



Sensor-based Authentication

Trend Report 2014



CENTER FOR DIGITAL TECHNOLOGY & MANAGEMENT



Sensor-based Authentication

Trend Report 2014

Other CDTM print publications

M. Huber, C. Bachmeier, A. Buttermann,
S. Vogel, P. Dornbusch (Eds.)

Smart Dust

ISBN 978-3-8311-4297-2. 2002.

X, 280 p.

M. Huber, P. Dornbusch, J. Landgrebe,
M. Möller, M. Zündt (Eds.)

**Visions of Advanced Mobile
Communications**

ISBN 978-3-9808842-0-4. 2003

VII, 272 p.

P. Dornbusch, M. Huber, M. Möller,
J. Landgrebe, M. Zündt (Eds.)

Leveraging Business with Web Services

ISBN 978-3-9808842-1-1. 2003.

VI, 238 p.

P. Dornbusch, M. Huber, J. Landgrebe,
M. Möller, U. Sandner, M. Zündt (Eds.)

**The Future of Telematics:
New Business Concepts and Technologies**

ISBN 978-3-9808842-2-8. 2004.

XII, 370 p.

P. Dornbusch, M. Möller, J. Landgrebe,
U. Sandner, M. Zündt (Eds.)

**Generation 50 Plus - Products and
Services in the TIME Sector**

ISBN 978-3-9808842-3-5. 2005.

VII, 338 p.

P. Dornbusch, U. Sandner, P. Sties,
M. Zündt (Eds.)

Fixed Mobile Convergence

ISBN 978-3-9808842-4-2. 2005.

V, 259 p.

B. Kirchmair, N. Konrad, P. Mayrhofer,
P. Nepper, U. Sandner, M. Zündt (Eds.)

**Seamless Context-Aware Services
in Converged Mobile- and
Enterprise-Networks**

ISBN 978-3-9808842-6-6. 2007.

344 p.

A. Balevic, B. Bozzonek, B. Kirchmair,
N. Konrad, P. Mayrhofer, P. Nepper,
U. Sandner (Eds.)

**Effective Collaboration in Dynamic
Communities with Service-oriented
Architectures**

ISBN 978-3-9808842-7-3. 2007.

VI, 150 p.

B. Kirchmair, N. Konrad, P. Mayrhofer,
P. Nepper, U. Sandner (Eds.)

The Future of Publishing

Trends for the Bookmarket 2020

ISBN 978-3-9812203-0-8. 2008.

260 p.

P. Nepper, N. Konrad (Eds.)

The Future of Social Commerce

ISBN 978-3-9812203-1-5. 2009.

XX, 320 p.

M.-L. Lorenz, P. Nepper, N. Konrad (Eds)

The Service Centric Car in 2020

ISBN 978-3-9812203-4-6. 2009.

XXII, 304 p.

M.-L. Lorenz, C. Menkens, N. Konrad (Eds.)

E-Energy

ISBN 978-3-9812203-5-3. 2009.

XXVIII, 382 p.

M.-L. Lorenz, C. Menkens, J. Sußmann,
N. Konrad (Eds.)

**Developer Platforms and
Communities in the Telecom Industry**

ISBN 978-3-9812203-6-0. 2010.

XXVI, 356 p.

B. Römer, J. Sußmann, C. Menkens,
M.-L. Lorenz, P. Mayrhofer (Eds.)

Smart Grid Infrastructures

ISBN 978-3-9812203-7-7. 2011.

XXVI, 333 p.

J. Sußmann, B. Römer (Eds.)

Urban Mobility Concepts

ISBN 978-3-9812203-8-4. 2011.

XXII, 382 p.

J. Sußmann, B. Römer (Eds.)

Ambient Assisted Living

ISBN 978-3-9812203-9-1. 2011.

XXIII, 307 p.

M. Schadhauer, J. Sußmann, B. Römer (Eds.)

The Future of Real-Time Communication

ISBN 978-3-9815538-1-9. 2012.

XXIII, 299 p.

V. Gamper, S. Nothelfer, M. Schadhauer

**Human-Machine-Interaction in Individual
Mobility**

ISBN 978-3-9815538-2-6. 2013.

XXIV, 298 p.

V. Gamper, S. Nothelfer

Data Marketplaces in Smart Cities

ISBN 978-3-9815538-3-3. 2013.

XXIII, 275 p.

Veronika Gamper · Stefan Nothelfer (Editors)

Sensor-based Authentication

Trend Report 2014

Class 2014 Spring

Center for Digital Technology and Management

Sensor-based Authentication. Trend Report 2014

Edited by: Veronika Gamper, Stefan Nothelfer

ISBN: 978-3-9815538-5-7

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

© 2014 Center for Digital Technology and Management, Munich, Germany
Printed in Germany

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitations, broadcasting, reproduction on microfilm or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from the Center for Digital Technology and Management. Violations are liable for prosecution under the German Copyright Law.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and thereof free for general use.

The Center for Digital Technology and Management (CDTM) is a joint institution of the Technische Universität München (TUM) and the Ludwig-Maximilians-Universität München (LMU). This report was created by CDTM students and is part of a project cooperation with T-Labs. The CDTM is part of the Elitenetzwerk Bayern.

Board of Directors:

Prof. Dr. Dr. h.c. Manfred Broy (TUM)
Prof. Bernd Brügge, Ph.D. (TUM)
Prof. Dr. Andreas Butz (LMU)
Prof. Dr.-Ing. Klaus Diepold (TUM)
Prof. Dr.-Ing. Jörg Eberspächer (TUM)
Prof. Dietmar Harhoff, M.P.A. Ph.D. (MCIER)
Prof. Dr. Heinz-Gerd Hegering (LMU)
Prof. Dr. Thomas Hess (LMU)
Prof. Dr.-Ing. Wolfgang Kellerer (TUM)
Prof. Dr. Dieter Kranzlmüller (LMU)
Prof. Dr. Tobias Kretschmer (LMU)
Prof. Dr. Helmut Krcmar (TUM)
Prof. Dr. Dres. h.c. Arnold Picot (LMU)
Prof. Dr. Martin Spann (LMU)
Prof. Dr. Isabell Welpe (TUM)

Center for Digital Technology and Management
Marsstr. 20-22, 80335 Munich, Germany
E-Mail: info@cdtm.de
Web: <http://www.cdtm.de>

Preface of the Editors

“Everybody can learn from the past. Today it is important to learn from the future.”

As the statement by Herman Kahn, one of the founding fathers of modern scenario planning, nicely states, it is tremendously important for strategy and policy makers to get a deep understanding of possible future developments in order to be prepared for them.

We will give a brief overview on the approach behind the creation of this trend report, which involved the creation of future scenarios and the development of innovative product and service ideas. This approach has been developed and refined over the last thirteen years in over twenty projects. The goal is to create trend studies and business ideas in the field of information and communication technologies (ICT). Thereby, we rely on a tight cooperation between industry partners and academia. Combining the creativity and external view of interdisciplinary participants from academia with the knowledge of larger corporations, the outcome are long-term foresights and innovative ideas on how to prepare for emerging challenges in a certain field and product and service ideas that may solve future needs. Recent industry partners were large corporations, for instance Siemens AG, Telekom Innovation Laboratories and BMW AG. Topics were diverse, ranging from Smart Grid Infrastructures and Ambient Assisted Living Technologies to Urban Mobility Concepts.

The Trend Seminar at CDTM is a university course with around 20-25 selected students of various disciplines, such as business administration, economics, computer science or electrical engineering that work on a relevant topic related to ICT. After the topic has been defined, it is broken down into smaller modules, that are then worked on by smaller, interdisciplinary teams.

The course stretches over seven intense weeks, fulltime, during which the participating students dive deeply into the new topic. Thereby, they apply the knowledge they bring along from their main studies and extend it by extensive research. They learn and apply new methodologies, conduct trend analyses, design future scenarios and develop business ideas for innovative products or services.

The Trend Seminar is structured into three phases: The Basic Phase, the Scenario Phase and the Ideation Phase.

In the Basic Phase, the class is split into five teams that look at different aspects of the overall topic. Following the STEP approach, the status quo and trends in the fields of technology, society, economy, politics, law, environment and business are analyzed. Knowledge is gathered by literature research, preceded by a series of input presentations by industry experts, held by our project partner or other organizations. At the end of the Basic Phase, teams present their key findings to each other in order for everyone to get a holistic view on the topic to build upon in the following phases.

The following Scenario Phase starts with a two-day workshop. Participants work in four teams, newly formed in order to have experts from every subtopic of the Basic phase in each new Scenario team. Within the workshop driving forces for the overall topic are identified and structured. Two key drivers are identified, which span a matrix of four different future scenarios of approx. fifteen years ahead. The scenarios as well as possible timelines to these diverse futures are sketched out within the workshop. After the workshop, each team elaborates a vivid view of the life in one of the four scenarios.

In the third phase, the Ideation Phase, participants are again regrouped into new teams. The goal of this phase is to develop innovative business concepts, which are then tested against the previously developed scenarios. The phase starts with a two-day workshop on ideation methods. Based on the work by Jacob Goldenberg, Roni Horowitz, Amnon Levav and David Mazursky, the applied ideation methods are a structured way to develop new products or services. At the end of the workshop each team is equipped with a broad set of ideas. Out of these, the most promising five ideas are selected and further developed into detailed business concepts. The business model canvas, developed by Alexander Osterwalder and Yves Pigneur, serves as base structure. At the end of the seminar, the business model concepts are presented to the project partner and guests.

We would like to take the opportunity to thank several people who made this CDTM Trend Report possible: We want to thank Dennis Gotta, Florian Reuter and Dr. Marc Wagener at our project partner Siemens Novel Businesses, who helped to define the topic and scope of the project and, together with their colleagues, provided great insight into current trends and future developments in the field. In addition, we would like to thank all lecturers for providing valuable input and contributing the Trend Seminar's success. Their expertise and motivation always result in a great lecture atmosphere and excellent outcomes. Finally, we want to say special thanks to the CDTM students of the class of Spring 2014. They put an enormous amount of energy and enthusiasm into this project, which made it a pleasure for us to supervise the course and coach the individual teams.

We hope you enjoy reading up on the results of this trend report and maybe get some inspirations on the future development of sensor-based authentication.

Veronika Gamper and Stefan Nothelfer
Center for Digital Technology and Management

Preface

As abstract as it may sound as a concept, authentication is one of the main activities in our daily life. Be it swiping a finger in a certain pattern across the smartphone's touch screen, wiring money or merely opening the door to our flat. Preventing unauthorized access to one's bank account is critical. And the same holds true for online accounts in order to protect our identity, just to name a few examples. It all starts with successful identification, but in order to also authenticate, a reliable verification is required. The most common tool to verify one's identity is using a password.

Yet, in all these increasingly digital and internet-based interactions, the balance between security and convenience is hard to find. How many passwords can we be expected to remember? How complex should they be? Should we use unique physical items to increase security? How can we avoid spending more energy on the log-in than on the actual activity? Such questions represent a growing customer pain – which should ultimately result in opportunities for profitable business models. And this growing customer pain is not necessarily limited to our private life – reliable authentication is at least as critical in business transactions and at industrial sites.

This is where we come in: our team at Siemens Novel Businesses founds start-ups in business areas of potential interest for Siemens, a global engineering powerhouse. “Sensor-based authentication” is one of these areas of potential interest, where a promising development seems to start in the consumer space and could spread to industrial applications later.

We picked this topic building upon two big trends: the spread of sensors and the growing need for security, identity management and reliable authentication. The main challenge in this field was and will be finding viable business models – which is why we deliberately chose the CDTM trend study as a tool to explore future solutions beyond our company's current scope and applications in a rapidly developing field.

The report at hand is the result of two intense months of work. It combines individual contributions from a unique group of students and the thorough methodology framework which channeled the creativity towards actual business models. We particularly valued the multiple perspectives provided and the fresh thoughts developed in the course of the program.

A big thank you to every single participant for your contributions and the inspiring conversations based upon them. Last but not least we want to thank Stefan and Veronika for managing the project, the pleasant collaboration, flawless organization and shaping the results.

All of us tremendously enjoyed working with such a unique, bright, motivated and creative group of students. We are looking forward to crossing parts again in the future - and will hopefully identify each other the old school way...

Marc Wagener, Florian Reuter and Dennis Gotta

Siemens Novel Businesses GmbH

The entire trend report was written by CDTM students under the close guidance of research assistants in 2014. The papers compiled here do not claim to be scientifically accurate in every case; they are rather meant to give a structured and broad overview of trends relevant in the context of Sensor-based Authentication.

For more information about the CDTM and its related projects, please visit <http://www.cdtm.de>

Contents

I	Trends	1
1	Technology Trends in Sensor-based Authentication	3
1.1	Introduction	4
1.2	Trends	5
1.2.1	Sensor trends	5
1.2.1.1	Increasing integration of sensors in mobile devices	5
1.2.1.2	Improvements in chemical sensor technologies .	6
1.2.1.3	Developments in biometric authentication . . .	7
1.2.2	Authentication trends	9
1.2.2.1	Growing adaptation of multifactor authentication	9
1.2.2.2	Increasing establishment of single-sign-on systems and federated identity	10
1.2.2.3	Growing need for sophisticated cryptographic methods	11
1.2.2.4	Emergence of soft authentication methods . .	11
1.2.3	Sensor-based authentication trends	12
1.2.3.1	Increasing usage of devices as authentication by witness	12
1.2.3.2	Rising importance of biometrics authentication	14
1.2.3.3	Eye-movement emerge as a combination of biometrical and behavioural authentication characteristics	15
1.2.3.4	Brain activity authentication methods develop as a feasible and unforgeable solution	16
1.3	Conclusion	17
2	Trends in Society and Customer Needs	27
2.1	Introduction	29
2.2	Trends	29
2.2.1	Increasing adoption of digital devices and sensors	30
2.2.1.1	Increasing number of connected devices	30
2.2.1.2	Growing acceptance of ubiquitous sensors . . .	30

2.2.1.3	Shift towards device and location independent data access	31
2.2.2	Growing environmental and social conscience	32
2.2.2.1	Growing interest in production process assessment and product origin	32
2.2.2.2	Evolution of a collaborative and sharing culture	33
2.2.3	Growing expectations towards convenience through technology	35
2.2.3.1	Movement towards consolidation of devices and digital identities	35
2.2.3.2	Increasing relevance of mobile applications and software as a service	36
2.2.3.3	Increasing importance of intelligent automation and control systems	37
2.2.4	Demand for personalization	37
2.2.4.1	Growing interest in personalized customer experience	38
2.2.4.2	Rapidly growing number of people in the Quantified Self movement	39
2.2.4.3	Individually customized use of shared devices and resources	40
2.2.5	Need for secure private data and personal data control	40
2.2.5.1	Trust in big organizations and governments is diminishing	40
2.2.5.2	Sensitive administrative tasks are digitized	41
2.3	Conclusion	42
3	Trends in Corporations and Business Eco Systems	51
3.1	Introduction	53
3.2	Trends	53
3.2.1	Organizational environment	53
3.2.1.1	Increasing organizational transparency for stakeholders	53
3.2.1.2	Growing importance of brands and counterfeit prevention	55
3.2.1.3	Increasing interconnectedness of businesses	56
3.2.1.4	Growing adoption of smart manufacturing	57
3.2.1.5	Increasing need for protection from external virtual threats	58
3.2.2	Employee work environment	59
3.2.2.1	Increasing commoditized and globalized white collar workforce	60
3.2.2.2	Flexibilization of workplace and working time	61

3.2.2.3	Increasing risk of confidential information disclosure	62
3.3	Conclusion	64
4	Political and Legal Trends	75
4.1	Introduction	76
4.2	Trends	76
4.2.1	Privacy and data protection regulations	76
4.2.1.1	Increasing regulations regarding data storage and data handling	77
4.2.1.2	Increasing pressure for high fines for data protection violations	78
4.2.1.3	Gaining importance of IT audits	79
4.2.1.4	Growing pressure towards common European privacy standards	80
4.2.1.5	New regulations regarding smart devices	81
4.2.1.6	Increasing challenges resulting from conflicting data protection regulations	82
4.2.2	Regulations on authentication	82
4.2.2.1	Further decrease of payment service-related cyber criminality	84
4.2.2.2	Reinforcement of existing regulations on authentication	84
4.2.3	Unified governmental authentication	85
4.2.3.1	Increasing government Involvement in Germany with eID	86
4.2.3.2	Increasingly diverse approaches for electronic government services authentication worldwide	88
4.2.4	Authentication of goods	90
4.2.4.1	Increasing regulations for food products	90
4.2.4.2	Increasing regulations of counterfeit goods	91
4.3	Conclusion	91
5	Emerging Business Models	101
5.1	Introduction	102
5.2	Trends	103
5.2.1	Security of authentication procedures	103
5.2.1.1	Switch from one-factor to multi-factor authentication	103
5.2.1.2	Increasing usage of secure one-factor authentication based on advanced sensor mechanisms	105
5.2.1.3	Increased security in digital postal traffic: De-Mail and E-Postbrief	106

5.2.2	Usability of authentication procedures	107
5.2.2.1	Elimination of multiple login activities by Single Sign-On	107
5.2.2.2	Adaption of authentication procedures according to the required level of security	109
5.2.2.3	Transfer of physical identities to the digital world	110
5.2.2.4	Increased convenience of authentication by sensor based methods with minimal personal interaction	111
5.2.3	Authentication of products	112
5.2.3.1	Growing number of authentication solutions in response to legal requirements	113
5.2.3.2	Increasing number of tracking solutions addressing consumer pressure	114
5.2.3.3	Increasing countermeasures against economic loss due to forgery	115
5.2.4	Application of sensors beyond authentication	115
5.2.4.1	Increasing collection and analysis of personal health data	116
5.2.4.2	Increased offerings for recognition and measurement of a person's environment	117
5.3	Conclusion	118

II Scenario Planning 129

6 Introduction 131

7 Driver Analysis 135

7.1	Key drivers	135
7.1.1	Standardization	135
7.1.2	Shareconomy	138
7.1.3	No collaborative consumption	139
7.1.4	Total collaborative consumption	140
7.2	Additional drivers	140
7.2.1	Trust in providers of sensor based authentication	140
7.2.2	Privacy awareness	141
7.2.3	Remote work	142
7.2.4	Market structure of authentication providers	144
7.2.5	Need for transparency in value chain	145
7.2.6	Counterfeit	147
7.2.7	Biometrics	148

8	Scenarios	151
8.1	Scenario I: The WEconomy	151
8.1.1	Scenario Description	151
8.1.2	Timeline	156
8.1.3	Signposts	158
8.2	Scenario II: Life in the Egosystem	160
8.2.1	Scenario Description	160
8.2.2	Timeline	164
8.2.3	Signposts	165
8.3	Scenario III: Fragmented Hypercapitalism	167
8.3.1	Scenario Description	168
8.3.2	Timeline	172
8.3.3	Signposts	174
8.4	Scenario IV: Complex Collaboration	175
8.4.1	Scenario Description	176
8.4.2	Timeline	180
8.4.3	Signposts	182
III	Ideation	187
9	FoodCheck	189
9.1	Introduction	191
9.2	Business idea	191
9.2.1	Value proposition	196
9.2.2	Customer segments	196
9.2.3	Channels	197
9.2.4	Customer relationships	197
9.2.5	Key resources	197
9.2.6	Key activities	198
9.2.7	Key partners	198
9.2.8	Revenues	198
9.2.9	Costs	199
9.3	Scenario robustness check	199
9.3.1	The Weconomy	199
9.3.2	Life in the Egosystem	199
9.3.3	Fragmented Hypercapitalism	200
9.3.4	Complex Collaboration	200
9.4	Conclusion	201
10	Convenient Payment	205
10.1	Introduction	207
10.2	Business idea: mamoru	208

10.2.1	Value proposition	210
10.2.2	Customer segments	212
10.2.3	Channels	213
10.2.4	Customer relationships	215
10.2.5	Key resources	216
10.2.6	Key activities	217
10.2.7	Key partners	217
10.2.8	Revenue Streams	218
10.2.9	Costs	219
10.3	Scenario robustness check	220
10.3.1	The Weconomy	220
10.3.2	Life in the Ecosystem	221
10.3.3	Fragmented Hypercapitalism	222
10.3.4	Complex Collaboration	222
10.4	Conclusion	223
11	RTM Technologies (Right Transfer Management)	227
11.1	Introduction	229
11.2	Business idea	229
11.2.1	Value proposition	232
11.2.2	Customer segments	233
11.2.3	Channels	234
11.2.4	Customer relationships	235
11.2.5	Key resources	235
11.2.6	Key activities	237
11.2.7	Key partners	237
11.2.8	Revenues	239
11.2.9	Costs	239
11.3	Scenario robustness check	240
11.3.1	The Weconomy	240
11.3.2	Life in the Ecosystem	241
11.3.3	Fragmented Hypercapitalism	241
11.3.4	Complex Collaboration	241
11.4	Conclusion	242
12	QRscratch	243
12.1	Introduction	245
12.2	Business idea: QRscratch	245
12.2.1	Value proposition	247
12.2.2	Customer segments	248
12.2.3	Channels	249
12.2.4	Customer relationships	249
12.2.5	Key resources	250

12.2.6	Key activities	250
12.2.7	Key partners	251
12.2.8	Revenues	251
12.2.9	Costs	252
12.3	Scenario robustness check	252
12.3.1	The Weconomy	253
12.3.2	Life in the Ecosystem	253
12.3.3	Fragmented Hypercapitalism	254
12.3.4	Complex Collaboration	254
12.4	Conclusion	255
13	Horcruxication	257
13.1	Introduction	258
13.2	Business idea	259
13.2.1	Value proposition	259
13.2.2	Customer segments	261
13.2.3	Channels	262
13.2.4	Customer relationships	263
13.2.5	Key resources	263
13.2.6	Key activities	266
13.2.7	Key partners	268
13.2.8	Revenues	269
13.2.9	Costs	270
13.3	Scenario robustness check	271
13.3.1	The Weconomy	271
13.3.2	Life in the Ecosystem	271
13.3.3	Fragmented Hypercapitalism	272
13.3.4	Complex Collaboration	272
13.4	Conclusion	273

List of Figures

7.1	Impact and uncertainty of drivers on the sensor-based authentication	136
8.1	Scenario matrix with four possible scenarios	152
8.2	Timeline, The WEconomy	157
8.3	Timeline, Life in the Egosystem	166
8.4	Timeline, Fragmented Hypercapitalism	173
8.5	Timeline, Complex Collaboration	181
9.1	Categorization of undesirable substances in food	194
10.1	Mamoru conceptual work-flow	211
10.2	Profile of a typical customer	214
10.3	The mamoru cost and revenue model	219
10.4	Essential components and suppliers	220
11.1	Use case of Deutsche Post DHL	230
11.2	RTM's technical infrastructure	236
12.1	Key Partners	252
13.1	HCX embodies the combination of security, privacy, and convenience	260
13.2	HCX and its relevant stakeholders	266
13.3	HCX branding as accelerator for multi-sided platform	267

The Center for Digital Technology and Management (CDTM) is a joint, interdisciplinary institution for education, research and entrepreneurship of the Ludwig-Maximilians-Universität München (LMU) and the Technische Universität München (TUM).

Building on the strengths of both universities, CDTM provides highly qualified and ambitious students with an academic education in the field of emerging digital technologies.

CDTM closely cooperates with industry partners, thereby focusing on the Telecommunication, Information Technology, Media, Entertainment, Health and Energy sectors.

e-mail info@cdtm.de
Internet <http://www.cdtm.de>

Veronika Gamper • Stefan Nothelfer (Eds.) Sensor-based Authentication

Numerous authentications take place in our everyday lives: From the use of passwords to access an email account, fingerprint scans to grant access to buildings to the confirmation of a product's origin to prevent counterfeits. Sensor technology at the same time has advanced tremendously over the last decades. Not only are sensors making things increasingly smart (e.g. smart homes, smart cars), sensors are also increasingly included in consumer products, such as cell phones or digital cameras.

The balance between security and convenience, however, is hard to find. This represents a huge business opportunity for new business models.

This report analyzes how sensor-based authentication may look like in the future, describes future scenarios and potential business ideas.

This report consists of three parts, one analyzing trends, one describing scenarios and one elaborating business ideas. First, the authors analyze trends regarding sensor-based authentication. Building upon these findings, four scenarios are described, vividly depicting possible futures. In the final Ideation part five business concepts are elaborated and tested against the scenarios.

The developed business concepts range from a product authentication solution against counterfeits, continuous multi-factor biometric authentication, a platform for the digital transfer of rights and permissions, a device detecting harmful food constituents to a solution for fragmenting traditional authentication.

