AUTKRYPTO

Kryptosystem Made-in-Austria

Programm / Ausschreibung	KIRAS, Kooperative F&E-Projekte, KIRAS-Kybernet-Pass CS Kooperative F&E Projekte (CS KFE_2023)	**Status**	laufend
Projektstart	01.10.2024	**Projektende**	31.03.2027
Zeitraum	2024 - 2027	**Projektlaufzeit**	30 Monate
Keywords	Verschlüsselungsgeräte, Post-Quanten-Kryptographie, Sichere Kommunikation		

Projektbeschreibung

Kommunikation von sensitiven oder klassifizierten Informationen wird unter anderem durch den Einsatz von Verschlüsselungsgeräten, die für den Hochsicherheitsbereich zugelassen sind, abgesichert. Da solche Verschlüsselungsgeräte nicht von österreichischen Produzenten angeboten werden, müssen sie aktuell aus Drittstaaten (etwa Deutschland, Schweiz) zugekauft werden. Dadurch werden Geräte, die möglicherweise unter dem Einfluss ausländischer Geheimdienste entwickelt wurden, zum Schutz nationaler klassifizierter Informationen eingesetzt. Aufgrund der fehlenden Verfügbarkeit von Verschlüsselungsgeräten “made in Austria” ergibt sich die Frage, ob in Österreich die nötigen Technologien und das Know-How vorhanden sind, um Verschlüsselungsgeräte mit international etablierten kryptographischen Algorithmen (wie beispielsweise AES, SHA) und nationaler Chain-of-Trust umsetzbar sind.
Das Projekt AUTKRYPTO befasst sich mit dieser Frage hinsichtlich dreier zentraler Aspekte. Zunächst gilt es die möglichen Stakeholder (Sicherheitsministerien und -behörden) und ihre Anforderungen zu identifizieren. Neben den Anforderungen hinsichtlich sicherer Kommunikation mittels eines post-quanten sicheren Virtual Private Networks (VPN), stellen sich hier Fragen von Trusted-Boot bis zu Wartungsmöglichkeiten, Kryptoagilität, Erweiterbarkeit bzgl. neuer kryptographischen Algorithmen und Zertifizierung, Auf technischer Ebene wird ein Demonstrator einer sicheren Hardwareplattform entwickelt, die mit einer FPGA/Software Co-Design-Architektur eine sichere post-quanten VPN-Implementierung umsetzen soll. Aus volkswirtschaftlicher Sicht wird der Aspekt untersucht, ob mit dem vorhandenen Technologien und Knowhow die Entwicklung eines österreichischen Verschlüsselungsgeräts aktuell umsetzen lässt oder ob weitere Investitionen in IT-Sicherheitsunternehmen, Bildungs- und Forschungsförderung nötig sind, um fehlende Kompetenzen aufbauen zu können.

Abstract

Communication of sensitive or classified information can be secured by the use of encryption devices that are approved for high-security use. Since such encryption devices are not offered by Austrian manufacturers, they currently have to be procured from other nations (e.g., Germany, Switzerland). As a result, devices that may have been developed under the influence of foreign intelligence services, are used to protect national classified information. Due to the lack of availability of encryption devices "made in Austria", the question arises as to whether the necessary technologies and know-how are available in Austria to implement encryption devices with internationally established cryptographic algorithms (such as AES,

SHA) and a national chain-of-trust.
The AUTKRYPTO project addresses this question with regard to three central aspects. The first step is to identify the potential stakeholders (e.g., security ministries and authorities) and their requirements. In addition to the requirements regarding secure communication using a post-quantum secure Virtual Private Network (VPN), questions arise from trusted boot to maintenance, crypto agility, extensibility with regards to new cryptographic algorithms and certification. On a technical level, a demonstrator of a secure hardware platform is being developed, which is intended to implement a secure post-quantum VPN implementation with an FPGA/software co-design architecture. From an economic point of view, the aspect is examined whether the development of an Austrian encryption device can currently be implemented with the existing technologies and know-how or whether further investments in IT security companies, education and research funding are necessary in order to be able to build up missing skills.

Projektkoordinator

- AIT Austrian Institute of Technology GmbH

Projektpartner

- Bundeskanzleramt
- Bundesministerium für Landesverteidigung
- xFace e.U.
- System Industrie Electronic GmbH
- REPUCO Unternehmensberatung GmbH