

# Secure Name Services for the Internet of Things

## DISSERTATION

zur Erlangung des akademischen Grades  
doctor rerum politicarum  
(Doktor der Wirtschaftswissenschaft)

eingereicht an der  
Wirtschaftswissenschaftlichen Fakultät  
der Humboldt-Universität zu Berlin

von

Herrn Diplom-Mathematiker Benjamin Fabian  
geboren am 29.1.1971 in Berlin

Präsident der Humboldt-Universität zu Berlin:  
Prof. Dr. Dr. h.c. Christoph Marksches

Dekan der Wirtschaftswissenschaftlichen Fakultät:  
Prof. Oliver Günther, Ph.D.

Gutachter:

1. Prof. Oliver Günther, Ph.D.
2. Priv.-Doz. Dr.-Ing. habil. Thomas Santen

eingereicht am: 26.06.2008

Tag der mündlichen Prüfung: 07.08.2008

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Problem Statement . . . . .	1
1.2	RFID and the Internet of Things . . . . .	1
1.3	Electronic Product Code . . . . .	2
1.4	EPC Tag and Data Standards . . . . .	3
1.5	Supply Chains . . . . .	4
1.6	Smart Homes . . . . .	5
1.7	Name Services . . . . .	6
1.8	Security . . . . .	7
1.9	Thesis Contributions and Outline . . . . .	8
<b>2</b>	<b>Name Service Requirements</b>	<b>11</b>
2.1	Introduction . . . . .	11
2.2	Functional and Performance Requirements . . . . .	12
2.3	Security Requirements . . . . .	17
2.3.1	Availability . . . . .	18
2.3.2	Integrity . . . . .	18
2.3.3	Confidentiality . . . . .	19
2.4	Requirements Overview . . . . .	26
2.5	Summary . . . . .	28
<b>3</b>	<b>ONS Security Challenges</b>	<b>29</b>
3.1	Introduction . . . . .	29
3.2	EPCglobal Network . . . . .	30
3.3	Object Naming Service (ONS) . . . . .	33
3.3.1	ONS Foundation: DNS . . . . .	33
3.3.2	DNS Names and Architecture . . . . .	33
3.3.3	DNS Protocol . . . . .	35
3.3.4	ONS Resolution Process . . . . .	35
3.4	ONS Security Analysis . . . . .	37
3.4.1	ONS Availability . . . . .	37
3.4.2	ONS Integrity . . . . .	39
3.4.3	ONS Confidentiality . . . . .	40
3.4.4	Query Confidentiality in the EPCglobal Network . . . . .	43

3.5	Summary . . . . .	45
<b>4</b>	<b>Evolution: Enhancing ONS</b>	<b>47</b>
4.1	Introduction . . . . .	47
4.2	Multipolar ONS . . . . .	48
4.2.1	Multipolarity . . . . .	48
4.2.2	Multipolar ONS Architecture . . . . .	51
4.2.3	MONS Prototype . . . . .	58
4.2.4	Modularity . . . . .	60
4.2.5	Conclusion . . . . .	60
4.3	Protecting Integrity: ONSSEC . . . . .	61
4.3.1	DNSSEC . . . . .	61
4.3.2	ONSSEC . . . . .	63
4.3.3	Multipolar ONSSEC . . . . .	64
4.4	Further ONS Risk Mitigation . . . . .	65
4.4.1	Network Design . . . . .	65
4.4.2	VPN and TLS . . . . .	66
4.4.3	Mixes and Onion Routing . . . . .	68
4.4.4	Private Information Retrieval . . . . .	70
4.5	Summary . . . . .	71
<b>5</b>	<b>Paradigm Shift: P2P-ONS</b>	<b>73</b>
5.1	Introduction . . . . .	73
5.2	Distributed Hash Tables . . . . .	76
5.3	OIDA . . . . .	78
5.3.1	Cryptographic Hash Functions . . . . .	78
5.3.2	OIDA Architecture . . . . .	79
5.3.3	Organizational Aspects . . . . .	83
5.4	OIDA Prototype . . . . .	84
5.4.1	PlanetLab . . . . .	85
5.4.2	Bamboo DHT . . . . .	85
5.4.3	Prototype Details . . . . .	88
5.4.4	Testing . . . . .	89
5.5	Scalability and Latency . . . . .	94
5.5.1	EPC Usage Estimation . . . . .	94
5.5.2	Class-Level vs. Serial-Level Resolution . . . . .	96
5.5.3	Update Propagation and Lookup Latency . . . . .	98
5.6	OIDA Security . . . . .	100
5.6.1	Overview . . . . .	100
5.6.2	Robustness and Availability . . . . .	101
5.6.3	Multipolarity . . . . .	104
5.6.4	Integrity . . . . .	105
5.6.5	Confidentiality . . . . .	106
5.7	OIDA Beyond ONS . . . . .	114

5.8	Architecture Comparison . . . . .	115
5.9	Summary . . . . .	115
<b>6</b>	<b>Conclusion</b>	<b>121</b>
6.1	Thesis Summary . . . . .	121
6.2	Open Questions . . . . .	122
	<b>Bibliography</b>	<b>140</b>
A	<b>OIDA Bamboo Configuration</b>	<b>141</b>
B	<b>OIDA Clients</b>	<b>143</b>
C	<b>Abbreviations</b>	<b>151</b>
D	<b>Acknowledgements</b>	<b>155</b>
E	<b>Selbständigkeitserklärung</b>	<b>157</b>