Kryptonormung 2013
"Anwendung und Mitgestaltung von Kryptonormen als Zukunftssicherung"

Workshop des Normenausschusses Informationstechnik und Anwendung, Arbeitskreis 27-02, in Zusammenarbeit mit den Fachgruppen KRYPTO *und* EZQN *der Gesellschaft für Informatik e.V. am 24. Mai 2013 in Berlin*

Kryptographische Verfahren, darunter Verschlüsselung, RNG, Hash-Summen, Zeitstempel, sind aus der heutigen Kommunikationswelt nicht mehr wegzudenken. Der Rückgriff auf bei ISO/IEC JTC 1/SC 27/WG 2 standardisierte kryptographische Verfahren unterstützt die korrekte und interoperable Implementierung (z.B. TLS/SSL bei HTTPS, RFID Chipkarten, AES) von bereits ausreichend untersuchten Sicherheitsverfahren als Stand der Technik. Vor allem auch leichtgewichtige Verfahren (lightweight algorithms) und die Anwendung von elliptischen Kurven bieten ein hohes Innovationspotential, zeigen aber auch noch einen hohen Standardisierungsbedarf. Gleichzeitig stehen international etablierte Normen derzeit vermehrt zur Revision an, was eine ausreichende Mitarbeit der Industrie notwendig erscheinen lässt, um den Exportstandort Deutschland nicht ohne Not zum Spielball anderer Wirtschaftsinteressen zu machen.

Vorträge mit konkreten Beispielen bieten Einblicke in die Normung von kryptographischen Verfahren, zeigen die Vorteile und Einsatzmöglichkeiten der Normung auf und wollen zu einer Fachdiskussion anregen. Der Workshop bietet eine Plattform zum Gedankenaustausch über Chancen der Zukunftssicherung mittels technischer Normung für Forscher, Entwickler, Anwender und Regulierer, die im Bereich von Kryptoverfahren und darüber hinaus tätig sind. Der Workshop soll aktuelle Normungsbedarfe mit den Teilnehmern zusammen aufnehmen und zu einer entsprechenden Mitarbeit und Mitgestaltung ermuntern.

Die Teilnahme am Workshop ist kostenlos. Bitte melden Sie sich unter Verwendung des Anmeldeformulars und Anerkennung der Teilnahmebedingungen bis zum 3. Mai 2013 an.

Der Workshop wird wie folgt stattfinden:

Ort: **DIN Deutsches Institut für Normung e.V.**
Burggrafenstrasse 6, 10787 Berlin
Raum 183

Zeit: **24. Mai 2013**
10:30 – 16:00 Uhr

DIN NIA-01-27-02 AK IT-Sicherheitstechniken und -mechanismen
<http://www.nia.din.de/sc/sicherheitsverfahren>

GI-Fachgruppe Evaluation, Zertifizierung, Qualitätssicherung, Normung (EZQN)
<http://fg-ezqn.gi.de>

GI-Fachgruppe Angewandte Kryptologie (KRYPTO)
<http://fg-krypto.gi.de>

Anmeldung zum Workshop "Anwendung und Mitgestaltung von Kryptonormen als Zukunftssicherung"

Zum kostenlosen Workshop **Kryptonormung 2013 – "Anwendung und Mitgestaltung von Kryptonormen als Zukunftssicherung"** am **24. Mai 2013** in **Berlin** melde ich mich unter Anerkennung der angegebenen Teilnahmebedingungen an.

Titel, Nachname	
Vorname	
Organisation / Abteilung	
Adresse	
Telefon	
E-Mail	

Teilnahmebedingungen

Die Teilnahme am Workshop ist kostenlos. Die Teilnehmerzahl ist begrenzt. Die Teilnahme ist daher nur mit bestätigter Anmeldung möglich.

Die Bestätigung der Teilnahme erfolgt in der zeitlichen Reihenfolge des Eingangs der Anmeldungen. Um rechtzeitige Anmeldung wird daher gebeten.

Bitte schicken Sie Ihre Anmeldung bis zum 3. Mai 2013 per Fax an +49 30 2601- 42591 oder per E-Mail an <martin.uhlherr@din.de>

Kryptonormung 2013
"Anwendung und Mitgestaltung von Kryptonormen als Zukunftssicherung"

Workshop des DIN Normenausschusses Informationstechnik und Anwendung, Arbeitskreis 27-02, in Zusammenarbeit mit den Fachgruppen KRYPTO und EZQN der Gesellschaft für Informatik e.V. am 24. Mai 2013 im DIN in Berlin

Programm

10:30 - 10:45 **Grußwort / Einführung**
Hans von Sommerfeld – Obmann NIA 27 IT-Sicherheitsverfahren

10:45 - 12:30 **Vorträge – Einblick in konkrete Beispiele aktiver Mitarbeit**

Hans von Sommerfeld – Obmann NIA 27 IT-Sicherheitsverfahren
„Anwendung und Nutzen von Kryptographie und Normung“

Dr. Erwin Hess – Siemens AG
„ELLI – Lightweight-Kryptographie basierend auf elliptischen Kurven“

Prof. Dr. Werner Schindler – Bundesamt für Sicherheit in der Informationstechnik (BSI) Bonn
„ISO / IEC 18031 "Random Bit Generation“

12:30 - 13:30 **Mittagspause**

13:30 - 15:00 **Vorträge – Möglichkeiten der Mitgestaltung und Innovation**

Prof. Dr. Christoph Ruland – Universität Siegen
„Kryptostandards als Fundus für Systeme“

Dr. Frank Niedermeyer – Bundesamt für Sicherheit in der Informationstechnik (BSI) Bonn
“Normung von Verfahren basierend auf elliptischen Kurven“

Prof. Dr. Stefan Katzenbeisser – Technische Universität Darmstadt
„Aktuelle Entwicklungen und Zukunftspotentiale angewandter Kryptologie“

15:00 - 15:15 **Kaffeepause**

15:15 - 16:00 **Zusammenfassung / Projektdefinition / abschließende Diskussion**

<http://fg-ezqn.gi.de/aktivitaeten/kryptonormung-2013.html>