

DigiSov-CrOSSD

Digital Sovereignty Through a Critical Open-Source Software Database

Programm / Ausschreibung	KIRAS, F&E-Dienstleistungen, KIRAS CS F&E-Dienstleistungen (CS FED_2025)	Status	laufend
Projektstart	01.10.2026	Projektende	31.03.2028
Zeitraum	2026 - 2028	Projektlaufzeit	18 Monate
Barwert der Projektförderung	€ 139.309		
Keywords	digitale Souveränität, Kritikalität, Metriken, Open-Source-Software		

Projektbeschreibung

Digitale Souveränität – also die Fähigkeit staatlicher, wirtschaftlicher und zivilgesellschaftlicher Akteure, selbstbestimmt über digitale Infrastrukturen und Abhängigkeiten zu entscheiden – gewinnt angesichts zunehmender geopolitischer Spannungen und wachsender Abhängigkeiten von nicht-europäischen Technologieanbietern erheblich an Bedeutung. Open-Source-Software (OSS) gilt dabei als zentrales Instrument zur Stärkung dieser Souveränität, birgt jedoch eigene Risiken: Hochkarätige Sicherheitsvorfälle wie der XZ-Utils-Backdoor, Log4Shell und Heartbleed haben strukturelle Verwundbarkeiten im OSS-Ökosystem offenbart. Zugleich fehlt bis dato eine einheitliche, operationalisierbare Definition digitaler Souveränität im Kontext von OSS – und damit eine wissenschaftlich fundierte Grundlage für evidenzbasierte Entscheidungen über deren souveränen und sicheren Einsatz.

DigiSov-CrOSSD begegnet dieser Lücke durch die gezielte Weiterentwicklung der bestehenden Plattform CrOSSD (Critical Open-Source Software Database) zu einer integrierten Bewertungsinfrastruktur für Sicherheit und digitale Souveränität von OSS. Das Projekt verfolgt vier aufeinander aufbauende Ziele: die technische Weiterentwicklung von CrOSSD um zusätzliche Datenquellen und Schnittstellen; die empirische Erhebung und Operationalisierung von Souveränitätskriterien und -metriken auf Basis qualitativer Stakeholder-Interviews; die Integration von CVE-Datenbanken, OpenSSF-Scorecard-Indikatoren und wissenschaftlich fundierten Vulnerability-Metriken; sowie die Validierung des Gesamtmodells durch Backcasting auf reale Sicherheitsvorfälle und die Erkennung von Qualitätsrisiken durch KI-generierten Code (Vibe-Coding). Der zentrale Innovationsbeitrag liegt in der erstmaligen systematischen Verbindung der normativen Ebene – was digitale Souveränität für konkrete OSS-Projekte bedeutet – mit der operativen Ebene ihrer datengestützten, reproduzierbaren Messung.

Als Ergebnis liefert DigiSov-CrOSSD ein validiertes Metrik-Framework zur Bewertung von OSS hinsichtlich digitaler Souveränität, Sicherheit und Resilienz, das auf der öffentlich zugänglichen CrOSSD-Plattform implementiert und nutzbar gemacht wird. Öffentliche Einrichtungen und Betreiber kritischer Infrastrukturen in Österreich erhalten damit eine evidenzbasierte Entscheidungsgrundlage für den souveränen und sicheren OSS-Einsatz; Handlungsbedarfe – etwa gezielte Förderung unterversorgter, kritischer OSS-Projekte – werden systematisch identifizierbar.

Abstract

Digital sovereignty (i.e. the ability of governmental, economic and civil society actors to make independent decisions about digital infrastructures and dependencies) is becoming increasingly important in light of growing geopolitical tensions and growing dependencies on non-European technology providers. Open-source software (OSS) is considered a key tool for strengthening digital sovereignty, but it also carries its own risks: High-profile security incidents such as the XZ Utils backdoor, Log4Shell and Heartbleed have revealed structural vulnerabilities in the OSS ecosystem. At the same time, there is currently no uniform, operationalisable definition of digital sovereignty in the context of OSS – and thus no scientifically sound basis for evidence-based decisions on its sovereign and secure use.

DigiSov-CrOSSD addresses this gap by extending the existing CrOSSD platform (Critical Open-Source Software Database) into an integrated assessment infrastructure for the security and digital sovereignty of OSS. The project pursues four interrelated goals: the technical advancement of CrOSSD to include additional data sources and interfaces; the empirical collection and operationalisation of sovereignty criteria and metrics based on qualitative stakeholder interviews; the integration of CVE databases, OpenSSF Scorecard indicators and scientifically based vulnerability metrics; and the validation of the overall model through backcasting of real security incidents and the detection of quality risks through AI-generated code (vibe coding). The main innovation and contribution lies in the first-ever systematic connection of the normative level – what digital sovereignty means for specific OSS projects – with the operational level of its data-supported, reproducible measurement.

As a result, DigiSov-CrOSSD provides a validated metric framework for evaluating OSS in terms of digital sovereignty, security and resilience, which is implemented and made available on the publicly accessible CrOSSD platform. Public institutions and operators of critical infrastructures in Austria thus receive an evidence-based decision-making basis for the sovereign and secure use of OSS; areas requiring action – such as targeted support of underserved, critical OSS projects – can be systematically identified.

Projektkoordinator

- Hochschule für Angewandte Wissenschaften St. Pölten GmbH

Projektpartner

- Bundeskanzleramt