

# HANSER



## Leseprobe

zu

## Authentifizierung und Autorisierung in der IT

von Andreas Lehmann, Mark Lubkowitz und Bernd  
Rehwaldt

Print-ISBN: 978-3-446-47949-4

E-Book-ISBN: 978-3-446-48000-1

E-Pub-ISBN: 978-3-446-48001-8

Weitere Informationen und Bestellungen unter

<https://www.hanser-kundencenter.de/fachbuch/artikel/9783446479494>

sowie im Buchhandel

© Carl Hanser Verlag, München

# Inhalt

<b>Vorwort</b> .....	<b>VII</b>
<b>1 Ressourcen schützen</b> .....	<b>1</b>
1.1 Rollenkonzepte .....	2
1.2 Lokale Authentifizierung .....	5
1.3 Zentrale Authentifizierung .....	6
1.4 Föderierte Authentifizierung .....	7
1.5 Prinzipien der Authentifizierung .....	8
1.6 Standards der Authentifizierung .....	9
1.7 Dezentrale Authentifizierung .....	10
<b>2 Anwendungsfälle</b> .....	<b>13</b>
2.1 Vertrauenswürdiger Client .....	14
2.2 Single Page Application .....	15
2.3 Anwenderdetails .....	17
2.4 Interne Vertrauensstellung .....	18
2.5 Ressourcenzugriff .....	20
2.6 Föderierte Authentifizierung .....	21
2.7 Föderierte Identität .....	23
2.8 Service-Kommunikation .....	24
2.9 Zusammenfassung .....	25

<b>3</b>	<b>OpenID</b> .....	<b>27</b>
3.1	OpenID-Rollen .....	28
3.2	URL-basierte Identität .....	29
3.3	Normalisierung .....	29
3.4	Discovery und Delegated Identity .....	30
3.5	Shared Secret und Association herstellen .....	32
3.6	Requesting Authentication .....	34
3.7	Autorisierung zusichern .....	36
3.8	Verifying Assertions .....	36
3.9	Extensions und Simple Registration .....	37
3.10	Einsatzgebiete für OpenID .....	38
3.11	Der OpenID-Authentifizierungsprozess in der Übersicht .....	39
<b>4</b>	<b>OAuth 2.0</b> .....	<b>41</b>
4.1	OAuth-Rollen .....	43
4.2	Der OAuth-Berechtigungsprozess „Authorization Code Grant“ .....	44
4.3	Überprüfen der Token durch den Resource Server .....	46
4.4	Identifizier .....	47
4.5	OAuth Grants (Flows) .....	48
4.6	OAuth-Einsatzgebiete .....	51
4.7	Beispielimplementierung für Java .....	53
<b>5</b>	<b>OpenID Connect</b> .....	<b>55</b>
<b>6</b>	<b>JSON Web Token</b> .....	<b>59</b>
6.1	Struktur .....	60
6.2	Claims .....	61
6.3	Einsatzgebiete .....	62
<b>7</b>	<b>UMA</b> .....	<b>63</b>
7.1	Rollen .....	64
7.2	Relevante Konzepte .....	65
7.3	Verwalten und schützen, kontrollieren und autorisieren .....	67
7.4	Möglicher Flow .....	68

<b>8</b>	<b>SAML</b> .....	<b>71</b>
8.1	SAML-Rollen.....	72
8.2	SAML Assertions.....	74
8.3	Channel Exchanges.....	74
8.4	Web Single-Sign-on.....	76
8.5	Primary Flows.....	78
8.6	Einsatzgebiete für SAML.....	78
<b>9</b>	<b>XACML</b> .....	<b>79</b>
<b>10</b>	<b>Policy Enforcement</b> .....	<b>81</b>
10.1	Endpoint Interceptor.....	82
10.2	Container Plugin.....	83
10.3	Gateway.....	84
10.4	Entscheidungshilfe.....	85
<b>11</b>	<b>Hashfunktionen</b> .....	<b>87</b>
11.1	In Deutschland einsetzbare Hashfunktionen.....	88
11.2	Salts.....	90
11.3	Work Factors.....	91
<b>12</b>	<b>Asymmetrische Verschlüsselung</b> .....	<b>93</b>
12.1	Einsetzbare, asymmetrische Verschlüsselungsfunktionen.....	94
12.2	Identitäten und Zertifikate.....	95
12.3	Technische Handhabung.....	96
<b>13</b>	<b>Abschließender Vergleich</b> .....	<b>97</b>
	<b>Stichwortverzeichnis</b> .....	<b>101</b>

# Vorwort

*The world's most valuable resource is no longer oil, but data.*

Economist, 2017

„The world's most valuable resource is no longer oil, but data“ ist die Titelzeile des Economist aus dem Jahr 2017. Sie hat sich mittlerweile zu „Data is the new oil“ weiterentwickelt. Adressierte der Economist mit ihr ursprünglich das Monopol der dominierenden Firmen im Digitalmarkt, wird sie heute meist verwendet, um die Wertigkeit und das Potenzial von Daten hervorzuheben. Die Existenz einiger der weltweit wirtschaftskräftigsten Unternehmen basiert rein auf Daten. Allgemeiner gesagt: Daten sind heute längst einer der wichtigsten Rohstoffe jedes Unternehmens.

Dieser Rohstoff ist wertvoll.

Dieser Rohstoff ist schutzwürdig.

Dieser Rohstoff benötigt besondere Behandlung.

Der Verlust oder die Veröffentlichung von vertraulichen Daten kann einerseits erheblichen Schaden für ein Unternehmen verursachen. Umfassen diese Daten andererseits personenbezogene Informationen, dann folgen auch strafrechtliche Konsequenzen mit teils empfindlichen Geldstrafen.

Lagerten Werte früher häufig in Tresoren, werden sie heute beinahe ausschließlich in IT-Systemen aufbewahrt. Ein Tresor schützt seinen Inhalt etwa durch Wissen in Form einer Zahlenkombination, Besitz in Form eines Schlüssels oder beides. Wer die Zahlenkombination kennt oder den Schlüssel besitzt, konnte sich autorisieren und auf den Inhalt des Tresors zugreifen. Eine Authentifizierung, also wer den Tresor öffnet, war nicht nötig.

Anders sieht es bei IT-Systemen aus. Um in IT-Systemen verarbeitete Daten angemessen zu schützen, müssen drei Ziele erreicht werden: Vertraulichkeit, Integrität, Verfügbarkeit.

- **Vertraulichkeit:** Die Daten sind nur den Personen und Systemen zugänglich, die diese zur Erfüllung ihrer jeweiligen Tätigkeit benötigen.
- **Integrität:** Die Daten sind inhaltlich korrekt und Änderungen nachvollziehbar.
- **Verfügbarkeit:** Die Daten sind gegen Löschen und sonstigen Verlust des Zugriffs gesichert.

Erreichen lassen sich diese drei Ziele, indem sich jede zugreifende Person und jedes zugreifende System authentifizieren und autorisieren müssen.

Welche Maßnahmen zum Schutz von Daten dafür heutzutage in Frage kommen und was es dabei zu beachten gilt, das ist Inhalt dieses Buches.

*München, Januar 2024*

*Andreas Lehmann, Mark Lubkowitz, Bernd Rehwaldt*

# 2

## Anwendungsfälle

*As we've come to realize, the idea that security starts and ends with the purchase of a prepackaged firewall is simply misguided.*

Art Wittmann

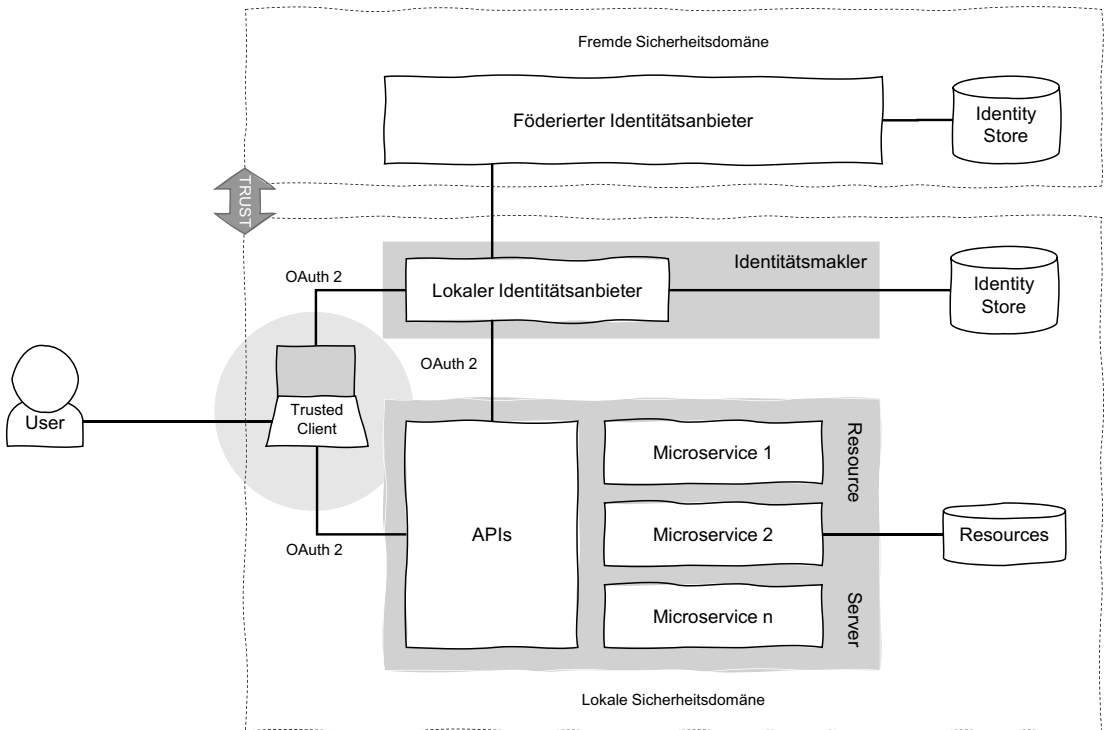
Warum Authentifizierung und Autorisierung in der IT heute ein entscheidender Faktor sind, lässt sich kurz und knapp mit dem hohen Geschäftswert von Daten beantworten. Außerdem mit dem Umstand, dass IT-Systeme im täglichen Geschäftsbetrieb unverzichtbar sind.

Offen ist die Frage: Wann sind Authentifizierung und Autorisierung relevant?

Die kurze und knappe Antwort: Jedes Mal, wenn der Zugriff auf Daten und Systeme erfolgen soll. Diese Situationen lassen sich in acht verschiedene Anwendungsfälle unterscheiden. Bei einigen Anwendungsfällen scheinen die Unterschiede eher geringfügig zu sein und fallen im ersten Moment nicht auf. Bei anderen ist der Unterschied sofort ersichtlich.

Die nachfolgenden Anwendungsfälle beschreiben daher stets eine eindeutige Ausgangssituation. Dazu gehört etwa, ob ein Anwender mit einem vertrauenswürdigen Client oder einem nicht-vertrauenswürdigen Client zugreifen möchte, ob der Anwender Informationen teilen oder auf Ressourcen zugreifen möchte, ob sich der Anwender mit einem allgemeinen Profil oder einem speziellen Profil authentifizieren möchte und Ähnliches.

## 2.1 Vertrauenswürdiger Client



**Bild 2.1** Vertrauenswürdiger Client: Der Anwender greift mit einem vertrauenswürdigen Client zu.

Einer der am häufigsten anzutreffenden Anwendungsfälle ist der Zugriff eines Anwenders mit einem vertrauenswürdigen Client. Dieser ist im Unternehmenskontext alltäglich. Bild 2.1 stellt diesen Anwendungsfall in der Übersicht dar.

Der Ausgangspunkt ist, dass der Anwender auf ihm gehörende oder ihm zugeordnete Ressourcen zugreifen möchte und dafür einen vertrauenswürdigen Client nutzt. Dieser Client gehört zur lokalen Sicherheitsdomäne, etwa eines Unternehmens.

Die Ressource selbst wird durch einen Microservice bereitgestellt, der wiederum durch eine API abgesichert ist. Auch die API ist geschützt respektive der Zugriff auf die API. Hierfür kommt ein lokaler Identitätsanbieter zum Einsatz. Der Zugriff auf die Ressource erfolgt also nicht direkt, sondern über mehrere Zwischenschritte, die die Sicherheitsrichtlinien umsetzen. Der Resource Server, der den Zugriff auf die Ressource schützt, prüft dann per OAuth Introspection das Token beim Identitätsanbieter auf Gültigkeit.

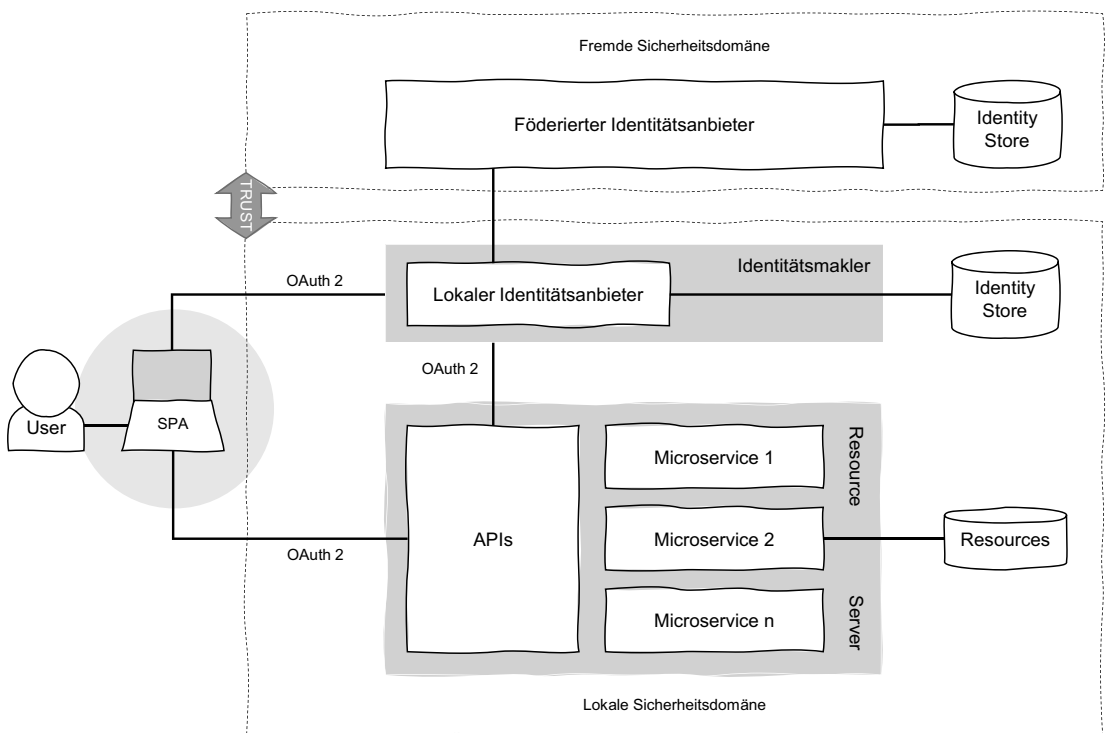


Mit OAuth, siehe Abschnitt 4.5, lässt sich dieser Anwendungsfall hervorragend absichern. Dabei bieten sich gleich drei verschiedene Grant Types an:

- *Authorization Code Grant Type*, beschrieben in Abschnitt 4.5
- *Resource Owner Credentials Grant Type*, beschrieben in Abschnitt 4.5
- *Client Credentials Grant Type*, beschrieben in Abschnitt 4.5

Das Bild 2.1 zeigt auch eine fremde Sicherheitsdomäne, die aber nicht in jedem Anwendungsfall vorkommen muss. Der Identitätsmakler dient in diesem Fall dazu, zwischen Identitätsanbietern einer lokalen und einer fremden Sicherheitsdomäne zu vermitteln. Wichtig ist dabei, dass zwischen der lokalen und der fremden Sicherheitsdomäne eine Vertrauensbeziehung bestehen muss.

## 2.2 Single Page Application



**Bild 2.2** Single Page Applications: SPAs gelten generell als nichtvertrauenswürdige Clients. Grund ist, dass sich Code und Speicherbereich meist problemlos einsehen lassen.

# Stichwortverzeichnis

## A

Access Management 4  
Access Token 37, 47  
Asserting Party 72  
Assertions 37  
– SAML 74  
– Security 71  
Association 34  
Association Session Request 33  
Association Session Response 33  
Asymmetrische Verschlüsselung 8  
Attribute Statement 74  
Authentication Statement 74  
Authentifizierung 10  
– fördert 7  
– verteilt 10  
Authentifizierungsschicht 57  
Authentisierung 11  
Authorization Code 47  
Authorization Code Grant Type 44, 48  
Authorization Decision Statement 74  
Authorization-Header-Field 60  
Authorization Server 43, 64  
Autorisierung 10  
Autorisierungsfluss 48

## B

Bcrypt 92  
Biometrie 4  
BSI 88

## C

Channel Exchanges 74  
– Back-Channel 75  
– Front-Channel 75  
Claims 61, 66  
– private 61  
– public 61  
– registered 61  
Claims Pushing 66  
Claim Token 66  
Client  
– nichtvertrauenswürdig 16  
– vertrauenswürdig 14  
Client Credentials Grant Type 49  
Client ID 47  
Cookie-Header-Field 60

## D

Delegated Identity Host 31  
Diffie-Hellman-Schlüsselaustausch 32  
Discovery 30, 31  
Distinguished Names 22

**E**

Elliptic-Curve Cryptography 94  
 Endpoint Interceptor 82  
 Extensible Access Control Markup  
 Language 79  
 Extensible Resource Descriptor  
 Sequence 31  
 Extensible Resource Identifier 29  
 Extensions 37

**F**

federated authentication 7  
 Federated Authorization 67  
 Flows 44, 48, 51  
 Föderierte Authentifizierung 21  
 Föderierte Identität 23

**G**

Grant Types 48

**H**

Hashfunktion 8, 87  
 Hashwert 87

**I**

IAM 4  
 Identitätsmerkmal 4  
 Identity and Access Management 4  
 Identity Provider 6  
 ID-Token 37  
 Implicit Grant Type 48  
 Integrität X  
 Interactive Claims Gathering 66

**J**

JSON Web Token 56, 59  
 JWT 59, 100

**K**

Keccak 89

Keystore 96

**L**

LDAP 22  
 Lightweight Directory Access  
 Protocol 22

**M**

Man in the Middle 50  
 Mehr-Faktor-Authentifizierung 4  
 Merkle-Damgård-Konstruktion 89

**N**

Normalisierung 29

**O**

OAuth 11, 41, 98  
 OAuth 2.0 41  
 OAuthLib 52  
 öffentlicher Schlüssel 93  
 OIDC 55  
 OpenID 11, 27, 98  
 OpenID 2.0 36  
 OpenID Connect 11, 55, 98  
 OpenID Connect-Provider 56  
 OpenID-Profil 38  
 OpenID-Provider 27, 28  
 OpenID Simple Registration 37

**P**

PAT 68  
 Payload 60  
 Permission Ticket 65  
 Persisted Claims Token 66  
 PKCE 50  
 PKI 95  
 Policy Enforcement 81  
 – Container 83  
 – Gateway 84  
 Prinzipal 24  
 privater Schlüssel 93, 95  
 Profilaustausch 37

Proof Key for Code Exchange 50  
Protection API 66  
Protection API Access Token 68  
Public-Key-Infrastruktur 95

## R

Rainbow Tables 90  
Realm 36  
Refresh Token 37, 48  
Refresh Token Grant Type 49  
Relying Party 27, 28  
Requesting Party 64  
Requesting Party Token 65, 68  
Resource Owner 43, 64  
Resource Owner Credentials Grant  
Type 49  
Resource Server 43, 64  
Ressourcen 1  
Ressourcengruppen 2  
Ressourcenschutz 3  
Richtliniendurchsetzung 82  
Rollenkonzepte 2  
RPT 68

## S

Salt 90  
SAML 71, 99  
SAML Assertion 81  
SAML Binding 75  
Schutzklassen 2  
Scope 43, 67  
Script 92  
Secure Hash Algorithm 89  
Security Assertion Markup Language 71  
Service Provider 72  
SHA-2 88  
SHA-3 88  
shared secret 32  
Sicherheitsdomäne 6  
Signatur 93  
Simple Registration 37  
Single Page Application 16  
Single-Sign-on 6

– Identity Provider initiated 78  
– Service Provider initiated 78  
– Web 76  
Sponge-Konstruktion 90  
SSO 6  
System Internal 46

## T

Token 42  
– self-encoded 47  
– signiert 47  
Token Introspection 46

## U

UMA 11, 63, 99  
UMA 2.0 67  
Uniform Resource Locators 29  
User-Managed Access 11, 63

## V

Verfügbarkeit X  
Verschlüsselung  
– asymmetrische 93  
– symmetrische 93  
Vertrauensverhältnis 42  
Vertraulichkeit X

## W

Wildcard 36  
Work Factor 92

## X

XACML 79, 99  
XRDS 31  
XRI 29

## Y

Yadis 32  
Yadis Resource Descriptor 32