



## Bundesministerium für Bildung und Forschung

### Bekanntmachung des Förderschwerpunkts „Neue Sicherheitstechnologien für das Internet der Dinge“ zur thematischen Ausgestaltung der Förderrichtlinie „Forschung Agil“

Vom 4. Juni 2019

#### 1 Gegenstand der Förderung

Die Vernetzung von Geräten im sogenannten Internet der Dinge (Internet of Things, IoT) nimmt weiterhin stark zu. Viele Alltagsgeräte wie GPS-Tracker, vernetzte Autos oder Smart-Home-Komponenten sind Teil dieses Netzes. Bis 2020 wird die Zahl der Geräte im IoT auf über 20 Milliarden angewachsen sein. Schon im Jahr 2017 gab es mehr vernetzte Gegenstände, als Menschen auf unserem Planeten leben. Diese vernetzten Dinge sind oft sehr einfache und günstige Geräte, die weder eigene Eingabemöglichkeiten haben, noch komplexe Berechnungen durchführen oder ausreichend Daten speichern können, um eine Authentifizierung der Geräte oder eine Verschlüsselung der Datenübertragung sicherzustellen. In der Folge können viele dieser Geräte in wenigen Minuten von Schadsoftware befallen werden.

Das MIRAI-Botnet (2016) und das MicroTik-Botnet (2018) haben eindrucksvoll gezeigt, wie groß die Gefahr durch unzureichend gesicherte Geräte im Internet sein kann. Diese Botnets bestanden aus ca. 400 000 mit dem Internet verbundenen und mit einer Schadsoftware (Bot) infizierten Geräten, die dadurch ferngesteuert werden konnten. Angreifer hatten so beispielsweise die Möglichkeit, Internetseiten mit zahlreichen gezielten Anfragen zu überlasten – sogenannte verteilte Denial-of-Service-(DoS)-Angriffe – oder auf den betroffenen Geräten heimlich Kryptogeld zu schürfen. Die enorme Intensität dieser Angriffe hatte Auswirkungen auf das gesamte Internet.

Vor diesem Hintergrund werden möglichst einfach benutzbare und ressourceneffiziente Verfahren benötigt, die eine inhärente Sicherheit im IoT herstellen. Ein Ansatz ist die Absicherung des Funkkanals zwischen dem drahtlos angebotenen IoT-Device und zugehörigem Empfänger durch Verfahren und Methoden der Informationstheorie, die auf Eigenschaften des elektromagnetischen Funkkanals und somit der physikalischen Umgebung eines Geräts basieren. Diese physikalischen Gegebenheiten des Funkkanals sind zwischen einem Sender und einem Empfänger einzigartig und können, geschickt eingesetzt, eine abhörsichere Kommunikation ermöglichen. Dies wird auch als Sicherheit auf der physikalischen Schicht (Physical Layer Security, PLS) bezeichnet.

Gegenstand der Förderung ist die Erforschung und Entwicklung von neuen Methoden und Verfahren, die die Sicherheit im IoT erhöhen und dabei die Sicherheit auf der physikalischen Schicht ausnutzen. Ziel ist unter anderem die Erforschung, Entwicklung und Erprobung von

- PLS-Verfahren für Integrität und Authentizität in IoT-Netzwerken;
- PLS-Verfahren zur sicheren Kommunikation und/oder zum geheimen Schlüsselaustausch in IoT Netzwerken;
- PLS-Verfahren gegen aktive Angriffe auf IoT-Netzwerke;
- Einsatzmöglichkeiten von PLS-Verfahren in sehr heterogenen IoT Netzwerken, die aus vielen unterschiedlichen Geräten bestehen, unterschiedliche Dienste nutzen bzw. bereitstellen und unterschiedliche Anforderungen an die Servicequalität stellen;
- Leistungsfähigkeit unterschiedlicher Kanalkodierungs- und Relayverfahren für PLS in Hinblick auf Ressourceneffizienz für einfache Geräte in IoT-Netzwerken;
- Auswirkungen beim Einsatz von Antennen mit vielen Antennenelementen (Massive MIMO) und Millimeterwellen (mm-Wave) auf PLS.

Die Lösungen müssen in einen Anwendungsfall einbettet und die Leistungsfähigkeit demonstriert werden. Im Rahmen des Förderschwerpunkts werden vorzugsweise Verbünde, in begründeten Ausnahmefällen auch wissenschaftliche Einzelvorhaben, in der Regel für bis zu drei Jahre gefördert.



## 2 Verfahren

Eine Förderung erfolgt im Rahmen der Richtlinie „Forschung Agil“ vom 4. Juni 2019 (BAAnz AT 19.06.2019 B3)

### 2.1 Einschaltung eines Projektträgers, Antragsunterlagen und sonstige Unterlagen

Mit der Abwicklung der Fördermaßnahme „Forschung Agil“ hat das BMBF derzeit folgenden Projektträger (PT) beauftragt:

VDI/VDE Innovation und Technik GmbH  
Projektträger Kommunikationssysteme; IT-Sicherheit  
Steinplatz 1  
10623 Berlin

Ansprechpartner ist Dr. Rainer Moorfeld

Telefon: 0 30/31 00 78-3 52

Telefax: 0 30/31 00 78-2 47

E-Mail: [rainer.moorfeld@vdivde-it.de](mailto:rainer.moorfeld@vdivde-it.de)

Internet: <https://www.forschung-it-sicherheit-kommunikationssysteme.de/foerderung/bekanntmachungen/agil>

Soweit sich hierzu Änderungen ergeben, wird dies im Bundesanzeiger oder in anderer, geeigneter Weise bekannt gegeben.

Vordrucke für Förderanträge, Richtlinien, Merkblätter, Hinweise und Nebenbestimmungen können beim Projektträger angefordert sowie unter folgender Adresse abgerufen werden:

<http://www.vdivde-it.de/projektfoerderung/dokumente-fuer-die-projektfoerderung>

### 2.2 Vorlage und Auswahl von Projektskizzen

In der ersten Verfahrensstufe ist dem PT VDI/VDE Innovation und Technik GmbH

bis spätestens zum 16. August 2019

eine Projektskizze vom Verbundkoordinator aus Gesamtvorhabensicht in elektronischer Form unter

<https://foerderportal.bund.de/easyonline/>

in deutscher Sprache vorzulegen. Die Vorlagefrist gilt nicht als Ausschlussfrist. Anträge, die nach dem oben angegebenen Zeitpunkt eingehen, können möglicherweise nicht mehr berücksichtigt werden.

Bonn, den 4. Juni 2019

Bundesministerium  
für Bildung und Forschung

Im Auftrag  
Dr. Herbert Zeisel

---