Erster automatisierter ACVP-Krypto-Testservice von atsec

Als weltweit erstes Labor hat atsec information security den Betrieb seines Testdienstes über das automatisierte Prüfprotokoll für kryptografische Verfahren (Automated Cryptographic Validation Protocol, ACVP) der US-Standardisierungsbehörde NIST aufgenommen. atsecs Testdienst (ACVT – Automated Crypto Validation Testing), der die Validierung der Kryptoverfahren gegen den nunmehr ebenfalls produktiven ACVP-Server von NIST durchführt, wurde von NIST für den operativen Betrieb und damit für den Zugriff auf den produktiven NIST-Server zugelassen, nachdem die Behörde die Ergebnisse des Dienstes für alle Algorithmen, die vom ACVP-Server zur Validierung angeboten werden, genau überprüft hatte. Dabei wurden zunächst SHA- und HMAC-Implementierungen über atsecs ACVP-Proxy geprüft.

Mit diesem privilegierten Zugriff automatisiert atsecs neuer Dienst mithilfe des ACVP-Produktionsservers den Prozess des Testens der Implementierungskorrektheit kryptografischer Algorithmen und verwandter Funktionen und bietet einen wesentlich effizienteren und effektiveren Prozess für die Erlangung der begehrten NIST-Zertifikate.

NIST hat das automatisierte Prüfprotokoll entwickelt, um der enorm gestiegenen Nachfrage nach Zertifikaten gemäß FIPS 140-2, dem US-Standard für Kryptomodule, gerecht zu werden. Zertifikate über die Korrektheit der Implementierung werden von NISTs Validierungsprogramm für kryptografische Algorithmen (CAVP, Cryptographic Algorithm Validation Program) ausgestellt. Diese Zertifikate werden als Voraussetzung für die Validierung von Kryptografiemodulen sowie für Common Criteria-Bewertungen in den USA benötigt.

atsecs CST-Labor in Austin, Texas hat bei der Entwicklung seiner Prüfwerkzeuge eng mit NIST zusammengearbeitet und mitgeholfen, den ACVP-Demoserver von NIST zu testen und damit die Voraussetzung für die jetzt erfolgte Freigabe des NIST-Produktionsservers zu schaffen. Stephan Müller von der atsecs Zentrale in München hat als Hauptentwickler des Test-Clients wesentlichen Anteil an diesem Erfolg. „Ich beglückwünsche NIST zu diesem Meilenstein des ACVP-Programms. Das Programm ist wichtig, um die erforderliche Zertifizierung kryptografischer Verfahren in IT-Sicherheitsprodukten mit den immer kürzeren, modernen Entwicklungszyklen in Einklang zu bringen.“

Auch atsecs Leiterin des CST-Labors, Dr. Yi Mao, äußerte sich positiv zum Start des Prüfdienstes: „Wir begrüßen die Initiative von NIST zur Einführung des ACVT-Programms und sind stolz darauf, sie bei der Erreichung dieses historisch bedeutsamen Meilensteins zu unterstützen. Kryptographie ist heute der harte Kern vieler IT-Sicherheitsprodukte. Automatisierte Tests sind der Weg in die Zukunft, um die hohe Nachfrage nach der dringend benötigten Vertrauenswürdigkeit im Zentrum der IT-Sicherheit aufrechtzuerhalten. Dies ist ein äußerst aufregender Moment, denn dank ACVT können unsere Kunden ab sofort von dieser viel schnelleren Validierung ihrer Algorithmen profitieren.“