

PersoSim simuliert den elektronischen Personalausweis – und mehr

Damit Entwickler, Unternehmen und Behörden Funktionalitäten des elektronischen Personalausweises mit geringem Aufwand testen können, wurde der Open-Source-Simulator PersoSim entwickelt. Nun ist die Software zusätzlich in der Lage, Funktionen eines eIDAS-Tokens zu simulieren.


Der elektronische Personalausweis bietet mit seinem integrierten Chip im Vergleich zu herkömmlichen Authentisierungsverfahren – wie beispielsweise einer Kombination

und jederzeit schnell an neue Bedürfnisse angepasst werden zu können. PersoSim simuliert dabei sämtliche Mechanismen und kryptographischen Protokolle, die die Technische Richtlinie BSI TR-03110 beschreibt. Der Simulator steht allen Interessierten mit samt zusätzlichen Informationen auf der Website <https://persosim.secunet.com> zur Verfügung. Entwickler finden den Sourcecode auf der Website <https://github.com/PersoSim>.

Das BSI selbst verfolgt mit dem Simulator

Vor diesem Hintergrund wurde PersoSim zu einem eIDAS-Token erweitert und die zusätzliche Funktionalität in Zusammenarbeit mit dem BSI implementiert. Mit dieser ersten Referenzimplementierung eines eIDAS-Tokens, das alle Funktionen der TR-03110 umsetzt, konnte die Funktionsweise dieser neuen Protokolle auch in der Praxis dargelegt werden. Zu den neuen Funktionen zählen beispielsweise pseudonyme Signaturen, mit denen Daten unter einem chip- und sektorspezifischen Pseudonym signiert werden können. Eine weitere Neuerung ist Enhanced Role Authentication (ERA). Mit diesem Mechanismus können zusätzliche Attribute wie der Beruf über die initial personalisierten Daten hinaus auf dem Chip gespeichert werden.

Der Zugriff auf den Simulator erfolgt über virtuelle Kartenleser, die für die gängigen Betriebssysteme bereitgestellt werden. Auf diese Weise kann der Simulator transparent in das jeweilige Betriebssystem eingebunden werden und verhält sich dort wie ein echter Personalausweis mit einem Basis- oder Standardkartenleser. Zudem ist der Simulator auch für Android verfügbar: Hier wird die NFC-Schnittstelle des Smartphones genutzt, um mit einem Kartenleser zu kommunizieren.

PersoSim bietet somit Entwicklern und interessierten Anwendern eine einfache und unbürokratische Möglichkeit, den elektronischen Personalausweis und andere elektronische Identitäten zu simulieren und damit eigene Implementierungen zu verifizieren. Darüber hinaus bietet der Simulator die Möglichkeit, die kryptographischen Protokolle, die auf dem integrierten Chip verwendet werden, zu verstehen und nachzuvollziehen. 



Holger Funke
holger.funke@secunet.com

Der Simulator kann transparent in das jeweilige Betriebssystem eingebunden werden und verhält sich dort wie ein echter Personalausweis mit einem Basis- oder Standardkartenleser.

aus Benutzername und Passwort – ein höheres Authentisierungsniveau: Anwender können ihren Personalausweis nutzen, um sich für Dienste im Internet anzumelden, und Dienstanbieter können sicherstellen, dass es sich bei dem Anwender auch tatsächlich um genau diesen Anwender handelt. Dieses Prinzip der gegenseitigen Authentifizierung ist der zentrale Vorteil des elektronischen Personalausweises.

Mit dem Open-Source-Projekt PersoSim hat secunet im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik (BSI) einen Simulator für die Funktionen der Chipkarte auf dem neuen Personalausweis bereitgestellt. Gegenüber physikalischen Testkarten hat der Simulator den Vorteil kostenfrei zur Verfügung zu stehen

zudem das Ziel, PersoSim sowohl zur Weiterentwicklung als auch zur prototypischen Umsetzung neuer Sicherheitsprotokolle einzusetzen. Die Weiterentwicklung bestehender sowie die Evaluierung neuer und stärkerer Sicherheitsprotokolle ist bei der Verwendung von physikalischen Chipkarten mit hohem zeitlichen und finanziellen Aufwand verbunden. Der Grund: Hier müssen einige externe Parteien einbezogen werden, wie Hersteller von Chips oder deren Betriebssystemen, Anwendungsentwickler und Kartenproduzenten. Mit dem Einsatz eines softwarebasierten Simulators entfallen diese Einschränkungen, da direkt auf das zu testende Protokoll zugegriffen werden kann und dieses direkt nach der Änderung durch eine einfache Kompilierung lauffähig ist.