

Zeitschrift: ASMZ : Sicherheit Schweiz : Allgemeine schweizerische
Militärzeitschrift
Herausgeber: Schweizerische Offiziersgesellschaft
Band: 179 (2013)
Heft: 11

Werbung

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

Conditions d'utilisation

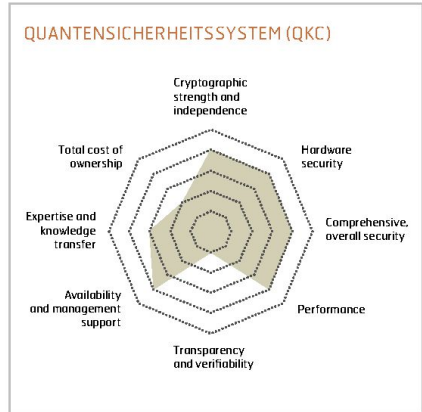
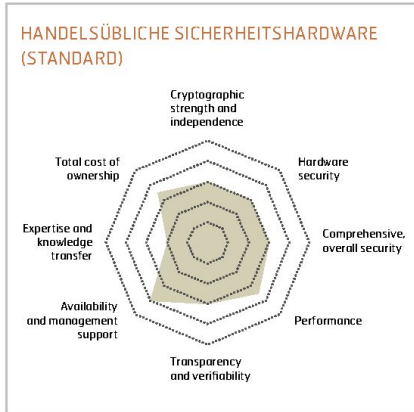
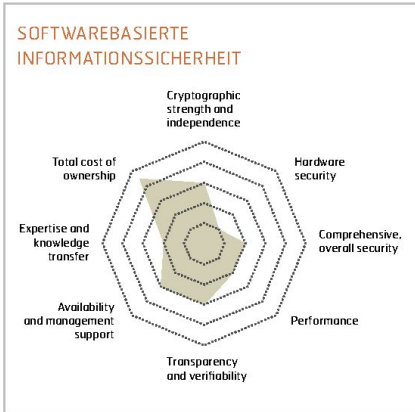
L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

Download PDF: 13.04.2026

ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>



teidigungslinien auf. Das heisst, dass mehr als nur ein Element für die Sicherheit des Kunden sorgt. Angriffe aller Ebenen werden immer mit der stärksten, zur Verfügung stehenden Sicherheitsmassnahme abgewehrt. Chiffrierung spielt dabei eine zentrale, aber nicht die alleinige Rolle:

- Hardwarebasierte Chiffrierung bildet die Grundlage für maximale Informationssicherheit, einerseits aus Geschwindigkeitsgründen, andererseits wegen ihrer Manipulationsresistenz;
- Chiffrierprozesse müssen gesondert von der Netzwerkfunktionalität ablaufen;

- Individualisiert erzeugte Kundenalgorithmen dürfen keinem anderen Kunden bekannt sein und von niemandem sonst benutzt werden. Somit ist selbst mit einem gleichen Gerät kein kryptografischer Angriff möglich. Auch der Lieferant darf keinen Zugriff haben. Daher muss das Algorithmusdesign so angelegt werden, dass der Kunde selbst seinen Algorithmus vervollständigt und so ausschliessliche Kontrolle über ihn hat;
- Ein computerbasiertes Sicherheitsmanagement dient zur nachhaltigen Erleich-

terung der täglichen Arbeit. Mit ihm lassen sich alle kryptografischen Parameter – inklusive Schlüssel verschiedener Hierarchien – sicher und zuverlässig erzeugen, verwalten und überwachen. ■



Hptm
Jahn Koch
lic. phil.
Customer Segment Manager
Defence, Crypto AG
6301 Zug



Wie wird die Welt der Bildung 2030 aussehen?

Dienstag, 12. November 2013

Chef aus Passion: von den Besten lernen

Donnerstag, 14. November 2013

Lilienberg Gespräch mit Andreas Meyer, CEO SBB

Dienstag, 19. November 2013

Weitere Informationen und Anmeldung unter www.lilienberg.ch