DoD Non-Acceptance of DoD-Approved Credentials:
Transglobal Secure Collaboration Participation White Paper

SUMMARY

The Problem. The DoD requires Federal contractors to perform strong authentication to DoD hosted applications. To fulfill this requirement today, Federal contractors are typically issued DoD credentials - either Common Access Cards (CAC) or DoD External Certificate Authority (ECA) software or hardware based certificates - in spite of DoD policy regarding the acceptance of external credentials.

Although existing DoD CIO policy ***encourages*** application owners to accept DoD-approved PIV-I credentials, it ***does not require*** or even promote their acceptance for eligible applications.*

The Consequences. The absence of such a requirement has led to: 1) slow to almost non-existent uptake on the part of DoD; 2) need for DoD and TSCP to support multiple identities for each individual and related infrastructures; 3) significantly higher than necessary costs of operations to both DoD and TSCP; 4) disconnect between areas in DoD enterprise services and individual application owners; 5) duplicate identities due to gaps in provisioning and de-provisioning of identities; 5) lack of data available to contractor companies regarding DoD credentials and user accounts; and, 6) resulting security gaps that introduce risk.

TSCP Recommendations. TSCP proposes the following recommendations to DoD CIO:

- ***Strengthen and Enforce Policy across DoD.*** Update and strengthen the policy to require the acceptance of PIV-I credentials whenever possible to include a due date for when all Services and Agencies must recognize and begin utilizing industry issued PIV-I credentials.
- ***Accept Highest Assurance Level Available.*** Request that DoD accept the highest assurance level of certificates held by the user.
- ***Establish Program Credential Requirements through Contracts Administration.*** Establish a consistent program notification mechanism to inform companies through the contracts process of the credential requirements for any given program.
- ***Consolidate Instructions and Information.*** Provide consistent information across DoD regarding credential acceptance to include a common and advertised website; clear and consistent information and instructions at each application owner website; and, the ability for each company to access information on its user accounts and certificates.
- ***Follow JPAS Model.*** Follow the JPAS model for the acceptance of Federal PIV, PIV-I for Non-Federal Issuers and other DoD-approved external credentials and implement its process for provisioning, requirements collection, implementation and communications.

* Relevant policy includes 22 July, 2008, *Approval of External Public Key Infrastructures*, 05 October, 2010, *Department of Defense Acceptance and Use of Personal Identity Verification-Interoperable (PIV-1) Credentials* and 05 November, 2011, *Department of Defense Continued Implementation of Homeland Security Presidential Directive-12 (HSPD-12) and Identity Credential and Access Management (ICAM) Guidance* (in support of 03 February 2011, OMB issued Memorandum 11-11, which requires the PIV enablement of applications across the Federal government) .

The purpose of this white paper is to extend a request from the Transglobal Secure Collaboration Participation, Inc. (TSCP) to the Department of Defense (DoD) CIO to work with industry to 1) increase the security of authentication between industry and DoD by strengthening existing DoD policy on the acceptance of DoD-approved external credentials, 2) accelerate the PIV enablement of DoD applications to accept strong external credential in accordance with Federal and DoD CIO policy, and 3) take advantage of cost efficiencies associated with optimizing the credential issuance process by having DoD and industry issue their own credentials and have them accepted by each other.

TSCP is an international cooperative association in which leading Defense companies and key government agencies work together to establish and maintain an open, standards-based framework for secure collaboration and assured information sharing between parties. Principal TSCP members are The Boeing Company, BAE Systems, EADS, Northrop Grumman, Lockheed Martin and Raytheon.

Background

DoD's Strong Authentication Requirement. The DoD requires Federal contractors to perform strong authentication to DoD hosted applications. To fulfill this requirement today, DoD Federal contractors are typically issued DoD credentials - either Common Access Cards (CAC) or DoD External Certificate Authority (ECA) software or hardware based certificates. Both options are time-consuming and costly to issue and maintain for both DoD and the Federal contractors and the approach of using DoD credentials for external users does not align with federated enterprise credential initiatives. In addition, because there is no formal process for notification of a contractor's status change, credentials in the DoD system are not de-provisioned consistently or in a timely fashion.

DoD Policy on DoD-Approved External Credentials. Recognizing these inefficiencies, on 22 July, 2008, the DoD CIO signed the memorandum, "Approval of External Public Key Infrastructures." Even prior to the memo, DISA's Joint Interoperability Test Command (JITC) had established a JITC testing process to approve credentials for DoD use. The memo authorized application owners to accept credentials issued by entities doing business with DoD that are at a medium level or higher and cross-certified with the Federal Bridge and successfully underwent DoD testing. In response, a number TSCP members (Federal contractors) made significant investments to making modifications to comply and establish PKIs and cross certify them with the Federal Bridge and undergo DoD testing. Because the cross-certification process and DoD interoperability testing verifies compliance to the credential processes and security requirements, these credentials are trusted at the same level as CACs and ECA hardware-based certificates.

Subsequent to the 2008 memo, in October 2010, DoD CIO issued Department of Defense Acceptance and Use of Personal Identity Verification-Interoperable (PIV-I) Credentials, which highly encouraged, but still did not require the acceptance of PIV-I credentials. In February 2011, OMB issued Memorandum 11-11, which requires the PIV enablement of applications across the Federal government; this OMB Memo was supported by a DoD CIO Memo issued on November 5 2011, "Department of Defense Continued Implementation of Homeland Security Presidential Directive-12 (HSPD-12) and Identity Credential and Access Management (ICAM) Guidance."

Policy vs. Practice. The uptake in DoD's acceptance of other Federal-issued PIV cards and conformant industry-issued PIV-I and Federal Bridge credentials has been extremely slow, to almost non-existent. DoD application owners with strong authentication requirements continue to issue CACs or ECAs to contractors in lieu of accepting approved Federal and industry issued credentials.

Approval for Use vs. Required Use. Rather than directing application owners to accept external credentials whenever possible, the language of the policy "approves for use" external credentials; it ***does not require*** their acceptance and use. In fact, the memo reiterates (and thus reinforces) the approval for use of ECA credentials. In essence, this relays the message to application owners that the acceptance of external credentials is optional.

Industry Experience at DoD Relying Parties

Risk to Industry Credential Programs. As it moves to medium and high level hardware credentials, DoD's inconsistency in guidance on enablement and use are having a disruptive impact on TSCP members' program execution

and introducing significant risk to their smart card strategies and deployment plans. TSCP members' issued credentials comply with PIV-I standards, the non-Federal issuer specification for PIV/CAC for interoperable Federal use, which is approved for use within the DoD. Because DoD systems accept CAC cards, the enablement of DoD applications for acceptance of TSCP credentials is a secure and simple adaptation of existing DoD Public Key (PK) enablement.

Excessive Investment & Operational Costs. TSCP members collectively have invested more than $400M in adapting their infrastructures to issue company credentials in the spirit of the DoD policy. In addition to incurring the costs of cross-certification to the Federal Bridge, the principal TSCP members have all established direct bi-lateral trusts with the DoD and undergone JITC testing. International members have committed to TSCP's specifications – which have been established to align with DoD policy - and expect acceptance of the credentials produced in compliance with those specifications. However, because uptake on the acceptance of their credentials is low, DoD and TSCP members are required to support three types of credentials. As a result, ***both*** TSCP and DoD incur excessive costs to maintain unnecessary redundant infrastructures that support multiple identities and credentials.

Acknowledging there may be unique circumstances requiring continued use of ECAs, the DoD policy nonetheless led to industry's expectation that DoD would progressively discontinue the issuance of ECA certificates and CACs for contractors in favor of partner-issued PIV-I credentials. Not only does the cost of distributing additional credentials to member contractor employees continue to be prohibitive, but also TSCP's European members are reluctant to have their employees' identities tied to a U.S. identity scheme. And because DoD does not make available a list of a company's users who already hold ECAs, TSCP member employees often end up with multiple ECAs.

Disconnect between DoD CIO/Enterprise and Application Owners. The absence of promotion of external credentials has led to a disconnect between areas in DoD responsible for providing related enterprise services and individual application owners, specifically, a lack of enterprise coordination, inconsistent policy and guidelines, non-availability of credential data, and inconsistent language and messaging. For additional detail, see Appendix A.

As an example, since 2008, Northrop Grumman has only been able to achieve a 21% acceptance of its OneBadge credential in DoD. See Appendix B for Northrop Grumman's experience with DoD Relying Parties. It is Illustrative of the experience of all the TSCP members.

The Opportunity: IT Efficiencies for DoD & Industry

DoD Excellence: Emulate the JPAS Model. TSCP wishes to call attention to DoD's excellent approach on the JPAS model for PK enablement as a potential model for the acceptance of external credentials going forward. This program accepts PIV-I and TSCP member credentials and has an outstanding process for provisioning, requirements collection, implementation and communications.

Elimination of Multiple Identities/Credentials. For TSCP members, the issuance, use and acceptance of PIV-I and medium hardware credentials is consistent with DoD, GSA and industry standards and direction (i.e., PIV and CAC). The process of proofing, vetting and binding of an individual to a credential is accomplished in a common manner across all TSCP member companies. DoD acceptance of these TSCP credentials would enable TSCP members to maintain a single identity and credential for each of its users. Equally important, DoD would have the opportunity to streamline its own infrastructure and realize IT efficiencies.

Cost Reduction. Acceptance of externally issued non-Federal credentials by DoD would significantly reduce the cost burden to the business areas and programs, as well as to DoD, by eliminating the need to procure, issue and administer expensive ECA and CAC credentials to meet program requirements. Today, as an employee moves from one program to another, ECA and CAC credentials are procured (and often duplicated), retired, and procured again, all creating a recurring and unnecessarily high cost of doing business. Often the ECA costs are charged back to DoD; thus DoD is paying for the JITC testing of a credential they don't accept while at the same time paying for the issuance of ECAs.

Error & Risk Reduction. Acceptance of a single external credential would reduce the opportunity for errors when users are required to have multiple credentials various encryption certificates to satisfy inconsistent requirements across DoD programs and contracts. This fragmentation of identity and authentication presents security challenges and introduces risk.

Increased Security/Facilitate Deployment to Supply Chain. Accepting the Personal Identity Verification Interoperability For Non-Federal Issuers (PIV-I) and medium hardware Federal Bridge credential will unleash the market opportunities associated with credentialing of the supply chain inside and outside the US. In effect, the full acceptance of TSCP member credentials will facilitate the deployment of the Trust Circle and at last make possible the legitimate Return-On-Investment for those who have made the effort and investment to comply.

Summary and Recommendations

In the years since the issuance of DoD memorandum, "Approval of External Public Key Infrastructures," TSCP members have made major investments in, and adaptations to, their infrastructures and program operations with the expectation of leveraging their secure company credentials to access DoD systems. However, because the policy does not mandate the acceptance of external credentials, the uptake has been much lower than anticipated and TSCP members (as well as DoD) have experienced significant adverse effects in the form of:

- ***Risks to credential programs*** due to lack of consistency, guidance and practices of DoD as a relying party;
- ***Expensive investment outlays*** by TSCP members who have issued DoD-approved strong credentials to support the DoD policy;
- ***High operational costs*** to comply with DoD policies that require TSCP members to support multiple identities, credentials and infrastructures across DoD contracts and application owners;
- ***Lack of enterprise coordination*** producing a disconnect between DoD CIO/Enterprise and application owners and resulting in a lack of standardization across the enterprise

By adequately addressing these issues, DoD and TSCP have the opportunity for significant IT efficiencies through the elimination of multiple identities/credentials, cost reduction, error and risk reduction, and increased security by facilitating deployment of high level credentials to the supply chain.

TSCP Recommendations

- ***Strengthen and Enforce Policy across DoD.*** Update and strengthen the policy to require the acceptance of PIV-I credentials whenever possible to include a due date for when all Services and Agencies must recognize and begin utilizing industry issued PIV-I credentials.
- ***Accept Highest Assurance Level Available.*** DoD should accept the highest assurance level of certificates available. Inconsistent application of directives leads to added costs for contractors.
- ***Establish Program Credential Requirements through Contracts Administration.*** Establish a consistent program notification mechanism to inform companies through the contracts (or contract MOD) process of the credential requirements for any given program. Currently, network administrators are directing contractors to procure or change certificate types, often after contract execution.
- ***Consolidate Instructions and Information.*** Provide consistent information across DoD regarding credential acceptance to include a common and advertised website; clear and consistent information and instructions at each application owner website; and, the ability for each company to access information on its user accounts and certificates.
- ***Follow JPAS Model.*** Going forward, follow the JPAS model for the acceptance of Federal PIV, PIV-I for Non-Federal Issuers and other DoD-approved external credentials and implement its process for provisioning, requirements collection, implementation and communications.

Appendix A

Disconnect between DoD CIO/Enterprise and Application Owners

The absence of promotion of external credentials has led to a disconnect between areas in DoD responsible for providing related enterprise services and individual application owners, specifically:

- **Lack of Enterprise Coordination.** Although there are services and tools available to facilitate the acceptance of external credentials, most application owners are unaware of their existence. DISA, for example, has established a website PK-enabling team that assists DoD application owners through the process of adding an external credential to their trust lists. However, it has been TSCP's experience that DoD application owners are unaware of the existence of this DISA service and notice of its availability is not posted on websites where application owners or partners would expect to see it.

- **Inconsistent Policy & Guidelines.** Because of the lack of dissemination of standard guidelines related to the acceptance of external credentials, if and when DoD institutes a decisive program to eliminate ECAs, for example, TSCP members are concerned about the potential risk associated with hundreds of programs, each instituting a unique set of guidelines, options, and immediate timelines, with no consistent policy or direction.

- **Lack of Credential Data Availability.** DoD does not make data related to its credential services available to its external partners. In particular, external partners are not notified of changes to accounts (e.g., certificate expiration). As a result, TSCP members are unable to maintain accurate records as to who and how many of its users have DoD accounts.

- **Inconsistent Language & Messaging.** Application websites deliver inconsistent and frequently incomplete language and messaging related to credential acceptance and required credential strength. For example, there are sites that use the term "credential" and "DoD CAC" interchangeably, even when they are actually referring to ECA hardware certificates. TSCP users spend an inordinate amount of time trying to determine exactly what each website requires.

Appendix B

Northrop Grumman Procedures for Gaining Acceptance to DoD Applications

The following is a specific example of Northrop Grumman's experience with DoD Relying Parties, however it is Illustrative of the experience of all the TSCP members.

Northrop Grumman has been pursuing acceptance of its OneBadge credentials among DoD application owners since completing JITC testing and execution of the Interoperability agreement with DoD in November of 2008. Since that time, Northrop Grumman has requested access to over 260 individual DoD web sites using its OneBadge to authenticate. Of those, 55 or 21% of those sites have agreed to accept OneBadge. The remainder requires that Northrop Grumman employees to purchase an ECA certificate or obtain a CAC card from DoD.

OneBadge DoD Website Production Status	Total	Pct.
Approved	55	20.7%
Testing w/OneBadge	1	0.4%
Declined	3	1.1%
Preliminary Discussions	13	4.9%
Initial Contact	54	20.3%
No Response from Site Owner	140	52.6%
Grand Total	**266**	

Approval time varies with each site; however average timeframe required from initial contact to acceptance is typically 120-180 days for those cases where OneBadge authentication was approved by the site. Generally, if a site has not accepted OneBadge within 180 days, there is little chance for success.

The approval challenges include identifying a site's owner including contact information and the approving security authority. Once identified, additional review up the chain of command is required. Another challenge is that many applications use a portal to authenticate users. This means that every application on the portal would have to approve use of OneBadge to authenticate for access. In order to gain acceptance of OneBadge, NG has established a standardized procedure.

1. NG employee must provide the web site URL, name and contact information of the application owner, number of NG employees who need access and the contract for which this access is required. A help desk contact is not acceptable as they won't provide contact information and seldom follow-up on a request.
2. NG reaches out to the web site owner and works to identify the approving authority for their site, portal, or application.
3. Once the proper parties are identified NG provides them with a detailed briefing package on external PKI acceptance including the applicable governing policies, referenced approvals, and other various inputs a such as our most recent external PKI audit letter.
4. The process requires a number of repeated emails, phone calls, etc. to press the site management or security office to consider this change. Sometimes re-starting the process is required as staff turns over or other matters take precedence and our requests are forgotten.
5. Once accepted, we test with their test system, if available, and then work with the site to implement.