HIGH ASSURANCE SUDI ICA CHAIN

Certificate Authority Practice Summary

Abstract

This document provides a summary of the controls around the High Assurance SUDI ICA Chain, a private PKI hierarchy maintained by Cisco's Cryptographic Services team.

Cryptographic Services

ciscopki-public@external.cisco.com

Data Classification: CISCO-PUBLIC

Cisco Confidential

Overview

The High Assurance SUDI ICA Chain is a PKI chain operated by Cisco's Cryptographic Services team. As with all CAs operated by Cryptographic Services, the High Assurance SUDI ICA chain is operated in close compliance with the WebTrust for CA guidelines maintained by CICA/AICPA. However, since the CA is not audited by an outside party, formal Certificate Policy and Certificate Practice Statement documents are not maintained by the team. Instead, the team provides this Certificate Authority Practice Summary for consumers of this CA to describe the uses and controls in place around the CA systems and certificates.

CA Chain and Purpose

The purpose of this document is to describe the practices that Cisco Systems ("Cisco") follows for the operation and management of the High Assurance SUDI ICA within Cisco Systems Inc., and the practices governing the issuance and life cycle of certificates issued from the High Assurance SUDI ICA, for the benefit of relying users.

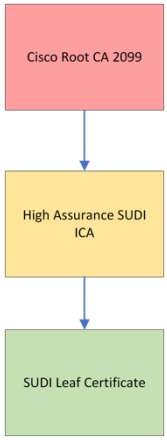

FIGURE 1 – HIGH ASSURANCE SUDI ICA CHAIN

CA Controls

Physical Controls

High Assurance SUDI ICA

The High Assurance SUDI ICA is maintained in a dedicated, offline operations room within Cisco's facilities. Access to the CA hardware requires two operators acting in concert. When not in use, CA key material is deactivated and kept in a safe that requires two operators acting in concert to unlock, guarded 24x7x365 by dedicated security personnel in a secure Cisco facility. Access to CA hardware is change-controlled and granted only for pre-approved functions; all functions are pre-scripted, logged, and witnessed by multiple operators.

Subordinated CAs

There are no subordinated CAs for the High Assurance SUDI ICA.

Common Controls

Physical access to all Cisco PKI cages and CA facilities is change-controlled and granted only for pre-approved functions. Data centers and facilities have flood and fire control/suppression

Data Classification: CISCO-PUBLIC

systems as well as power and network redundancy maintained by Cisco's corporate business operations teams and tested regularly to ensure proper functionality. Cisco data centers, dedicated PKI cages, and the secure racks containing HSMs all include multiple layers of physical security controls including multi-factor authentication for access. Facilities, cages, and racks used for PKI operations are kept under 24x7x365 camera surveillance monitored by Cisco's Safety & Security team.

Keys and associated CA operations material such as revocation lists are securely backed up to Cisco facilities in multiple geographic locations under the same physical access controls described above.

Logical Controls

High Assurance SUDI ICA

The High Assurance SUDI ICA is only operated in a secure, fully air-gapped operations facility with no network connection except the direct connection between the CA system and its hardware security module (HSM). Key generation and key usage for the CA only takes place inside an HSM certified to the FIPS 140-2 level 3 standard; all key backups from the HSM are encrypted such that no clear-text copy of any keys exist outside the HSM.

Subordinated CAs

There are no subordinated CAs for the High Assurance SUDI ICA.

Leaf Certificates

The High Assurance SUDI ICA only issues digital certificates to TAm-enabled hardware products ("subscribers") manufactured for or on behalf of Cisco Systems. The High Assurance SUDI ICA validate that the Trust Anchor module ("TAm") chip serial number listed in the certificate signing request matches the serial number of a TAm chip pre-registered by the chip manufacturer as valid. This ensures that the request originates from a legitimate TAm chip, and that the serial number in question is valid.

The High Assurance SUDI ICA have implemented technical and procedural controls that verify the identifying information of applying subscribers. Applying subscribers should present sufficient information with their certificate signing request to ensure the High Assurance SUDI ICA can perform this verification. The High Assurance SUDI ICA have implemented technical and procedural controls such as encrypted communications channels and encrypted data storage that protect communications with applying subscribers and that adequately protect and store information presented to the CA by the signature applicant.