

Hannes Raddatz, Michael Rethfeldt
Martin Kasparick, Arne Wall, Dirk Timmermann

Absicherung der Gerätekommunikation im Smart Home unter Verwendung des Schutzprofils für Smart Meter Gateways

F 3081

Bei dieser Veröffentlichung handelt es sich um die Kopie des Abschlussberichtes einer vom Bundesinstitut für Bau-, Stadt- und Raumforschung (BBSR) im Bundesamt für Bauwesen und Raumordnung (BBR) im Rahmen der Forschungsinitiative »Zukunft Bau« geförderten Forschungsarbeit. Die in dieser Forschungsarbeit enthaltenen Darstellungen und Empfehlungen geben die fachlichen Auffassungen der Verfasser wieder. Diese werden hier unverändert wiedergegeben, sie geben nicht unbedingt die Meinung des Zuwendungsgebers oder des Herausgebers wieder.

Dieser Forschungsbericht wurde mit modernsten Hochleistungskopierern auf Einzelanfrage hergestellt.

Die Originalmanuskripte wurden reprototechnisch, jedoch nicht inhaltlich überarbeitet. Die Druckqualität hängt von der reprototechnischen Eignung des Originalmanuskriptes ab, das uns vom Autor bzw. von der Forschungsstelle zur Verfügung gestellt wurde.

© by Fraunhofer IRB Verlag

2018

ISBN 978-3-7388-0229-0

Vervielfältigung, auch auszugsweise,
nur mit ausdrücklicher Zustimmung des Verlages.

Fraunhofer IRB Verlag

Fraunhofer-Informationszentrum Raum und Bau

Postfach 80 04 69

70504 Stuttgart

Nobelstraße 12

70569 Stuttgart

Telefon 07 11 9 70 - 25 00

Telefax 07 11 9 70 - 25 08

E-Mail irb@irb.fraunhofer.de

www.baufachinformation.de

www.irb.fraunhofer.de/tauforschung

Absicherung der Gerätekommunikation im Smart Home unter
Verwendung des Schutzprofils für Smart Meter Gateways



Endbericht

Der Forschungsbericht wurde mit Mitteln der Forschungsinitiative Zukunft Bau
des Bundesinstitutes für Bau-, Stadt- und Raumforschung gefördert.

(Aktenzeichen: SWD-10.08.18.7-15.10 / II3-F20-14-1-012)

Die Verantwortung für den Inhalt des Berichtes liegt bei den Autoren.

Bearbeiter: M.Sc. Hannes Raddatz, M.Sc. Michael Rethfeldt,
Dipl.-Inf. Martin Kasparick, M.Sc. Arne Wall

Projektleiter: Prof. Dr.-Ing. Dirk Timmermann

Inhaltsverzeichnis

Abbildungsverzeichnis	3
Tabellenverzeichnis	5
Abkürzungsverzeichnis	6
1. Einführung.....	7
2. Aktuelle Entwicklungen.....	9
2.1. Smart Metering und Smart Home	9
2.2. Open Source im Smart Home	11
2.3. Protokoll-Trends.....	14
3. Grundlagen.....	16
3.1. Entwicklungen aus vorangegangenen BBSR-Projekten.....	16
3.2. Smart Meter Gateway	17
3.2.1. Schnittstellen.....	17
3.2.2. BSI Schutzprofil und Technische Richtlinien.....	18
3.3. Protokolle	20
3.3.1. Constrained Application Protocol (CoAP).....	20
3.3.2. Concise Binary Object Representation (CBOR)	23
3.3.3. CBOR Object Signing and Encryption (COSE).....	23
3.3.4. Object Security for Constrained RESTful Environments (OSCORE)	23
3.3.5. OAuth 2.0 & OpenID Connect	24
3.3.6. Authentication and Authorization for Constrained Environments (ACE)	25
3.3.7. Lightweight M2M (LwM2M).....	26
3.4. Weiterführende Informationen	26
3.4.1. Videostreaming über CoAP	26
3.4.2. Online-Ausweisfunktion des neuen elektronischen Personalausweises	28
3.4.3. Binary Decision Diagrams (BDDs)	29
4. Sicherheits-Framework	33
4.1. Problemstellung	34
4.2. Anwendungsszenarien	35
4.3. Allgemeine Anforderungen	38
4.4. Abgeleitete Anforderungen vom BSI Schutzprofil für das Smart Meter Gateway.....	40
4.5. Konzept.....	41
4.5.1. Kombinierte Smart Home- und Smart Metering-Infrastruktur	42
4.5.2. Protokolle des Sicherheits-Framework	44

4.5.3.	Kommunikationsabläufe	46
4.5.4.	Ergänzungen für eine beschleunigte Umsetzung	51
4.6.	Erweiterungen auf Basis des Sicherheit-Framework.....	54
4.6.1.	Dezentrales Regelmanagement	54
4.6.2.	ANTs.....	65
5.	Demonstrator - Konzeption & Entwicklung von Prototypen.....	67
5.1.	Aktivierung eines Nutzergerätes mithilfe des neuen elektronischen Personalausweises....	67
5.2.	Hinzufügen und steuern eines neuen Smart Home-Gerätes	67
5.3.	Mehrwertdienst durch Anbindung an Service Plattform.....	70
5.4.	Audio/Video-Gegensprechanlage	71
6.	Fazit und Ausblick	72
7.	Ergebnistransfer	73
	Literaturverzeichnis.....	75
	Anlagen	80