

Rich Communication Services als Nachfolger der SMS

David Olbertz
Hochschule Bonn-Rhein-Sieg
Sankt-Augustin, Germany
davidolbertz@gmail.com

Abstract—Der Abstract wurde noch nicht verfasst.

Index Terms—Diese, index, terms, existieren, noch, nicht

I. EINLEITUNG

Heutzutage ist das Smartphone ein wichtiger Bestandteil des Alltags. Es ermöglicht unter anderem die Kommunikation über große Distanzen hinweg, egal ob im privaten oder beruflichen Umfeld.

Zur Kommunikation existiert neben der Telefonie der altbekannte Short Message Service (SMS), welcher es ermöglicht, einfache Kurznachrichten zu versenden. Allerdings wird diese Kommunikationsmethode mittlerweile immer weniger genutzt und wurde größtenteils durch Over-the-Top Instant Messenger, welche deutlich mehr Funktionalitäten bieten, wie z.B. Gruppenchats und das Teilen von Medien. Zusätzlich sind Nachrichten meist Ende-zu-Ende-Verschlüsselt und das Senden ist gebührenfrei [1]. Dieser Trend bewog die GSM Association dazu, einen neuen moderneren Kommunikationsstandard zu entwickeln, welcher ähnliche Funktionen wie die Over-the-Top Instant Messenger bieten. Anders ist, dass es von Mobilfunkbetreibern anstatt von einem großen Unternehmen betrieben wird und dadurch auf fast allen Endgeräten verfügbar ist [2], [3].

Ziel dieser Seminararbeit ist, Rich Communication Services (RCS) als Nachfolger der SMS zu betrachten. Dazu werden zuerst die aktuell gängigen Technologien behandelt und anschließend auf RCS im Detail eingegangen. Neben der Definition und Funktionsweise werden auch weitere Aspekte, wie die Vor- und Nachteile der RCS, dargestellt. Dabei werden auch die Eigenschaften von RCS mit denen von SMS verglichen, wobei besonders in heutigen Zeiten die Sicherheit eine große Rolle spielt.

II. ENTWICKLUNG

A. Short Message Service

Der Short Message Service, kurz SMS, ist seit den späten 1990er Jahren im Einsatz. Dieser erlaubt es Nutzern mittels eines Mobiltelefons kurze Textnachrichten an andere Personen zu verschicken, unabhängig von der Distanz [4].

...

Das Mobilfunknetz besteht aus Basisstationen, mit denen sich die Endgeräte drahtlos verbinden können, und aus Short Message Service Centers (SMSC), welche die versendeten Nachrichten an den korrekten Empfänger weiterleiten.

Während der Übermittlung der Nachricht ist der Bereich zwischen dem Endgerät und der Basisstation verschlüsselt, innerhalb des Mobilfunknetzes allerdings nicht mehr. External Short Message Entities sind ebenfalls Bestandteil des Netzes und werden meist von Unternehmen genutzt. Verwendungszweck dafür ist das Senden und Empfangen einer großen Menge an Nachrichten. Dies wird z.B. für das Versenden von One-Time-Passworts oder Notfallmeldungen genutzt. External Short Message Entities fungieren als Schnittstelle und erlauben so einen direkten Zugriff auf die SMSCs oder Verlaufen den Zugriff an Dritte weiter [4].

B. Over-the-Top Instant Messenger

- jeder Nutzer muss Client installieren

[2]

...

Ein populäres Beispiel für einen OTT Messenger ist WhatsApp. WhatsApp wurde ursprünglich 2009 als eigenständiges Unternehmen gegründet und ist seit 2014 Teil von Meta Platforms Inc [5]. Früher war die Nutzung des Dienstes mit einem kostenpflichtigen Abo verbunden, ist allerdings mittlerweile vollständig kostenlos nutzbar [6].

Der WhatsApp Messenger bietet zahlreiche Funktionen an, die über einfache Textnachrichten hinaus gehen. Es ist möglich, verschiedene Arten von Medien zu versenden, wie unter anderem Fotos, Videos, Audio und Dokumente. Weitere Nachrichtentypen, wie Live-Standort und Kontaktdaten sind ebenfalls vorhanden. Auf Nachrichten kann mit Emojis reagiert werden. Für sensiblere Nachrichten gibt es die Möglichkeit, selbstlöschende Nachrichten zu aktivieren, welche nach einer voreingestellten Zeit oder nach einmaligem anschauen automatisch gelöscht werden [7]. Damit die Sicherheit und Privatsphäre der Nutzer gewährleistet sind, sind alle Nachrichten Ende-zu-Ende-Verschlüsselt und können nur auf den entsprechenden Endgeräten der Nutzer entschlüsselt werden. Der komplette Nachrichtenverkehr wird über die WhatsApp-Server abgewickelt [8]. Gruppenchats erlauben die Kommunikation mit mehreren Personen gleichzeitig. Die Telefonie-Funktion beinhaltet den Videoanruf, welcher Live-Videos von den teilnehmenden Personen übertragen. Während dem Anruf kann man weiterhin auf die Chats zurückgehen und wie gewohnt parallel nutzen [7]. Wer WhatsApp gerade nicht auf einem mobilen Endgerät nutzen möchte, kann auf WhatsApp Web oder WhatsApp Desktop ausweichen, um

den Dienst auch auf anderen Plattformen wie Desktop-PCs zu nutzen. Die Verknüpfung des Accounts findet über das Scannen eines QR-Codes statt [7], [8].

Mit WhatsApp Business ist es möglich, dass Nutzer mit Unternehmen kommunizieren können. Dies kann für z.B. Support, aber auch automatisierte Chatbots genutzt werden. Allerdings muss bedacht werden, dass nicht alle Unternehmen direkt über WhatsApp Business kommunizieren, sondern mittels eines Dienstes Dritter über die WhatsApp API. Dadurch ist die Ende-zu-Ende-Verschlüsselung nicht mehr vollständig gewährleistet [8].

III. RICH COMMUNICATION SERVICES

A. Definition

Seit dem Aufstieg von OTT sinkt die Nutzung von klassischen Kommunikationsarten wie SMS. Laut einer Statistik der Bundesnetzagentur ist die Nutzung von SMS im Jahr 2015 bereits um 41% gesunken [1]. 2008 veröffentlichte die "Groupe Speciale Mobile Association" (GSMA) die erste Version des Universal Profiles, welche die Funktionen der Rich Communication Services (RCS) definiert [9]. Zu den Grundideen gehört unter anderem die Verknüpfung verschiedener Dienste, wie das Nachrichtenschreiben, die Kontakte-App und die Kontakte-App. Außerdem sollen die Funktionen nativ im Betriebssystem implementiert sein. Für die Implementation sind die Entwickler des Betriebssystems bzw. der Gerätehersteller zuständig. Beispiel dafür ist die Android-Implementation in Samsung Messages oder Google Messages [Quelle folgt]. Seit 2024 ist RCS auch auf iOS-Geräten über iMessage verfügbar [Quelle folgt]. Alternativ gibt es die Möglichkeit, RCS-Funktionalität durch das Installieren einer dafür entwickelten App zu erhalten [3].

B. Funktionen

- erste Version nur enriched phonebook, enriched calling, enriched messaging
- phonebook
 - Profil erstellen
 - andere können Profil sehen (freiwillig, beide müssen Profil teilen)
- calling
 - Multimedia während dem Anruf teilen (Videoanruf)
- messaging
 - Dateitransfer
 - Gruppenchats
- bereits da Idee, dass es nativ im Betriebssystem integriert sein sollte

[9]

- "1-to-1 Messaging" - einfacher Nachrichtenaustausch zwischen zwei Personen
- Dateitransfer ist möglich (egal welcher Typ, Status: Pending, Progress, Cancelled, Sent, Delivered)
- bestimmte Dateien sollen auf bestimmte Art und Weise dargestellt werden (Video, Bild, Audio, GIF, PDF)
- man kann Sprachnachrichten aufnehmen und versenden

- man kann den aktuellen Status der Nachricht sehen (Versendet, Fehler, SMS-Fallback, Gelesen)
- man kann sehen, wenn der Kontakt am schreiben ist
- man kann seinen (Live-)Standort teilen
- Gruppenchats
- "Enriched Calling" - Dateitransfer während Anruf möglich → Videoanruf
- Chatbots für z.B. Unternehmen (Gemini Integration ! Quelle nötig !), enthalten Beschreibung
- (mit Chatbots kann anonym gechattet werden)
- Spam kann vermieden werden

[3]

C. Technik

- unified composer (entscheidet selbst, ob als SMS oder MMS gesendet wird und sagt user bescheid)

[9]

- damit alles nahtlos funktioniert, müssen die Mobilfunk-Operatoren sich auf eine gängige Implementierung einigen
- 2011 unter anderem Deutsche Telekom, Telefonica, Vodafone angekündigt, Zusammenschluss zu bilden für eine gemeinsame RCS Implementierung, auch RCS-e (oder Rich Communication Services enhanced) genannt

[2]

- "Capability Discovery" zeigt den Clients, welche RCS Funktionen verfügbar sind
- RCS Dienste werden automatisch aktiviert
- es wird dem Nutzer direkt angezeigt, ob RCS verfügbar ist und falls nicht, wird auf SMS als Backup zurückgegriffen

[3]

D. Sicherheit

- zur Authentifizierung am Endgerät Sim-basierte Authentifizierung nutzen, auf anderen Geräten andere Möglichkeiten (Login mit Username & Passwort / Pairing über Code)
- Verschlüsselung von Allem mit gängigen Protokollen, wie TLS und IPsec

[3]

IV. VORTEILE VON RCS GEGENÜBER SMS

SMS

- Nachricht zwischen Base Station und Gerät verschlüsselt, innerhalb des Systems allerdings nicht
- Gateways speichern Nachrichten teilweise für längere Zeit
- External Short Message Entities können für Betrug genutzt werden

[4]

- anstatt für jeden Instant Messenger eigenen Client zu installieren, der Leistung braucht, universeller integrierter Messenger

- es ist möglich, RCS über ein Mobilgerät oder auch PC zu nutzen

[2]

- man kann clients auf mehreren Geräten nutzen
- bei Dual-SIM ist RCS mit beiden Karten gleichzeitig möglich

[3]

V. SCHWÄCHEN VON RCS

- SMS SIM Swap Attack
 - Angreifer gibt sich als das Opfer aus, um neue SIM-Karte zu erhalten oder eine Umleitung einzurichten
 - kann Nachrichten abfangen, wie One-Time-Passwords
 - durch RCS nicht gelöst, da es auch über die Telefonnummer läuft

[4]

- alle Mobilfunkanbieter müssen zusammenarbeiten, damit die Kommunikation auch über Ländergrenzen hinweg nahtlos funktionieren kann, es sollte eine standardisierte Implementation geben
- alle Hersteller von Mobilgeräten müssen RCS implementieren, damit die Verbreitung besser vorangetrieben wird

[2]

- Samsung Messages
- Google Messages
- iMessage (nur neuste iOS Version)

VI. FAZIT

...

REFERENCES

- [1] N. Wellmann, "Are OTT messaging and mobile telecommunication an interrelated market? An empirical analysis", *Telecommun. Policy*, Bd. 43, Nr. 9, Oktober 2019, doi: 10.1016/j.telpol.2019.101831.
- [2] M. Lin und J. Arenzana Arias, "Rich Communication Suite: The challenge and opportunity for MNOs", in *2011 15th International Conference on Intelligence in Next Generation Networks*, Okt. 2011, S. 187–190. doi: 10.1109/ICIN.2011.6081071.
- [3] GSMA. "RCS Universal Profile Service Definition Document". Zugegriffen: 06.11.2024. [Online]. Verfügbar unter: <https://www.gsma.com/solutions-and-impact/technologies/networks/wp-content/uploads/2019/10/RCC.71-v2.4.pdf>
- [4] B. Reaves, N. Scaife, D. Tian, L. Blue, P. Traynor, und K. R. B. Butler, "Sending Out an SMS: Characterizing the Security of the SMS Ecosystem with Public Gateways", in *2016 IEEE Symposium on Security and Privacy (SP)*, Mai 2016, S. 339–356. doi: 10.1109/SP.2016.28.
- [5] "Danke für 10 Jahre", WhatsApp.com. Zugegriffen: 4. Dezember 2024. [Online]. Verfügbar unter: <https://blog.whatsapp.com/thank-you-for-10-years>
- [6] "WhatsApp kostenlos und nützlicher machen", WhatsApp.com. Zugegriffen: 4. Dezember 2024. [Online]. Verfügbar unter: <https://blog.whatsapp.com/making-whats-app-free-and-more-useful>
- [7] "WhatsApp-Hilfebereich". Zugegriffen: 4. Dezember 2024. [Online]. Verfügbar unter: <https://faq.whatsapp.com/>
- [8] WhatsApp. "WhatsApp Encryption Overview Technical White Paper". Zugegriffen: 4. Dezember 2024. [Online]. Verfügbar unter: <https://faq.whatsapp.com/820124435853543#nachrichtenaustausch-mit-unternehmen>
- [9] K. Henry, Q. Liu, und S. Pasquereau, "Rich Communication Suite", in *2009 13th International Conference on Intelligence in Next Generation Networks*, Okt. 2009, S. 1–6. doi: 10.1109/ICIN.2009.5357089.