Bild: Albert Hulm

Messenger-Esperanto

EU und IETF gegen babylonische Messenger-Verwirrung

Die Industrie verliert im Wettbewerbseifer gerne den Blick fürs große Ganze und so auch bei der Entwicklung der Messenger: Weil jeder Hersteller nur an sein eigenes Süppchen denkt, bleibt die Interoperabilität auf der Strecke. Nun wird die EU die Anbieter wohl dazu zwingen.

Von Monika Ermert

Es kommt selten vor, dass sich Gremien der Normungsinstitute und der Politik so günstig ergänzen, dass die Vorteile ihres gemeinsamen Ziels unmittelbar einleuchten. Aktuell kann man das bei Messenger-Diensten beobachten: Politiker der EU fordern von Messenger-Herstellern, ihre Plattformen füreinander zu öffnen und Wege zur herstellerübergreifenden Kommunikation von WhatsApp, iMessage oder Skype zu schaffen. Das kann man dem Anfang Mai durchgesickerten, finalen Entwurfstext zum „Gesetz über digitale Märkte“ entnehmen (Digital Markets Act, DMA, siehe ct.de/y4h2).

Passend dazu arbeitet die Internet Engineering Task Force (IETF) an geeigneten Protokollen, sodass sich die Messenger-Hersteller diese Arbeit sparen können. Wenn es so kommt, dann schließen die Messenger-Entwickler beispielsweise zu den Telefonherstellern auf, die seit vielen Jahrzehnten vormachen, wie Interoperabilität geht.

Bisher stehen vor allem Smartphone-Nutzer unter Druck, immer neue Clients zu installieren, um mit möglichst jeder Person aus dem Umkreis per Messenger kommunizieren zu können. Dem Druck geben viele nicht nach und bleiben ausgeschlossen, während die anderen Lebenszeit vergeuden: immer mehr Messenger-Apps installieren, sich an immer mehr Plattformen anmelden und immer mehr Bedienkonzepte lernen. Geht das Smartphone verschütt, an das all die Messenger gebunden sind, fängt die Zeitvergeudung von vorn an.

Die aktuellen Textpassagen zur Messenger-Interoperabilität gehen weitgehend auf das Engagement des Europäischen Parlaments zurück; es sieht sie als wettbewerbsfördernde Maßnahme. Im Trilog setzte es sich gegen schwächere Vorgaben der EU-Kommission durch, während der Rat der EU das Thema gar nicht erst auf dem Zettel hatte.

Der Gesetzentwurf sieht mehrere Etappen vor: Als erstes müssen die großen, marktbeherrschenden Unternehmen wie Facebook oder Microsoft (im EU-

Sprech Gatekeeper genannt [1]) ihre Dienste für den Austausch von Textnachrichten für anfragende Wettbewerber öffnen – wenn also der kleine Messenger Wire eine Kreuzkompatibilität will, müssen WhatsApp, Facebook Messenger oder Skype mitspielen.

Neun Monate Vorfreude

Tritt das Gesetz so in Kraft, haben einmal als Gatekeeper eingestufte Unternehmen ein halbes Jahr Zeit, eine Basisinteroperabilität herzustellen. Die kleineren Wettbewerber müssen anschließend den Austausch mit einem Gatekeeper selbst beantragen und dem Großen noch drei Monate Zeit geben. Unter Basisinteroperabilität versteht die EU bilaterale Textkommunikation und den Austausch von Sprach- und Videonachrichten zwischen den Nutzern zweier Dienste.

Für interoperable Gruppen-Chats mitsamt Video-, Sprach- und Bildübertragung bleiben zwei Jahre und für gruppenübergreifende interoperable Voice- und Video-Calls sollen die Messenger-Entwickler vier Jahre Zeit erhalten, heißt es in dem vom Privacy- und Interop-Forscher Ian Brown geleakten Dokument (siehe ct.de/y4h2).

Der Rat und das Parlament müssen das Gesetz im Lauf des Jahres noch verabschieden. In Kraft treten könnte es zusammen mit der Schwester Digital Services Act (DSA) im Jahr 2023.

Ian Brown hat im aktuellen Entwurf auch Kröten gefunden, die man wohl wird schlucken müssen: Die Frist für plattformübergreifende Video-Calls findet Brown zu lang, vor allem vor dem Hintergrund, dass diese Kommunikationsform seit der Coronavirus-Pandemie stark genutzt wird. Zudem können die großen Plattformen den Anschluss von kleinen Mitbewerbern hinauszögern, etwa, indem sie bei der EU fundierte Sicherheitsbedenken beispielsweise bezüglich der Diensteintegrität vorbringen.

Ungünstig ist nach Ansicht Browns auch, dass nur ganz große Unternehmen unter die Auflage fallen (über 45 Millionen aktive Nutzer, mindestens 7,5 Milliarden Euro Umsatz in den letzten drei Geschäftsjahren). So mancher kleine Mitbewerber – etwa der kommerzielle Dienst Threema – hat schon signalisiert, sich an plattformübergreifender Kommunikation nicht beteiligen zu wollen. Das könnte die Großen stärken, sorgt sich Brown.

Weniger Gedanken macht er sich um die Ende-zu-Ende-Verschlüsselung. Diese stuft das EU-Dokument ausdrücklich als unverhandelbare Pflicht ein. Metadaten, etwa IP-Adressen oder Nutzerkennungen, sollten nur nach Maßgabe der Datenschutzgrundverordnung erhoben werden.

Die EU schreibt im Gesetzentwurf, dass die Kommission europäische Organisationen auffordern könne, Standards für die Interoperabilität zu entwickeln. Fachleute glauben, dass das nicht erforderlich wird, denn es gibt bereits weit fortgeschrittene Spezifikationen der Internet Engineering Task Force, auf die sich die Messenger-Branche als Standard einigen kann. Beispielsweise ist für die Verschlüsselung die Message Layer Security (MLS) im Gespräch. Der aktuelle MLS-Entwurf geht zurück auf einen Vorschlag von Rohan Mahy, Vizepräsident des Messenger-Anbieters Wire. Aber auch das Open-Source-Protokoll Matrix gilt als Kandidat.

Die IETF arbeitet in der Gruppe Messenger Layer Security seit 2018 an der Verschlüsselung von Gesprächen zwischen zwei und mehr Teilnehmern. Die Architektur und Details der Schlüsselhandhabe sowie der Authentifizierung stehen kurz vor dem Abschluss. Ursprünglich hatten die Autoren keine Interoperabilität im Sinn, aber so, wie der Entwurf inzwischen beschaffen ist, liefert er eine gute Grundlage auch für die Authentifizierung von Nachrichten und Gruppenmitgliedern und für das Key-Handling in Gruppenchats.

Nun soll eine neue IETF-Arbeitsgruppe die letzten Hürden nehmen, um zunächst gemäß den Anforderungen der EU eine Grundlage für Gespräche zwischen den Nutzern verschiedener Anbieter zu erarbeiten. Dafür machte sich Mahy im März beim Treffen der IETF in Wien stark. Innerhalb von sechs Monaten könnten zumindest Basisfunktionen für Gespräche zwischen unterschiedlichen Messengern entwickelt werden, glaubt er.

Das ist zugleich die Frist, die der EU-Gesetzgeber europäischen Anbietern zur grundlegenden Implementierung der Interoperabilität einräumt.

Erst mal Content-Typen aushandeln

Mahy, der auch schon an der Spezifikation der SIP-Standards für die Internettelefonie beteiligt war, stellte die nächsten Bausteine auf dem Weg zur Interoperabilität auf dem IETF-Treffen ausführlich vor. Gemäß einer „relativ schlichten“ Erweiterung der MLS-

c't kompakt

- Messenger sollen bald über Herstellergrenzen hinweg miteinander kommunizieren können.
- Die Interoperabilität legt die EU per Gesetz fest.
- Für die Umsetzung können Hersteller auf Protokollvorarbeiten der Internet Engineering Task Force zurückgreifen.

EU maßregelt Gatekeeper

Welche großen Messengerplattformen die EU an die Kandare nehmen will, schreibt sie nicht wörtlich. Aber anhand Umsatz- und Kundenzahlen kommt man leicht auf die üblichen Verdächtigen Facebook Messenger, Instagram, Skype oder auch Apples iMessage.

Gatekeepern wird es nicht gestattet sein:

- ihre eigenen Produkte übermäßig zu bewerben
- Zahlungsmöglichkeiten auf ihre eigene Zahlungsmethode zu beschränken
- die im Rahmen eines Dienstes erhobenen personenbezogenen Daten für die Zwecke eines anderen Dienstes weiterzuverwenden
- gewerblichen Nutzern unfaire Bedingungen aufzuerlegen
- bestimmte Software-Anwendungen vorzuinstallieren
- gewerbliche Nutzer von Plattformen einzuschränken
- bestimmte Bündelungspraktiken einzusetzen (z.B. Verkauf verschiedener Produkte als Paket)

1. Gatekeeper sind Firmen mit über 45 Millionen Endnutzer im Monat

2. Gatekeeper erwirtschaften einen Umsatz von mindestens 7,5 Milliarden € in den letzten drei Geschäftsjahren.

Bild: EU

Architektur (siehe ct.de/y4h2) könnte ein Client die von ihm bevorzugten Content-Typen seinem Gegenüber in Form von MIME-Types mitteilen. So können beide die Schnittmenge ermitteln und sich auf gemeinsame Content-Typen einigen.

Der Vorschlag unterscheidet zwischen erforderlichen und optionalen MIME-Types. Ein Client, der sich für die in einem Gruppenchat genutzten MIME-Types nicht eignet, kann dieser Gruppe nicht beitreten.

Laut Mahy lässt sich diese Erweiterung einfach in den Key-Packages des MLS-Verfahrens unterbringen. Key-Packages sind signierte Objekte, die laut RFC-Text „die Identität und die Fähigkeiten eines Clients beschreiben und einen öffentlichen Hybrid-Public-Key enthalten, der für diesen Client zum Verschlüsseln verwendet werden kann."

Ursprünglich waren Content-Formate kein Bestandteil des MLS-Verfahrens, es war allein der Ende-zu-Ende-Verschlüsselung gewidmet. Laut Mahy ist die Aushandlung der Content-Formate der nächste logische Schritt auf dem Weg zu interoperablen Messengern. Die MLS-Arbeitsgruppe sieht die komplette Erweiterung als kleinen Schritt, den sie selbst bewältigen kann.

Mahy stellte aber auch einen größeren Vorschlag zur Definition einer Syntax für Content-Typen vor. Zu dessen Hauptmerkmalen gehören detaillierte Aushandlungen von Inhaltsformaten. Dazu gehören Plain- und Rich-Text-Nachrichten, Zustell- und Lesebenachrichtigungen, Antworten, Reaktionen, Anklopfen und Pings, Dateien, Audio- und Videodaten und natürlich Anrufe und Konferenzen.

Die verschiedenen Messenger könnten, so schreibt Mahy in seinem Vorschlag, sowohl die proprietären als auch die für die Kommunikation mit fremden Clients standardisierten Formate melden und aushandeln.

App-Expertise nachgefragt

Doch für die Einzelheiten brauche man laut der aktuellen Arbeitsgruppe mehr App-Expertise und kaum Security-Fachwissen. Deshalb soll für diese Aufgabe eine neue Arbeitsgruppe gegründet werden. Vorgeschaltet ist entsprechend dem üblichen IETF-Verfahren ein Treffen, bei dem in meist hitziger Debatte die Ziele der Gruppe festgezurrt werden (Birds of a Feather).

Mahy versichert: „Diese Arbeiten sind kein Hexenwerk. Viele Bausteine sind längst standardisiert, etwa die Echtzeitkommunikation mit Ton, Bild und Datenübertragung mittels WebRTC". Und für das Überwinden der Router-Hürde Network Address Translation (NAT) könne man das Protokoll STUN nutzen. Mit dem absehbaren Abschluss der Ende-zu-Ende-Verschlüsselung von Gruppenchats werde man bald einen weiteren dicken Brocken aus dem Weg räumen.

Skeptische Beobachter verweisen jedoch auf die vielen erfolglosen Versuche, einen IETF-Standard für Instant Messaging zu etablieren. Ted Hardie, ehemaliger Vorsitzender des Internet Architecture Board und nun bei Cisco verantwortlich für globale technische Standards, nannte einige Ansätze, die fruchtlos endeten.

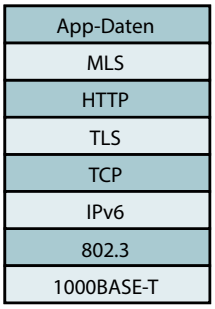
Hardie war Area Director, als 2004 das Common Profile for Instant Messaging verabschiedet wurde (RFC-Spezifikation 3860), das die erste Welle proprietärer IM-Clients unter einen Hut bringen sollte. Große Unternehmen wie Microsoft und AOL hatten die bis dahin intern für die Firmenkommunikation genutzten Clients zu Internetdiensten für ihre wachsende Nutzerschaft erweitert, rekapitulierte er vor einiger Zeit in einem Aufsatz (siehe ct.de/y4h2).

Doch gerade die Großen waren wenig interessiert, neue, interoperable Protokolle aufzunehmen. Denn die proprietären Messenger erleichterten durch den Lock-In, Nutzer an ein Unternehmen zu binden und so die zunehmende Nutzerzahl für den eigenen Vorteil zu nutzen, so Hardie. Und Mahy bestätigt: „Gäbe es einen wirtschaftlichen Grund für Facebook und Microsoft, dann hätte man die interoperablen Messenger heute schon".

Politik bewegt Technik

Mit dem Digital Markets Act der EU wendet sich das Blatt aber. Darauf verwies Wire-Chef Alan Duric. Er schrieb in seinem LinkedIn-Profil, dass Wire sowohl am DMA als auch an der Forderung der Interoperabilität mitgewirkt habe. Mahy zufolge bemüht sich Wire um die Interoperabilität schon seit langem. Allen sei eigentlich längst klar, dass es so nicht weitergehen könne mit der Inselbildung, bestätigte auch der langjährige IETF-Experte Stephen Farrell vom University College Dublin.

Die IETF-Spezifikation ist freilich nicht der einzige Weg, um eine plattformübergreifende Kommunikation zu ermöglichen. Die Bundesnetzagentur hat im Dezember 2021 ein Positionspapier veröffentlicht, in dem sie verschiedene Wege aufzeichnet, darunter auch einfaches Bridging, bei dem ein Übersetzerdienst zum Beispiel Textnachrichten automatisch ins passende Format umsetzt, wenn sie die Grenzen einer Plattform verlassen sollen.



Die Kommunikation eines MLS-Clients mit einem Verteildienst ist bisher nicht spezifiziert, aber dafür bietet sich TLS-verschlüsseltes HTTP an, also HTTPS.

Nur als zweite Alternative stuft die Agentur einen gemeinsamen Schnittstellenstandard ein, weil er deutlich aufwändiger sei. Und erst an dritter Stelle folgt eine herstellerübergreifende Standardisierung; für diese sieht die Agentur wegen noch höheren Aufwands kaum Chancen.

Große Schatten in Wien

Nach Wien waren aber nicht nur interessierte Entwickler gereist, sondern auch Mitarbeiter mancher Messenger-Hersteller. Ein Vertreter von Facebook signalisierte Interesse an der neuen Arbeitsgruppe und Mahy kündigte im Gespräch mit c't ein baldiges „informelles Treffen mit mehreren interessierten Entwicklern verschiedener Firmen" an.

Er selbst plane, das ursprünglich von Google und Wire im Jahr 2019 aufgelegte Dokument zu „Messaging Layer Security Federation" wiederzubeleben und das Thema kryptografisch gesicherter Identitäten anzugehen. Letztere seien beim Zusammentreten von Nutzern aus verschiedenen Systemen besonders wichtig.

Glaubt man Mahy und vertraut auf die normative Kraft der EU, dann wird es also bald Brücken geben zwischen den IM-Inseln, wenn nicht zwischen allen, dann doch zwischen vielen. *(dz@ct.de)* **ct**

Literatur

[1] Holger Bleich, Gegen das Gatekeepen, EU-Parlament schärft den DMA-Entwurf nach, c't 2/2022, S. 30

Entwurf DMA, Spezifikationen:
ct.de/y4h2