# RTR AKTUELL

## Telekommunikation und Post

TK 03/2021 vom 11.10.2021

## INHALT



Rundfunk und Telekom Regulierungs-GmbH (RTR)

Mariahilfer Straße 77–79
1060 Wien, Österreich
www.rtr.at

E: rtr@rtr.at
T: +43 1 58058 – 0
F: +43 1 58058 – 9191
twitter.com/RTRTelekomPost

EDITORIAL

# Digitale Identität baut auf Sicherheit und Vertrauen

(©APA-Fotoservice/Martin Hörmandinger)

Liebe Leserinnen und Leser!

**„Hilfe, was mache ich ohne Facebook?“** titelte die Headline des Kurier am 06. Oktober 2021. Und Karikaturist Michael Pammesberger sah dabei auf Seite 2 schon das physische Ende von mindestens 470.000 Influencerinnen und Influencern als Folge davon. Hintergrund war ein weltweiter Totalausfall von Facebook und seiner anderen Dienste am 05. Oktober2021. Wir sind also schon an einem Punkt angekommen, wo bereits die Nichtverfügbarkeit eines Dienstes im Internet unser Leben aus dem Lot bringen kann. Das sollte uns zu denken geben und zeigt, wie abhängig wir mittlerweile vom Internet geworden sind. Und es gibt eigentlich kein Zurück mehr. Immer mehr Menschen wird dies auch bewusst.

Und diese Abhängigkeit führt mich auch gleich zum eigentlichen Hauptthema dieses Newsletters, der Sicherheit. Sicherheit ist dabei ein vielschichtiges Thema, das sich in einer vernetzten Welt wie heute mit vielen unterschiedlichen Fragestellungen zu befassen hat.

Da ist zum einen einmal die physische und technische Sicherheit unserer Netze als kritischer Infrastruktur in unserem Land und darauf aufbauend die Sicherheit der von diesen Netzen bereitgestellten Services. Für beides war der Fachbereich Telekkommunikation und Post der RTR auch bisher schon in einem gewissen Ausmaß verantwortlich. Im neuen Telekommunikationsgesetz werden wir dazu mit dem Netzsicherheitsbeirat weitere Aufgaben bekommen. Aufgabe dieses Beirates wird es sein, potentielle Risiken zu monitoren und wo notwendig, der Bundesministerin für Landwirtschaft, Regionen und Tourismus als für die Telekommunikationsinfrastruktur zuständige Fachministerin Vorschläge zur Abhilfe beim Auftreten von Risiken zu machen. In diesem Beirat werden neben dem Fachbereich Telekommunikation und Post der RTR auch die verantwortlichen Bundesministerien, aber auch weitere Stakeholder aus der Wirtschaft und der Zivilgesellschaft vertreten sein. Details dazu in unserem nächsten Newsletter, in dem wir uns mit dem neuen Telekommunikationsgesetz befassen werden.

Aber das ist nur ein Bereich der Sicherheit, der uns interessiert. Auf der Sicherheit der Netze aufbauend gibt es das breite Spektrum der Datensicherheit und der Vertrauensdienste. Ohne solche Vertrauensdienste wäre nämlich die volle Nutzung der Möglichkeiten, die uns das Internet bietet, gar nicht möglich. Konkret sprechen wir dabei über die elektronische Signatur, die es ermöglicht, bereits heute viele Erledigungen im öffentlichen Bereich vorzunehmen. Ohne digitale Signatur wäre auch der Elektronische Pass in der vorliegenden Form nicht möglich gewesen. Die elektronische Signatur ist daher eine zentrale Voraussetzung für unser digitales Leben, um eine rechtssichere digitale Identität zu erhalten. Damit digitale und physische Identität übereinstimmen und damit Vertrauen geschaffen werden kann in einer Welt, die immer mehr in den virtuellen Raum expandiert, ist es notwendig, die rechtlichen Grundlagen dafür parat zu haben und komplexe Anforderungen zu managen. Die RTR befasst sich schon lange damit. In einem ausführlichen Beitrag von

EDITORIAL

unserem Experten Mag. Ullrich Latzenhofer dürfen wir Ihnen dazu tiefere Einsichten geben. Mehr dazu also gleich im Anschluss.

Und dann geht es natürlich auch um die Sicherheit von allen kritischen Infrastrukturen, aber auch Privaten und Systemen, die ebenfalls über das Internet und die Telekommunikationsnetze verbunden sind. Stichwort Cybersecurity, ein Thema, zu dem wir fast jeden Tag Schlagzeilen finden. In diesem Bereich tragen wir ebenfalls mit unserer Expertise gemeinsam mit anderen verantwortlichen öffentlichen Stellen dazu bei, dass Österreich sicher ist. Die Anforderungen, die sich dabei im Zusammenhang mit 5G und Campusnetzen ergeben, sind nicht zu unterschätzen.
Denn eines ist klar: Wenn Facebook ausfällt, bricht für einige Menschen vielleicht eine „Welt“ zusammen, wenn jedoch die Netze ausfallen, kann das lebensgefährlich werden. Sicherheit der Netze und im Netz ist daher kein theoretisches Thema mehr, sondern praktisch in allen Lebensbereichen mehr als nur relevant unverzichtbar.

Und damit es diese sicheren Netze gibt, sie auch gebaut werden und damit sich unsere Konsumentinnen und Konsumenten darauf verlassen können, überall zu angemessenen Bedingungen sicher verbunden zu sein, braucht es auch die richtigen gesetzlichen Rahmenbedingungen. Das in Kürze in Kraft tretende Telekommunikationsgesetz bildet hier einen wesentlichen Meilenstein für die Zukunft. Es handelt sich dabei um die umfassendste Neukodifikation des Telekommunikationsrechts seit 2003 auf Basis des EECC von 2019. Neben den voraussichtlichen Aufgaben im Netzsicherheitsbeirat, wie oben angedeutet, wird es darin noch eine Reihe weitere Neuerungen, auch für den Fachbereich Telekom und Post der RTR geben. Nach dem Ministerratsbeschluss im September erwarten wir, dass sich das Plenum des Parlaments und der Bundesrat ab Mitte Oktober damit befassen werden. Was dann neu sein wird, ist jedenfalls das Thema unseres nächsten Newsletters. Seien Sie gespannt, wir sind es auch!

In diesem Sinne lesen Sie wohl!

Ich freue mich auch über ihr Feedback (gerne auch persönlich via mail unter klaus.steinmaurer@rtr.at) und verbleibe

**Klaus M. Steinmaurer**
Geschäftsführer der RTR
Fachbereich Telekommunikation und Post

VERTRAUENSDIENSTE

# Infrastruktur für elektronische Signaturen

Zwanzig Jahre lang bescheinigten ihr viele ein Mauerblümchendasein, doch die Pandemie hat sie in den Blickpunkt gerückt: die elektronische Signatur. Einerseits ist sie ein wesentliches Element bei digitalen Arbeitsabläufen und Genehmigungsprozessen, deren Bedeutung durch das Home-Office erheblich zugenommen hat. Andererseits hat hierzulande die Einführung des „Grünen Passes“ die Nachfrage nach der Handy-Signatur erhöht, die wohl auch deshalb bereits von mehr als 30 Prozent der Bevölkerung genutzt wird.

Seit Inkrafttreten des Signaturgesetzes am 1. Jänner 2000 obliegt die Aufsicht über die Anbieter elektronischer Signaturen der Telekom-Control-Kommission. Als deren Geschäftsstelle hatte die RTR-GmbH von Anfang an den Auftrag, die Aufsichtsstelle zu unterstützen und die für die Prüfung elektronischer Signaturen erforderlichen Verzeichnisse der Anbieter und ihrer Dienste zu führen. Seit 2008 betreibt die RTR ein Service zur Prüfung elektronischer Signaturen. Seit 2009 führt sie für Österreich die unionsrechtlich geregelte „Vertrauensliste“. Der vorliegende Beitrag soll diese Tätigkeiten, die seit 2016 im Signatur- und Vertrauensdienstegesetz (SVG) verankert sind, einer breiteren Öffentlichkeit bekanntmachen.

## Das europäische System der Vertrauenslisten

Eine elektronische Signatur wird in der Regel mit Hilfe eines kryptographischen Schlüssels erstellt, der an die Person des Unterzeichners gebunden ist. Für die Prüfung der elektronischen Signatur muss man wissen, welcher Person dieser Schlüssel zugeordnet ist. Diesen Zweck erfüllt das Zertifikat – eine Datenstruktur, mit der ein sogenannter Vertrauensdiensteanbieter (kurz VDA) die Zugehörigkeit des Schlüssels zu einer bestimmten Person bestätigt. Das Zertifikat enthält seinerseits eine elektronische Signatur des VDA, die nach demselben Prinzip mit einem Zertifikat geprüft wird, das eine übergeordnete Instanz dem VDA ausgestellt hat.

Technisch ist die Ausstellung von Zertifikaten nicht auf VDA beschränkt: Wer das Betriebssystem Linux installiert, setzt dabei vielleicht einen Webserver auf und stellt für diesen – bewusst oder unbewusst – ein Zertifikat aus. Für die Ausstellung von Zertifikaten für elektronische Signaturen bedarf es jedoch nicht nur der technischen Fähigkeit, sondern vor allem auch der Erfüllung von Sicherheitsanforderungen. Die höchsten Sicherheitsanforderungen gelten für Anbieter qualifizierter Zertifikate, die man für qualifizierte elektronische Signaturen benötigt: Nur diese haben die gleiche Rechtswirkung wie eine handschriftliche Unterschrift. Nicht alle Zertifikate sind daher gleichermaßen vertrauenswürdig. Welche Zertifikate bzw. welche VDA akzeptiert werden, ist eine der wichtigsten Fragen bei der Prüfung elektronischer Signaturen.

Für die Nutzung elektronischer Signaturen im europäischen Binnenmarkt ist es erforderlich, dass elektronische Signaturen grenzüberschreitend geprüft werden können und dass zwischen den involvierten Parteien ein Grundkonsens über die Akzeptanz von Zertifikaten besteht. Seit 2009 ist jeder Mitgliedstaat der Europäischen Union und in weiterer Folge auch jeder Vertragsstaat des Abkommens über den

VERTRAUENSDIENSTE

Europäischen Wirtschaftsraum zur Führung einer Vertrauensliste mit Mindestangaben über die von ihm beaufsichtigten VDA und die von diesen erbrachten Vertrauensdienste verpflichtet. Diese Informationen dienen vor allem der Prüfung qualifizierter Zertifikate und umfassen daher auch die hierfür erforderlichen übergeordneten Zertifikate der VDA. Während Informationen über qualifizierte Vertrauensdienste von allen Mitgliedstaaten zu erfassen sind, nehmen einige dieser Staaten freiwillig auch Angaben über nichtqualifizierte VDA auf (in Österreich auf Antrag des jeweiligen VDA). Um die Interoperabilität zu wahren, weisen die Vertrauenslisten aller Mitgliedstaaten ein einheitliches Format auf (XML gemäß einem vom Europäischen Institut für Telekommunikationsnormen ETSI spezifizierten und kontinuierlich weiterentwickelten Schema). Zur Gewährleistung der Authentizität und der Integrität der Vertrauensliste enthält jede Vertrauensliste eine elektronische Signatur der sie ausstellenden Behörde.

Die Vertrauenslisten der einzelnen Mitgliedstaaten sind in sicherer Weise miteinander verknüpft: Eine von der Europäischen Kommission geführte Linkliste enthält Links zu allen aktuellen nationalen Vertrauenslisten, des Weiteren jene Zertifikate, mit denen die nationalen Vertrauenslisten signiert werden können, und überdies eine elektronische Signatur der Europäischen Kommission. Umgekehrt enthält jede Vertrauensliste eines Mitgliedstaats einen Link zur europäischen Linkliste und jene Zertifikate, mit denen die Linkliste signiert werden kann. Sollte einer der beteiligten Listen kompromittiert sein, so würde dies sofort auffallen, weil die elektronische Signatur ungültig wäre. Sogar der Versuch, eine Vertrauensliste durch eine ältere Version zu überschreiben, würde dank der fortlaufenden Nummerierung der Vertrauenslisten auffallen.

Jede Vertrauensliste ist zumindest halbjährlich zu aktualisieren. Änderungen im Status eines Vertrauensdienstes (z.B. Verleihung oder Entzug des Qualifikationsstatus) sind aber innerhalb eines Tages einzutragen. Dabei wird der bisher aktuelle Status in eine Historie verschoben. So lässt sich auch nachträglich feststellen, welchen Status ein Vertrauensdienst in einem bestimmten Zeitpunkt aufwies. Umgekehrt bedeutet dies, dass die Vertrauensliste mit äußerster Sorgfalt geführt werden muss, da jeder Fehler auch nach dessen Korrektur für immer in der Historie erhalten bliebe.

Aufgrund ihrer essentiellen Bedeutung für die Anerkennung von Zertifikaten und somit für die Prüfung elektronischer Signaturen müssen Vertrauenslisten, über das Jahr gerechnet, zu mindestens 99,9 Prozent verfügbar sein (dies entspricht einer maximalen Ausfallsdauer von ca. 8¾ Stunden pro Jahr). Die Verfügbarkeit wird von der Europäischen Kommission laufend überwacht.

Vertrauenslisten dienen primär zur maschinellen Verarbeitung, beispielsweise im Rahmen von Validierungsdiensten oder dem von der RTR betriebenen Prüfservice (siehe unten). Als XML-Dateien sind sie für Laien kaum lesbar. Die Europäische Kommission betreibt aber unter https://esignature.ec.europa.eu/efda/tl-browser/#/screen/home einen „Trusted List Browser“, der die in den nationalen Vertrauenslisten enthaltenen Informationen lesbar aufbereitet.

VERTRAUENSDIENSTE

## Prüfservice für elektronische Signaturen

Unter https://www.signaturpruefung.gv.at/ betreibt die RTR ein Service, mit dem sich elektronische Signaturen auch ohne die Installation spezieller Software prüfen lassen. Zu diesem Zweck wird ein Dokument, das die zu prüfenden elektronischen Signaturen enthält, zum Server hochgeladen. Als Ergebnis erhält man einen Prüfbericht, der zu jeder elektronischen Signatur angibt,

(a) ob die elektronische Signatur den signierten Daten entspricht (Spalte S),
(b) ob das Zertifikat im Zeitpunkt der Signaturerstellung (bzw. im Zeitpunkt der Signaturprüfung, falls der Zeitpunkt der Signaturerstellung nicht feststellbar ist) gültig war (Spalte Z) und
(c) sofern das Signaturformat ein „Manifest“ vorsieht, ob dieses gültig ist (bei PDF irrelevant).

Ein positives Prüfergebnis wird jeweils durch grün hinterlegtes „OK“ zum Ausdruck gebracht, ein negatives durch rot hinterlegtes „X“. Wenn eine elektronische Signatur (bzw. bei einem mehrfach signierten Dokument die zuletzt erstellte elektronische Signatur) nicht das gesamte Dokument umfasst, wird das Prüfergebnis gelb hinterlegt. Über einen Link „Prüfbericht“ können detaillierte Prüfergebnisse in Form einer von der RTR signierten PDF-Datei abgerufen werden. Ob es sich um eine (der handschriftlichen Unterschrift gleichwertige) qualifizierte elektronische Signatur handelt, ist in diesem Prüfbericht ersichtlich: Dieser enthält zu jeder im geprüften Dokument enthaltenen elektronischen Signatur einen Abschnitt „Zertifikat“, in dem u.a. die „Qualität“ beschrieben wird. Eine qualifizierte elektronische Signatur liegt in der Regel dann vor, wenn sowohl ein „qualifiziertes Zertifikat“ als auch eine „sichere Signaturerstellungseinheit“ ausgewiesen wird (siehe Abbildung 1).

Abbildung 1: Informationen zum Zertifikat im Prüfbericht

| **Zertifikat** | |
|---|---|
| Seriennummer | dez.: 627580152, hex.: 25:68:1c:f8 |
| Qualität | Qualifiziertes Zertifikat (Quelle: TSL), sichere Signaturerste Zertifikat) |
| zeitliche Gültigkeit | gültig von 2019-02-20T10:45:54Z bis 2024-02-20T10:45:5 Der Prüfzeitpunkt liegt innerhalb des Gültigkeitszeitraumes |
| Verwendungszweck | Digitale Signatur, Nichtabstreitbarkeit |
| Zertifizierungsstatement | http://www.a-trust.at/docs/cp/a-sign-premium-mobile |

Fortgeschrittene elektronische Signaturen weisen bestimmte Eigenschaften auf, die sie von einfachen elektronischen Signaturen abheben. Im Einzelfall kann aber anhand einer elektronischen Signatur oder dem zugehörigen Zertifikat technisch nicht festgestellt werden, ob alle Kriterien für das Vorliegen einer fortgeschrittenen elektronischen Signatur erfüllt sind. Auch das Prüfservice erlaubt eine solche Feststellung nicht.

VERTRAUENSDIENSTE

Das Prüfservice eignet sich für eine Vielzahl von Dokumenten- und Signaturformaten, z.B. international übliche Formate wie PAdES (PDF Advanced Electronic Signatures), XAdES (XML Advanced Electronic Signatures), CAdES (CMS Advanced Electronic Signatures) und ASiC (Associated Signature Containers), aber auch das in österreichischen E-Government-Anwendungen jahrelang gebräuchliche Format PDF-AS.

Für die Prüfung von Zertifikaten wird auf das europäische System der Vertrauenslisten zurückgegriffen. Im Idealfall sind somit alle von Anbietern im europäischen Wirtschaftsraum ausgestellten qualifizierten Zertifikate prüfbar. Vereinzelt kommt es allerdings vor, dass eine nationale Vertrauensliste unter der vorgesehenen Adresse nicht abrufbar ist oder, beispielsweise wegen eines syntaktischen Fehlers, nicht verarbeitet werden kann. In solchen Fällen können Zertifikate von Anbietern aus dem betroffenen Staat mit Hilfe des Prüfservice nicht geprüft werden, solange das Problem nicht behoben ist (dies liegt meist nicht im Bereich der RTR).

Amtssignaturen sind ein österreichisches Spezifikum. Sie bringen die Herkunft eines Dokuments von einem Verantwortlichen des öffentlichen Bereichs (z.B. einer Behörde) zum Ausdruck. Amtssignaturen sind an einem bestimmten Attribut im Zertifikat erkennbar. Enthält ein Zertifikat das dieses Attribut, so weist das Prüfservice diesen Umstand in einer Fußnote aus.

Ein amtssigniertes elektronisches Dokument hat auch in ausgedruckter Form die Beweiskraft einer öffentlichen Urkunde. Allerdings kann eine Amtssignatur mit Hilfe des Prüfservice nicht anhand eines Scans oder eines Fotos des ausgedruckten Dokuments, sondern ausschließlich anhand des elektronischen Originals geprüft werden. Für den Fall, dass das elektronische Original nicht vorliegt, hat die ausstellende Behörde ein Verfahren zur Verifikation des Dokuments anzubieten. Das Dokument hat einen Hinweis auf dieses Verfahren zu enthalten (§ 20 E-GovG). Sollte ein solcher Hinweis fehlen, so empfiehlt es sich, mit der ausstellenden Behörde in Kontakt zu treten.

Unter https://www.signature-verification.gv.at/ steht das Prüfservice in englischer Sprache zur Verfügung. Auch Prüfberichte lassen sich in englischer Sprache abrufen. Nützlich ist dies beispielsweise dann, wenn man ausländischen Stellen eine Prüfmöglichkeit für amtssignierte österreichische Dokumente (z.B. Zeugnisse) bieten will.

Für Organisationen, die die Signaturprüfung in automatisierte Arbeitsabläufe integrieren wollen, stellt die RTR eine SOAP-Schnittstelle bereit. Das Webservice steht kostenlos zur Verfügung. Voraussetzung für die Nutzung ist jedoch eine Authentifizierung mittels Benutzername und Passwort. Interessenten können Zugangsdaten und die Dokumentation des Webservice unter signatur@signatur.rtr.at anfordern.

## Vertrauensinfrastruktur

Jeder VDA, der qualifizierte Zertifikate ausstellt, hat eine Zertifikatsdatenbank zu führen, in der er die von ihm ausgestellten Zertifikate sowie (permanente) Widerrufe bzw. (temporäre) Aussetzungen von Zertifikaten erfasst. Nach österreichischem Recht muss die Zertifikatsdatenbank allgemein frei zugänglich sein. Die Abfrage der Zertifikatsdatenbank muss unentgeltlich und ohne Identifikation möglich sein (§ 5 Abs. 1 SVV).

Nach neueren Spezifikationen (z.B. PAdES, XAdES, CAdES) enthalten elektronische Signaturen als Zusatzinformation die zugehörigen Zertifikate, sodass diese bei der Prüfung der elektronischen Signatur nicht aus einer anderen Quelle abgerufen werden müssen. Allerdings ist gerade bei qualifizierten elektronischen Signaturen, die beispielsweise zum Unterschreiben von Verträgen verwendet werden, die langfristige Prüfbarkeit wichtig. Es muss daher auch weiterhin möglich sein, ältere elektronische Signaturen zu prüfen, die aufgrund ihrer Spezifikation das Zertifikat nicht enthalten. Ein Beispiel dafür ist die textuelle Variante des Signaturformats PDF-AS, die lediglich eine Referenz auf das der elektronischen Signatur zugrundeliegende Zertifikat vorsieht. In diesem Fall ermöglicht der Zugang zur Zertifikatsdatenbank, das zu einer elektronische Signatur gehörige Zertifikat abzurufen und mit dessen Hilfe die Gültigkeit der elektronischen Signatur zu prüfen.

Datenschutzrechtlich steht es jedem Nutzer zu, die Einwilligung zur Veröffentlichung seines Zertifikats zu verweigern und eventuelle Hürden bei der Prüfung elektronischer Signaturen in Kauf zu nehmen. In allen anderen Fällen sind jedoch qualifizierte Zertifikate nach geltender Rechtslage in der Zertifikatsdatenbank zu veröffentlichen. Entgegen anderslautenden Medienberichten liegt hierbei kein Datenleck vor.

Auch bei der Führung von Zertifikatsdatenbanken kommt der Aufsichtsstelle eine Rolle zu: Stellt ein qualifizierter VDA seine Tätigkeit ein, so hat er dafür Sorge zu tragen, dass seine Zertifikatsdatenbank von einem anderen qualifizierten VDA weitergeführt wird. Kommt er dieser Verpflichtung nicht nach, so hat die Aufsichtsstelle als Teil ihrer Vertrauensinfrastruktur für die Weiterführung der Zertifikatsdatenbank auf Kosten des qualifizierten VDA Sorge zu tragen.

## Ausblick

Derzeit erneuert die RTR ihre Infrastruktur für elektronische Signaturen. Das Ziel der Migration besteht nicht nur darin, die Hardware angesichts zunehmender Anforderungen aufzurüsten, sondern auch in der Schaffung zusätzlicher Redundanzen, um die permanente Verfügbarkeit der österreichischen Vertrauensliste weiterhin zu gewährleisten und Ausfälle des Prüfservice hintanzuhalten. Beim Prüfservice wird überdies eine neue Software-Version zum Einsatz kommen, die gegenüber der derzeit eingesetzten Software eine Reihe von Verbesserungen bringt.

NUTZERSCHUTZ

## Große Plage: Fake-SMS-Wellen zum Lieferstatus von Paketsendungen und zu Voicemails

Die Meldestelle für Rufnummernmissbrauch verzeichnet seit Wochen täglich unzählige Meldungen zu Fake-SMS. Ziel der Fake-SMS ist, die Empfängerinnen und Empfänger dazu zu verlocken, den im SMS enthaltenen Link anzuklicken und folglich zu schädigen.

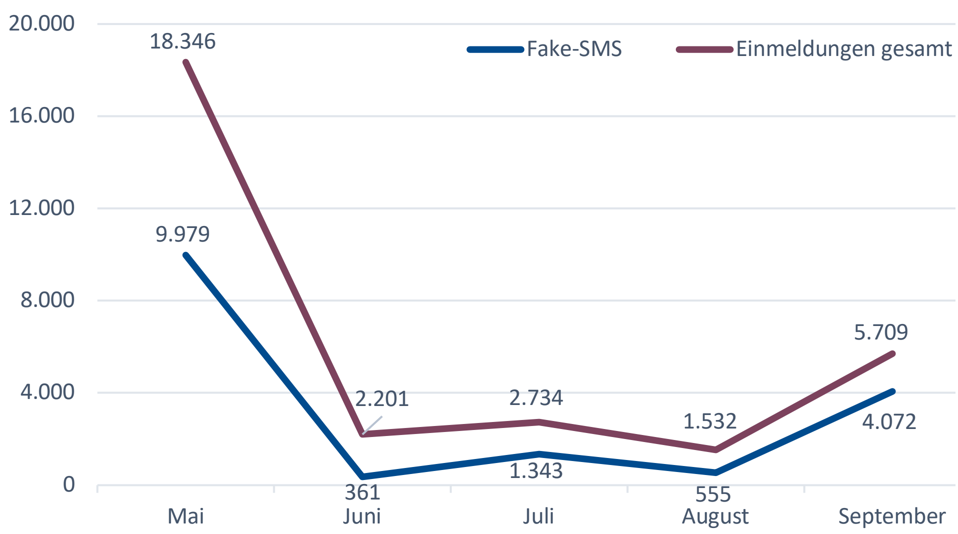
Beschwerden zu Fake-SMS explodieren!

Insgesamt mehr als 16.000 Meldungen zu Fake-SMS trafen im Zeitraum Mai bis September bei der Meldestelle für Rufnummernmissbrauch ein. Zwei inhaltliche Schwerpunkte kristallisierten sich dabei heraus:

**Variante 1:** Im SMS wird die bevorstehende Lieferung eines Paketes vorgetäuscht. Der enthaltene Link dient als Lockmittel, um durch Anklicken eine bösartige App auf die Handys zu schleusen.

**Variante 2:** Im SMS wird der Erhalt eines Voicemails vorgegaukelt, das angeblich über den mitgesendeten Link abrufbar ist.

Abbildung 2: Einmeldungen bei der Meldestelle für Rufnummernmissbrauch gesamt und zu Fake-SMS (Mai bis Septemeber 2021)



NUTZERSCHUTZ

## Ziel der Betrüger: Schadsoftware zu installieren, Daten auszuspähen, tausende SMS zu versenden

Durch das Lesen von Fake-SMS entstehen weder Kosten noch Schäden am Smartphone. Haarig könnte es allerdings in Folge werden: Klickt man den im SMS mitgeschickten Link an, wird man aufgefordert, eine App zu installieren. Folgt man dieser Aufforderung, hat man ein echtes Problem. Die App spioniert persönliche Daten (Kontakte, Bankdaten, etc) aus und übermittelt diese den Tätern.
In vielen Fällen werden vom infizierten Handy massenhaft SMS ins Ausland und ins Inland versendet, um den Link weiterzuverbreiten. Das kann wiederum dazu führen, dass die Handyrechnung explodiert.

## Schaden für Nutzerinnen und Nutzer, hoher Aufwand für Mobilfunkanbieter

Ist die „böse“ App einmal installiert, kann sie nur schwer entfernt werden. Man sollte jedenfalls unverzüglich beim Smartphone den Flugmodus aktivieren oder abschalten und sich umgehend an seinen Mobilfunkanbieter wenden. Diese unterstützen betroffene Kundinnen und Kunden bei der Entfernung der bösartigen App.

Von den drei großen Mobilfunkanbietern ist bekannt, dass sie auf ihren Websites umfassende Informationen und Tipps zur Verfügung stellen. Wir haben die Links auf unserer Website für Betroffene unter https://www.rtr.at/verdaechtige_rufnummernbereiche zusammengefasst.

## Wirksamste Prävention – ein „gesundes“ Misstrauen

Die Betrüger kalkulieren mit der Unvorsichtigkeit und der Neugier der Smartphone-Besitzer. Eine wirksamste Waffe gegen die Betrüger ist daher, SMS kritisch zu lesen und samt Link zu löschen. Seriöse Mobilfunkanbieter würden niemals verlangen, dass man eine dubiose App unbekannter Herkunft herunterlädt, sondern per Link auf den offiziellen App-Store verweisen. Erhält man SMS von unüblichen und ausländischen Rufnummern, ist immer Vorsicht geboten!

## Fake-SMS unter rufnummernmissbrauch.at melden

Absenderkennungen von SMS und Rufnummern, die missbräuchlich verwendet werden, können unter rufnummernmissbrauch.at bekannt gegeben werden. Damit können wir betrügerische Aktivitäten, die gehäuft auftreten, rasch erkennen und die Bevölkerung informieren.

INTERNATIONALES

# 3. BEREC Plenum 2021 stellt Weichen für 2022

Das 3. BEREC Plenum 2021 bzw. das 48. Plenum seit Gründung von BEREC fand zum ersten Mal seit Beginn der Covid-19-Pandemie wieder physisch (in Dubrovnik, Kroatien) statt und, um den Vertreterinnen und Vertretern möglichst aller Regulierungsbehörden die Teilnahme zu ermöglichen, zusätzlich auch virtuell.

Das 3. Plenum bringt jedes Jahr größere Neuerungen mit sich, denn es wird ein neues BEREC Board gewählt und der Entwurf des Arbeitsprogramms für das kommende Jahr verabschiedet.

## BEREC Vorsitz für 2023 geht an Griechenland

Im Jahr 2023 wird Konstantinos Masselos (EETT, Griechenland) den Vorsitz führen und als Incoming Chair 2022 an der Seite von BEREC Chair Annemarie Sipkes (ACM, Niederlande) und dem Outgoing Chair Michel Van Bellinghen (BIPT, Belgien) arbeiten. Zusätzlich zu den beiden frisch gewählten BEREC Vice-Chairs Emmanuel Gabla (ARCEP, Frankreich) und Pål Wien Espen (NKom, Norwegen - als Mitglied der Länder ohne Stimmrecht) wird auch Klaus M. Steinmaurer (RTR, Fachbereich Telekommunikation und Post) das BEREC Board ergänzen und damit die Interessen Österreichs aktiv einbringen können.


Quelle: BEREC

INTERNATIONALES

Unser Geschäftsführer zeigte sich sehr erfreut, im nächsten Jahr als Teil eines international besetzten Führungsteams die umfangreichen Arbeiten, die in BEREC anstehen, anzugehen und die auch für die RTR wichtigen Themen voranzutreiben. Zukunftsthemen wie Nachhaltigkeit oder die Regulierung digitaler Märkte, wo die RTR und BEREC im Gesetzgebungsprozessen gerne beratend zur Seite stehen, sind dabei genauso von Bedeutung wie Kernaufgaben, beispielsweise den Binnenmarkt zu fördern und eine harmonisierte Anwendung von Gesetzen sicherzustellen. Ein besonderes Anliegen ist Steinmaurer bei der gemeinsamen Arbeit auf europäischer Ebene, möglichst viel voneinander zu lernen und die Regulierungspraxis stetig zu verfeinern.

## BEREC Arbeitsprogramm 2022

Einen Ausblick auf die internationalen Arbeiten in 2022 bietet der Entwurf zum BEREC Arbeitsprogramm 2022, welches bis 5. November konsultiert wird. Mit insgesamt 49 Projekten ist der Vorschlag sehr umfangreich und gibt damit BERECs vielfältige Aufgaben und Tätigkeitsbereiche wieder. Ein besonderer Fokus der Arbeit wird im nächsten Jahr auf dem Erfahrungsaustausch zur weiteren Umsetzung des EECCs liegen, um eine möglichst einheitliche Regulierungspraxis in der EU zu ermöglichen. Damit fördert BEREC auch den Ausbau von Netzen und trägt dazu bei, dass die europäischen Konnektivitätsziele im Einklang mit Cybersicherheitsmaßnahmen und Nachhaltigkeitszielen erreicht werden.

Konnektivität

Im strategischen Bereich Konnektivität werden unter anderem jeweils ein Bericht zur 5G-Wertschöpfungskette und zur regulatorischen Behandlung von Geschäftskundenprodukten vorgeschlagen. Zwei Berichte widmen sich dem Thema Infrastruktur: einerseits die Eignung von Breitband per Satellitenverbindung für die Versorgung im Universaldienst und andererseits der Wettbewerb zwischen NGA-Betreibern in einem bestimmten geografischen Gebiet. Außerdem ist eine externe Studie geplant, in der die Marktverhältnisse für Telekomunternehmen ohne eigene Infrastruktur (MVNOs) untersucht werden.

Digitale Märkte

Zum Themenbereich der digitalen Märkte ist unter anderem ein Bericht zur Regulierung von digitalen Gatekeepern geplant. Zur Stärkung der Rechte von Endnutzerinnen und Endnutzern sind neben anderen Projekten auch ein Workshop zur digitalen Kluft (digital divide) und ein Bericht zu den besten Vorgehensweisen zur Sicherung des äquivalenten Zugangs und der äquivalenten Auswahl für Nutzerinnen und Nutzer mit Behinderungen.

Roaming

Wichtige Projekte wie die Anpassung der Roaming Guidelines angesichts der neuen Roaming-Verordnung, die Beschäftigung mit den EuGH-Urteilen im Bereich Netzneutralität und mit den State Aid Guidelines oder die Auseinandersetzung mit dem Thema Nachhaltigkeit im digitalen Sektor werden ebenfalls intensiv behandelt.

INTERNATIONALES

## Berichte aus den BEREC-Arbeitsgruppen: Neuerscheinungen

Unter den im Plenum beschlossenen Dokumenten finden sich wieder umfangreiche Berichte zu vielen verschiedenen Themen.

Studie zu COVID-19

Eine Studie zu den Auswirkungen von Covid-19 auf die digitale Kluft, die im Auftrag von BEREC von dem spanischen Beratungsunternehmen Iclaves durchgeführt wurde, enthält umfangreiche Analysen sowie mehrere Fallstudien aus unterschiedlichen BEREC-Mitgliedstaaten. Aufbauend auf den Studienergebnissen werden Empfehlungen für nationale Telekom-Regulierungsbehörden erarbeitet, welche diese nutzen können, um Maßnahmen zur Überbrückung der digitalen Kluft zu entwickeln. Die Studie wird auf der Website von BEREC in Kürze veröffentlicht.

Zu den Arbeiten zu OTT-Diensten und digitalen Plattformen wurden dieses Mal zwei Berichte veröffentlicht. Der Bericht zu OTT-Indikatoren enthält Empfehlungen, welche Indikatoren nationale Regulierungsbehörden heranziehen sollten, wenn sie Daten von nummernunabhängigen interpersonellen Kommunikationsdiensten erheben. Im BEREC Bericht zur ex ante Regulierung von digitalen Gatekeepern werden ex-ante Maßnahmen präsentiert, die den Wettbewerb in diesem Bereich sicherstellen soll. Dieser Bericht ist einer von bereits mehreren Inputs von BEREC, der in den Gesetzgebungsprozess zum Digital Markets Act (DMA) eingekippt wird.

Der BEREC-Bericht zur regulatorischen Handhabung von fixed und mobile Backhaul (die Anbindung der mobilen an die feste Telekom-Infrastruktur) vergleicht die Situation in den BEREC Mitgliedstaaten und präsentiert die Ergebnisse einer Umfrage unter den Telekomunternehmen. Dieser Bericht wird bis 5. November 2021 konsultiert.

Ein weiterer Bericht beschäftigte sich mit Entgelten von Drittanbietern auf Mobilfunk-Rechnungen. Der Ergebnisbericht gibt einen Überblick, wie die Mitgliedstaaten solche Entgelte im Sinne des Konsumentenschutzes handhaben. Vor der Implementierung des EECCs hatten einige nationale Regulierungsbehörden bereits Maßnahmen zu den beiden häufigsten Formen der Zahlungsabwicklung mit Drittanbietern, „Direct Carrier Billing“ und Mehrwertdienste, getroffen. Durch Preisregulierungen und Transparenz auf den Rechnungen wird die Position der Endkundinnen und Endkunden gestärkt.

Abschließend möchten wir auch auf den Call for Input zur Berücksichtigung der EuGH-Urteile in den BEREC-Leitlinien zur Open Internet Verordnung hinweisen. Feedback dazu kann bis 20. Oktober eingereicht werden.

VERANSTALTUNGEN

# Cloudification: Entwicklungen und aktuelle Themen

Eine Veranstaltung im Rahmen der Serie RTR Netz-Werk-Digital

Die dritte Veranstaltung aus der Serie RTR Netz-Werk-Digital wird am 14. Oktober 2021 stattfinden und ist dem Themenfeld „Cloudification – Entwicklungen und aktuelle Themen“ gewidmet. Wie alle Veranstaltungen aus der Reihe RTR Netz-Werk-Digital ist die als Online-Veranstaltung konzipiert und für eine Dauer von zwei Stunden angesetzt.

## Eckpunkte der Veranstaltung

| | |
|---|---|
| **Wann** | **14. Oktober 2021**, 15:00 – 17:00 Uhr |
| **Wo** | Virtuell via Zoom |

Link zur Veranstaltung und zur Anmeldung:
https://www.rtr.at/TKP/aktuelles/veranstaltungen/veranstaltungen/netz-werk-digital/cloudification.de.html

Clouds und Cloudification ist eines der großen Themen aktueller technologiepolitischer Diskussionen. Fakt ist, dass allein der weltweite Public Cloud Markt zwischen 2018 und 2021 (Prognose) von knapp unter 200 Mia US$ auf mehr als 310 Mia US$ anwachsen wird, ein Wachstum, das allen Prognosen nach auch in Zukunft ähnlich stark sein wird. Auch in Österreich verläuft die Entwicklung stürmisch. So berichtet etwa KPMG in ihrem Cloud Monitor 2021, dass aktuell etwa 32 Prozent der befragten Unternehmen in Österreich Public Cloud Services benutzen und ein ebenso großer Anteil plant, diese IT-Infrastruktur einzuführen. Cloud-Wachstum ist also auch in Österreich ein wesentliches Thema.

Um einen Überblick über die verschiedenen Arten von Clouds (Public, Private, Hybrid) und über die verschiedenen Diensteangebote, Anwendungsszenarien und globalen Trends zu bekommen, wird Frau Dr. Gull, Mitautorin vom Wissenschaftlichen Institut für Kommunikationsdienste (WIK) einen einführenden Vortrag halten.

Der zweite Vortrag ist dem Thema europäischer und österreichischer Cloudpolitik gewidmet. Was ist die Absicht der Europäischen Kommission hinter ihrer Cloud Politik – strategische Autonomie im Technologiebereich, Sicherheitsüberlegungen und/oder anderes? GAIA-X, eine Initiative, die zunächst von Deutschland und Frankreich gegründet wurde, nimmt zunehmend an Fahrt auf. Auch die Ö-Cloud, die vor wenigen Monaten offiziell gegründet wurde, soll einer dieser GAIA-X Hubs werden. Wir freuen uns, Herrn Horst Bratfisch (msg plaut austria) zu Ausführungen zu diesem Themenfeld begrüßen zu dürfen.

Im dritten Vortrag der Veranstaltung werden wir auf die Frage von Kooperationen großer Carrier mit Hyperscalern eingehen. Erst jüngst gingen Berichte einer neuen und umfassenden Kooperation zwischen Telekom Deutschland (T-Systems) und Google Cloud durch die Medien, mit der sog. „souveräne Cloudlösungen“ für

VERANSTALTUNGEN

verschiedene Sektoren (Logistik, Fertigung, Automobil, öffentlicher Bereich etc.) geschaffen werden sollen. Parallel dazu kooperiert die Telekom Deutschland etwa auch mit Microsoft, um besonders geschützte und sichere Cloud-Plattformen zu schaffen. Was sind nun die Überlegungen, die ein Unternehmen wie Telekom Deutschland zu Kooperationen mit Hyperscalern bewegen, was deren spezifische Vorteile und wie sieht die „Arbeitsteilung“ aus? Um diese und andere Fragen zu beleuchten, freuen wir uns auf die Ausführungen von Herrn Roland Fadrany, Partner von Detecon International.

Ein vierter Vortrag stellt das Thema Clouds von MNOs bzw. 5G ins Zentrum. Einige MNOs haben Teile ihre Cloudaktivitäten zur Erbringung von Endkundendiensten, aber auch verschiedene betriebliche Prozesse bis hin zu Leistungen des operativen Netzbetriebs an Clouddienste-Anbieter ausgelagert (z.B.: Vodafone an IBM, AT&T an Microsoft). Welche Cloud- Edge Strategie oder Herausforderungen sind für MNOs erkennbar, welcher Weg der richtige? Wo ist man gegebenenfalls zwingend auf Kooperationen mit Hyperscalern angewiesen (etwa KI)? Wir freuen uns auf einen Vortrag von Herrn Martin Lukas, Head of Network Virtualization & 5G bei Drei.

In einem fünften Beitrag stehen Clouddienste für Klein- und Mittelbetriebe sowie die öffentliche Verwaltung im Vordergrund. Gibt es eher individuelle Anforderungen von KMUs oder stehen dort eher Branchenlösungen zur Diskussion bzw. stehen Beratung und Systemintegration eher im Mittelpunkt? Welche Rolle spielt allenfalls ein Österreich-Bezug (Ö-Cloud) für ein entsprechendes Clouddiensteangebot? Für diese und weitere Themen im Zusammenhang Cloud und ISP-Lösungen konnten wir Herrn Alexandros Osyos, Leiter Produktmanagement bei next layer, gewinnen.

Die Veranstaltung wird durch eine Diskussion, in der die Experten wie auch das Publikum Fragen stellen können, abgerundet.

Nächste Veranstaltung: voraussichtlich im November

Für November ist eine vierte Veranstaltung aus der Serie RTR-Netz-Werk-Digital geplant. Über möglich Inhalte wird im Rahmen der Veranstaltung „Cloudification“ abgestimmt.

**RTR** AKTUELL 3/2021

## Autorinnen und Autoren

Die Beiträge der aktuellen Ausgabe von RTR AKTUELL 3/2021 des Fachbereichs Telekommunikation und Post wurden verfasst von:

Daniela Andreasch
Valerie Xenia Hafez
Ulrich Latzenhofer
Paul Pisjak
Klaus Steinmaurer