



Authentication, Authorization & Audit Design Pattern Public Forum

Office of Technology Strategies

April 9, 2014

Meeting Summary

Purpose: The Office of Technology Strategies' (TS) Design Pattern Team has been soliciting input for the development of the Authentication Authorization & Audit (AA&A) Design Pattern covering internal VA user authentication to applications. 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. In this Public Forum, the TS Design Pattern Team shared their findings and presented an updated version of the design pattern document to gain concurrence on the content for version 1.0.

Overview: The TS Design Pattern Team presented their updated design pattern for Authentication, Authorization & Audit internal VA user authentication to applications. An introduction of the department was provided by Chief Technology Strategist Joe Paiva, followed by an overview presented by Dusty Jackson, VA Technical Products Team. Steve Lang of the AA&A Design Patterns Team then presented the design pattern and covered the details of its content and development. Stakeholders from various OIT 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 two (2) hours.

Key Discussion Points:

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

- MVI as Identity Store
 - *Question – John Horton (SRA):* Why is MVI being used as identity store? There should be two separate data stores for internal vs. external users.
 - *Response – Damien DeAntonio (IAM):* MVI is the identity store and provisioning service is the attribute store. Both are closely integrated, but they are still separate. The reason it is one entity is that maintaining identity and attribute stores as two completely separate entities can run the risk of multiple accounts for individual users who are both internal and external (employee vs. veteran).
- Authentication Protocol Related Discussion
 - *Question – Mark Russell (MITRE):* What technology is the IAM SSOi solution currently built on?
 - *Response – Damien DeAntonio (IAM):* CA SiteMinder.
 - *Question – Derrick Harcey (Oracle):* Is SAML 2 the only means for accepting indirect authentication, or are other tokens leveraged too?

- *Response – Damien DeAntonio (IAM):* There are a couple of different ways to get user information to application based on the needs of that application. Not limited to SAML 2.
- Level of Assurance (LOA)
 - *Question – Mark Russell (MITRE):* Do we have a sense of how many LOA 4 applications we'll encounter in VA?
 - *Response – Steve Lang (TS):* There has not been a deep dive into the current metrics for risk assessment of applications within VA, but it does not appear that there will not be too many applications that are at LOA 4.
 - *Damien DeAntonio (IAM):* So far, IAM has only had 3 applications rated at LOA 3 based on risk assessment of their application(s).
 - *Question – Mike Davis (VHA):* If a user is authenticated to the network at LOA 4, why aren't we using that across the board for authentication to applications?
 - *Response – Steve Lang (TS):* We are encouraging applications to use the PIV LOA 4 authentication protocol if appropriate, but based upon discussion with industry experts it seems to be less realistic to implement PIV/PKI authentication at LOA 3-1, the use of PIV/PKI and isn't the current best practice.
 - *Question – Eric Jurasas (VA SDE):* Unaware we couldn't achieve LOA 3 & 4 using AD if NTLMv2 is used. Is this a correct understanding? Where is the language to support that in the NIST guidance? NIST documents should be the authoritative source.
 - *Response – Steve Lang (TS):* This statement was based upon a discussion with DISA/NIST about the DoD AD infrastructure. *We will set up a follow up call with relevant parties to discuss this point and get the right information.*
- Mobile Authentication
 - *Question – Kevin Todd ():* Does the content in this Design Pattern cover mobile user authentication?
 - *Response – Steve Lang (TS):* The current Design Pattern is focused on PIV enabled internal users, but not mobile. Mobile presents a lot of additional challenges, such as the inability to use a PIV card. Future Design Pattern increments may address mobile authentication.
 - *Comment – LJ Neve (BAH IAM BPMO):* For internal mobile devices, NIST has two (2) DRAFT documents on derived credentials, where PIV is used to create a virtual credential for mobile user authentication.
- Design Pattern Development
 - *Question – Andrew Welchel (RSA) –* Do you see any primary next increment connections to this authentication DP? What's the typical development timeframe?
 - *Response – Steve Lang (TS):* Design Patterns are being developed quarterly according to the government fiscal year. Based on discussions with the ESS

Security Working Group, next iterations may have something to do with the passing of tokens and the security around data calls through the Enterprise Service Bus (ESB). There has also been discussion on covering external user authentication or user authorization (appropriately scoped). There has not yet been a final decision made with respect to an increment two focus.

Next Steps:

1. The TS will accept additional comments and input for two weeks (04/09 – 04/23)
2. The TS team will finalize the Design Pattern for formal internal review after the comment period is closed and prepare the document to be published to VA's Enterprise Architecture.
3. Survey will be sent to Forum participants to gain insight into process and potential improvements.
4. TS DP Team will set up a meeting with DISA, Microsoft, OIS, and NIST to discuss Kerberos/NTLM limitations and risks in greater detail.

Appendices:

- A. Participant List
- B. Presentation Slide Deck

Appendix A: Attendee List

<i>Last Name</i>	<i>First Name</i>	<i>Affiliation</i>
Akst	Glenn	Oracle
Baggs	Marcus	OIT
Beecher	Lauren	BAH
Beeler	Dave	IBM
Behr	Steven	BAH
Behseta	Parker	IBM
Brooks	Joseph	VA – TS
Church	Al	MITRE
Coppinger	Todd	VHA
Cunningham	Robert	OIT, IAM BPMP
Daldos	Ronnie	MITRE
Dam	Steve	BAH
Davis	John	IPO
Davis	Mike	VHA
DeAntonio	Damien	HPTI, IAM
Dinkel	Chris	VA
Duncan	Douglas	VA
Dyer	Mike	VA, CH33
Ellsworth	Caitlin	MPS
Emery	Rodney	DoD/VA IPO
Fernandez	Ernest	ACET
Fredricks	William	ACET
Gauss	Scott	IBM
Golden	Deborah	Deloitte
Grasso	Gayle	IBM
Hajj	Ramsey	KPMG
Harcey	Derrick	Oracle
Hernandez-Bethea	Giselle	POA
Horton	John	SRA
Irizarry	Gabe	IBM
Jackson	Dusty	VA – TS
Joe	Paiva	VA – TS
Jurasas	Eric	SDE
Kauffman	Caroline	KPMG
Lambert	Christal	PwC
Lang	Steven	BAH
Lawton-Belous	Joshua	VA – TS
Luedtke	Terry	OIT

<i>Last Name</i>	<i>First Name</i>	<i>Affiliation</i>
Mallia	Anthony	ESC
May	Thomas	PwC
McCarthy	Megan	PwC
Meadows-Stokes	Jacqueline	VA - TS
Neve	Laurence	BAH IAM BPMP
Pearcy	Patrick	DoD/VA IPO
Perez-Cohen	Stephany	MPS
Pooley	Don	ASD/ACET
Renzi	Mauricio	RSA
Rikarts	Andrew	OIT, OCS
Riordan	Kevin	CA
Ronkowitz	Justin	BAH
Russell	Mark	MITRE
Santana	Al	VBA
Sastry	Anand	HPTI
Saxena	Riteh	IBM
Schmidt	Robert	IAM
Sikorski	Scott	PwC
Todd	Kevin	VHA OIA
Urbanski	Joe	OIFO
Veach	Kathleen	ACET
Vessel	Perry	IAM
Vogel	Skip	Oracle
Welchel	Andrew	RSA
Weldon	Larry	OIT
Yi	Chih-Weh	Deloitte