Krypto-Workstation

Österreichische Krypto-Workstation zur hochsicheren Datenverschlüsselung auf PCs inkl. Schlüsselmanagement

Programm / Ausschreibung	KIRAS, Kooperative F&E-Projekte, KIRAS CS Kooperative F&E-Projekte (CS KFE_2025)	**Status**	laufend
Projektstart	01.09.2026	**Projektende**	30.11.2027
Zeitraum	2026 - 2027	**Projektlaufzeit**	15 Monate
Barwert der Projektförderung	€ 149.925		
Keywords	Datenverschlüsselung; One-Time Pad; Open-Source Hardware und Software; Telekommunikation; Physikalische Kryptografie		

Projektbeschreibung

Daten werden immer wichtiger und damit auch die Sicherheit der Daten. Viele schützenswerte Daten von Behörden und Unternehmen entstehen auf dem eigenen PC (Desktop, Laptop, Notebook) in einem Büroumfeld, im Home-Office oder unterwegs und müssen schon dort ausreichend sicher geschützt werden.

Im Projekt entsteht eine kostengünstige und benutzerfreundliche Krypto-Workstation, die auf herkömmlichen PCs alle wichtigen Anwendungen in diesem Umfeld, wie z.B. Office (Libre Office), Messenger- und Videokonferenzdienste etc., von unverschlüsselt bis zur hochsicheren Verschlüsselung ermöglicht und wo die Kryptografie aus Österreich kommt und alles andere ist Open-Source SW und auf Wunsch auch Open-Source HW. Und das Ganze erfolgt für die Datenspeicherung am PC und die Telekommunikation.
Dafür wird auf PCs des Marktes ein Multi-Sessionbetrieb mit verschiedenen Sicherheitsniveaus (von gering bis hochsicher) auf Betriebssystem Ebene umgesetzt, damit der gleiche PC als offener PC, aber auch als hochsichere Krypto-Workstation für sehr schützenswerte Daten agieren kann.
Ein kryptografisches Zugriffskontrollsystem mit Rollen-basiertem Berechtigungssystem ermöglicht eine hochsichere Datenspeicherung für Dateien und einzelnen Elementen von Datenbanken. Die Kryptografie für die Datenverschlüsselung und dem Schlüsselaustausch reicht von mathematischen Verfahren wie AES und PQXDH (Post Quantum Diffie Hellman) über den neuen One-Time Pad nahen Modus XTSC [PS] bis zur beweisbar 100%igen Sicherheit mit einem One-Time Pad und MKD-Schlüsselaustausch [PS] mit geeigneten Speichermedien. Eine Hauptspeicherverschlüsselung liefert noch eine weitere Sicherheit. Neben dem PC ist im Hochsicherheitsniveau nur ein kostengünstiges MKD-Speichermedium [PS] oder HSM in Zigarettenschachtelgröße erforderlich.

In den vergangenen drei Jahren erfolgte in Österreich die SW-Entwicklung der hochsicheren Kryptografie-Lösung, die bisher mit über einer Million Euro gefördert wurde. Aufbauend darauf wird im Rahmen des vorliegenden Projektes eine kostengünstige und hochsichere Krypto-Workstation auf Basis von herkömmlichen PCs, insbesondere Open-Source Laptops,

implementiert. Der gleiche PC kann dabei offen (zum Internet etc.) und auch hochsicher betrieben werden.
Die Krypto-SW kommt aus Österreich, die HW und sonstige SW sind Open Source und eigene Algorithmen und hohe Skalierbarkeit sind möglich. Mit dieser Lösung ist eine Verschlüsselung des gesamten Speichermediums, aber auch feingranular auf einem rollenbasierenden Berechtigungssystem möglich. Des Weiteren erfolgt über eigene Server eine Einbindung des Open Source Messengerdienstes Matrix und Videokonferenzdienstes Visio mit einer für die Telekommunikation hochsicheren Verschlüsselung bis zur 100%-igen Sicherheit mit One-Time Pad.

Durch die Verwendung von Open Source HW und SW ist eine umfassende Überprüfbarkeit der Sicherheit der Komponenten möglich. Die Open-Source SW und HW fördert auch die digitale Souveränität, Nachhaltigkeit und eine Zukunft mit modularen, reparierbaren Systemen. Und die für die Sicherheit besonders wichtige Kryptografie kommt aus Österreich.
Die Krypto-Workstation kann auch Tempest (SDIP 27 A, B, C) erfüllen, wenn dafür zertifizierte PCs/Laptops, die am Markt verfügbar sind, verwendet werden. Ob dies mit geeigneten Erweiterungen auch mit Open-Source HW möglich ist, wird im Projekt geprüft. Im positiven Fall wäre es ein sichertechnisch wichtiger Schritt, der auch die Kosten erheblich senken würde.

Abstract

Data is becoming increasingly important, and with it, data security. Much of the sensitive data held by public authorities and companies is created on personal computers (desktops, laptops, notebooks) in an office environment, at home, or on the move, and must be adequately protected at these locations.

This project is developing a cost-effective and user-friendly crypto workstation that enables all important applications in this environment, such as Office (Libre Office), messenger and video conferencing services, etc., from unencrypted to highly secure encryption on conventional PCs, with the cryptography coming from Austria and everything else being open-source software and, if desired, open-source hardware. And all of this is done for data storage on the PC and telecommunications.
To this end, multi-session operation with different security levels (from low to high security) is implemented at the operating system level on commercially available PCs so that the same PC can function as an open PC, but also as a highly secure crypto workstation for highly sensitive data.
A cryptographic access control system with a role-based authorization system enables highly secure data storage for files and individual elements of databases. The cryptography for data encryption and key exchange ranges from mathematical methods such as AES and PQXDH (Post Quantum Diffie Hellman) to the new One-Time Pad-like mode XTSC [PS] to provably 100% security with a One-Time Pad and MKD key exchange [PS] with suitable storage media. Main memory encryption provides even greater security. In addition to the PC, only an inexpensive MKD storage medium [PS] or HSM the size of a cigarette packet is required for high security.

Over the past three years, the software for the high-security cryptography solution has been developed in Austria, with over one million euros in funding to date. Building on this, the present project aims to implement a low-cost and highly secure crypto workstation based on conventional PCs, in particular open-source laptops. The same PC can be operated openly (for the Internet, etc.) and also with a high level of security.
The crypto software comes from Austria, the hardware and other software are open source, and proprietary algorithms and high scalability are possible. This solution enables encryption of the entire storage medium, but also fine-grained encryption based on a role-based authorization system. Furthermore, the open-source messenger service Matrix and the video conferencing service Visio are integrated via proprietary servers with highly secure encryption for telecommunications,

offering up to 100% security with one-time pad.

The use of open source hardware and software enables comprehensive verification of component security. Open source software and hardware also promote digital sovereignty, sustainability, and a future with modular, repairable systems. And the cryptography that is particularly important for security comes from Austria.
The crypto workstation can also comply with Tempest (SDIP 27 A, B, C) if certified PCs/laptops available on the market are used. The project is investigating whether this is also possible with open source hardware using suitable extensions. If so, it would be an important step in terms of security that would also reduce costs.

Projektkoordinator

- Hochschule für Angewandte Wissenschaften St. Pölten Forschungs GmbH

Projektpartner

- Bundeskanzleramt
- Hochschule für Angewandte Wissenschaften St. Pölten GmbH
- insitu software gmbh
- Land Niederösterreich