

Mobile Devices Payment Protocol (MDPP)

Bezahlungsfunktion für digitale und physische Güter in Mobilfunknetzen

Whitepaper (Stand 09/2007 Änderung oder Irrtum vorbehalten)

Das MDP-Protokoll wurde zur Authentifikation von Kunden in mobilen Datennetzen sowie zur anonymen Nutzung und Abrechnung von Internet-Inhalten entwickelt. Es beruht auf dem Prinzip dezentraler Informationsbereitstellung, zentraler Benutzerauthentifizierung und signierter Nachrichten [Token], welche zwischen einem Diensteanbieter [Content Provider, CP], einem Konsumenten [Mobile User] und einem Mobilfunkbetreiber [Network Operator] ausgetauscht werden.

Die Kommunikation zwischen einem CP und einem MU erfolgt über HTTP.

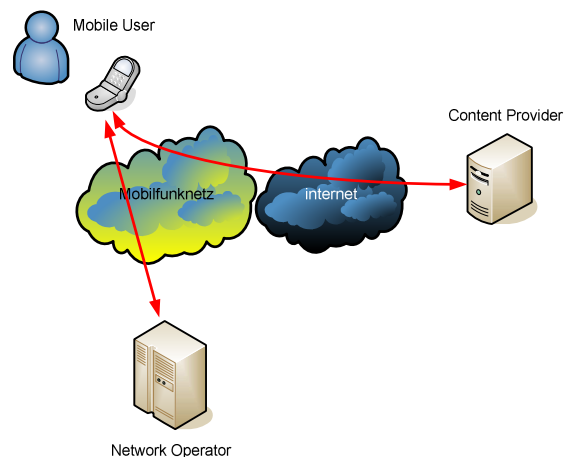
Die Kommunikation zwischen einem MU und einem NO erfolgt ebenfalls über HTTP. Gegebenenfalls kann an dieser Stelle, statt eines HTTP Aufrufes, ein SOAP basierter Webservice genutzt werden. Dieser wird direkt aus einer HTML-Seite, über eine API oder eine Applikation gestartet.

Zur Sicherstellung der Autorisierung von Kundenanfragen wird die Kommunikation zwischen Mobile User, Content Partner und Network Operator um ein "trusted Token" angereichert. Dieses wird vom Network Operator erstellt und digital signiert. Dem CP ist somit die Möglichkeit gegeben, die Authentizität einer Kundenanfrage nachzuprüfen. Des Weiteren dient das "trusted Token" als Grundlage für die Abrechnung.

Das MDP-Protokoll erfordert prinzipiell keine weitere Online Kommunikation zwischen Content Providern und Network Operatoren. Jedoch bleibt es

den Kommunikationspartner unbelassen, übermittelte „trusted Token“, z.B. ab einem definierbaren Betrag online zu verifizieren. Hierfür stehen geeignete Protokolle, z.B. SOAP zur Verfügung. Es werden keine zusätzlichen Kommunikationskomponenten, wie z.B. Gateways oder Access Proxies benötigt.

Die nachfolgende Graphik verdeutlicht die Kommunikationsbeziehungen:



Ein MU kommuniziert mit einem Content Provider über das Internet um freie und / oder kostenpflichtige Dienste zu nutzen. Hierbei wird der Zugang zum Internet über das Mobilfunknetz eines Network Operators gewährleistet.

Zur Autorisierung von kostenpflichtigen Angeboten kommuniziert der Mobile User mit dem Network Operator.

Service Autorisierung

Sobald der MU eine kostenpflichtige Dienstleistung eines Content Providers nutzen möchte, wird der CP diese dem

Kunden mittels einer Autorisierungsanfrage anbieten.

Mobile User Authentisierung

Der NO überprüft vor jeder Dienste Autorisierung die Authentizität des Mobile Users.

Das Autorisierungsobjekt prüft – nach erfolgreicher Authentisierung des MU – die übermittelten Parameter auf Plausibilität. Die übermittelten Informationen werden gegen ein Content Repository abgeglichen. Weiterhin überprüft der NO, ob der MU über ein ausreichendes Guthaben verfügt, um den angeforderten Dienst nutzen zu können.

Content Autorisierungsprozess

Nachdem der MU das Service Angebot akzeptiert hat, wird durch das Autorisierungsobjekt eine digitale Signatur erzeugt und der Datensatz persistent beim NO gespeichert. Der NO erzeugt eine signierte Antwort, welche es dem Content Provider erlaubt, die Authentizität des Kaufvorgangs zu überprüfen und den angebotenen Inhalt an den MU auszuliefern.

Abrechnungsprinzipien

Der Content Provider ist in der Lage, auf Basis der zurück gelieferten Autorisierungsantworten des NO's, Abrechnungslisten zu erstellen und einem Network Operator zuzuordnen.

Weiterhin ist der NO in der Lage, die autorisierten Dienstleistungen mittels der MSISDN einem Kunden zuzuordnen.

Die Grundlage für eine Abrechnung mit einem Content Provider sind die Datensätze des NO.

Sicherheitsbetrachtungen

Man-in-the-Middle

Durch die Nutzung von End2End SSL/TLS Verbindungen kann eine Man-in-the-Middle Attacke wirkungsvoll unterbunden werden.

Replay Angriffe

Durch die temporäre Erzeugung des CP SessionID und die Kopplung der Zugangsinformationen an die SessionID sind Replay Attacken praktisch ausgeschlossen, da nach der erfolgreichen Auslieferung des Contents die Session zerstört wird.

Reproduktion von Tokens

Durch die Verwendung des asynchronen RSA Verfahrens ist dies nur möglich, wenn ein potentieller Angreifer in Besitz des nicht-öffentlichen Schlüssels gelangt. Dieser ist jedoch, wie prinzipiell alle Geheimnisse – für Dritte unzugänglich aufzubewahren.

Identifikation des Benutzers

Eine Identifikation des Benutzers seitens des Content Providers ist nicht möglich, da keinerlei personenbezogenen Informationen, wie z.B. MSISDN oder wiederkehrende Informationen, z.B. XID übertragen werden.

Betrug durch Parameter Manipulation

Durch die erforderliche Registrierung des Content Providers beim Network Operator und die dadurch mögliche Plausibilitätsprüfung der übermittelten Daten, können Manipulationen erkannt und die Authentifizierung abgebrochen

werden. Ein CP erkennt maximal die Zugehörigkeit eines MU zu einem NO.

Betrug durch falsche Token Parameter

Bedingt durch die Tatsache, dass die Content relevanten Informationen seitens des CP vorgehalten werden und nicht an den zu übermittelnden „trusted Token“ geknüpft sind, kann ein CP Manipulationen erkennen und die Content Auslieferung verhindern.

Betrug durch falsche Abrechnungsdaten eines Content Providers

Abrechnungsdaten eines CP werden mit den Autorisierungsdatensätzen des NO verglichen. Falsche Daten können erkannt und aussortiert werden.

Generelle Betrachtung

Durch die dezentrale Datenhaltung und die Möglichkeit übertragene Parameter abzugleichen, sind Manipulationen direkt feststellbar. Weiterhin gewährleistet das RSA Signatur Verfahren eine zuverlässige Verifikation von Autorisierungstoken.

Weiterhin sind Angriffe gegen das Autorisierungssystem des NO als unwahrscheinlich einzustufen, da es nur innerhalb des GPRS/UMTS – Netzwerkes eines NO erreichbar ist und keinen Zugang aus dem Internet besitzt.

Betrügerische Manipulationen gegen das Autorisierungssystem sind immer an eine SIM Karte gebunden. Somit können böswillige Kunden erkannt und blockiert werden. Bei der missbräuchlichen Nutzung von z.B. entwendeten SIM Karten besteht die Möglichkeit der netzseitigen Sperrung.

Schutzrechte

Das MDPP ist in Deutschland patentiert und international zum Patent angemeldet.

Kontakt

open | MVNO
Heiner-Stuhlfauth-Str. 28
90480 Nürnberg

Tel: 0911 / 180 91 05
Fax: 0911 / 180 91 09
Kontakt: info@openMVNO.org
Web: <http://www.openMVNO.org>