



Secure Messaging, AAA Design Pattern Public Forum Office of Technology Strategies February 18, 2015

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 Secure Messaging, and provide feedback prior to the Design Pattern's finalization, publication and implementation

Background: The Technology Strategies Design Patterns Team has been soliciting input for the development of Secure Messaging 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. An introduction of the department was provided by Stephany Perez-Cohen followed by an overview presented by Joe Brooks of the Office of Technology Strategies. Tony Chiang and Brian James 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 hour.

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.

- What is the eMI security level? Do you see that the eMI will be the conduit to take over the role of access / verify from the local vista to an enterprise level?
 - Tokens are provided by IAM. eMI can process them and sends to another service to verify them again. Currently working a reference implementation.
 - eMI verifies the copy. VISTA verifies that it came from eMI. Doesn't cover other connection methods. SAML token processing method could also be useful for other tokens.
- Slide 10, "While TLS/SSL are essential for foundational data transmission security it is insufficient to protect data in a SOA environment." Can you elaborate on the security issues relative to SSL/TLS?

- Instead of insufficient we can change to a better word. Idea is that it's necessary for point-to-point security but it's not well suited when there are intermediaries. We need more security than that. We can change the word insufficient.
- There are other types of encryption that we use for point-to-point. Looking for an overall enterprise solution. It's not the most efficient way to do things and does not allow us to manage efficiently across the board.
- Why isn't REST security part of the scope?
 - REST is handled differently than SOAP messages. We're covering enterprise solutions and SOAP is used more frequently in VA. Not addressing it here because it's very different. MITRE team looking at how to manage secure REST messages but it's a different dynamic.
 - We're developing something that isn't hitting the intended audience. Maybe folks are looking to understand SOAP-based security better and get guidelines for that. If we're going to leave it out we should have it quickly coming behind.
- Is there a use case for data at rest encryption on a mobile device?
 - Yes, we have begun a description of that in the Mobile Architecture DP (approved in January). Expect we'll flesh this out in future increments within a separate discussion with everyone on the line as well as other pertinent stakeholders.
- eMI contains an API/XML gateway (slide 15). Are there two gateways?
 - Vendors that we spoke to said that we want to separate eMI from the gateway to conduct those same functions (echo...)
 - Within the eMI stack there's an API/XML gateway. If there's another one we'll need to be clear in our guidance about that.
- Is there a distinction between clients on the left that are internal vs. external to VA? Is there a different pattern for internal vs. internet clients?
 - Per the AA&A we are not distinguishing between the two. The point of this document is to show that we're securing the messages and that credentials will not be altered as they traverse the middleware. Focused on the current use of SOAP. MITRE is piloting the use of other paradigms but we're talking to approved standards.

Next Steps:

The TS Design Pattern Team will finalize the Design Pattern document to address feedback from this Public Forum, and begin formal approval staffing. Updates will include additional inputs regarding architectural guidance and references to implementation guidance. The document will be edited to ensure Section 508 compliance, and the final approved version will be posted onto the ASD TS public-facing website: http://www.techstrategies.oit.va.gov/docs_design_patterns.asp

Appendices:

- A. Participant List
- B. Presentation Slide Deck

Appendix A: Attendee List

Last Name	First Name	Affiliation
Barnard	Jason	
Beeler	Dave	IBM
Behr	Steven	
Brooks	Joseph	VA - TS
Brown	Randy	
Chiang	Tony	BAH
Croswell	Thomas	
Cunningham	Robert	
Dance	Michael	BAH
Dell	John	
Fowler	Dennis	SMS
Gaus	Scott	<u>IBM</u>
Gordon	Adrian	BAH
Hart	Michael	MITRE
Hasedzic	Semir	MPS
Hilton	Travis	BAH
Holt	Russell	
James	Brian	BAH
Lin	David	
Luedtke	Terry	VA
Lycas	John	
Mallia	Tony	
McDonough	William	Insignia
Monadizadeh	Shari	BAH
Murphy	David	
Oster	Steven	
Perez-Cohen	Stephany	MPS
Shah	Nimish	
Simmons	Michael	Leidos
Susarla	Narasa	Leidos
Seymour	Dennis	
Vessels	Perry	
Wimsatt	Kenneth	VA - VBA
Zetervall	Matt	

Appendix B: Presentation Slide Deck



Secure Messaing
DP Public Forum (2-

DRAFT