Federal Public Key Infrastructure Policy Authority

SHA-256 Transition Lessons Learned

Version 1.0

May 21, 2011

Document History

Status	Release	Date	Comment	Audience
Final	1.0	5/21/11	Final Version	

Table of Contents

1. INTRODUCTION

1.1 Background

Beginning January 1, 2011, the Federal government requires the use of SHA-256 in all digital signatures generated by Certification Authorities (CAs) signing Personal Identity Verification (PIV) Cards. In addition, beginning January 1, 2011, the Federal government requires the use of SHA-256 in all digital signatures generated. While some limited use of SHA-1 in a deprecated mode is allowed, use in the PIV environment is not permitted after January 1, 2011. The risk of continued use of SHA-1 is significant, and 80-bit security strength for cryptography does not provide an acceptable level of protection. These risks increased the urgency for transition. Therefore, the FPKI Community transitioned its infrastructures to the stronger SHA-256 algorithm.

1.2 Objective and Audience

The FPKI SHA-256 Working Group was established to support the transition from SHA-1 to SHA-256 within the FPKI Community and provide a forum for inter-agency communication and information sharing. During and after the transition, a number of suggestions for improvement were discussed that could be applied to future transitions. The objective of this document is to identify the lessons learned during the FPKI community's transition to SHA-256. This document will be used by appropriate parties to improve current or future transitions.

2. LESSONS LEARNED

2.1 Technical Support

Number	SHA-256 Transition Lesson Learned	Recommendations	Status
1.	Need technical guidance for the migration.	- Sponsor Technical Exchange Conferences to develop Technical Guidance - Capture and publish technical guidance documentation for a particular migration	
2.	Testing Support: Need testing support and coordination among test environments o Need better test environments to support cross agency testing (requires cooperation/coordination across the Government). o Guidance to Agencies on testing (what needs to be tested, when and what pitfalls of which to be aware, etc.). o Need a refresh of PKITS & PDTS (NIST).	- Maintain and expand a centrally managed test environment that includes all stakeholders and mirrors the operational environment. - Develop formal test suites and guidance. - Develop Test Plans that address all phases of the process (from development through production). - Establish mechanisms for sharing test report data. - Develop a plan for vendor testing (e.g., establishing an APL, testing against existing test tools/formal methodology validation, or self-assertions).	

Number	SHA-256 Transition Lesson Learned	Recommendations	Status
3.	Algorithm Support o Need to provide guidance (that is outside the scope of the CP) for what algorithms need to be supported and the timeframes. o Need applications to support algorithm changeover. o Add language to procurement documents to require this type of support.	- Develop guidance for developers, contract specialists, operators, and implementers for items/issues that are not covered by Federal system policy documents. - Include technical requirements in procurement/contract documents to ensure vendors support Government needs.	
4.	Status Updates o Need a mechanism to share technical status of various products. o Post a summary report to a single place, describing a list of CAs and their status during a transition (who has transitioned to what algorithms and architectures, etc.).	- Establish a centralized forum and mechanisms for sharing technical and test information and reports including status of various vendor product capabilities.	
5.	Need a transition strategy for production systems o It would have been useful to establish a parallel PKI and allow end entity certificates to die a natural death.	- Develop and implement a transition strategy for production systems that minimizes operational disruptions (e.g. establishing parallel infrastructures such that the old systems die a natural death). - Identify methods for ensuring old configuration information is not retained in systems such that is causes operational issues (e.g., ensuring that old trust paths are removed from PKI systems). - Review current policy documents to ensure the policies support future transition strategies.	

2.2 Communications

Number	SHA-256 Transition Lesson Learned	Recommendations	Status
1.	Need communications with application owners *and* vendors in time for them to plan changes to and testing of their systems.	- Develop a communications plan. - Identify stakeholders. - Leverage relationships (e.g.. ICAMSC, CIO Council, Federal Computer Security Managers (FCSM) Forum) to establish lines of communications with appropriate stakeholders. - Host multiple, ongoing Government Workshops for stakeholders (including vendors and application owners).	

Number	SHA-256 Transition Lesson Learned	Recommendations	Status
2.	Need a "big stick" to encourage vendor support for technical needs (related to adding language to procurement documents). Need to involve vendors early and ensure there are actually products that support the requirements o Needs to be keyed to the budget cycle (can't just give one year notice, since budget is on a two year cycle). o Include Procurement people to try to include something in the FAR regarding transitions (e.g., require compliance with NIST standards, etc). o Need a single point of contact speaking for entire Federal Government to the vendors (the big stick).	- Include technical requirements in procurement/contract (FAR) documents to ensure vendors support Government needs o Need to give vendors notice about upcoming requirements as early as possible to allow for development time. o Need to give agencies enough time to include appropriate budget items to procure products that meet agency requirements. - Identify a single Point of Contact (POC) (person or office) representing the entire Federal Government for each specific transition. - Align technical requirement timelines to budget cycles (can't just give one year notice of new requirements, since budget is on a two year cycle).	
3.	Develop a Communications Plan early (even if it's generic).	- Develop a Master Communications Plan that includes: o A master timeline for all transitions in the foreseeable future. o Specific communications plans for each critical event. o Solicit guidance/direction from OMB related to a specific transition (if applicable). o Feedback from vendors about realistic timelines for when their products will be able to support a particular technology or configuration. o Guidance on product testing requirements (e.g., if an APL is established for a particular technology/configuration).	
4.	Share information more broadly o Include information about specific impacts of transition timelines to operations (need to ensure mechanisms are in place to gather this info). o Identify dependencies and impacts from other technology deployments (e.g., if an agency is planning a major technology transformation, how does this impact an algorithm transition).	- Post information about the Master Timeline and specific transitions to the IDManagement.gov web site (or other web sites as appropriate). - Include links on web sites to APLs, test results, lists of impacts/dependencies or other information as appropriate. - Post previous lessons learned documentation.	

Number	SHA-256 Transition Lesson Learned	Recommendations	Status
5.	Garner high level (CIO Council) buy-in on the transition early in the process.	- Present briefings to the CIO Council (or other appropriate high level bodies) to educate them on the criticality, timelines, and impacts of each specific transition so they understand and support action plans for executing the transition.	
6.	Communications within agencies to app owners o Include a Government-wide list of PKI-enabled products (continue use of the spreadsheet) – because of OMB M-11-11. ALL applications s will need to be included. o Include education of application owners so they really understand the implications of these transitions.	- See Recommendation for creating a Master Communications Plan above.	

2.3 Timing

Number	Lesson Learned	Notes	Status
1.	While some deadlines are unavoidable, as much time as possible should be given to allow for a smooth transition.	- See Recommendation for creating a Master Communications Plan above.	
2.	Get the word out sooner (e.g., ECC coming soon and we will be providing additional detail and dates soon).	- See Recommendation for creating a Master Communications Plan above.	

2.4 Planning

Number	Lesson Learned	Notes	Status
1.	The cross-agency coordination that was facilitated by the SHA-256 WG was useful, but a detailed project plan should be generated to view the transition from a higher level, and make sure communications and guidance are sent to the right people as early as possible.	- Develop Master Roadmap to present a high level picture of transitions over the long term. The roadmap should include: o The Master Communications Plan described above. o A list of stakeholders identified for each specific transition. o Roles and Responsibilities of each stakeholder. - Identify stakeholders and methods to coordinate with those stakeholders to get buy-in and participation from high level policy makers to system owners/implementers.	
2.	Undisciplined Change Management will lead to errors and transition issues.	- Each specific transition plan should include disciplined Change Management processes aligned with a common transition framework. - Identity the authority (e.g., the FPKIMA for the FPKI) responsible for formal configuration management. - Ensure that adequate funding is provided for proper configuration management and quality assurance by coordinating with senior management to obtain their buy-in and support.	

Number	Lesson Learned	Notes	Status
3.	Dissonance in policy – need to have a unified policy framework (this will get worse as the FPKI community grows) o Suggests consolidation of FBCA and Common would be beneficial.	- Identify opportunities for consolidating policies and systems to improve efficiencies across a particular environment o FPKI-Specific Recommendation: combine the FBCA and Common policies and CAs to reduce complexities and improve efficiencies. - Include an evaluation step in the Master Roadmap to determine if a specific transition provides the opportunity to consolidate policies and systems to increase efficiencies (i.e., determine when such consolidations would be possible/appropriate).	