Inhaltsverzeichnis

1 Einleitung **1**
1.1 Motivation und Problemstellung . . . 1
1.2 Zielsetzung der Dissertation . . . 3
1.3 Aufbau der Dissertation . . . 4

2 Stand der Technik und Wissenschaft **7**
2.1 Additive Fertigung . . . 7
2.1.1 Technologie der additiven Fertigungsverfahren . . . 8
2.1.1.1 Strangablegeverfahren . . . 9
2.1.1.2 Laser-Sintern und Strahlschmelzen . . . 10
2.1.2 Prozesskette zur additiven Fertigung . . . 11
2.1.3 Datenformate der additiven Fertigung . . . 12
2.1.3.1 STL-Schnittstelle . . . 13
2.1.3.2 Schichtdaten . . . 14
2.1.3.3 NC-Daten . . . 15
2.1.4 Verteilte additive Fertigung . . . 16
2.2 Virtuelle Produktentstehung . . . 18
2.2.1 Produkt- und Bauteildaten . . . 18
2.2.2 Produktentstehungsprozess . . . 19
2.3 Sicherheit in der Informationstechnik . . . 20
2.3.1 Schutzziele . . . 21
2.3.2 Sicherheitsmaßnahmen . . . 22
2.3.2.1 Juristische Maßnahmen . . . 22
2.3.2.2 Strategische Maßnahmen . . . 22
2.3.2.3 Organisatorische Maßnahmen . . . 23
2.3.2.4 Technische Maßnahmen . . . 23
2.3.3 Sicherheitsnormen . . . 24
2.4 Kryptologie . . . 24
2.4.1 Verschlüsselung . . . 25
2.4.2 Symmetrische Kryptografie . . . 27
2.4.2.1 Strom- und Blockchiffren . . . 28
2.4.2.2 AES-Algorithmus . . . 31
2.4.3 Asymmetrische Kryptografie . . . 32
2.4.3.1 RSA-Kryptosystem . . . 33
2.4.3.2 Elliptische-Kurven-Kryptografie . . . 35
2.4.3.3 Pairing-basierte Kryptografie . . . 36
2.4.4 Kryptografische Hashfunktionen . . . 36
2.4.5 Digitale Signaturen . . . 37

2.4.6 Zertifikate . . . 38
2.4.7 Zugriffskontrolle und Rechtemanagement . . . 39
2.5 Existierende Forschungsansätze . . . 40
2.6 Fazit . . . 42

3 Anforderungsprofil **45**
3.1 Handlungsbedarf . . . 45
3.2 Betrachtete Anwendungsfälle . . . 47
3.2.1 Systemakteure . . . 47
3.2.2 Systemgrenze . . . 49
3.3 Angreifermodellierung . . . 49
3.3.1 Angriffsvektoren . . . 52
3.4 Zieldefinition . . . 53
3.5 Anforderungen . . . 53
3.5.1 Anforderungen an die Methodenkonzeption . . . 54
3.5.2 Anforderungen an die Implementierung der Methoden . . . 58
3.6 Fazit . . . 61

4 Konzeption zum durchgängigen Schutz von Daten in der verteilten additiven Fertigung **65**
4.1 Konzeptioneller Ansatz . . . 65
4.2 Struktur des Gesamtkonzepts . . . 66
4.3 Entwicklung der erweiterten Prozesskette . . . 68
4.3.1 Integration der Autorisierung in die Prozesskette . . . 68
4.3.2 Übersicht über die erweiterte Prozesskette . . . 70
4.4 Definition von fertigungsbezogenen Attributen . . . 72
4.4.1 Attributkonvention . . . 74
4.4.2 Berechtigungsrichtlinien . . . 76
4.4.3 Struktur der Richtlinien . . . 77
4.5 Repräsentation geschützter Bauteil- und Fertigungsdaten . . . 79
4.5.1 Segmentierung der Fertigungsdaten . . . 80
4.5.2 Symmetrische Verschlüsselung der Fertigungsdatensegmente . . . 81
4.5.3 Pseudonymisierung . . . 83
4.5.4 Randomisierung . . . 85
4.5.4.1 Vorgehensweise . . . 88
4.5.5 Authentizitätsschutz . . . 89
4.6 Zugriffsautorisierung für Bauteil- und Fertigungsdaten . . . 90
4.6.1 Zustandsbehaftete Autorisierung . . . 91
4.6.2 Erzeugung der Inhaltsschlüssel . . . 92
4.6.3 Verknüpfung der Teilschlüssel . . . 94
4.6.4 Autorisierungsprotokoll . . . 94
4.7 Attributbasierte Autorisierung der Segmentzuordnung . . . 96
4.7.1 Auswahl der kryptografischen Parameter . . . 97
4.7.2 Bilineare Abbildung . . . 99
4.7.3 Infrastruktur zur Verwaltung von Schlüsseln und Berechtigungen . . . 101

4.7.4 Schlüsselerzeugung . . . 102
4.7.5 Verschlüsselung der Segmentzuordnungsdaten . . . 103
4.7.6 Entschlüsselung der Segmentzuordnungsdaten . . . 104
4.8 Präsentation von geschützten Bauteil- und Fertigungsdaten . . . 105
4.8.1 Assoziation von Bauteilpräsentation und Fertigungsdaten . . . 106
4.8.1.1 Geometrische Transformation . . . 107
4.8.2 Geometrische Detailreduktion . . . 109
4.8.3 Anbindung von Stützstrukturen . . . 111
4.9 Fazit . . . 112

5 Prototypische Implementierung **115**
5.1 Architektur des Gesamtsystems . . . 115
5.2 Randbedingungen der Implementierung . . . 117
5.3 SIAM-Assistenzsystem . . . 118
5.3.1 Grafische Benutzungsoberfläche . . . 119
5.3.1.1 Bauteilpräsentation und Transformationen . . . 120
5.3.2 Repräsentation der Transformationsmatrix . . . 125
5.3.3 Generierung der Fertigungsattribute . . . 125
5.3.4 Bauteilimport und Export . . . 126
5.3.5 Segmentgenerierung und Randomisierung . . . 127
5.3.6 Umsetzung der kryptografischen Funktionen mit der SIAMCrypto-Klasse 128
5.4 Datenaustauschformat SIAM-XML . . . 132
5.4.1 Authentisierung der Fertigungsdatensätze . . . 134
5.5 Autorisierungsinstanz . . . 135
5.5.1 Hochladen von Teilschlüsseln . . . 135
5.5.2 Abruf von Teilschlüsseln . . . 136
5.5.3 Widerruf von Teilschlüsseln . . . 137
5.5.4 Schutz der Schlüsselübertragung . . . 138
5.5.5 Implementierung der Datenbank . . . 138
5.6 Prozesssimulation . . . 139
5.7 SIAM-Maschinensteuerung . . . 143
5.7.1 Desktop-FDM-Maschine . . . 144
5.7.2 Eingebettete Maschinensteuerung . . . 145
5.7.3 Hardwarearchitektur . . . 145
5.7.4 Software . . . 147
5.8 Maschinenzertifizierung . . . 148
5.8.1 Prüfbauteil . . . 150
5.9 Fazit zur Implementierung . . . 150

6 Verifikation und Validierung **153**
6.1 Methodik zur Verifikation und Validierung . . . 153
6.2 Beispielbauteile . . . 154
6.3 Testfall . . . 157
6.4 Bewertung der Sicherheit . . . 159
6.4.1 Statistische Güte der SIAM-Datensätze . . . 159

6.4.2 Kryptografische Sicherheit 163
6.4.2.1 Sicherheit der Nutzdaten 163
6.4.2.2 Sicherheit der Segmentzuordnung 164
6.4.2.3 Sicherheit der Schlüsselverteilung 164
6.4.3 Angriffsvektoren im SIAM-System 165
6.5 Bewertung der Datenbeschreibung und Funktionalitäten 167
6.6 Bewertung der Leistung 169
6.6.1 Produktivitätsverlust im In-Prozess 169
6.6.2 Verbindungslatenz 173
6.6.3 Skalierbarkeit 174
6.6.3.1 Speicherbedarf 174
6.6.3.2 Rechenaufwand 176
6.7 Validierung 177
6.8 Fazit 180

7 Ausblick **183**

8 Zusammenfassung **185**

Literaturverzeichnis **187**

A Verwendete Schlüssel **199**

B Beispiel für einen SIAM-XML-Datensatz **201**

C Elektronische Schaltung der SIAM-Steuerung **203**