FICC Shared Service Provider (SSP) Industry Day, 3/11

Questions and Answers

A request to repeat the URL where the presentation and documents will be stored was made.

-Judith Spencer repeated the URL, www.cio.gov/ficc/ssp_documents.htm, to the audience

Why is the SSP necessary when services are currently available on the ACES and GSA smart card contract?

-Judith Spencer replied the SSP program does not establish a contract but creates a qualified bidders list. The CIO Council last April tasked the FICC to implement a common policy for PKI services. The Subcommittee does not want to limit agencies to one solution. The Subcommittee does want to set a standard for PKI that implements this common policy in the Federal government. There are approximately 80 smaller government agencies that would like to use SSP services.

The SSP Roadmap document, Section 4 indicates that deviations to the order of the process may happen to accelerate generation of a qualified bidders list for June 30. Given that other providers will be looking to be added after June 30, what process will they use and will the initial deviations give unfair advantage to the first providers?

-Tim Polk replied the process deviation clause was added to speed up the qualification process by permitting activities to occur in parallel, as opposed to in a step by step manner. The Roadmap document was changed to explicitly allow for activities to occur in parallel, so there is no longer a need to allow for deviations. The out clause will be removed from the SSP Roadmap document.

What audit instruments will be recognized for Step 3? (SAS 70, WebTrust, Other)

-Tim Polk replied SAS 70 and WebTrust have been used in the past. There is not a requirement to use a specific audit instrument. This is designed to maximize vendor flexibility. The compliance auditor must review whether or not the CPS meets all Common Policy requirements and whether the vendor operates in compliance with the CPS.

Can OCD testing be accomplished in a test environment or must the infrastructure be production CAs, Repository, etc.?

-Tim Polk responded by stating vendors are encouraged to use a test environment. The Subcommittee does not expect vendors to use a live environment.

Does the environment need to be subordinate to the Common Policy Root prior to OCD testing?

-Tim Polk replied no, we are not conducting path validation testing during the OCD. The Common Policy Root CA will issue a certificate to your CA upon completing the qualification process. CAs will not be required to be re-keyed.

Tim Polk mentioned that in the OCD there will be a demonstration PIN reset. Will this include a requirement to prove that data that was previously encrypted can be accessed again?

-Tim Polk replied the SSP was interested in these results. We will check access to keys for decryption.

The ACES program has OMB approval to gather information. Will this approval also be granted to the SSPs?

-John Cornell replied, OMB has granted ACES a privacy act number for ACES as a system of records. The federal identity credentials now in existence have OMB privacy act numbers as agency specific systems of records. These existing authorizations will be revised to accommodate the new identity credentials, on an agency by agency basis.

Will the Schedule 70 contract cover compliance assessments and C&A or will it just address items provided by qualified SSPs?

-John Cornell replied the SSPs are authorized to provide provisioning of PKI services under the Common Policy. Not everything will fit into the Schedule 70. Compliance assessments and C&A are open for discussion and the SSP will have to take this issue to the FSS. The SSP would like to add additional items to the Schedule 70. There might be a special item number for PKI related services and another for non-related services. Additional information on this topic will be provided at a later date.

The requirements of the Repository seem to be contradictory regarding self-issued and self-signed certificates. Why wouldn't all certificates, including self-signed certificates, be included in the repository?

-Nelson Hastings responded to this question by stating that self-signed certificates do not need to be in the repository since they are not needed for path discovery or validation. Self-signed certificates are only used as trust anchors and should be obtained by relying parties through secure, out-of-band mechanisms. However, while there is no requirement to place self-signed certificates in the repository, there is no prohibition against it either.

Fred Catoe mentioned the ability to use flexible certificate profiles. Experience shows that profile differences can create issues. Is there an overarching definition of certificate profile?

-David Cooper addressed this question by stating the CRL and Certificate document provides the overarching definition. This document contains tables for CRLs, CA certificates, end entity certificates, etc. It provides some flexibility for adding non-critical extensions. The approved flexibility should not cause interoperability issues.

The Certificate and CRL Profile states that in distinguished names (DNs), where an attribute value is of type DirectoryString, the PrintableString encoding shall always be used. It provides an exception, however, for the common name attribute in the subject field of certificates issued to humans, where UTF8String may be used if the person's name can not be encoded as PrintableString. Encoding some attributes as PrintableString and others as UTF8String in the same DN causes Microsoft to crash.

-David Cooper responded that there is no solution to this issue. Encoding the entire end entity subject name using UTF8String may avoid crashes with Microsoft, but it would cause name constraints processing to fail (as is permitted by RFC 3280). So, the best option is to leave the profile unchanged and hope that Microsoft will fix the problem that leads to crashing. In the meantime, agencies should avoid the use of UTF8String whenever possible.

The Federal Bridge CA has been a key architectural element of the PKI effort. Is full certification with the FBCA a mandatory requirement of the SSP effort? Or will they need to demonstrate bilateral trust between themselves and the agencies on the Bridge?

-Judith Spencer responded that neither cross certification nor bi-lateral trust were mandatory. The Common Policy root is going to cross-certify with the FBCA.

How is the Common Policy Framework different from the FBCA CP?

-Judith Spencer replied that the FBCA CP was used as the source document for developing the Common Policy; however, the FBCA CP identifies four levels of assurance. The Common Policy Framework is written at the equivalent of medium level of assurance as defined by the FBCA CP. In the future the SSP will add an equivalent to high level of assurance.

Are you seeking a total vendor solution for all components? Can a vendor submit for partial components such as: Policy development, certification and accreditation, RA& End User training? Are you willing to accept teaming vendor solutions?

-Judith Spencer replied the Subcommittee is seeking to qualify PKI shared service providers. Partnering is acceptable. The Subcommittee is looking for a total solution that meets the specified criteria.

What steps have you taken or do you plan to take to gauge the interest within the government for these certifications? What is the demand and is there a current demand for the services?

-Judith Spencer responded by stating the FICC has membership from 25 primary agencies including the cabinet level agencies. The CIO Council has specifically asked for this work to be completed. This program is an important part of efforts to improve security within the government and ensuring federal employees are credentialed in a consistent manner. Most agencies are moving in this direction and interest is very high. A letter released by OMB in July 2003 instructed Federal agencies to participate with FICC in deploying PKI solutions.

When will the SSPs issue certificates to agencies? Is the Common Policy root up and is the existence of the Common Policy root a requirement for the SSPs? Can SSPs issue certificates without the root?

-Tim Polk answered this series of questions by stating, the Common Policy is finalized and the Common Policy root should be up by 6/30. The existence of the Common Policy root is not a requirement for the SSP program. The Federal Bridge can issue certificates to the SSP as an alternative approach if the Common Policy root is not available.

Is the intent of the effort to leverage existing CAs or existing business capabilities of Service Providers? If CAs- does this mean that existing CAs must now be rooted under the new Federal CA?

-Tim Polk replied, the Subcommittee intends to leverage existing CAs where possible. After qualifying as an SSP, certificates can be issued with the new Common Policy OIDs. The only additional action required will be for the Common Policy root to issue CA certificates to the SSP.

When will you issue qualification instructions?

-Tim Polk responded by stating the roadmap document provides the qualification instructions. The Subcommittee is working with C&A people at NIST concerning compliance audits. A checklist of items for the C&A audit will be developed to identify requirements concerning the Common Certificate Policy, compliance audit, and WebTrust. The Subcommittee would like to publish the checklist by the end of April. Tim asked the vendors to contact the Subcommittee if they feel additional qualification instructions are required.

Please advise me on how to provide a legitimate compliance auditor.

-Judith Spencer recommended the audience go to the website of the IACPA or seek expertise in PKI technology evaluation. Vendors can contact the Subcommittee to confirm recognition and acceptability of the auditor under consideration.

The OCD and C&A process will require an interested provider to make major investments to qualify as an SSP. Some of us have been down this road before, promised major business opportunities with the government in exchange for the investment made to become qualified as a provider of a specialized service, and just as the business starts to materialize the government changes the rules. What assurance do businesses have that we won't face the same situation here in 3 years?

-Judith Spencer responded that there is no intention of derailing on-going initiatives. The program is seeking to build on existing capabilities within the government. No guarantees can be made about the state of the initiative three years from now; however, we will continue to work to keep the direction consistent as far as possible.

What is the impact on my existing CA if we decide to issue certificates as an SSP? How does subordination under the Common Policy root affect my previously issued certificates?

-Tim Polk replied the root CA will issue a certificate with the subject name of SSP CA and SSP CA public key. The Common Policy CA will generate a self-signed certificate that may be distributed by your CA to its users for use as a trust anchor. However, users that currently rely upon the existing CA as the trust anchor should not be affected.

Vendors will be required to describe their CA architecture solution in their initial submission to the Subcommittee. Vendors operating more than one CA are encouraged to establish a hierarchy so that only one CA need be certified by the Common Policy root.

Will there be a key escrow policy?

-Tim Polk responded by stating the agencies will determine the policy for key escrow and services. The Subcommittee will not evaluate key escrow capability. Key recovery is not a requirement to be on the qualified bidders list (QBL). To be listed on the QBL, a vendor must be able to support smart cards.

Will card personalization be tested?

-Tim Polk answered this question by stating there is another group defining this policy. Currently there are no plans to test card personalization.

Once my solution is certified via the OCD, how can I update or upgrade it? What if I want to add new products or vendors to the solution base being offered? Is another OCD or C&A process required?

-Tim Polk stated major upgrades require a new C&A. However, a delta C&A covering modifications to the system can be performed instead of repeating the entire C&A process. The OCD does not have to be repeated when new pieces are added.

What are the C&A requirements for the agencies?

-Marianne Swanson stated agencies will have to certify and accredit the RAs they run and define how their system interfaces with the SSP. Agencies are required to complete C&A every three years.

What are the naming conventions for the certificates?

-Tim Polk replied the Common Policy defines the conventions but leaves flexibility concerning name forms.

For agencies in the process of implementing PKI, do they continue or reset their efforts (Department of Justice for example)?

-Judith Spencer replied this initiative does not require any agency already in the process of deploying a PKI or who already have an operational PKI to abandon their efforts. However, new funding for PKI deployment beginning in 2006 will require compliance with the FICC roadmap and SSP guidelines.

How will you verify a company can do smart cards? What about biometrics and physical access?

-Judith Spencer replied the OCD will validate the ability of PKI service providers to populate the GSC-IS compliant smart card. Government Smart Card Interoperability Specification (GSC-IS) compliant cards will be used to support the OCD. Biometrics are being addressed by another work group.

The last question was, Will use of the Qualified Bidders List (QBL) be mandatory? What compels the agencies to use the SSP?

-Judith Spencer replied that OMB will make this call and reminded the audience of the memorandum released in July 2003 mandating compliance with FICC policies on new PKI solutions. The FICC SSP has been tasked with the responsibility of providing FICC compliant solutions for credentialing Federal employees. Currently, use of the QBL is not mandatory.