Center for Medical Interoperability
8 City Boulevard, Suite 203
Nashville, TN 37209

C4MI Base Period Review

Policy and Design Review of CA and PKI Infrastructure and Secure Transport Architecture

Submitted to: Center for Medical Interoperability
November 30, 2019 | Prepared by Lark Security

Introduction

This report will serve as the formal documentation of the initial review of the Center for Medical Interoperability and their Policy and Design Review of Certificate Authority (CA) and Public Key Infrastructure (PKI). This review was requested and agreed upon in a Statement of Work dated October 6, 2019 and executed in a Subcontract Agreement dated October 24, 2019.

This report is intended to be used during the drafting process to validate work on the draft policy, during the final review of the policy, or during an annual review to determine areas that may need minor enhancement or require additional provisions to ensure that the policy is comprehensive in addressing all of the recommended core policy concepts.

All aspects of the documentation were reviewed to ensure alignment with Purpose Statements, Policy Applicability both from a Compliance and Technical perspective. Additionally, all documentation was reviewed to ensure future Governance and Oversight functions were accounted for and the ability to adapt to new and changing technological requirements.

Overview

The documents reviewed by Lark Security were:

1. C4MI Assigned Names and Numbers - V1
2. C4MI Trust Platform Identity and Secure Transport Requirements - V1
3. C4MI Trust Platform PKI Certificate Hierarchy - V1
4. Trust Platform Certificate Policy - V1

Lark Security Review Comments

Below are the comments from Lark Security for the documents reviewed. Additional client comments, discussions, and resolutions are documented in the Client Resolutions section of this report.

C4MI Assigned Names and Numbers - V1

There were no findings or observations within scope for this document. Lark Security and C4MI discussed additional requirements around using specific OID's to maintain the document version number to track and enforce certificate compliance with policy versions.

Trust Platform Certificate Policy - V1

1. Original documents allowed email as an authentication method for certificate request/renewals/revocations
    a. Lark Security Recommended:
        i. Further detail on requirements around how users are authenticated as authorized agents for the requesting organization.
        ii. Recommend specifically not allowing email as an authentication method.
        iii. Had detailed conversation with C4MI about alternate methods.
2. Original document allowed for optional multi factor physical access, video surveillance and on-site security staff
    a. Lark Security Recommendation:
        i. Should require a CA facilities to be manned 24x7 with security staff
        ii. MFA for physical access should not be optional.
        iii. Video surveillance of ingress/egress points should not be optional
3. Original document did not specifically stipulate the encryption of backup media.
    a. Lark Security Recommended:
        i. Specifically require that all backup media is encrypted in accordance with FIPS 140-2 requirements.
4. Original document allowed for Active-Active multi site configurations to not keep off-site backups.
    a. Lark Security Recommended:
        i. There should be a specific requirement for air-gapped backups to protect against corruption or destructive attacks propagating across multi-site architectures.
    b. Client Resolution:
        i. We already have this in other sections.
5. Recording events; we ask for logs to be kept on various activities such as key generation/destruction, access to accounts .
    a. Lark Security Recommended:
        i. Explicitly require logs of access to the private key access (esp. for non-repudiation), perhaps even with distributed access
    b. Client Resolution:

i. We added requirements to require access to private key access; we left the logs as-is since we strengthened onsite requirements and have requirements for backup access.

6. The original document required only 2 months of log retention.
    a. Lark Security Recommended:
        i. Recommended at least 12 months of retained logs
    b. Client Resolution:
        i. Agreed.
7. The original document had requirements for split responsibilities for most CA "rituals" but not specifically require this for key destruction.
    a. Lark Security Recommended:
        i. Recommended requiring 2 people to verify CA key destruction
8. Original document did not require any specific vetting of hardware against credible sources.
    a. Lark Security Recommended:
        i. Recommended additional requirements around vetting hardware and software manufacturers against DISA/DOD approved manufacturer lists to prevent the use of cryptographic functions on known compromised hardware and software platforms. Current examples are SuperMicro, ZTE and HuaWei
    b. Client Resolution:
        i. We added a requirement to check the National Vulnerability Database

C4MI Trust Platform PKI Certificate Hierarchy - V1

1. The original documents had the following validity periods: 50 years for the Root CA, 30 years for the Sub-CAs, and up to 20 for end-entity certificates (FYI: the docs limited the end-entity certs to at most 2 years).
    a. Lark Security Recommended:
        i. Reducing the Root CA validity periods to 20 years due to the high probability that changes in cryptography will force changes in keys well before the 50 year mark.
        ii. Reducing the Sub-CA validity periods to 10 years due to the high probability that changes in cryptography will force changes in keys well before the 30 year mark.
        iii. Leaving the End-entity validity periods at 2 years.
    b. Client Resolution:
        i. See Discussion Below
2. The draft documents listed the size of RSA key for sub-CAs at SHA-384 with a length of 3072.
    a. Lark Security Recommended:
        i. Increase the size of the RSA key to SHA-512 with a length of 4096.

   b. Client Resolution:
      i. Agreed
3. The draft documents listed the size of ECC key for sub-CAs at Secp384r1.
   a. Lark Security Recommended:
      i. Increase the size of the ECC key to Secp521r1 as future resistance choice.
   b. Client Resolution:
      i. Agreed

C4MI Trust Platform Identity and Secure Transport Requirements - V1

1. The original document listed a requirement for TLS 1.2 or greater.
   a. Lark Security Recommended:
      i. TLS 1.3 or greater as this standard has been through very thorough review and vetting.
   b. Client Resolution:
      i. See Discussion Below
2. The original document listed the use of Diffie-Hellman for TLS without specifying key length restrictions or configuration restrictions to know vulnerabilities.
   a. Lark Security Recommended:
      i. Diffie-Hellman should be configured with 2048 bit or higher key lengths
      ii. Disable the support for export cipher suites.
   b. Client Resolution:
      i. Under consideration
3. While a great number of specific requirements where listed in the draft document no specific mention of penetration testing was listed.
   a. Lark Security Recommended:
      i. Regularly scheduled penetration testing of the environment to include but not limited to:
         1. Testing of allowed and dis-allowed cyphers and where applicable.
         2. Input filter verification including the use of a fussing tool.
         3. Injection
         4. Broken Authentication
         5. Sensitive Data Exposure
         6. XML External Entities (XEE)
         7. Broken Access Control
         8. Security Misconfiguration
         9. Cross-Site Scripting
         10. Insecure Deserialization
         11. Using Components With Known Vulnerabilities
   b. Client Resolution:

        i. Consider for Phase Two
4. While authenticity and freshness requirements are noted in the draft document specificity are not fully defined.
    a. Lark Security Recommended:
        i. There should be language around whether freshness nonces or time based tolerances will be used and parameters of those items.
    b. Client Resolution:
        i. See Discussion Below
5. Private Key storage is critical to the integrity of the entire platform.
    a. Lark Security Recommended:
        i. All access to the private keys be logged and those logs be carefully monitored for unauthorized or suspect access.
    b. Client Resolution:
        i. Agreed

Client Resolutions

Lark Security had submitted all findings, observations and comments for client review on November 15, 2019. Subsequently a call was scheduled between Lark Security's review team and the C4MI team to discuss the Review Comments.

1. Specifies Authenticity and Freshness requirement
    a. Lark Security Recommendation:
        i. "Should there be any language around whether freshness nonces or methods are to be used? should tolerance be defined here?"
    b. Client Response:
        i. It's a good question; while generally not included, we should ask and understand what partners uses for future questions, pen testing, etc.
2. TLS 1.2 vs TLS 1.3
    a. Reference:
        i. For reference, TLS 1.2 (RFC 5246) was released August 2008 and TLS 1.3 (RFC 8446) was released August 2018. In October 2018, Apple, Google, Microsoft, and Mozilla jointly announced they would deprecate TLS 1.0 and 1.1 in March 2020. TLS 1.2 was built on the TLS 1.1 specification.
    b. Lark Security Recommendation:
        i. It is best to start out with the most current and strongest encryption available at the time.
    c. Client Response:

        i. Many vendors can't yet support TLS 1.3, so we will continue to use TLS 1.2 for now.

3. The original documents had the following validity periods: 50 years for the Root CA, 30 years for the Sub-CAs, and up to 20 for end-entity certificates (FYI: the docs limited most end-entity certs to 2 years)
    a. Lark Security Recommendation:
        i. 20, 10, and 2 years, respectively, to be cognizant of current best practices based on vulnerabilities etc.
    b. Client Response:
        i. We discussed the implications on deployments since some of the certs may not go into production for a few years and we will need to have a plan to consider replacements within the lifetime of end-entities - especially - medical devices
    c. Client Resolution:
        i. Root-CA for 30 years, [Sub-CA] for 20 years, [end-certificates] most for 2 years (code verification being the exception to avoid disruption)