



Andreas LEHMANN
Mark LUBKOWITZ
Bernd REHWALDT

Authentifizierung und Autorisierung in der IT

Grundlagen und Konzepte

HANSER

•msg

Lehmann/Lubkowitz/Rehwaldt
**Authentifizierung und Autorisierung
in der IT**



Blieben Sie auf dem Laufenden!

Unser **Computerbuch-Newsletter** informiert Sie monatlich über neue Bücher und Termine. Profitieren Sie auch von Gewinnspielen und exklusiven Leseproben. Gleich anmelden unter:

www.hanser-fachbuch.de/newsletter



Andreas Lehmann
Mark Lubkowitz
Bernd Rehwaldt

Authentifizierung und Autorisierung in der IT

Grundlagen und Konzepte

HANSER

Alle in diesem Werk enthaltenen Informationen, Verfahren und Darstellungen wurden nach bestem Wissen zusammengestellt und mit Sorgfalt getestet. Dennoch sind Fehler nicht ganz auszuschließen. Aus diesem Grund sind die im vorliegenden Werk enthaltenen Informationen mit keiner Verpflichtung oder Garantie irgendeiner Art verbunden. Autoren und Verlag übernehmen infolgedessen keine juristische Verantwortung und werden keine daraus folgende oder sonstige Haftung übernehmen, die auf irgendeine Art aus der Benutzung dieser Informationen – oder Teilen davon – entsteht. Ebenso wenig übernehmen Autoren und Verlag die Gewähr dafür, dass die beschriebenen Verfahren usw. frei von Schutzrechten Dritter sind. Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt also auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Die endgültige Entscheidung über die Eignung der Informationen für die vorgesehene Verwendung in einer bestimmten Anwendung liegt in der alleinigen Verantwortung des Nutzers.

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

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.

Dieses Werk ist urheberrechtlich geschützt.

Alle Rechte, auch die der Übersetzung, des Nachdruckes und der Vervielfältigung des Buches, oder Teilen daraus, vorbehalten. Kein Teil des Werkes darf ohne schriftliche Genehmigung des Verlages in irgendeiner Form (Fotokopie, Mikrofilm oder ein anderes Verfahren) – auch nicht für Zwecke der Unterrichtsgestaltung – mit Ausnahme der in den §§ 53, 54 URG genannten Sonderfälle –, reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

© 2024 Carl Hanser Verlag München, www.hanser-fachbuch.de

Lektorat: Brigitte Bauer-Schiewek

Copy editing: Petra Kienle, Fürstenfeldbruck

Umschlagdesign: Marc Müller-Bremer, München, www.rebranding.de

Umschlagrealisation: Max Kostopoulos

Titelmotiv: © stock.adobe.com/tomozina1

Druck und Bindung: Hubert & Co. GmbH & Co. KG BuchPartner, Göttingen

Printed in Germany

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

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

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

Inhalt

Vorwort	VII
1 Ressourcen schützen	1
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
2 Anwendungsfälle	13
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

3	OpenID	27
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
4	OAuth 2.0	41
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
5	OpenID Connect	55
6	JSON Web Token	59
6.1	Struktur	60
6.2	Claims	61
6.3	Einsatzgebiete	62
7	UMA	63
7.1	Rollen	64
7.2	Relevante Konzepte	65
7.3	Verwalten und schützen, kontrollieren und autorisieren	67
7.4	Möglicher Flow	68

8	SAML	71
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
9	XACML	79
10	Policy Enforcement	81
10.1	Endpoint Interceptor.....	82
10.2	Container Plugin.....	83
10.3	Gateway.....	84
10.4	Entscheidungshilfe.....	85
11	Hashfunktionen	87
11.1	In Deutschland einsetzbare Hashfunktionen.....	88
11.2	Salts.....	90
11.3	Work Factors.....	91
12	Asymmetrische Verschlüsselung	93
12.1	Einsetzbare, asymmetrische Verschlüsselungsfunktionen.....	94
12.2	Identitäten und Zertifikate.....	95
12.3	Technische Handhabung.....	96
13	Abschließender Vergleich	97
	Stichwortverzeichnis	101

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