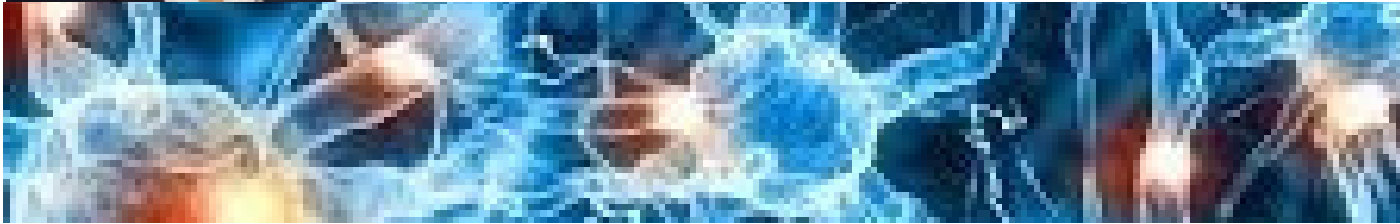




Parole Libre & Liberté Vraie

Dr Anne-Marie YIM

Chemiker | Unabhängige Forscherin



Biometrischer Reisepass: PACE-Protokoll und e-Gate

Laut einem Artikel der luxemburgischen Zeitung „Virgule“ vom 8. September 2026 hatten Reisende mit luxemburgischer Staatsangehörigkeit im Ausland Probleme beim Passieren der automatisierten Kontrollschleusen, da das Auslesen des Chips oder der Passdaten nicht immer reibungslos funktionierte.

Die luxemburgischen Behörden haben erklärt, dass der Reisepass keinerlei technische Mängel aufweise und alle geltenden internationalen Sicherheitsstandards vollständig erfülle.

Sie machen jedoch die Lesegeräte oder die Software bestimmter ausländischer Flughäfen dafür verantwortlich, die manchmal aktualisiert werden müssen, um sich an die RFID-Chip-Technologie anzupassen, die eine Identifizierung per Funkfrequenz ermöglicht und auf der NFC-Technologie (Near Field Communication) dieser neuen Dokumente basiert. Der RFID-Chip arbeitet gemäß der internationalen Norm ISO/IEC 14443 auf der Frequenz von 13,56 MHz.

Luxemburg hat sich dafür entschieden, bereits jetzt das Sicherheitsprotokoll PACE (Password Authenticated Connection Establishment) zu verwenden, das als die Technologie gilt, die schrittweise zum internationalen Standard für das sichere Auslesen der elektronischen Chips in Reisepässen werden soll. Das PACE-Protokoll schützt die aus dem Reisepass ausgelesenen Daten, und die e-Gates lesen diesen physischen Reisepass an den Flughäfen aus.

E-Gates oder automatische Kontrollschleusen sind automatisierte Kontrollstellen, an denen Reisepässe gescannt und die Identität der Reisenden mithilfe der Gesichtserkennung sowie anhand der Fingerabdrücke beider Zeigefinger überprüft werden kann.

Das PACE-Protokoll (Password Authenticated Connection Establishment) ist ein kryptografisches Sicherheitsprotokoll der neuen Generation, das zur Sicherung des Zugriffs auf die Mikrochips in biometrischen Reisepässen und Personalausweisen verwendet wird. Es ersetzt schrittweise das ältere BAC-Protokoll (Basic Access Control).

Laut Gemini wurde das PACE-Protokoll von der Internationalen Zivilluftfahrt-Organisation (ICAO) standardisiert, um maximalen Schutz zu bieten:

Starke Verschlüsselung:

Im Gegensatz zum BAC-Protokoll, dessen Verschlüsselungsschlüssel anfällig für Brute-Force-Angriffe wurden, nutzt PACE asymmetrische Kryptografie, insbesondere auf elliptischen Kurven.

Schutz vor Skimming und Abfangen:

Es verhindert das betrügerische Auslesen des kontaktlosen Chips aus der Ferne, wenn der Reisepass geschlossen ist, beispielsweise in einer Tasche, da die zwischen dem Lesegerät des e-Gates und dem Chip ausgetauschten Daten vollständig verschlüsselt sind.

Authentifizierung:

Das e-Gate muss zunächst den maschinenlesbaren Bereich (MRZ) oder die Zugangsnummer (CAN) des Dokuments optisch scannen, um nachzuweisen, dass es physischen Zugriff auf den Reisepass hat, bevor es einen sicheren Kanal zum Chip herstellt.

Die weltweite Einführung von PACE führt daher zu einer Phase des technologischen Wandels. Aus diesem Grund wurden in jüngster Zeit, insbesondere mit der Einführung von Pässen der neuen Generation wie dem neuen luxemburgischen Reisepass, der am 11. Mai 2026 eingeführt wurde, bei mehreren Reisenden zu erheblichen Störungen:

Software-Inkompatibilität:

Die IT-Systeme vieler e-Gates im Ausland haben ihre Aktualisierung noch nicht abgeschlossen oder sind nicht richtig konfiguriert, um diesen neuen technologischen Standard zu lesen.

Lesefehler:

Wird ein Reisepass, der ausschließlich das PACE-Protokoll verwendet, an einem veralteten e-Gate vorgelegt, weigert sich der Chip, Daten zu übermitteln, oder das Lesegerät kann die Daten nicht entschlüsseln, wodurch sich das Tor nicht öffnen lässt.

Die Einführung des digitalen biometrischen Reisepasses in Verbindung mit dem e-Gate sowie kryptografische Signaturen ermöglichen die Überprüfung der Echtheit und Integrität der Daten auf dem Chip; sie verstärken somit die verstärkte Kontrolle der Bevölkerung und eine digitale Massenüberwachung.

An den Binnengrenzen des Schengen-Raums muss jedoch das Prinzip der grenzenlosen Freizügigkeit gelten, das durch Artikel 21 AEUV über die Freizügigkeit der EU-Bürger garantiert ist. Kann ein Staat das Recht auf Überschreitung einer EU-Binnengrenze von der obligatorischen Teilnahme an einer automatisierten und eindeutig unverhältnismäßigen biometrischen Erfassung abhängig machen? Das ist die berechnete Frage, die sich jeder europäische Bürger zu stellen berechtigt ist.

Dr. Anne-Marie Yim, PhD

<https://www.virgule.lu/luxembourg/des-difficultes-de-lecture-du-nouveau-passeport-luxembourgeois-signalees-dans-certains-aeroports>