

eSECURITY®

Academy

esecurity.academy

Signal-Protokoll

**Moderne End-zu-End-Nachrichtenverschlüsselung
für Messaging-Dienste wie WhatsApp**

Kurs in Bern

28. November 2024

Viele Messaging-Dienste bieten heute eine durchgehende End-zu-End-Verschlüsselung für Text-, Bild- und/oder Videonachrichten an, die synchron oder asynchron ausgetauscht werden können. In vielen dieser Dienste kommt ein Protokoll zum Einsatz, das ursprünglich für den Signal-Messenger entwickelt worden ist und sich seither breit durchgesetzt und als Industriestandard etabliert hat. Das Protokoll basiert zwar auf bekannten kryptografischen Basisverfahren und -mechanismen, kombiniert diese aber auf eine nichttriviale und erklärungsbedürftige Art und Weise. Das entsprechende Signal-Protokoll markiert heute den Stand der Technik.

Im Rahmen der eSECURITY Academy bietet Prof. Dr. Rolf Oppliger einen 1-tägigen Kurs an, um sowohl die Entstehungsgeschichte des Signal-Protokolls als auch dessen grundlegende Funktionsweise mit seinen Vor- und Nachteilen zu erläutern.

Der Kurs basiert auf dem 2020 erscheinenden Buch «End-to-End Encrypted Messaging» (Artech House, ISBN 978-1-63081-732-9), das zusammen mit den Folien an die Kursteilnehmenden abgegeben wird.

Der Kurs findet am Donnerstag, 28. November 2024, in Bern statt (Ort und genaue Zeit werden noch bekanntgegeben).

Die Teilnahmegebühren betragen CHF 980.00 (inkl. MWST, Buch, Unterlagen und Verpflegung).

Melden Sie sich bitte bis am 28. Oktober 2024 per E-Mail an registration@esecurity.academy an.

Für Fragen stehen wir Ihnen telefonisch (+41 79 654 84 37) oder per E-Mail (info@esecurity.academy bzw. rolf.oppliger@esecurity.ch) sehr gerne zur Verfügung.