FAPI Angreifer-Modell für den Schutzbedarf Hoch und Sehr hoch

> 👎 👍 → Feedback und Anmerkungen zu diesem Dokument geben

Zusammenfassung

Das vorliegende Dokument beschreibt das Angreifer-Modell, das die Entscheidungen über die von den FAPI-Sicherheitsprofilen verwendeten Sicherheitsmechanismen beeinflusst. Es ist vor allem für den Schutzbedarf Hoch und Sehr hoch relevant und wurde auf Basis des "FAPI Attacker Models" [attackermodel] Dokuments der OpenID Foundation (OIDF) erstellt.

Einleitung

In diesem vorliegenden Begleitdokument werden die Sicherheitsanforderungen anhand von Sicherheitszielen und Angreifer-Modellen dargestellt. Aus diesen Anforderungen leiten sich die im Schutzbedarf Hoch und Sehr hoch verwendeten Sicherheitsmechanismen ab, abgeleitet aus "FAPI Attacker Models" [attackermodel].

Entwickler und Nutzer können dem vorliegenden Dokument entnehmen, welche Bedrohungen vom Sicherheitsprofil berücksichtigt wurden und welche außerhalb des Anwendungsbereichs des Sicherheitsprofils liegen.

Eine systematische Definition der Sicherheitsanforderungen und ein Angreifer-Modell ermöglichen Nachweise der Sicherheit des FAPI 2.0-Sicherheitsprofils, ähnlich den Nachweisen in [arXiv.1901.11520] für FAPI 1.0, auf die sich diese Arbeit stützt. Formale Nachweise können große Klassen von Angriffen ausschließen, die in der Logik von Sicherheitsprotokollen begründet sind.

Die formale Analyse dieses Angreifer-Modells und des FAPI 2.0-Sicherheitsprofils, die in Kapitel 9 beschrieben wird, hat dazu beigetragen, dieses Dokument und das FAPI 2.0-Sicherheitsprofil zu verfeinern und zu verbessern.

Es wird empfohlen das vorliegende Dokument zu nutzen, um die Umsetzung von Anforderungen besser zu bewerten und die IT-Sicherheit von API-Absicherungen weiter zu erhöhen.

Schlüsselwörter

Die Schlüsselwörter „MUSS“ (DARF NUR), „DARF NICHT“, „SOLLTE“, „SOLLTE NICHT“, „DARF“ und „KANN“ in diesem Dokument sind gemäß DIN-Norm DIN 820-2 - 2022-12 [DIN 820-2] zu interpretieren. Diese Schlüsselwörter werden nicht als Wörterbuchbegriffe verwendet, sodass jedes Vorkommen als Schlüsselwort zu interpretieren ist und nicht mit ihrer natürlichen Sprachbedeutung.

1. Geltungsbereich

Dieses Dokument beschreibt die Sicherheitsziele, das Angreifer-Modell, die Rollen und Fähigkeiten von Angreifern sowie die Einschränkungen der FAPI 2.0-Profile.

2. Normative Verweise

Auf die folgenden Dokumente wird im Text in einer Weise verwiesen, dass ihr Inhalt ganz oder teilweise Anforderungen dieses Dokuments darstellen. Bei datierten Verweisen gilt nur die zitierte Ausgabe. Bei undatierten Verweisen gilt die neueste Ausgabe des referenzierten Dokuments (einschließlich aller Änderungen).

Normative Verweise sind in Kapitel 10. Informative Referenzen sind in Kapitel 11.

3. Begriffe und Definitionen

Für die Zwecke dieses Dokuments gelten die in [RFC6749] und [OIDC] definierten Begriffe. Zum besseren Verständnis werden im vorliegenden Dokument OAuth und OpenID Connect spezifische technische Begriffe in ihrem englischen Terminus verwendet.

4. Symbole und Abkürzungen

API – Application Programming Interface

CSRF – Cross-Site Request Forgery

DNS – Domain Name System

JWKS – JSON Web Key Set

URL – Uniform Resource Locator

5. Sicherheitsziele

5.1. Allgemeines

Im Folgenden werden die Sicherheitsziele für das FAPI 2.0-Sicherheitsprofil in Bezug auf die Autorisierung und, bei Verwendung von OpenID Connect, die Authentifizierung definiert.

5.2. Autorisierung

Das FAPI 2.0-Sicherheitsprofil soll sicherstellen, dass **kein Angreifer auf andere geschützte Ressourcen** als seine eigenen zugreifen kann.

Das Access Token ist die ultimative Berechtigung für den Zugriff auf Ressourcen in OAuth. Dieses Sicherheitsziel ist daher erreicht, wenn kein Angreifer erfolgreich ein Access Token für den Zugriff auf andere geschützte Ressourcen als seine eigenen erhalten und verwenden kann.

5.3. Authentifizierung

Das FAPI 2.0-Sicherheitsprofil soll sicherstellen, dass **kein Angreifer sich unter der Identität eines anderen Benutzers bei einem Client anmelden kann**.

Das ID-Token ist die Berechtigung für die Authentifizierung in OpenID Connect. Dieses Sicherheitsziel ist daher erreicht, wenn kein Angreifer ein ID-Token erhalten und verwenden kann, das einen anderen Benutzer für die Anmeldung identifiziert.

5.4. Sitzungsintegrität

Die Sitzungsintegrität befasst sich mit Angriffen, bei denen ein Benutzer dazu verleitet wird, sich unter der Identität des Angreifers anzumelden oder versehentlich die Ressourcen des Angreifers anstelle der eigenen Ressourcen zu nutzen. Zu den Angriffen in diesem Bereich gehören CSRF-Angriffe (die traditionell durch die Verwendung von „state" in OAuth abgewehrt werden) und Sitzungsaustausch-Angriffe.

Im Einzelnen:

- Für die Authentifizierung: Das FAPI 2.0-Sicherheitsprofil soll sicherstellen, dass **kein Angreifer einen Benutzer dazu zwingen kann, sich unter der Identität des Angreifers anzumelden**.
- Für die Autorisierung: Das FAPI 2.0-Sicherheitsprofil soll sicherstellen, dass **kein Angreifer einen Benutzer dazu zwingen kann, die Ressourcen des Angreifers zu nutzen**.

6. Angreifer-Modell

Dieses Angreifer-Modell definiert sehr weitreichende Fähigkeiten für Angreifer. Es wird davon ausgegangen, dass Angreifer diese Fähigkeiten ausnutzen werden, um Angriffe auf die oben definierten Sicherheitsziele zu entwickeln. Um ein sehr hohes Maß an Sicherheit zu gewährleisten, wird davon ausgegangen, dass Angreifer sehr mächtig sind und unter anderem Zugriff auf ansonsten verschlüsselte Kommunikation haben.

Dieses Modell definiert bewusst keine konkreten Bedrohungen. Ein Angreifer, der beispielsweise in der Lage ist, eine Autorisierungsanfrage abzuhören, könnte diese Fähigkeit für verschiedene Arten von Angriffen nutzen, die unterschiedliche Bedrohungen darstellen, z. B. das Einfügen einer geänderten Autorisierungsanfrage. In einem komplexen Protokoll wie OAuth oder OpenID Connect können jedoch, wie in der Vergangenheit gezeigt wurde, noch unbekannte Arten von Bedrohungen und Varianten bestehender Bedrohungen auftreten. Um keine potenziellen Angriffe zu übersehen, zielt FAPI 2.0 daher nicht darauf ab, konkrete, eng gefasste Bedrohungen zu behandeln, sondern alle Angriffe auszuschließen, die für die hier aufgeführten Angreifer-Typen denkbar sind. Dies wird durch eine formale Sicherheitsanalyse unterstützt, siehe Kapitel 9.

Dieses Angreifer-Modell geht davon aus, dass bestimmte Teile der Infrastruktur und Protokolle korrekt funktionieren. Ausfälle in diesen Teilen führen wahrscheinlich zu Angriffen, die außerhalb des Geltungsbereichs dieses Angreifer-Modells liegen. Diese Bereiche müssen im Rahmen einer Anwendung der FAPI 2.0-Sicherheitsprofile unter Verwendung von Bedrohungsmodellen oder anderen Techniken separat analysiert werden.

Wenn beispielsweise eine schwerwiegende Schwachstelle in TLS gefunden würde, die die Datenintegrität in TLS-Verbindungen untergräbt, könnte ein Netzwerkangreifer (A2, siehe unten) praktisch alle OAuth- und OpenID Connect-Sitzungen auf verschiedene Weise kompromittieren. Dies wäre fatal, da selbst die Signierung und Verschlüsselung auf Anwendungsebene auf der Schlüsselverteilung über TLS-Verbindungen basiert. Ein weiteres Beispiel: Wenn ein menschlicher Fehler zur Offenlegung geheimer Schlüssel für die Authentifizierung führt und ein Angreifer diese Anmeldedaten missbrauchen könnte, würde dieser Angriff nicht von diesem Angreifer-Modell abgedeckt sein.

Die folgenden Teile der Infrastruktur fallen nicht in den Geltungsbereich dieses Angreifer-Modells:

- **TLS**: Es wird davon ausgegangen, dass TLS-Verbindungen nicht kompromittiert werden, d. h. Datenintegrität und Vertraulichkeit sind gewährleistet. Zum Aufbau von Verbindungen werden die richtigen öffentlichen Schlüssel verwendet, und private Schlüssel sind Angreifern nicht bekannt (mit Ausnahme von explizit kompromittierten Parteien).
- **JWKS**: Bei Verwendung funktionieren Schlüsselverteilungsmechanismen wie vorgesehen, d. h., Verschlüsselungs- und Signaturprüfschlüssel von nicht kompromittierten Parteien werden von den richtigen Endpunkten abgerufen.
- **Browser und Endpunkte**: Von Ressourcenbesitzern verwendete Geräte und Browser gelten als nicht kompromittiert. Andere Endpunkte, die nicht von einem Angreifer kontrolliert werden, verhalten sich gemäß dem Protokoll.
- **Identitäts- und Sitzungsmanagement**: Die Identitätsprüfung, Authentifizierung, Identitäts- und Zugriffsverwaltung des Endbenutzers auf einem Client oder Authorization Server fallen nicht in den Geltungsbereich dieser Spezifikation. Es wird davon ausgegangen, dass Clients sicherstellen, dass die Sitzungen verschiedener Benutzer ordnungsgemäß voneinander und vor Angreifern geschützt sind. Clients, die Identitätsattribute mit OpenID Connect abrufen, müssen überprüfen, ob die zurückgegebenen Identitätsattribute ihren Anforderungen entsprechen.

7. Angreifer

7.1. Allgemeines

FAPI 2.0-Profile zielen darauf ab, die oben aufgeführten Sicherheitsziele für beliebige Kombinationen der folgenden Angreifer zu gewährleisten, die möglicherweise zusammenarbeiten, um ein gemeinsames Ziel zu erreichen:

7.2. A1 – Web-Angreifer

Dies ist das Standardmodell für Web-Angreifer. Der Angreifer:

- kann wie jede andere Partei, die einen oder mehrere Endpunkte im Internet kontrolliert, Nachrichten senden und empfangen,
- kann als normaler Benutzer an Protokollflüssen teilnehmen,
- kann beliebige Tools (z. B. Browser-Entwicklertools, benutzerdefinierte Software, lokale Abfang-Proxys) auf seinen eigenen Endpunkten verwenden, um Nachrichten zu manipulieren und neue Nachrichten zusammenzustellen,
- kann Links an ehrliche Benutzer senden, die dann von diesen Benutzern aufgerufen werden.

Das bedeutet, dass der Web-Angreifer in der Lage ist, beliebige Anfragen von den Browsern der Benutzer auszulösen, sofern ihm deren Inhalt bekannt ist.

Der Angreifer kann keine zwischen anderen Parteien gesendeten Nachrichten abfangen oder blockieren und keine Verschlüsselung brechen, es sei denn, er hat die entsprechenden Entschlüsselungsschlüssel in Erfahrung gebracht. Abweichend vom üblichen Web-Angreifer-Modell kann A1 nicht die Rolle eines legitimen Authorization Servers im Ökosystem übernehmen (siehe A1a).

7.3. A1a – Web-Angreifer (als Authorization Server teilnehmend)

Dies ist eine Variante des Web-Angreifers A1, aber dieser Angreifer kann auch als Authorization Server am Ökosystem teilnehmen.

Es muss beachtet werden, dass dieser Authorization Server Nachrichten, die er von ehrlichen Authorization Servern erhalten hat, wiederverwenden/wiederholen und Benutzer an Endpunkte ehrlicher Authorization Server weiterleiten kann.

7.4. A2 – Netzwerkangreifer

Dieser Angreifer kontrolliert das gesamte Netzwerk (wie ein betrügerischer WLAN-Zugangspunkt oder ein anderer kompromittierter Netzwerkknoten). Dieser Angreifer kann Nachrichten, die für andere Personen bestimmt sind, abfangen, blockieren und manipulieren, aber die Verschlüsselung nicht knacken, es sei denn, er hat die entsprechenden Entschlüsselungscodes erfahren.

Hinweis: Die meisten Angriffe, die ausschließlich von dieser Art von Angreifer ausgehen, können durch den Einsatz von Transportschichtschutz wie TLS abgewehrt werden.

7.5. Angreifer am Autorisierungsendpunkt: A3a – Autorisierungsanfrage lesen

Es wird davon ausgegangen, dass dieser Angreifer über die Fähigkeiten des Web-Angreifers verfügt, aber zusätzlich die Autorisierungsanfrage lesen kann, die im Frontkanal vom Browser eines Benutzers an den Authorization Server gesendet wird.

Dies kann auf mobilen Betriebssystemen (auf denen Apps für URLs registriert werden können), auf allen Betriebssystemen über den Browserverlauf oder aufgrund von Cross-Site-Scripting auf dem Authorization Server geschehen. Es gab Fälle, in denen Antivirensoftware TLS-Verbindungen abgefangen und URLs gespeichert/analysiert hat.

Hinweis: Ein Angreifer, der die Autorisierungsantwort lesen kann, wird hier nicht berücksichtigt, da ein solcher Angreifer mit der aktuellen Browsertechnologie die meisten Sicherheitsprotokolle untergraben kann. Dies wird unter „Browser-Swapping-Angriffe" in den Sicherheitsüberlegungen im FAPI 2.0-Sicherheitsprofil behandelt.

Hinweis: Die Angreifer für die Autorisierungsanfrage sind komplexer als diejenigen für den Token-Endpunkt und den Ressourcen-Endpunkt, da diese Nachrichten die komplexe Umgebung des Browsers/der App/des Betriebssystems des Benutzers mit einer größeren Angriffsfläche durchlaufen. Dies erfordert eine detailliertere Analyse.

Hinweis: Für die Autorisierungs- und Ressourcenendpunkte wird davon ausgegangen, dass der Angreifer Nachrichten nur passiv lesen kann, während für den Token-Endpunkt davon ausgegangen wird, dass der Angreifer Nachrichten auch manipulieren kann. Die zugrunde liegende Annahme ist, dass Lecks aus der Autorisierungsanfrage oder -antwort in der Praxis sehr häufig sind und Lecks aus der Ressourcenanfrage möglich sind, aber eine vollständig kompromittierte Verbindung zu einem der beiden Endpunkte sehr unwahrscheinlich ist. Insbesondere für den Autorisierungsendpunkt würde eine vollständig kompromittierte Verbindung die Sicherheit der meisten umleitungsbasierten Authentifizierungs-/Autorisierungsschemata, einschließlich OAuth, untergraben.

7.6. Angreifer am Token-Endpunkt: A4 – Lesen und Manipulieren von Token-Anfragen und -Antworten

Dieser Angreifer zwingt den Client, einen Token-Endpunkt zu verwenden, der nicht der des vertrauenswürdigen Authorization Servers ist. Dieser Angreifer kann daher Nachrichten lesen und manipulieren, die an diesen Token-Endpunkt gesendet werden und von diesem empfangen werden, den der Client für einen ehrlichen Authorization Server hält.

Wichtig: Dieser Angreifer ist ein Modell für falsch konfigurierte Token-Endpunkt-URLs, die in FAPI 1.0 berücksichtigt wurden. Da das FAPI 2.0-Sicherheitsprofil vorschreibt, dass die Token-Endpunktadresse von einer autoritativen Quelle und über einen geschützten Kanal, d. h. über OAuth-Metadaten, die vom ehrlichen Authorization Server bezogen werden, bezogen wird, ist dieser Angreifer in FAPI 2.0 nicht relevant. Die Beschreibung hier dient nur zu Informationszwecken.

7.7. Angreifer auf dem Ressourcenserver: A5 – Lesezugriff auf Ressourcenanfragen

Dieser Angreifer verfügt über die Fähigkeiten des Web-Angreifers, kann jedoch auch Anfragen lesen, die an den Ressourcenserver gesendet wurden, nachdem sie vom Ressourcenserver verarbeitet wurden, beispielsweise weil der Angreifer TLS-Interception-Proxy-Protokolle auf der Seite des Ressourcenservers lesen kann.

Hinweis: Ein Angreifer, der die Antworten vom Ressourcenserver lesen kann, wird hier nicht berücksichtigt, da ein solcher Angreifer dem oben genannten Autorisierungsziel direkt widersprechen würde. Wenn er die Antworten manipulieren könnte, würde er zusätzlich das Ziel der Sitzungsintegrität auf einfache Weise unterlaufen.

8. Einschränkungen

8.1. Allgemeines

Über die bereits in der Einleitung zum Angreifer-Modell beschriebenen Einschränkungen hinaus sind folgende Einschränkungen zu beachten:

8.2. Protokollschichten

FAPI 2.0-Profile definieren nur das Verhalten der API-Autorisierung und -Authentifizierung auf bestimmten Protokollschichten. Wie oben beschrieben, können Angriffe auf niedrigere Protokollschichten (z. B. TLS) unter bestimmten Bedingungen die Sicherheit von FAPI 2.0-konformen Systemen beeinträchtigen. Das Angreifer-Modell berücksichtigt jedoch einige Brüche in der durch TLS gewährleisteten End-to-End-Sicherheit, indem es bereits die entsprechenden Angreifer-Modelle (A3a/A5/A7) einbezieht. Ebenso werden viele andere Angriffe auf niedrigere Schichten bereits berücksichtigt, zum Beispiel:

- DNS-Spoofing-Angriffe werden durch den Netzwerk-Angreifer (A2) abgedeckt.
- Lecks von Autorisierungsanforderungsdaten, z. B. durch falsch konfigurierte URLs oder System-/Firewall-Protokolle, werden durch (A3a) abgedeckt
- Das Weiterleiten von Benutzern auf bösartige Websites liegt im Rahmen der Möglichkeiten des Web-Angreifers (A1)

FAPI 2.0 zielt darauf ab, sicher zu sein, wenn Angreifer diese Angriffe und alle oben beschriebenen für Angreifer möglichen Angriffe ausnutzen, auch in Kombination.

Andere Angriffe werden vom Angreifer-Modell nicht abgedeckt. Beispielsweise werden die Offenlegung von Benutzeranmeldedaten durch falsch konfigurierte Datenbanken oder Remote-Code-Execution-Angriffe auf Authorization Server durch das Angreifer-Modell weder verhindert noch berücksichtigt. Ein weiteres Beispiel: Wenn ein Benutzer einen kompromittierten Browser und ein kompromittiertes Betriebssystem verwendet, ist es schwierig, die Sicherheit des Benutzers aufrechtzuerhalten. Phishing-resistente Anmeldedaten können in diesem Fall helfen, fallen jedoch, wie im Folgenden beschrieben, nicht in den von FAPI 2.0 definierten Bereich.

8.3. Geheimnisse

Die Sicherheitsbewertung geht davon aus, dass Geheimnisse so erstellt werden, dass Angreifer sie nicht erraten können – z. B. Nonces und geheime Schlüssel. Schwache Zufallszahlengeneratoren können beispielsweise zu Geheimnissen führen, die von Angreifern erraten werden können, und somit zu Schwachstellen.

8.4. Systemgrenzen

Die FAPI 2.0-Profile konzentrieren sich auf Kernaspekte der API-Sicherheit und schreiben beispielsweise keine Endbenutzerauthentifizierungsmechanismen, Firewall-Einrichtungen, Softwareentwicklungspraktiken oder Sicherheitsaspekte interner Architekturen vor. Alles, was außerhalb der Grenzen von FAPI 2.0 liegt, muss im Kontext des Ökosystems, der Bereitstellung oder der Implementierung bewertet werden, in dem bzw. der FAPI 2.0 verwendet wird.

8.5. Implementierungsfehler

API-Sicherheitsprofile definieren, wie Authentifizierung und Autorisierung implementiert werden sollen, und ein formales Modell bewertet, ob die Profile sicher sind und mit idealen Implementierungen übereinstimmen. Reale Implementierungen weichen natürlich manchmal vom spezifizierten und formal analysierten Verhalten ab und enthalten Sicherheitslücken auf verschiedenen Ebenen. Während die FAPI 2.0-Profile so konzipiert sind, dass sie nach Möglichkeit mehrere Verteidigungsebenen bieten, müssen Implementierungen sichere Best Practices für die Softwareentwicklung und -bereitstellung verwenden, um sicherzustellen, dass Schwachstellen entdeckt und behoben werden können.

8.6. Veränderungen im Laufe der Zeit

Neue Technologien oder veränderte Verhaltensweisen von Komponenten (z. B. Browsern) können im Laufe der Zeit zu neuen Sicherheitslücken führen, die zum Zeitpunkt der Entwicklung dieser Spezifikationen möglicherweise noch nicht bekannt waren.

9. Formale Analyse

Das FAPI 2.0-Sicherheitsprofil wird von einer formalen Sicherheitsanalyse [analysis.FAPI2] begleitet, die ein formales Modell des FAPI 2.0-Sicherheitsprofils und einen Nachweis der Sicherheit des FAPI 2.0-Sicherheitsprofils innerhalb dieses Modells liefert. Das formale Modell basiert auf dem in diesem Dokument definierten Angreifer-Modell und den Sicherheitszielen.

Zu beachten ist, dass die Analyse auf einer früheren Version des Angreifer-Modells basiert, in der eine andere Nummerierung für die Angreifer verwendet wurde. Einige der zuvor berücksichtigten Angreifer-Modelle

standen im Widerspruch zu den Sicherheitszielen und wurden daher entfernt. Die Zuordnung zwischen dem Angreifer-Modell in diesem Dokument und dem in der Analyse verwendeten Modell ist wie folgt:

Tabelle 1

Analyse	Dieses Dokument
A1	A1
A1a	A1a
A2	A2
A3a	A3a
A3b	entfernt – siehe Hinweis in Kapitel 7.5
A5	A4
A7	A5 – mit reduzierten Fähigkeiten, siehe Hinweis in Kapitel 7.7
A8	entfernt – siehe Hinweis in Kapitel 7.7

Da die Aktualisierungen des Angreifer-Modells vorgenommen wurden, um es an die formale Analyse anzupassen, sind die Analyseergebnisse für das aktualisierte Angreifer-Modell weiterhin gültig.

10. Normative Verweise

[attackermodel]

Fett, D., "FAPI 2.0 Attacker Model", 18 February 2025, https://openid.net/specs/fapi-attacker-model-2_0-final.html.

[OIDC]

Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., and C. Mortimore, "OpenID Connect Core 1.0 incorporating errata set 1", 8 November 2014, http://openid.net/specs/openid-connect-core-1_0.html.

[RFC6749]

Hardt, D., Ed., "The OAuth 2.0 Authorization Framework", RFC 6749, DOI 10.17487/RFC6749, October 2012, https://www.rfc-editor.org/info/rfc6749.

11. Informative Referenzen

[analysis.FAPI2]

Hosseyni, P., Küsters, R., and T. Würtele, "Formal Security Analysis of the OpenID FAPI 2.0: Accompanying a Standardization Process", 1 October 2022, https://openid.net/wordpress-content/uploads/2022/12/Formal-Security-Analysis-of-FAPI-2.0_FINAL_2022-10.pdf.

[arXiv.1901.11520]

Fett, D., Hosseyni, P., and R. Küsters, "An Extensive Formal Security Analysis of the OpenID Financial-grade API", arXiv 1901.11520, 31 January 2019, http://arxiv.org/abs/1901.11520/.

[DIN 820-2]

Normungsarbeit - Teil 2: Gestaltung von Dokumenten (ISO/IEC Directives - Part 2:2021, modifiziert); Deutsche und Englische Fassung CEN-CENELEC-Geschäftsordnung - Teil 3:2022, https://www.dinmedia.de/de/norm/din-820-2/358748335

Anhang A. Hinweise zu Rechten am Dokument

Das vorliegende Dokument ist ein aus dem FAPI 2.0 Profil abgeleitetes Dokument, weshalb die dafür genannten Copyright Regeln der OpenID Foundation zu beachten sind:

Anhang B. Wesentliche Unterschiede zu FAPI Attacker Model [attackermodel]

Kapitel	FAPI 2.0 Attacker Model	Dieses Dokument	Gründe
Schlüsselwörter		DIN Norm	Deutsch
Allg.	Kapitel 10	nicht enthalten	