

BRANCHEAFTALE VEDR. SMS SENDER-ID BESKYTTELSE

mellem

Nuuday A/S
Teglholmegade 1,
2450 København SV
CVR-nr. 40075291
og

Telia Danmark, Filial af Telia Nättjänster Norden AB, Sverige
Ørestads Boulevard 45
2300 København S
CVR-nr. 20 36 79 97
I
og

Telenor A/S
Frederikskaj 8
2450 København SV
CVR-nr. 19433692
og
Hi3G Denmark ApS
Fadet 4
1799 København V
CVR-nr. 26123445

(hver for sig en "MNO" og i fællesskab "MNO'erne")

Baggrund

Baggrunden for nærværende brancheaftale (Aftalen) er at fastsætte fælles forpligtelser og retningslinjer for samarbejdet omkring etablering af SMS sender ID-beskyttelse (ID-beskyttelse) via en fælles ansøgningsproces hos Operator Clearing House (OCH) og formalisering af eksisterende samarbejde, der er påbegyndt med hhv. NemID og MitID, og skal dermed afdække det stigende behov for beskyttelse mod misbrug af virksomheders SMS sender ID (Sender-ID).

For at kunne opretholde beskyttelsen i ordningen, er det en forudsætning, at MNO'erne forpligter sig til at etablere beskyttelse i overensstemmelse med nærværende Aftale.

Aftalens formål og omfang

Formålet med Aftalen er at etablere afsender ID-beskyttelse for virksomheder, der ønsker at beskytte sine kunder imod spoofede SMS'er, med samme eller lignende Sender-ID som legitime SMS'er afsendt fra virksomheden via en aggregator.

Samarbejdet begrænser sig til ID-beskyttelse for virksomheder, myndigheder og organisationer, som er potentielle mål for spoofede SMS'er, og som selv har adgang til nummeropslag eller afsender deres SMS'er via en aggregator, der har adgang til nummeropslag.

Beskyttelsen iværksættes ved, at hver MNO indgår aftale med en aggregator med adgang til nummeropslag, om hvilken kilde, i form af SMS large account, der repræsenterer den legitime trafik, og derved samtidig definerer alle øvrige kilder som ikke-legitime kilder. Processen kan sammenlignes med computer firewalls, der arbejder med "allow" og "deny" regler.

ID-beskyttelse påkræver, at MNO'erne implementerer sikkerhedsforanstaltninger, der kontrollerer Sender-ID i den SMS-trafik, der sendes til MNO fra forskellige kilder. Oversigt over mulige kilder til SMS-trafik fremgår af bilag 4.

For at ID-beskyttelse skal fungere optimalt, bør antallet af legitime kilder begrænses, da flere mulige legitime kilder (large accounts) eksponerer en større risiko for beskyttelsen. Dette skal naturligvis afvejes med evt. ønske om alternative afsendelsesmuligheder for den afsenderbeskyttede kunde.

Proces for indgåelse af aftaler om ID-beskyttelse

Det er den ansvarlige aggregator/mobilselskab for kundeforholdet, der skal sikre og efterprøve at virksomheden, som anmoder om ID-beskyttelse, også er den retteadkomsthaver til det navn, der ønskes beskyttet.

Det er Virksomheden, der skal fremlægge dokumentation for adkomst til det ID, der søges beskyttet. Dokumentation kan eksempelvis være i form af udskrift fra Det Centrale Virksomhedsregister eller i form af varemærkeregistreringsbevis.

MNO afgør diskretionært, om der skal gennemføres ID-beskyttelse. MNO er således ikke forpligtet til at gennemføre ID-beskyttelse.

Virksomheden, der ønsker ID-beskyttelse, skal give en fuldmagt til den aggregator, der er ansvarlig for virksomhedens SMS-afsendelser. Fuldmagten indeholder en erklæring om, at virksomheden har rettighed til det Sender-ID, der ønskes beskyttet. Endvidere skal fuldmagten give aggregatoren tilladelse til at igangsætte ansøgningsprocessen.

I processen for opsætning af ID-beskyttelsen, anmoder aggregatoren på vegne af virksomheden om beskyttelse af Sender-ID, således at alene dette Sender-ID kan afsendes af virksomheden selv og samtidig blokeres fra alle andre kilder.

Aggregator kan henvende sig til enhver MNO der har tiltrådt brancheaftalen, som derefter initierer anmodning om forhåndsgodkendelse af det ønskede Sender-ID, der søges beskyttet. Det er en forudsætning for indsendelse af ansøgning om forhåndsgodkendelse, at aggregator har modtaget en fuldmagt fra virksomheden. Skabelon for ansøgning og fuldmagt fremgår af bilag 1 og bilag 2.

Når alle MNO'er har godkendt ansøgningen, kan aggregator henvende sig til sine kontaktpersoner hos hver MNO for indgåelse af aftale om ID-beskyttelse.

ID-beskyttelses service udbydes på de af MNO'en egne fastsatte vilkår.

En ansøgningsprocedure består af følgende skridt:

- 1) Aggregator/mobilselskab indhenter fuldmagt fra tegningsberettiget fra den virksomhed, der ønsker at opnå SenderID BESKYTTELSE (skabelon for fuldmagt fremgår af bilag)

- 2) Mobilselskabet indsender ansøgningskema via OCH (skabelon for ansøgningskema fremgår af bilag)
- 3) Ansøgningen går derefter automatisk til hvert mobilselskab til godkendelse. Selskaberne undersøger og vurderer i denne proces blandt andet, om det pågældende Sender ID, der skal beskyttes, bliver brugt som muligt legitimt Sender ID fra flere kilder og afsendere
- 4) Hvis alle mobilselskaber har godkendt ansøgningen, gives en positiv bekræftelse til ansøgende aggregator/mobilselskab
- 5) Aggregator skal på denne baggrund henvende sig til sin daglige kontakt hos MNO'erne for at implementere blokeringer samt fremsende fuldmagt som dokumentation.

Ansvar og konsekvenser

Aggregator skal i deres infrastruktur sikre sig, at kun den legitime afsender har mulighed for at sende SMS med det beskyttede Sender-ID og samtidig sikre, at alle andre tilsluttede virksomheder og samarbejdspartnere ikke kan fremsende SMS med det pågældende Sender-ID.

MNO skal sikre, at kun SMS'er afsendt af den pågældende aggregator med beskyttet Sender-ID kommer frem til modtageren, og alle andre mulige kilder blokeres af MNO.

Såfremt ID-beskyttelse etableres hos MNO, vil dette også betyde at den almindelige udveksling af trafik mellem MNO'erne også vil blive begrænset, så snart der er tale om et beskyttet Sender-ID.

Hvis der er uoverensstemmelse mellem oplysninger om nummerets tilhørsforhold på aggregator-siden, og en modtagers reelle kundeforhold er til en anden MNO, vil disse SMS'er, såfremt disse er afsenderbeskyttet, ligeledes blive afvist.

Blokering af ikke -legitim trafik sker efter best effort. MNO kan ikke holdes erstatningsansvarlig i tilfælde af, at blokering omgås eller der på anden vis fremsendes ikke legitime sms'er.

MNO kan ikke holdes erstatningsansvarlige for, at en Virksomheds ID-beskyttelse medfører, at en tredjeparts legitime sms'er bliver blokeret som følge af en Virksomheds ID-beskyttelse.

MNO'erne fraskriver sig ethvert ansvar for såvel direkte som indirekte tab og følgeskader hos Virksomhed eller tredjepart, herunder driftstab, tabt avance, tab af besparelser, og tab som følge af ID-beskyttelsen.

Tvister

Såfremt en aggregator ønsker at gøre indsigelse mod en afvisning af afsenderbeskyttelse for et specifikt Sender-ID i forbindelse med en ansøgningsproces, kan denne indsigelse indsendes til Teleindustrien, som vil behandle indsigelsen. MNO'erne er forpligtet til at følge Teleindustriens afgørelse.

Såfremt en tredjepart ønsker at gøre indsigelse mod en allerede iværksat afsenderbeskyttelse, kan dette gøres til Teleindustrien. Teleindustrien vil som første skridt i processen, på baggrund af den med indsigelsen medfølgende dokumentation, tage stilling til, om MNO'erne bør sætte ID-beskyttelsen i bero, indtil behandlingen af indsigelsen er afsluttet.

Teleindustrien bestræber sig på at træffe afgørelse herom indenfor 14 arbejdsdage.

I tilfælde af at en tredjepart får medhold, vil Teleindustrien orientere MNO om at ophæve blokering af det konkrete Sender-ID.

Teleindustrien træffer ikke afgørelser om navnetvister mellem en Virksomhed og en tredjepart. Såfremt en indsigelse fra tredjepart giver begrundet anledning til tvivl om parternes adkomst til Sender-ID, vil Teleindustrien orientere MNO om, at ingen af parterne kan opnå beskyttelse af Sender-ID.

Service Level Agreement (SLA)

MNO'erne forpligtiger sig til at behandle ansøgning om ID-beskyttelse indenfor 5 arbejdsdage.

Herefter kan aggregator henvende sig til de enkelte MNO'er, som forpligtiger sig til implementering af spærring indenfor 15 arbejdsdage efter at aftale mellem MNO og aggregator er indgået.

MNO'erne forpligtiger til at etablere beskyttelse af den eksakte SMS Sender-ID. Eventuel spærring af varianter af Sender-ID, eksempelvis. med eller uden mellemrum er op til den enkelte MNO, da dette kan være afhængig af systemmæssige kapaciteter.

Omkostninger

MNO'erne er enige om, at omkostningerne til etablering af fælles OCH-løsning fordeles ligeligt imellem parterne. MNO'erne forpligtiger sig ikke til yderligere omkostninger, idet de konkrete spærringsprocesser varetages af den enkelte MNO.

Ikrafttræden

Aftalen træder i kraft, når den er underskrevet af alle parter.

Aftalen tages op til revision ca. et år efter med henblik på at vurdere, om formål og omfang er dækket Aftalen, herunder om virkningen af løsningen har den ønskede effekt.

Hver aftalepart kan kræve nærværende Aftale genforhandlet, såfremt forudsætningerne for Aftalen er væsentligt ændret, eller der i øvrigt er rimelig grunde hertil, herunder som følge af ændringer af ændret lovgivning. Genforhandlingen skal påbegyndes senest to måneder efter anmodning herom er fremsat.

Opsigelse

Hver aftalepart kan opsiges Aftalen med 6 måneders varsel til udgangen af en måned.

Såfremt en part opsiger Aftalen, vil Aftalen tages op til revision af de øvrige parter, idet den aftalte ID-beskyttelse er betinget af Parternes fælles indsats.

Bilag

Bilag 1 – Ansøgningsskabelon til OCH

Bilag 2 – Fuldmagt fra virksomhed om ansøgning om SMS AFSENDER ID BESKYTTELSE

Bilag 3 – Definitioner

Bilag 4 – Teknisk beskrivelse – kilder til modtagelse af SMS

Underskrifter

For Nuuday A/S:

Dato:

Navn:
[Navn på underskriver]

Stilling:
[stillingsbetegnelse]

Navn:
[Navn på underskriver]

Stilling:
[stillingsbetegnelse]

For Telenor A/S:

Dato:

Navn:
[Navn på underskriver]

Stilling:
[stillingsbetegnelse]

Navn:
[Navn på underskriver]

Stilling:
[stillingsbetegnelse]

For: Telia Danmark, Filial af Telia Nättjänster Norden AB, Sverige

Dato:

Navn:
[Navn på underskriver]

Stilling:
[stillingsbetegnelse]

Navn:
[Navn på underskriver]

Stilling:
[stillingsbetegnelse]

For: Hi3G Denmark ApS

Dato:

Navn:
[Navn på underskriver]

Stilling:
[stillingsbetegnelse]

Navn:
[Navn på underskriver]

Stilling:
[stillingsbetegnelse]

**Bilag 1 Ansøgningskabelon til OCH
[separat dokument]**

**Bilag 2 Power of attorney regarding application for SMS SENDER ID PROTECTION
[separat dokument]**

Bilag 3 Definitioner

FORKORTELTSE	BESKRIVELSE
MNO	Mobile Network Operator. Betegnelsen for en netværksoperatør. I Danmark er disse : TRE, TDC, TELENOR & TELIA
MVNO	Mobile Virtual Network Operator. Betegnelsen for et teleselskab der ikke har eget radionetværk, men benytter radionetværket hos en eller flere MNO. En MVNO kan have egen SMS infrastruktur eller benytte en MNO's infrastruktur. Trafik fra MVNO homeroutes hos MNO der varetager radionetværket, og SMS beskeder fra en MVNO vil således blive beskyttet på lige fod med trafik der foretages fra MNO's egen infrastruktur.
SENDER ID	Det navn der præsenteres på modtagers mobiltelefon / enhed som afsender af SMS. Det kan bestå af op til 11 alfanumeriske tegn
AO-MT	Application Originated – Mobile Terminated. Den tekniske betegnelse for en SMS besked der afsendes maskinelt og termineres (leveres) til en mobiltelefon/enhed.
A2P SMS	APPLICATION TO PERSON – betegnelse for en maskinafsendt SMS der afleveres til en personlig enhed
P2P SMS	PERSON TO PERSON – betegnelsen for almindelig SMS trafik mellem to personer – denne trafik er ikke omfattet af denne aftale.
INTERWORKING	Interworking er betegnelsen for SMS trafik der foretages mellem operatører (nationale eller internationale), hvor der er indgået en aftale om bilateral aftale om trafikudveksling af A2P trafik. En sådan aftale vil som udgangspunkt tillade at der kan sendes SMS med Alfanumeriske Afsendernavne til den modtagende MNO
INTERCONNECT	Interconnect er betegnelsen for helt almindelig udveksling af P2P sms mellem operatører. Da denne trafik kun omfatter sms sendt fra mobilnumre, vil der ikke kunne afsendes Alfanumeriske Afsendernavne mellem operatører med en sådan aftale
AGGREGATOR	En aggregator fungerer som bindeled mellem MNO og 3 parts kunder / brands ved at indgå aftaler om SMS afsendelser med en eller flere MNO. Aggregatører har som udgangspunkt forbindelse til samtlige danske MNO for at kunne sikre levering af SMS til alle mobilkunder i DK
OCH	

Bilag 4 Teknisk beskrivelse – kilder til modtagelse af SMS

En MNO kan modtage A2P SMS fra følgende kilder:

Internationale Operatører

SMS hubs

Nationale Operatører

SMS Gateway / SMS platforme der drives af MNO

Aggregatorer (kan også have flere led udad)

