PREPARED

Post-Quanten-sichere eID für Österreich

Programm / Ausschreibung	KIRAS, Kooperative F&E-Projekte, KIRAS Kooperative F&E-Projekte 2022	**Status**	laufend
Projektstart	01.10.2023	**Projektende**	31.01.2026
Zeitraum	2023 - 2026	**Projektlaufzeit**	28 Monate
Keywords	Post-Quanten-Kryptographie, eID, Privacy		

Projektbeschreibung

eGovernment-Anwendungen wie FinanzOnline oder die App „Digitales Amt“ werden durch die Verfügbarkeit eines digitalen Identitätsmanagement-Systems (eID) ermöglicht. Grundlage für solche eID Systeme sind kryptographische Signaturen, die einerseits die Authentizität von Zertifikaten garantieren, andererseits den Bürger:innen die Möglichkeit bieten, sich zu authentifizieren bzw. Dokumente zu unterzeichnen. Signaturen und eID-Systeme sehen sich jedoch mit neuen Herausforderungen und Anforderungen konfrontiert.
Bei digitalen Signaturen ist zu beachten, dass aktuell in der Praxis eingesetzte Verfahren durch Angriffe mit leistungsstarken Quantencomputern bedroht sind. Deshalb wurde durch das US-amerikanische National Institute of Standards and Technology (NIST) ein Standardisierungsprozess für post-quanten-sichere Verfahren zur Substituierung bisheriger Signaturverfahren gestartet. Ergebnisse aus diesem NIST-Prozess ermöglichen es nun, Systeme für die Migration auf Post-Quanten-Kryptographie vorzubereiten. Jedoch fehlen bis dato in vielen Bereichen praktische Erfahrungen für einen solchen Migrationsprozess. Im Projekt PREPARED setzten wir uns deshalb das Ziel, post-quanten-sichere Signaturverfahren im Kontext von eID-Systemen zu analysieren. Insbesondere wird ein Migrationsplan entwickelt, da gerade Systeme mit langlebigen Zertifikaten und Signaturen eine entsprechende Vorbereitung benötigen, um eine Migration rechtzeitig und problemlos durchführen zu können.
Weitere Herausforderungen ergeben sich durch Paradigmenwechsel, die sich in eID-Systemen beobachten lassen, wie zB die Einführung von Identity-Wallets (ID-Wallets). Benutzer:innen können mit solchen ID-Wallets unterschiedlichste offizielle Dokumente (Ausweise, Zeugnisse etc.) digital vorweisen. Bereichsspezifische Personenkennzeichen (bPK), die bisher ein zentrales Element zur Verknüpfung von Daten darstellen, sind in solchen ID-Wallets allerdings nicht mehr im selben Ausmaß einsetzbar. Aus kryptographischer Sicht können hier so genannte Zero-Knowledge-Beweise und attributsbasierte Credentialsysteme Abhilfe schaffen. PREPARED untersucht deshalb diese kryptographischen Techniken zur Verknüpfung der Daten in eID-Systemen, damit die Funktionalität von bPKs in ID-Wallets bestehen bleibt.
Zuletzt ist noch ein sehr häufig verwendeter Prozess zur Erstellung von PDF-Signaturen von Interesse. Hierbei ist anzumerken, dass aktuell die Übertragung der zu signierenden Dokumente an einen Vertrauensdienstleister nötig ist. Berücksichtigt man die zunehmenden Anforderungen hinsichtlich Datenschutzes und Sicherheit (Privacy-by-Design, Security-by-Design), setzt sich PREPARED das Ziel, diesen Prozess um Signaturen mit neuen Funktionalitäten – sogenannten blinden

Signaturen – zu erweitern damit diese Übertragung zugunsten der Risikominimierung nicht mehr erforderlich ist. In einem weiteren Schritt soll der Prozess auch so verändert werden, dass die Kontrolle über den Signaturprozess vollständig in der Hand der Benutzer:innen liegt und Vertrauensdienstleister und Benutzer:innen den Signaturprozess nur kooperativ durchführen können.
Die entwickelten Lösungsansätze werden hierbei mit Sicherheitsbeweisen der Verfahren und -analysen der entstehenden Architekturen begleitet. Ebenfalls wird die Demonstration der erreichbaren Funktionalität durch Software-Prototypen unterstützt. Aufgrund der Bedeutung von eID-Systemen für eGovernment-Anwendungen werden die entwickelten technischen Lösungsansätze durch eine rechtliche Analyse begleitet. Damit soll sichergestellt werden, dass die entwickelten Architekturen und Verfahren den rechtlichen Anforderungen entsprechen.

Wiedereinreichung: Bei dem Projekt handelt es sich um eine Wiedereinreichung des gleichnamigen Antrags aus dem Vorjahr (KIRAS 2021). Das Projekt wurde für eine Förderung vorgesehen, musste aber aufgrund der Einstufung des Partners SIC als Großunternehmen durch das Konsortium abgelehnt werden. Bei der Wiedereinreichung nimmt SIC im Rahmen seiner nicht-wirtschaftlichen Tätigket nun als wissenschaftlicher Partner teil. Das Konsortium wurde dafür um die PrimeSign GmbH und die sproof GmbH als KMU-Partner ergänzt. Entsprechend der Änderung im Konsortium wurden die Aufgabenverteilung, der Arbeitsplan, die Verwertungsstrategie und das Projektbudget entsprechend angepasst, sowie allgemein technologische und regulatorische Entwicklungen seit der letzten Einreichung berücksichtigt. Die Integration und Evaluierung des PQ-Providers in eID-Systemen bzw. für PDF-Signaturen wird nun von PrimeSign und sproof maßgeblich mitgestaltet und durchgeführt. Aufgrund von Änderung der Personalsituation bei einzelnen Partnern hat sich die Zusammensetzung des Projektteams geändert. Durch die Umsetzung von gezielten Maßnahmen konnte der Frauenanteil des Projekts auf 20% erhöht werden.

Abstract

eGovernment applications such as FinanzOnline or the "Digitales Amt" app are made possible by the availability of a digital identity management system (eID). The basis for such eID systems are cryptographic signatures, which on the one hand guarantee the authenticity of certificates and on the other hand offer citizens the opportunity to authenticate themselves or sign documents. However, signatures and eID systems are confronted with new challenges and requirements.
In the case of digital signatures, the schemes currently used in practice are threatened by attacks with powerful quantum computers. For this reason, the US National Institute of Standards and Technology (NIST) has started a standardization process for post-quantum-safe methods to replace currently deployed digital signature schemes. Results from this NIST process now make it possible to prepare systems for migration to post-quantum cryptography. However, there is still a lack of practical experience for such a migration process in many areas. In the PREPARED project, we therefore set ourselves the goal of analyzing post-quantum-secure signature procedures in the context of eID systems. In particular, a migration plan is developed, as systems with long-lived certificates and signatures need appropriate preparation in order to be able to carry out a migration on time and without any problems.
Further challenges arise from paradigm shifts that can be observed in eID systems, such as the introduction of identity wallets (ID wallets). With such ID wallets, users can digitally present a wide variety of official documents (ID cards, certificates, etc.). However, area-specific personal identifiers (bPK), which have so far been a central element for linking data, can no longer be used to the same extent in such ID wallets. From a cryptographic point of view, so-called zero-knowledge proofs and attribute-based credential systems can help to preserve the functionality under this new paradigm. PREPARED is therefore investigating these cryptographic techniques for linking the data in eID systems so that the functionality of bPKs in ID wallets remains.

Finally, a very common process for creating PDF signatures is of interest. It should be noted that it is currently necessary to transfer the documents to be signed to a trust service provider. Taking into account the increasing requirements regarding data protection and security (privacy-by-design, security-by-design), PREPARED sets itself the goal of extending this process to signatures with new functionalities – so-called blind signatures – so that this transfer is no longer necessary in favor of risk minimization. In a further step, the process is also to be changed in such a way that control over the signature process is completely in the hands of the users and trust service providers and users can only carry out the signature process cooperatively.
The developed solution approaches are accompanied by safety proofs of the procedures and analyses of the resulting architectures. The demonstration of the achievable functionality is also supported by software prototypes. Due to the importance of eID systems for eGovernment applications, the developed technical solutions are accompanied by a legal analysis. This is to ensure that the developed architectures and procedures meet the legal requirements.

Endberichtkurzfassung

Das Projekt PREPARED untersuchte, wie bestehende elektronische Identitätssysteme schrittweise auf post-quanten-sichere Kryptographie umgestellt werden können. Hintergrund ist die absehbare Bedrohung klassischer kryptographischer Verfahren durch Quantencomputer, wodurch insbesondere langfristig gültige digitale Signaturen und Identitäten betroffen sind.

Ausgehend davon wurden bestehende eID-Systeme, insbesondere die ID Austria, detailliert analysiert. Ziel war es, jene Komponenten zu identifizieren, die für Sicherheit, Datenschutz und Betrieb besonders kritisch sind, und daraus konkrete Anforderungen für eine Migration abzuleiten.

Darauf aufbauend wurde eine realistische Migrationsstrategie entwickelt. Diese setzt auf einen schrittweisen Übergang mit Pilotphasen, frühe Absicherung von Systemteilen unter eigener Kontrolle sowie eine koordinierte Weiterentwicklung im Einklang mit europäischen Initiativen wie der EUDI Wallet. Ein zentrales Element ist dabei der langfristige Parallelbetrieb klassischer und post-quanten-sicherer Verfahren, um Stabilität und Kompatibilität sicherzustellen.

Die entwickelten Konzepte wurden auch praktisch umgesetzt. Dazu wurden ausgewählte post-quanten-sichere Signaturverfahren implementiert, in die Infrastruktur eines Vertrauensdiensteanbieters integriert und in weiterer Folge in bestehende digitale Workflow-Systeme eingebunden. Umfangreiche Benchmark-Analysen zeigen, dass diese Verfahren deutlich höhere Anforderungen an Rechenleistung, Speicher und Bandbreite stellen, teilweise um Größenordnungen. Dies erfordert Anpassungen auf Systemebene, insbesondere bei Vertrauensdiensteanbietern und Infrastrukturkomponenten. Für Endnutzer bleibt der Ablauf hingegen weitgehend unverändert, da die Änderungen im Hintergrund erfolgen.

Ergänzend wurden zahlreiche weiterführende Forschungsarbeiten durchgeführt, die über die unmittelbare Migration hinausgehen. Dazu zählen insbesondere Arbeiten zu neuen und effizienteren post-quanten-sicheren Signaturverfahren, bei denen sowohl Signaturgrößen als auch Laufzeiten verbessert werden konnten. Darüber hinaus wurden moderne kryptographische Konzepte wie Zero-Knowledge-Beweise, attributbasierte Credentials und delegierbare Pseudonyme untersucht. Diese Ansätze zielen darauf ab, zukünftige digitale Identitätssysteme nicht nur sicherer, sondern auch datenschutzfreundlicher und flexibler zu gestalten.

Parallel dazu erfolgte eine umfassende rechtliche Analyse der untersuchten Technologien und Migrationsansätze. Dabei

wurden insbesondere die Anforderungen der eIDAS-Verordnung sowie datenschutzrechtliche Rahmenbedingungen berücksichtigt. Ziel war es, die rechtliche Zulässigkeit post-quanten-sicherer Signaturen und neuer Identitätsmechanismen zu bewerten und mögliche Auswirkungen einer Migration frühzeitig zu identifizieren. Auf dieser Basis konnten auch erste Handlungsempfehlungen abgeleitet werden, um technische Innovationen im Einklang mit bestehenden regulatorischen Vorgaben umzusetzen.

Insgesamt liefert PREPARED eine fundierte Grundlage für die zukünftige Weiterentwicklung digitaler Identitätssysteme und zeigt konkrete Wege auf, wie eine sichere und praktikable Migration in Richtung Post-Quanten-Kryptographie umgesetzt werden kann.

Projektkoordinator

- AIT Austrian Institute of Technology GmbH

Projektpartner

- Universität Linz
- Bundeskanzleramt
- Stiftung Secure Information and Communication Technologies - Sic
- PrimeSign GmbH
- Technische Universität Graz
- sproof GmbH