standards.
  - OAuth support is being developed, and will provide support for implicit and authorization grant models. It will be external only, and will include user consent management, client registration, device registration and other components.
- ***Design Patterns Governance and Compliance Issues***
    - TS is currently working with ESS Security Workgroup to identify other AAA-related strategies and what constitutes useful outputs to operationalize them. In terms of implantation strategies, executive-level policy directives may end up being the lever to implement new patterns and policies. TS staff are focusing on compliance and coordination issues, ensuring that Design Pattern compliance checks are tied into the PMAS and AERB and other EA-related processes to ensure that new system development compliance with Design Patterns is measured and governed. ETA and OneVA compliance checklists are still being finalized.
    - For existing steady-state systems, there isn't currently a forcing function to make legacy applications and systems compliant with Design Patterns. It is possible that security issues or requirements may emerge and force the transition of current systems to be compliant with the Design Pattern.

**Next Steps:**

1. The TS team will finalize the Design Pattern for VAIQ submission and formal review.
2. After formal approval, AAA Design Pattern will be worked into an overarching model for authentication frameworks across the enterprise.

**Appendices:**

- A. Participant List
- B. Presentation Slide Deck

## Appendix A: Attendee List

<i>Last Name</i>	<i>First Name</i>	<i>Affiliation</i>
<i>Beeler</i>	<i>Dave</i>	<i>IBM</i>
<i>Bogden</i>	<i>Nicholas</i>	<i>VA - TS</i>
<i>Brooks</i>	<i>Joseph</i>	<i>VA - TS</i>
<i>Burke</i>	<i>John</i>	<i>VA - OI&amp;T</i>
<i>Cox</i>	<i>Keith</i>	<i>VA</i>
<i>Cronkite</i>	<i>Wesley</i>	<i>MPS</i>
<i>Davis</i>	<i>John</i>	<i>VA</i>
<i>DeAntonio</i>	<i>Damien</i>	<i>Engility</i>
<i>Divi</i>	<i>Kamal</i>	<i>MITRE</i>
<i>Donnelly</i>	<i>Sean</i>	<i>RSA</i>
<i>Eiben</i>	<i>Kevin</i>	<i>MITRE</i>
<i>Ellsworth</i>	<i>Caitlin</i>	<i>MPS</i>
<i>Grant</i>	<i>Walter</i>	<i>VA</i>
<i>Grassi</i>	<i>Paul</i>	<i>NIST</i>
<i>Grasso</i>	<i>Gayle</i>	<i>IBM</i>
<i>Harcey</i>	<i>Derrick</i>	<i>Oracle</i>
<i>Herndon</i>	<i>William</i>	<i>MITRE</i>
<i>Iglehart</i>	<i>Gordon</i>	<i>VA - VBA</i>
<i>Irizarry</i>	<i>Gabriel</i>	<i>IBM</i>
<i>Jackson</i>	<i>Dusty</i>	<i>VA - TS</i>
<i>Lang</i>	<i>Steven</i>	<i>BAH</i>
<i>Lee</i>	<i>Vernon</i>	<i>Microsoft</i>
<i>Luedtke</i>	<i>Terry</i>	<i>VA - ASD</i>
<i>Mallia</i>	<i>Anthony</i>	<i>ESC</i>
<i>May</i>	<i>Thomas</i>	<i>PwC</i>
<i>Richer</i>	<i>Justin</i>	<i>MITRE</i>
<i>Riordan</i>	<i>Kevin</i>	<i>CA</i>
<i>Russell</i>	<i>Mark</i>	<i>MITRE</i>
<i>Saxena</i>	<i>Ritesh</i>	<i>IBM</i>
<i>Vessels</i>	<i>Perry</i>	<i>Engility</i>
<i>Welchel</i>	<i>Andrew</i>	<i>RSA</i>
<i>Wippich</i>	<i>Michael</i>	<i>RSA</i>