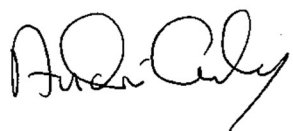


Datum: 2022-03-07

Utlåtande

Utlåtande – MÅL NR 4107–21 – Laglighetsprövning
av beslut avseende resesystem för Kalmar Länstrafik

Version 1.0



André Catry



CATRY
consulting

1. Utredning

Utredningen syftar till att:

- Klargöra Microsofts tillgång till personuppgifter i klartext vid tillhandahållande av Azures molntjänster för Kalmar Länstrafiks resesystem.
- Påvisa hur vissa regler i amerikansk rätt och deras tillämpning specifikt FISA 702, EO 12333, SCA (CLOUD Act) och NSL träffar det amerikanska bolaget Microsoft samt hur Microsoft får kommunicera att det sker.
- Analys av Region Kalmar åberopad statistik av utlämnanden som sker med stöd av amerikansk lagstiftning till amerikanska myndigheter.

1.1. Utredare

André Catry

Catry Consulting AB

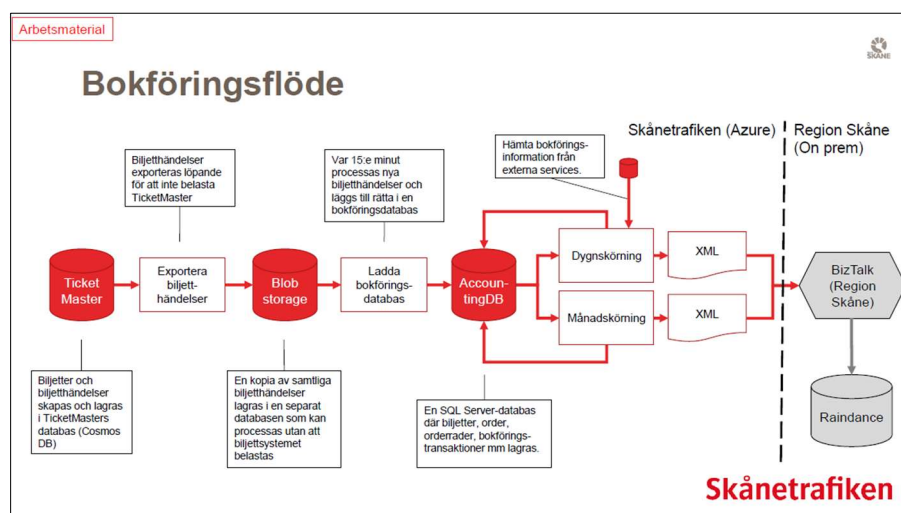
1.2. Beställare

Johan Roos Tibbelin

2. Microsofts tillgång till personuppgifter i klartext i resesystemet.

Det system som analysen omfattar är Skånetrafikens resesystem (fortsättningsvis benämnd systemet), vilket är det system som Region Kalmar anger att de avser ta i bruk. Systemet är ett resesystem som utvecklats i samverkan mellan Skånetrafiken, Blekinge Länstrafik och Östgötatrafiken. Den tekniska plattformen för tillhandahållande av systemet är Azure som leverans i form av en molntjänst¹ av Microsoft. Utredningen har använt sig av i ärendet ingivna handlingar som underlag för systembeskrivning.

Figur 1 visar på delar av arkitekturen för systemet.



Figur 1 beskrivning från Växjö FR 4107–21 Aktebil 16, Komplettering från motpart

2.1. Kryptering och pseudonymisering för skydd av personuppgifter i systemet

Metoden som används för analys baseras inte på djupgående studie av krypteringsfunktioner. Den tekniska utredningen visar på att det i detta fall är tillräckligt att observera resultatet av skyddsåtgärderna som Region Kalmar hävdar används för att skydda personuppgifterna i systemet.

2.1.1. Region Kalmar påstår följande

Systemet använder kryptering och pseudonymisering som skydd för personuppgifter på en teknisk nivå som inte medger åtkomst av personuppgifter i systemet för leverantören Microsoft och därmed kan de amerikanska myndigheterna inte ta del av personuppgifter i klartext från systemet genom att begära ut personuppgifter från Microsoft.

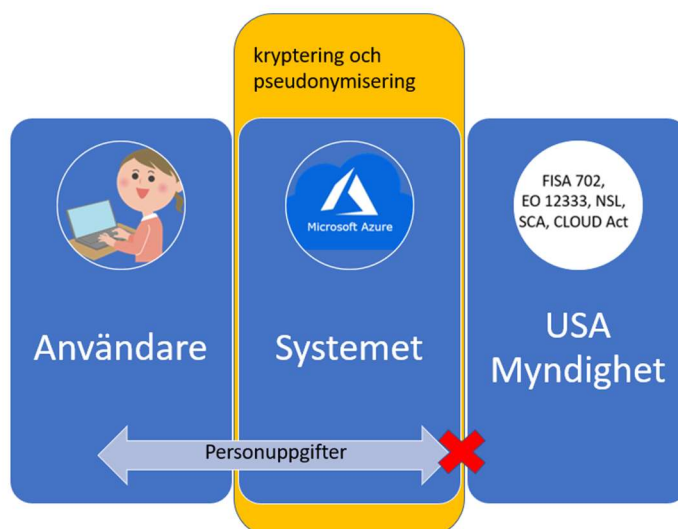
¹ Microsoft utvecklar, underhåller, övervakar och tillhandahåller tjänsten från egna lokaler och på utrustning som är helt under Microsofts fysiska och logiska kontroll.

2.1.2. Johan Roos Tibbelin påstår följande

Även om systemet använder kryptering och pseudonymisering som skydd för en del personuppgifter sker det på en teknisk nivå som ändå medger åtkomst av personuppgifter i systemet för leverantören Microsoft och därmed kan även de amerikanska myndigheterna få del av personuppgifter i klartext från systemet genom att begära ut dessa från Microsoft.

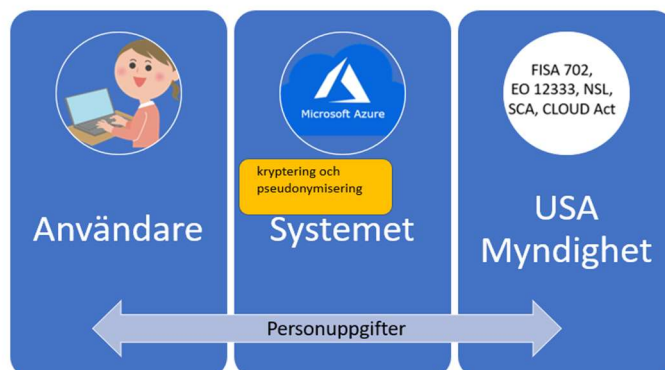
2.1.3. Hypoteser

Hypotes A som Region Kalmar framför är att Microsoft inte kan få tillgång till personuppgifter i klartext i systemet, och därmed kan amerikanska myndigheter inte heller få dessa uppgifter i klartext.



Figur 2 Personuppgifter skyddas av kryptering och pseudonymisering

Hypotes B som Johan Roos Tibbelin framför är att Microsoft kan få tillgång till personuppgifter i klartext i systemet och därmed kan också amerikanska myndigheter få dessa uppgifter utlämnade i klartext.



Figur 3 Personuppgifter skyddas inte av kryptering och pseudonymisering

För att pröva att falsifiera hypoteserna genomförs en teknisk utredning av systemet för att observera om det förekommer personuppgifter i klartext som hanteras i systemet.

2.2. Analys

Den tekniska utredningen (se 5.1 sidan 20) visar att det förekommer personuppgifter som hanteras i klartext i systemet. Eftersom resenären själv kan ta del av sina egna uppgifter i klartext direkt från systemet följer med nödvändighet att dessa också behandlas i klartext i systemet. Av det följer att leverantören har samma åtkomstmöjlighet till uppgifterna, och alltså kan lämna ut dem i klartext till amerikanska myndigheter.

Biljettsystemet behandlar inte personuppgifter i krypterat tillstånd. Förvisso används transportkryptering och det innebär att den som har möjlighet att avlyssna kommunikationen som sker mellan biljettsystemet och resenärens webbläsare inte med rimliga resurser kommer kunna bryta igenom skyddet och ta del av de uppgifter som överförs. Här har emellertid leverantören, i egenskap av en av de kommunicerande parterna, tillgång till uppgifterna i klartext.

Överföring av personuppgifter är enligt artikel 4.2 GDPR också är en behandling av personuppgifter och därmed är det utrett att leverantören Microsoft behandlar personuppgifter i systemet i klartext när de till användaren överför dessa uppgifter, oavsett i vilken form de i övrigt behandlas.

Den information som tillhandahålls från molntjänsten bär inga spår av att vara pseudonymiserad, utan uppgifterna kan i sin helhet tillskrivas den fysiska person som registrerats.

2.3. Slutsats

Den kryptering och pseudonymisering som enligt Region Kalmars uppgifter möjligen används inom systemet utgör inget hinder för att leverantörens åtkomst till personuppgifter i klartext i systemet. Av detta följer att den kryptering och pseudonymisering som möjligen används inte heller utgör något hinder för att leverantören Microsoft ska kunna lämna ut dessa personuppgifter i klartext på begäran av amerikanska myndigheter.

Biljettsystemet, så som det avses användas, faller därför inom ramen för användningsfall nummer 6 i EDPB:s vägledning².

² https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf

3. Vissa regler i amerikansk rätt och deras tillämpning

I detta förklaras hur vissa regler i amerikansk rätt och deras tillämpning specifikt *Foreign Intelligence Surveillance Act* (FISA) sektion 702, *Executive Order* (EO) 12333, *Stored Communications Act* (SCA) kompletterad med *The Clarifying Lawful Overseas Use of Data Act* (CLOUD Act) samt *National Security Letters* (NSL) träffar det amerikanska bolaget Microsoft samt hur Microsoft får kommunicera att utlämnade enligt dessa rättsakter sker.

Att genomlysna hela den amerikanska lagstiftning på området är en grannliga uppgift.

Angreppssättet jag valt för detta utlåtande är att belysa de områden som Region Kalmar själva hänvisar till i ärendet samt de uppgifter i förhållande till detta som Microsoft publicerat på sin hemsida.

Microsoft delar upp sin rapportering i två huvudområden. Nämligen *Law Enforcement Requests Report*³ (rättsvårdande) och *US National Security Orders Report*⁴ (underrättelsetjänst).

Det är viktigt att särskilja områdena rättsvårdande och underrättelsetjänst då olika restriktioner och sekretess gäller för dessa. FISA 702, EO 13222 och NSL är amerikansk underrättelselagstiftning som främst avser underrättelsetjänst. CLOUD Act, som inte är en övervakningslagstiftning⁵, används främst av rättsvårdande myndigheter.

Det som är av betydelse för denna analys är amerikanska myndigheters möjlighet att via domstols eller andra myndighetsbeslut begära ut information från Microsoft.

3.1. *Law Enforcement Requests Report* (rättsvårdande)

Den information som inkluderas i dessa rapporter är förfrågningar som Microsoft får från brottsbekämpande myndigheter runt om i världen.

³ <https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report>.

⁴ <https://www.microsoft.com/en-us/corporate-responsibility/us-national-security-orders-report>.

⁵ Man bör särskilja de olika tvångsmedel som användes och dess syfte. Tex begäran om **utlämning** av vissa uppgifter som redan finns jmf med en begäran om kontinuerlig utlämnade dvs **övervakning** av information eller kommunikation till/från ett visst konto.

3.1.1. CLOUD Act

Det som CLOUD Act främst tillförde SCA⁶ var det uttalade kravet i 18 U.S. Code § 2713⁷ som befäster att lagen är tillämplig för data utanför USA⁸. Lagstiftningen är därmed extraterritoriell.

Kravet på utlämnade enligt 18 U.S. Code § 2703⁹ till Microsoft kan komma i form av en *warrant*¹⁰ från en domstol eller en *governmental entity*¹¹.

Enligt de amerikanska myndigheterna så förändrar inte CLOUD Act i sig inte tillämpningen av amerikansk lag¹².

3.1.2. Bestrida beslut och meddela kund

Microsoft har under vissa omständigheter rätt att bestrida beslutet vilket Microsoft påstår att de alltid gör. Någon dokumentation som visar på att Microsoft de facto agerar så finns dock inte.

Enligt Microsoft själva hade de fram till 2016 sammanlagt lämnat in 4 stämningsansökningar¹³.

I en av dessa 4 stämningsansökningar grundar de sina på följande: *“Under de senaste 18 månaderna har den amerikanska regeringen krävt att vi behåller sekretess angående 2 576 juridiska krav, vilket i praktiken har tystat Microsoft att meddela kunder om husrannsakan eller andra juridiska processer som söker deras data. Noterbart och till och med överraskande innehöll 1 752 av dessa sekretessorder, 68 procent av det totala antalet, inget fast slutdatum alls. Detta innebär att vi i praktiken för alltid är förbjudna att berätta för våra kunder att regeringen har erhållit deras data.”*¹⁴(min översättning)

Det ovan redovisade ger inte en bild av att Microsoft skulle bestrida samtliga krav. Därav följer också att Microsoft, när de får krav på utlämnande av uppgifter, ofta

⁶ 18 U.S. Code Chapter 121 - STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS - <https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121>

⁷ 18 U.S. Code § 2713 - Required preservation and disclosure of communications and records

⁸ disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.

⁹ 18 U.S. Code § 2703 - Required disclosure of customer communications or records

¹⁰ Jmf med en husrannsaktionsorder.

¹¹ the term “governmental entity” means a department or agency of the United States or any State or political subdivision thereof

¹² Does the amendment of the Stored Communications Act in the CLOUD Act create new authority for U.S. law enforcement to obtain information? No. The clarification of the Stored Communications Act in the CLOUD Act restores certainty under United States law to ensure its consistency with long-standing practice källa: <https://www.justice.gov/dag/page/file/1153466/download>

¹³ <https://blogs.microsoft.com/on-the-issues/2016/04/14/keeping-secrecy-exception-not-rule-issue-consumers-businesses/>

¹⁴ <https://s3.documentcloud.org/documents/2803526/ECPA-Complaint.pdf>

får kravet tillsammans med en s.k. gag order¹⁵ enligt 18 U.S.C. § 2705(b) som förhindrar Microsoft att meddela kunden om ordern.

3.2. *US National Security Orders Report* (underrättelsetjänst)

Den information som Microsoft presenterar under detta huvudområde delas upp på två underdelar.

1. *Foreign Intelligence Surveillance Act (FISA) Orders*
2. *National Security Letters (NSL)*

Microsofts webbsida¹⁶ är otydlig då data och fakta presenteras om både FISA 702 och NSL (*National Security Letters*) om vart annat. Det är svårt att i texten avgöra när FISA eller NSL avses. Dessa är olika lagar med olika regelverk som styr sekretessen.

Som exempel så anges det i löpande text på en sida att *"We have successfully challenged requests in court, and will continue to do so, when we believe there are reasonable grounds for a challenge."* Det är korrekt att Microsoft vid ett tillfälle som är känt bestridit en (1) NSL order¹⁷. Dock finns det inget som tyder på att Microsoft någonsin bestridit en FISA 702 order.

Nedan är två citat från Microsofts webbsida som belyser några problemen som FISA 702 och NSL ger Microsoft.

"Current law prohibits recipients of FISA orders from ever disclosing the existence of a FISA order."

"US law prohibits us from disclosing more specific information regarding national security legal demands including FISA orders and NSLs. Microsoft disagrees with these laws and believes that greater transparency is critical to maintaining trust in the rule of law. Both in courts and in Congress, Microsoft has a long and successful history of advocating for additional transparency, and we are committed to working with policy makers to continue expanding our ability to provide more meaningful information to the public."

Vad avser statistik för amerikanska övervakningslagstiftningar som Microsoft får publicera är dessa omgärdade med kraftiga restriktioner på grund av amerikansk sekretess.

3.2.1. *Foreign Intelligence Surveillance Act (FISA) Orders*

FISA skiljer mellan amerikanska och utländska medborgare. Medan amerikanska medborgares rätt till privatliv skyddas av USA:s konstitution gäller detta skydd inte

¹⁵ Sekretess

¹⁶ <https://www.microsoft.com/en-us/corporate-responsibility/us-national-security-orders-report>

¹⁷ <https://blogs.microsoft.com/on-the-issues/2014/05/22/new-success-in-protecting-customer-rights-unsealed-today/>

för utländska medborgare. Utländska medborgare har således inga bindande rättigheter som kan göras gällande mot amerikanska myndigheter, vilket innebär att enskilda inte har någon rätt till effektiva rättsmedel i USA¹⁸.

FISA är indelad i titlar, som var och en innehåller avsnitt, som specificerar medel, krav och begränsningar för insamling av utländsk underrättelseinformation:

- 1) FISA Probable Cause Authorities (warrant)
 - a) Title I concerns electronic surveillance
 - b) Title III applies to physical searches,
 - c) Title VII applies to various forms of collection concerning U.S. persons located outside the United States located outside the United States,
 - i) Section 703, U.S. person who is reasonably believed to be located outside the United States.
 - ii) Section 704, U.S. person reasonably believed to be located outside the United States under circumstances in which the U.S. person has a reasonable expectation of privacy
- 2) FISA Section 702 (*Certification*)
- 3) FISA Title IV – Use of Pen Register and Trap and Trace (PR/TT) Devices (warrant)

Requires individual FISC order to use PR/TT device to capture dialing, routing, addressing, or signaling (DRAS) information.
- 4) FISA Title V – Business Records (warrant)

FISA¹⁹ beslut kan enligt ovan delas upp i 2 huvuddelar, inhämtning som sker med:

1. *Certification* – Inhämtning som sker inom ramen för ett intresseområde, certifikat.
2. *Warrant* – Inhämtning som sker efter domstolsbeslut från FISC.

Det är främst FISA Section 702 (Certification) som vi benämner FISA 702 som är intressant för laglighetsprövningen.

¹⁸ Court of Justice of the European Union in Case C-311/18

¹⁹ <https://www.govinfo.gov/content/pkg/BILLS-110hr6304pcs/html/BILLS-110hr6304pcs.htm>

3.2.1.1. FISA 702 Certification

För inhämtning av via *Certification* så baseras detta på beslut från *Intelligence Surveillance Court* (FISC) som godkänner de certifikat som tas fram av justitieministern (*Attorney General*, AG) och chefen för nationella underrättelsetjänsten (*Director of National Intelligence*, DNI). Dessa ansöker årligen om att FISC ska godkänna aktuella *Certifications*.

Certification som ska godkännas av FISC avser inte enskilda personer utan gäller intresseområden av uppgifter som ska samlas in av underrättelsemyndigheterna.

FISC beslutet omfattar ett antal intresseområden som tydliggörs genom en hemlig bilaga benämnd EXHIBIT F (Figur 4 och Figur 5). Det finns idag tre kända²⁰ intresseområden samt ett osäker:

1. *The foreign government groups that are the subject of Certification* - A
2. *Targeting Directed at Foreign Terrorist Groups Certification* – B
3. *Targeting Directed at Persons, Groups and Entities Involved in the Proliferation of Weapons of Mass Destruction, Advanced Conventional Weapons, Disruptive Technologies and their Deliver Systems – Certification* – C
4. *Cyber Threats Certification* – D (Osäkert)²¹

ODNI (*Office of the Director of National Intelligence*) publicerar sedan 2014²² en årlig en rapport där antalet FISA 702 Orders anges²³.

Det är just med stöd av *Certification A* som NSA och CIA kan inhämta information från Microsoft via selektorer såsom politiker_n@regionkalmar.se, tenant saabgroup.com, 'all_epost'@regeringen.se och telefonnummer.

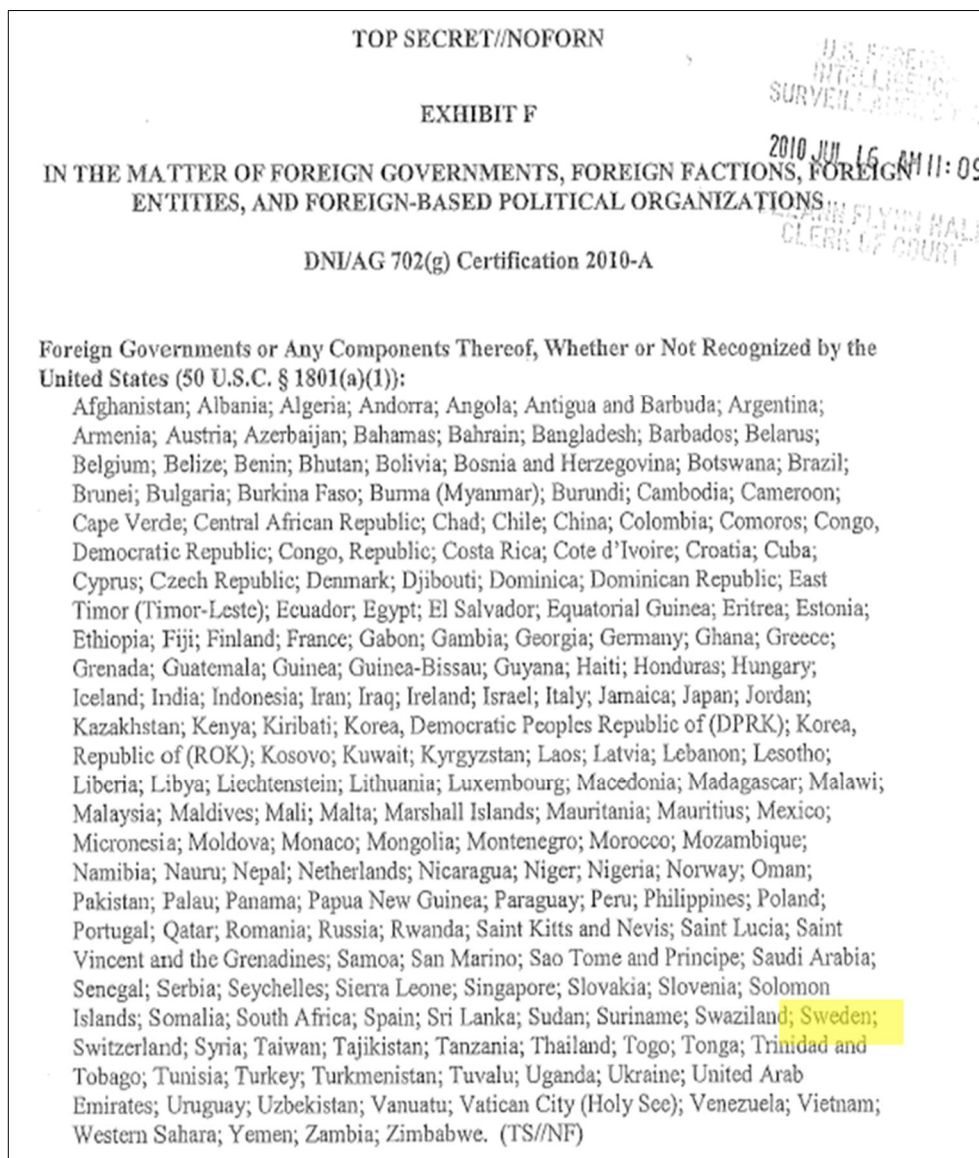
²⁰ Dokument som läcktes av Edward Snowden.

²¹ <https://cryptome.org/2015/06/cyber-spy-nyt-15-0604-2.pdf>

²² https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2013

²³ <https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2021/item/2210-statistical-transparency-report-regarding-national-security-authorities-calendar-year-2020>

Sverige, Norge, Finland och Danmark som nationer omfattas av *Certification A* (Figur 4). Även svenska bolag ingår här. Det ger därmed NSA möjlighet att spionera på dessa nationer och dess bolag.



Figur 4 Nationer angivna

Det är bara Canada, Storbritannien, Australien och Nya Zeeland som inte är uppräknad bland de erkända nationerna. De tillhör samarbetet FIVE EYES²⁴. Dock

²⁴ FIVE EYES ett underrättelsesamarbete, <https://www.dni.gov/index.php/ncsc-how-we-work/217-about/organization/icig-pages/2660-icig-fiorc>

så listas en hel del andra organisationer såsom EU, FN, Världsbanken osv också som legitima mål (Figur 5).



Figur 5 namngivna organisationer

NSA kan med stöd av FISC-beslutet (*Certification*) vända sig till Microsoft med order om "förelägganden som uppmanar leverantörer av elektroniska kommunikationstjänster att tillhandahålla all teknisk assistans som krävs för att genomföra den auktoriserade utländska underrättelseinsamlingen"²⁵. Just detta beslut finns det enligt FISA 702 en möjlighet att bestrida²⁶. Bolaget Yahoo försökte 2008 bestrida just en sådan FISA 702 order²⁷. Detta resulterade i en order från FISC som innebar att det kostade Yahoo 250 000 dollar per dag som de inte följde FISA 702 ordern²⁸.

Det finns en legal möjlighet för Microsoft att överklaga ordern från AG eller DNI att ansluta sig. Dock så kan man på goda grunder anta att Microsoft är ansluten till FISA 702 då Microsoft regelbundet publicerar FISA 702 statistik. Det kan noteras att enligt NSA dokument²⁹ anslöt sig Microsoft till underrättelseprogrammet PRISM den 11 september 2007 vilket är före den 10 juli 2008 då FISA Amendments Act of (FISA 702) antogs³⁰.

²⁵ immediately provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition; se FISA section 702

²⁶ (4) Challenging of directives.-- ``(A) Authority to challenge.--An electronic communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition to modify or set aside such directive with the Foreign Intelligence Surveillance Court, which shall have jurisdiction to review such petition. Se FISA section 702.

²⁷ <https://www.inc.com/associated-press/us-threatened-yahoo-with-huge-fines.html>

²⁸ <https://www.theguardian.com/technology/2013/jul/11/yahoo-wants-fisa-objections-revealed>

²⁹ www.dni.gov/files/documents/Facts%20on%20the%20Collection%20of%20Intelligence%20Pursuant%20to%20Section%20702.pdf och <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>

³⁰ <https://www.congress.gov/bill/110th-congress/house-bill/3773/text>

Microsoft förneka att NSA har direkt access till deras system, de förnekar dessutom att de var anslutna till underrättelseprogrammet PRISM³¹. Det finns ett dokument från NSA som bekräftar existensen av underrättelseprogrammet PRISM samt beskriver³² teknisk anslutning. Vilket också är det ord som idag används av USA ”*provide any technical assistance necessary*”³³. Figur 6 visar ytterligare ett dokument från NSA som på en arkitektturnivå beskriver anslutning till FISA 702 övervakningssystemen³⁴ PRISM, BLARNEY, FAIRVIEW, STORMBREW och OAKSTAR.

³¹ <https://blogs.microsoft.com/datalaw/our-practices/#did-participate-in-prism-program>

³² www.dni.gov/files/documents/Facts%20on%20the%20Collection%20of%20Intelligence%20Pursuant%20to%20Section%20702.pdf

³³ FISA; orders directing electronic communication service providers to provide any technical assistance necessary to implement the authorized foreign intelligence collection; : källa <https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2021/item/2210-statistical-transparency-report-regarding-national-security-authorities-calendar-year-2020>

³⁴ <https://cryptome.org/2015/06/cyber-spy-nyt-15-0604-2.pdf>



Figur 6 FISA 702 tekniskanslutning

3.2.2. Omfattning av FISA 702 övervakning

För att förstå omfattningen av övervakning som genomförs via FISA 702 kan man studera de rapporter "Annual Statistical Transparency Report"³⁵ som "Office of the Director of National Intelligence" (fortsättningsvis benämnd rapporten) årligen publicerar. Publiceringen sker med lagstöd i 50 U.S.C. § 1873(b).

I Figur 7 (Figure 3 i rapporten) visas att all underrättelseinhämtningen enligt FISA 702 för ett år normalt sker under en (1) FISC order.

³⁵ <https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2021/item/2210-statistical-transparency-report-regarding-national-security-authorities-calendar-year-2020>

Figure 3: Section 702 Orders

Section 702 of FISA	CY2018	CY2019	CY2020
Total number of orders issued	1	2*	1

See 50 U.S.C. § 1873(b)(2).
*This number includes (a) the FISC order dated September 4, 2019, which authorized the amended 2018 certifications and made public on October 8, 2019, and (b) a FISC order dated December 6, 2019, which authorized the 2019 certifications. The number does not include the FISC-R order, dated July 9, 2019, and made public on October 8, 2019, because the FISC-R order did not authorize any certifications.

Figur 7 Annual Statistical Transparency Report - Office of the Director of National Intelligence – April 2012

I Figur 8 (Figure 4 i rapporten) visas att det för år 2020 var det 202 723 Targets (non-UPS³⁶) som träffades under en (1) FISC order.

Figure 4: Section 702 Targets (recall that only non-USPs are targeted)

Section 702 of FISA	CY2018	CY2019	CY2020
Estimated number of targets of such orders	164,770	204,968	202,723

See 50 U.S.C. § 1873(b)(2)(A).

Figur 8 Annual Statistical Transparency Report - Office of the Director of National Intelligence – April 2012

Ett **Target** (Mål) har i detta sammanhang en specifik definition och definieras såsom:

”TARGET. Inom den amerikanska underrättelsegemenskapen (*Intelligence Community*’s, IC) har termen ”target” flera betydelser. Med avseende på statistiken i denna rapport används termen ”target” som ett substantiv och definieras som individuell person, grupp, entitet som består av flera individer eller *foreign power* som använder en *selector*, t.ex. ett telefonnummer eller e-postadress, som är föremål för insamling.”³⁷ (min översättning)

Enligt definitionen ovan är det tydligt att en *target* kan vara allt ifrån en individ till en hel nation. Detta medför att siffran 202 723 *targets* för år 2020 inte på något enkelt sätt går att översätta till antal individer som övervakats.

En *selector* är något som unikt identifierar ett *target* vilket också ger att ett angivet antal *selector* inte på något enkelt sätt går att översätta till antal individer som övervakats.

3.3. Microsoft Redovisad statistik

Vad avser statistik för amerikanska övervakningslagstiftningar som Microsoft får publicera är dessa omgärdade med kraftiga restriktioner på grund av amerikansk sekretess.

³⁶ non-U.S. person

³⁷ TARGET. Within the IC, the term “target” has multiple meanings. With respect to the statistics provided in this report, the term “target” is used as a noun and defined as the individual person, group, entity composed of multiple individuals, or foreign power that uses a selector, e.g., a telephone number or email address, subject to collection.

Microsoft har rätt enligt 50 U.S. Code § 1874³⁸ att publicera vissa data för bland annat NSL order.

Som framgår av 3.2.2 sidan 14 finns det för FISA 702 bara en order att redovisa. Hur detta hanterats i den redovisning som Microsoft visar för FISA 702 framgår inte³⁹.

Microsoft anger att det är följande data som inkluderas i FISA redovisningen.

*”Q: How does Microsoft define a FISA order seeking disclosure of content?
A: This category would include any FISA electronic surveillance orders (50 U.S.C. § 1805), FISA search warrants (50 U.S.C. § 1824), and FISA Amendments Act directives or orders (50 U.S.C. §1881 et seq.) that were received or active during the reporting period.”*⁴⁰

*”Q: How does Microsoft define a FISA order requesting disclosure of noncontent?
A: This category would include any FISA business records (50 U.S.C. § 1861), commonly referred to as 215 orders, and FISA pen register and trap and trace orders (50 U.S.C. § 1842) that were received or active during the reporting period.”*⁴¹

För inhämtning/övervakning av data anges följande paragrafer:

- *FISA electronic surveillance orders (50 U.S.C. § 1805)*
- *FISA search warrants (50 U.S.C. § 1824)*
- *FISA Amendments Act directives or orders (50 U.S.C. §1881 et seq.)*

För inhämtning av kontouppgifter anges följande paragrafer:

- *FISA business records (50 U.S.C. § 1861)(FISA 215)*
- *FISA pen register and trap and trace orders (50 U.S.C. § 1842)*

Det som är uppenbart är att *FISA Electronic surveillance authorization without court order (50 U.S.C. § 1802)* saknas i listorna ovan. Vad detta har för betydelse för den samlade statistiken går inte att kvantifiera då data saknas.

Enligt 50 U.S. Code § 1874 *Public reporting by persons subject to orders* så kan Microsoft publicera antal *Orders seeking disclosure of content*, det är svårt att

³⁸ 50 U.S. Code § 1874 - Public reporting by persons subject to orders: <https://www.law.cornell.edu/uscode/text/50/1874>

³⁹ <https://www.microsoft.com/en-us/corporate-responsibility/us-national-security-orders-report>

⁴⁰ <https://blogs.microsoft.com/datalaw/our-practices/#how-does-microsoft-define-fisa>

⁴¹ <https://blogs.microsoft.com/datalaw/our-practices/#how-microsoft-define-fisa-request-disclosure>

omsätta det till ett antal då *Office of the Director of National Intelligence* i sin rapport anger antalet order till ett (1).

I 50 U.S. Code § 1874 som är den lagstöd för Microsofts publicering av FISA data används begreppet *customer selectors targeted*. Ser man till hur *selectors* och *target* definieras (3.2.2 sidan 14) så kan det omfatta en individuell person, grupp, entitet som består av flera individer eller *foreign power*.

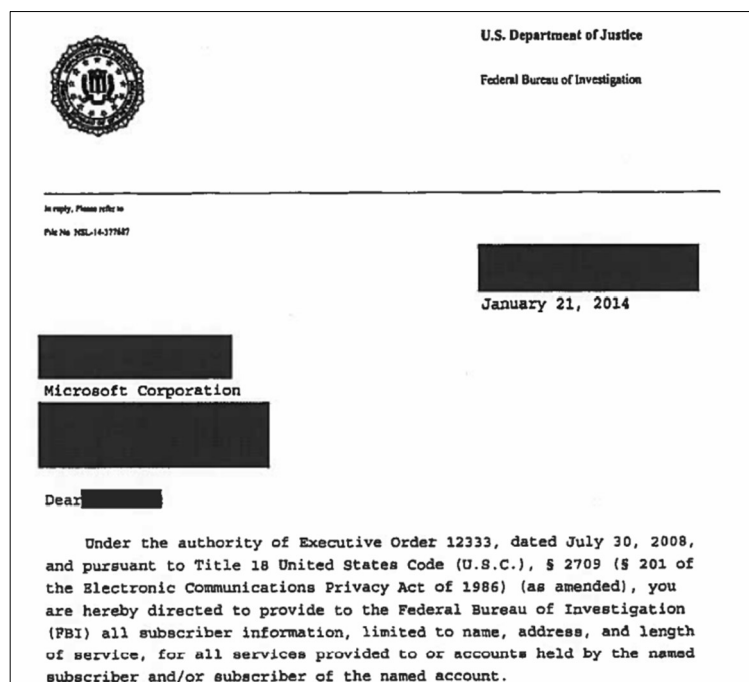
Svårigheten med att tolka statistiken är att det inte går att direkt översätta texten till svenska. Det är ord som har definitioner i lagtexten, såsom definition av *foreign power* eller *Person* vilket man lätt kunde tänka sig att det översättas till en individ eller person. Men *Person* har faktisk en mycket bred betydelse då, definitionen i 50 U.S. Code § 1801 – *Definitions* anger att en *Person* ”*“Person” means any individual, including any officer or employee of the Federal Government, or any group, entity, association, corporation, or foreign power.*”, anger att *Person* kan vara en individ, en grupp, ett företag eller en *foreign power*.

Ovan ger att det data som Microsoft presenterar inte på enkelt sätt kan kvantifieras till antal individer. Det går inte utifrån den av Microsoft presenterad data för FISA dra någon slutsats kring hur många förfrågningar eller personer som berörs av FISA 702.

3.3.1. *National Security Letters (NSL)*

I regionens yttrande punkt 32. anges nedan:

”Presidentdirektivet E.O. 12333 som ofta tas upp i dessa sammanhang är enligt uppgift inte tillämplig på Microsofts verksamhet.”



Figur 9 EO 12333 order Microsoft

Informationen i Figur 9 talar för att Microsoft träffas av EO 12333. Därmed vederlägg regionens yttrande i punkt 32.

4. Analys av Region Kalmar åberopad statistiken

Då Region Kalmar kan ha missförstått definitionen för begrepp såsom *target*, *person* och *selector* är det lätt att man också kan ha missförstått den statistik som redovisas av Microsoft.

De siffror från Microsoft som det hänvisas till i regionens yttrande punkt 31 och punkt 34 måste läsas mot bakgrund av det som Microsoft anger att detta data representera:

Punkt 31

”Vad gäller FISA Section 702 mottog Microsoft under perioden juli till december 2020 0–499 förfrågningar från amerikansk underrättelsetjänst som berörde 14 500–14 999 konton och 0–499 förfrågningar som rörde annat än innehåll på konton, vilket berörde mellan 0–499 konton”

Punkt 34

”Den ovan beskrivna riskbedömningen kan även kvantifieras. Microsoft hade år 2019 ca 75 miljoner kunder⁴². Av det totala antalet kunder var det (baserat på ovan angiven statistik) – högt räknat ca 0,02% av kunderna som berördes av utlämningsordrar under perioden. För att sannolikheten att uppgifter i biljettsystemet ska bli föremål för en begäran ska överstiga 50 %, skulle det krävas att biljettsystemet användes i ca 1 700 år.

Sannolikhet på 1 år = $0,02 \cdot 2 = 0,04\%$. Sannolikhet om 50% beräknas genom $\text{LN}(1 - 0,5) / \text{LN}(1 - 0,04\%) = 1732$ år. Beräkningen kan kontrolleras genom att räkna åt andra hållet. Sannolikhet för att det inte sker någon obehörig tillgång ett visst år är $1 - 0,04\% = 99,96\%$ eller 0,996. Sannolikheten för ingen tillgång på tio år är då $0,996^{10} = 99,6\%$. För att beräkna sannolikheten för att tillgång sker är formeln $1 - (0,996^{10})$. Sannolikheten för att tillgång sker på 1732 år är $1 - (0,996^{1732}) = 0,5 = 50\%$.”

Från ovan exempel har Region Kalmar dragit slutsatsen att konton kan översättas till individer.

Det går inte att direkt översätta det redovisade underlaget till antal individer. Ett misstag som är försåtligt om man bokstavligt översätter benämningar såsom *target*, *person* och *selector* till individ (se 3.2.2 och 3.3).

⁴² <https://www.microsoft.com/investor/reports/ar19/>

5. Bilagor

5.1. Teknisk utredning

För att verifiera om kryptering och pseudonymisering används som ett effektivt skydd i systemet genomförs ett antal partiska tester.

Syftet är att få en förståelse på en teknisk nivå hur systemet fungerar.

För samtliga tester används samma klient⁴³ och webbläsare⁴⁴.

Den tekniska analysen (se 5.3.3 sidan 26) av kommunikation som genomförs mellan användarens webbläsare och molntjänsten visar att de personuppgifter som tillgängliggjorts i resenärens webbläsare kommer i klartext från molntjänsten och därmed också tillgängliga i klartext för leverantören Microsoft.

Mot ovan kan man inte anse att kryptering och pseudonymisering i systemet är ett effektivt skydd som förhindrar leverantörer Microsoft från att ta del av personuppgifter i klartext.

5.1.1. Test 1

Testet 1 ansluta en klient med en webbläsare till Skånetrafikens hemsida skanetrafiken.se.

5.1.1.1. Transportkryptering

Hänglåset i webbläsarens adressfält (Figur 13), markerad med en blå pil bilden, visar att överföringen mellan biljettsystemet och webbläsaren är krypterad. Det är denna del som benämns transportkryptering. Det innebär att den som har möjlighet att avlyssna kommunikationen som sker mellan biljettsystemet och resenärens webbläsare inte med rimliga resurser kommer kunna bryta igenom skyddet och ta del av de uppgifter som överförs. Här har emellertid leverantören, i egenskap av en av de kommunicerande parterna, tillgång till uppgifterna i klartext.

5.1.1.2. IP Adress

Via upplag mot tjänsten Domaintools⁴⁵ fås att hemsidan skanetrafiken.se har IP adressen 20.50.170.49 (Figur 11) samt att IP adressen tillhör Microsoft Corporation. Det aktuella IP-numret tillhör alltså molntjänstleverantören och den tjänst som Skånetrafiken köper genom Microsoft.

⁴³ PC med Microsoft Windows 11 Pro - 10.0.22000 version 22000

⁴⁴ Microsoft Edge Version 98.0.1108.56 (Officiell version) (64 bitar)

⁴⁵ <https://whois.domaintools.com/skanetrafiken.se>

5.1.1.3. Spårning av användare

Via tjänsten Fouanalytics⁴⁶ visas (Figur 17) att sidan har 36 annons och 10 spårnings förfrågningar. Totalt sker 102 olika förfrågningar för metadata för användaren.

5.1.2. Test 2

Test 2 ansluta en klient med en webbläsare till Skånetrafikens hemsida skanetrafiken.se och logga in en användare.

5.1.2.1. Användare för test

För att testa systemet har en användare med fiktiva personuppgifter tidigare registreras.

5.1.2.2. Inloggning

I Figur 13 har en resenär loggat in i Skånetrafikens portal genom att ange den e-postadress som användes vid registreringen samt det lösenord som då valdes. Efter inloggningen sker en lång rad anrop, varav ett sådant anrop sker gentemot ett så kallat applikationsgränssnitt där resenärens personuppgifter lämnas ut i klartext.

Hänglåset i webbläsarens adressfält (Figur 13), som markerats med (1), visar att överföringen mellan biljettsystemet och webbläsaren är krypterad. Det är denna del som benämns transportkryptering. Det innebär att den som har möjlighet att avlyssna kommunikationen som sker mellan biljettsystemet och resenärens webbläsare inte med rimliga resurser kommer kunna bryta igenom skyddet och ta del av de uppgifter som överförs. Här har emellertid leverantören, i egenskap av en av de kommunicerande parterna, tillgång till uppgifterna i klartext.

Den del av webbläsarfönstret som markerats med (2) visar resenärens personuppgifter i klartext.

Frågan blir om dessa uppgifter på något sätt tillgängliggjorts i resenärens webbläsare genom att information tillförts från annat håll än via molntjänsten, eller om uppgifterna existerat i molntjänsten i klartext och därifrån förts över i oförändrat skick för att visas i resenärens webbläsare.

⁴⁶ <https://adsbydomain.fouanalytics.com/q/SkaneTrafiken.se?f=>

5.1.2.3. Personuppgifter i klartext

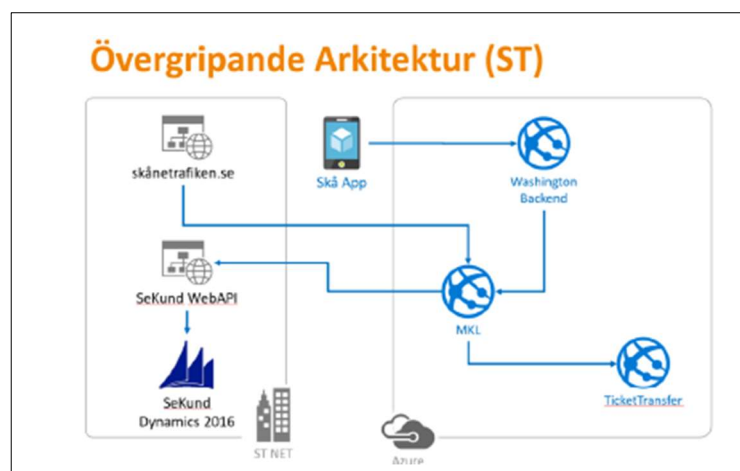
I Figur 14 visas en utvecklarvy av den hämtade sidan. Där kan enkelt ses vilket anrop som gjorts, mot vilken nätverksadress och vilka uppgifter som har förts över. I detta fall ser man att ett anrop gjorts (5) i form av ett get-account och att samtliga personuppgifter som inhämtats i registreringskedet överförts från leverantören Microsoft i klartext.

I bild nummer 5 syns en annan del av utvecklarvyn. Här syns att anropet get-account skett mot en nätverksadress med IP-numret 20.50.170.49 och TCP port nummer 443.

Denna adress administreras av American Registry for Internet Numbers (ARIN), och hör till Microsoft Corporation. Det aktuella IP-numret (Figur 11) tillhör alltså molntjänstleverantören och den tjänst som Skånetrafiken köper genom Microsoft.

Här sker således en överföring av resenärens personuppgifter direkt från Microsofts tjänst, som tillhandahåller uppgifterna i klartext.

Att systemet fungerar på just detta sätt bekräftas även av Region Kalmars egna handlingar. I skriften Utredning om samverkan s.25 återfinns följande systemskiss (Figur 10):



Figur 10 beskrivning från Växjö FR 4107–21 Aktebil 16, Komplettering från motpart

Här framgår tydligt att kommunikationen sker gentemot IT-miljön i Microsofts Azure.

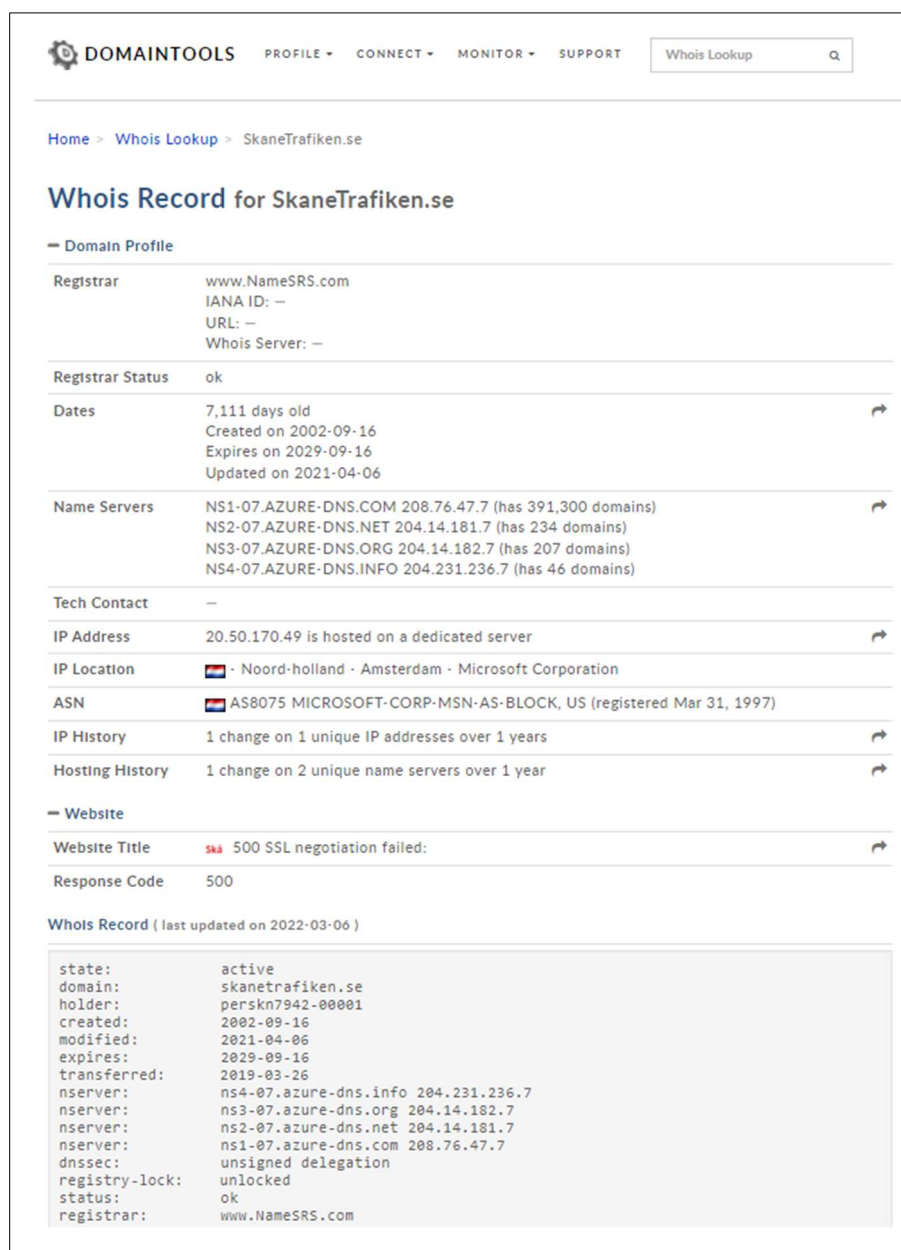
Ovan gör klart att de personuppgifter som tillgängliggjorts i resenärens webbläsare kommer i klartext från molntjänsten och därmed också tillgängliga i klartext för leverantören Microsoft.

5.2. Domäner

5.2.1. skanetrafiken.se

Uppslag av domänen skanetrafiken.se den 6 mars 2022 14:25

Detta visar på att skanetrafiken.se har IP Adressen 20.50.170.49 samt att IP Adressen tillhör Microsoft Corporation.



The screenshot shows the DomainTools Whois Lookup page for the domain skanetrafiken.se. The page is titled "Whois Record for SkaneTrafiken.se" and includes a "Domain Profile" section with various details. The "IP Address" field shows 20.50.170.49, which is hosted on a dedicated server. The "IP Location" field shows Noord-holland · Amsterdam · Microsoft Corporation. The "ASN" field shows AS8075 MICROSOFT-CORP-MSN-AS-BLOCK, US (registered Mar 31, 1997). The "IP History" field shows 1 change on 1 unique IP addresses over 1 years. The "Hosting History" field shows 1 change on 2 unique name servers over 1 year. The "Website" section shows the Website Title as "ska 500 SSL negotiation failed:" and the Response Code as 500. The "Whois Record" section shows the following details:

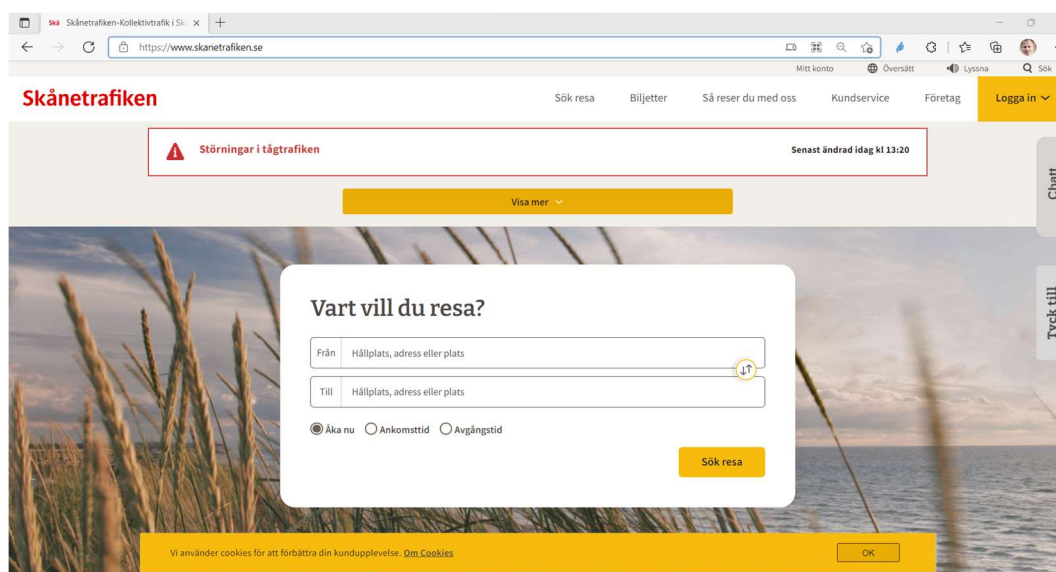
```
state: active
domain: skanetrafiken.se
holder: perskn7942-00001
created: 2002-09-16
modified: 2021-04-06
expires: 2029-09-16
transferred: 2019-03-26
nservers: ns4-07.azure-dns.info 204.231.236.7
nservers: ns3-07.azure-dns.org 204.14.182.7
nservers: ns2-07.azure-dns.net 204.14.181.7
nservers: ns1-07.azure-dns.com 208.76.47.7
dnssec: unsigned delegation
registry-lock: unlocked
status: ok
registrar: www.NameSRS.com
```

Figur 11 skanetrafiken.se har IP Adressen 20.50.170.49

5.3. Skärmsklipp

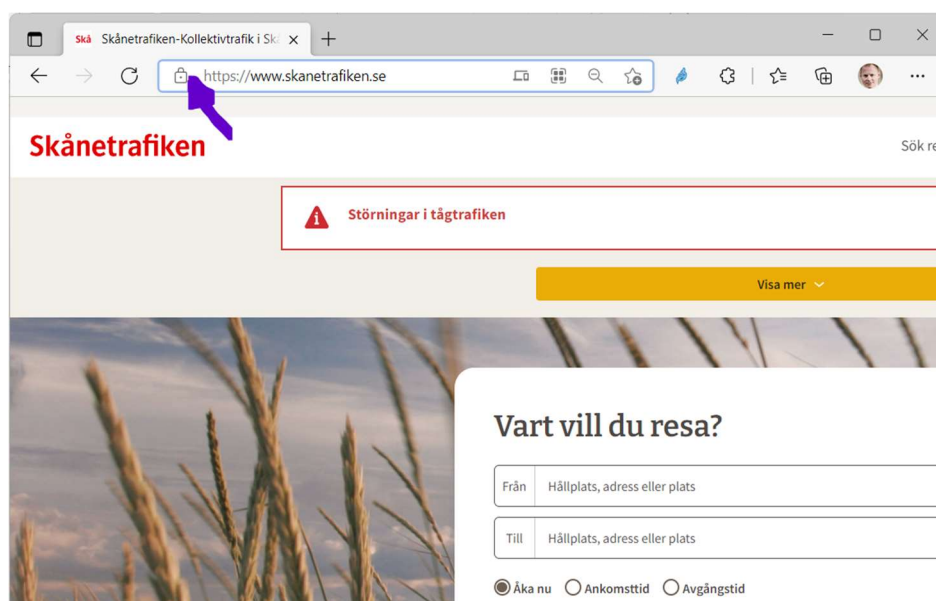
5.3.1. skanetrafiken.se

Skärmsklippet nedan visar på hur sida skanetrafiken.se såg ut den 6 mars 2022 14:06.



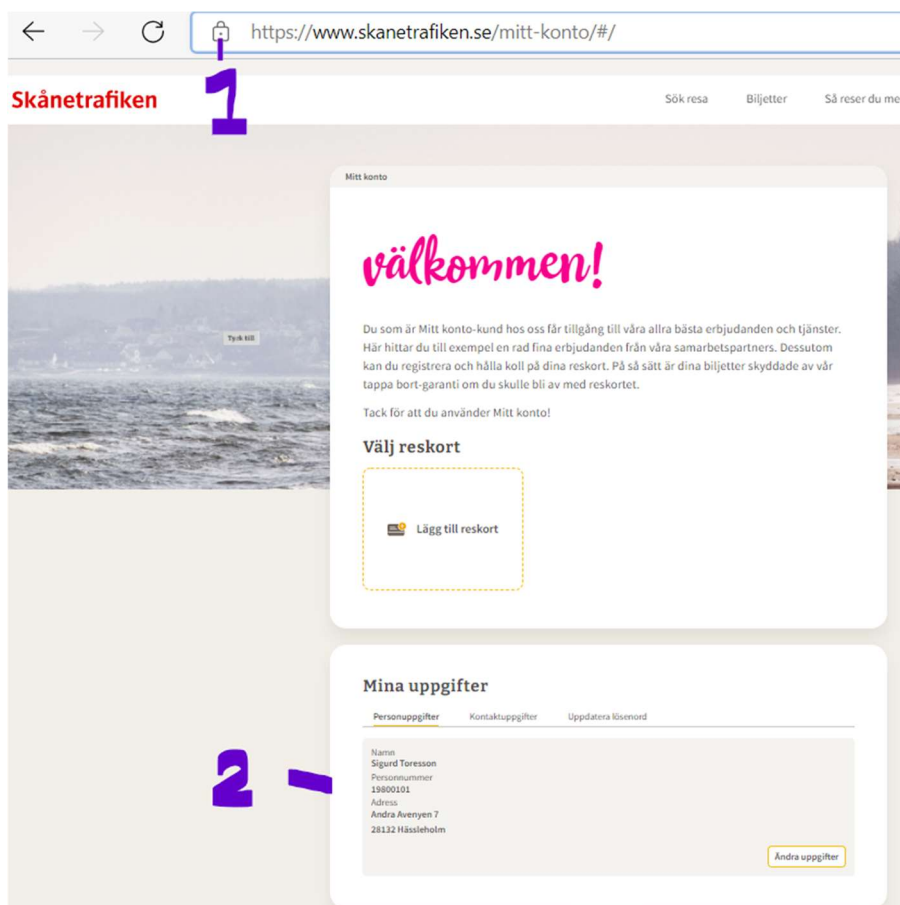
Figur 12 skanetrafiken.se

Skärmsklippet nedan visar på en detalj för sida skanetrafiken.se den 6 mars 2022 14:15.



Figur 13 Hänglås

5.3.2. Inloggning till skanetrafixen.se



Figur 14 Inloggning mitt konto

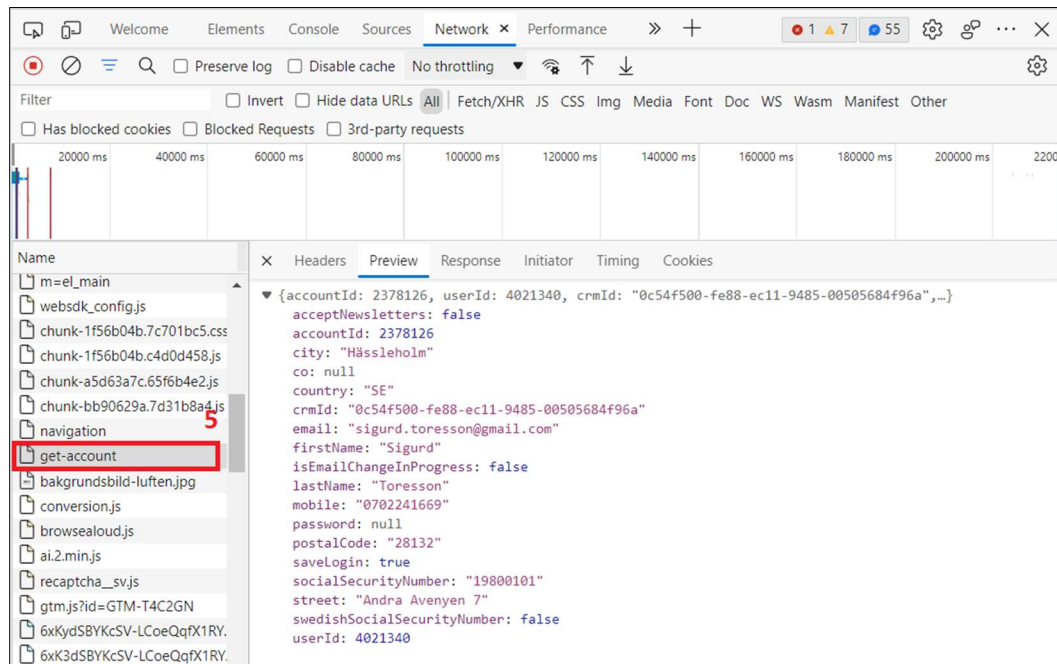
Utlåtande – MÅL NR 4107–21 – Laglighetsprövning av beslut avseende resesystem för Kalmar Länstrafik

André Catry

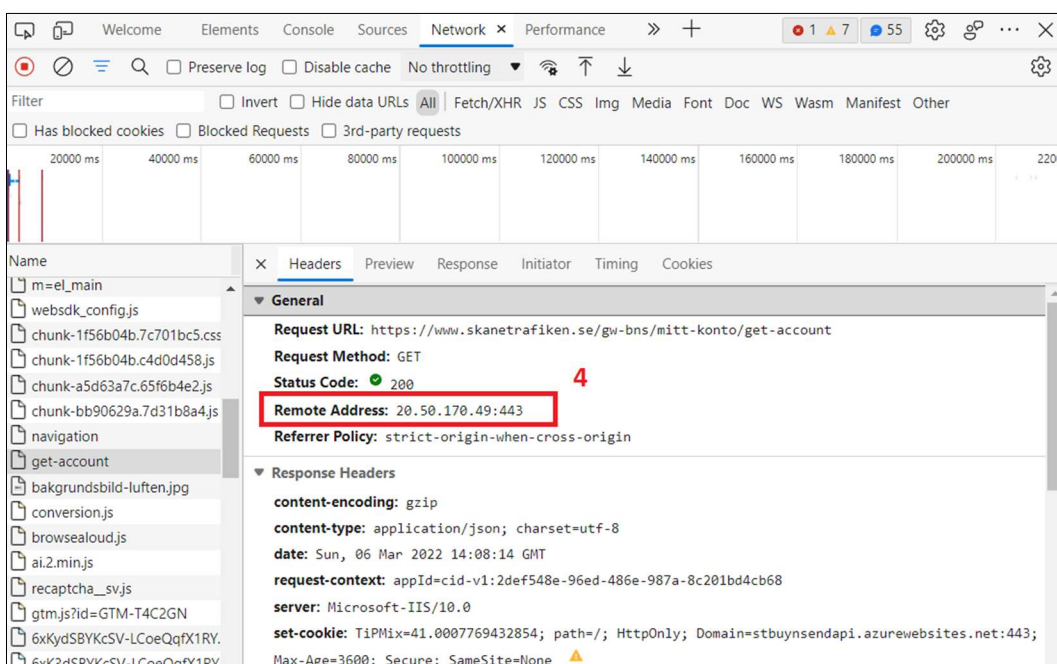
Version 1.0

2022-03-07

5.3.3. Trafikdata skanetrafiiken.se - personuppgifter



Figur 15 trafikdata skanetrafiiken.se – personuppgifter

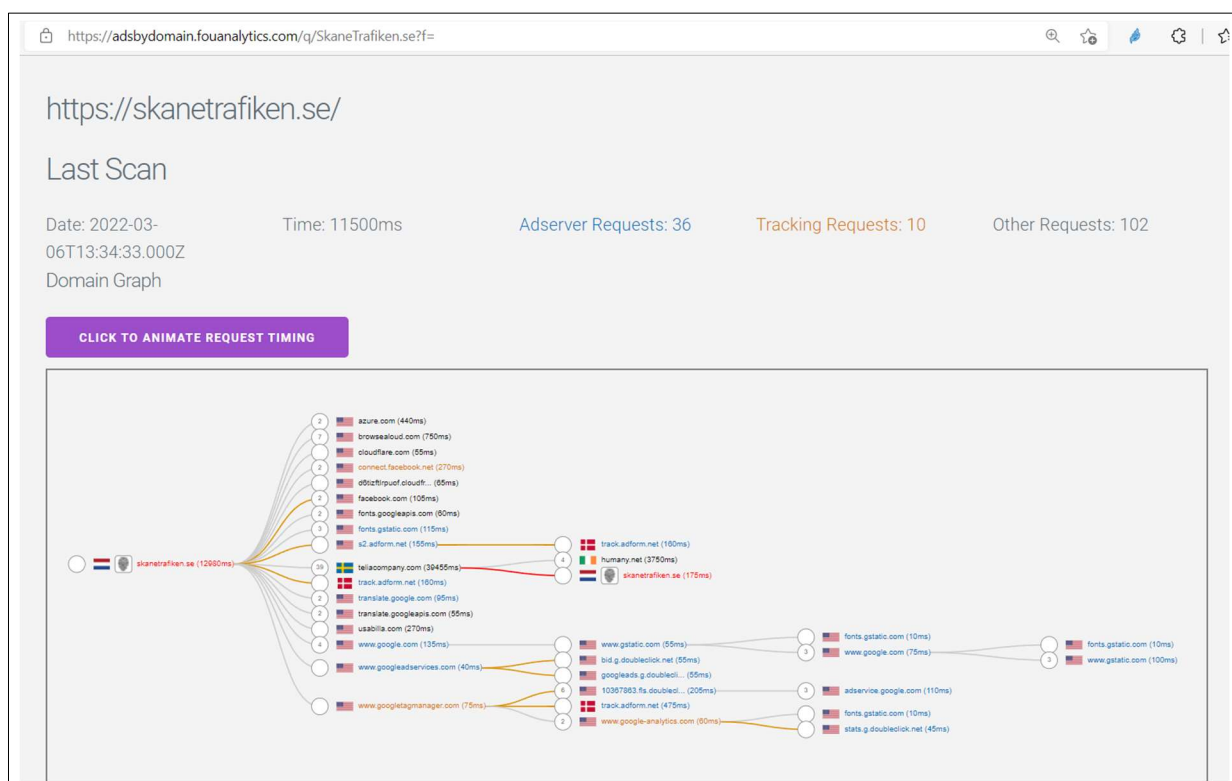


Figur 16 trafikdata skanetrafiiken.se – IP

5.3.4. Spårningsanalys <https://skanetrafiken.se/>

Via tjänsten <https://adsbydomain.fouanalytics.com/> har en analys av sidan skanetrafiken.se genomförts.

Resultatet visas i Figur 17. Adserver Requests: 36 Tracking Requests: 10 Other Requests: 102



Figur 17 spårning

5.4. Utredare André Catry

Senior Advisor IT-/information security and cyber risk, author – independent consultant

André Catry är en av Sveriges främsta experter inom IT-/informationssäkerhet och cyberrisk. Han har över 25 års erfarenhet av avancerad offensiv och defensiv cyberriskhantering. Utöver olika uppdrag inom Försvarmakten, bland annat inom konceptutveckling för IT-försvarsförbandet, har han varit avdelningsdirektör vid Säkerhetspolisen. Han har även lång erfarenhet som senior IT-säkerhetskonsult i bolag som han själv har grundat och han har anlitats globalt i flera uppmärksammade IT-brottsutredningar och uppdrag. Han har även medverkat som teknisk expert i eSams arbete kring förutsättningar för myndigheter att använda molntjänster på ett lagligt och lämpligt sätt. Bolaget Bitsec AB som André drev under 11 år hade uppdrag för FRA och MUST för att säkerhetsgranska kryptosystem.

ERFARENHET:

Senior Advisor inom IT-/informationssäkerhet och cyberrisk, Advokatfirman

Kahn Pedersen, 2020-

Contractor / Chief Engineer / Senior IT Security Advisor / IT & Security

Architect, Saab, 2016-2022

Strategic Advisor, Nixu Corporation, 2017-2020

Founder / Owner / CEO / CTO, Bitsec AB, 2006-2017

Föreläsare, Kungliga tekniska högskolan, 2017 -

Föreläsare, Försvarshögskolan, 2008

Contractor / Senior Advisor, Försvarmakten, 2005-2006

Senior Security Consultant, Ekelöw, 2002-2005

Contractor US Navy, 2004

Avdelningsdirektör, Säkerhetspolisen, 1999-2001

Departementssekreterare, Council of the European Union, 1998–2000

Departementssekreterare, Regeringskansliet, Utrikesdepartementet, 1995-1999

UTBILDNING:

Computer Science, KTH 2014

Juridik, Lunds universitet 2014

Computer Science, KTH 2001

Computer Science, KTH 1985

Innehållsförteckning

1. Utredning.....	1
1.1. Utredare	1
1.2. Beställare	1
2. Microsofts tillgång till personuppgifter i klartext i resesystemet.	2
2.1. Kryptering och pseudonymisering för skydd av personuppgifter i systemet	2
2.1.1. Region Kalmar påstår följande	2
2.1.2. Johan Roos Tibbelin påstår följande.....	3
2.1.3. Hypoteser	3
2.2. Analys	4
2.3. Slutsats	5
3. Vissa regler i amerikansk rätt och deras tillämpning	6
3.1. <i>Law Enforcement Requests Report</i> (rättsvårdande).....	6
3.1.1. CLOUD Act	7
3.1.2. Bestrida beslut och meddela kund.....	7
3.2. <i>US National Security Orders Report</i> (underrättelsetjänst).....	8
3.2.1. Foreign Intelligence Surveillance Act (FISA) Orders	8
3.2.2. Omfattning av FISA 702 övervakning	14
3.3. Microsoft Redovisad statistik	15
3.3.1. <i>National Security Letters</i> (NSL).....	18
4. Analys av Region Kalmar åberopad statistiken	19
5. Bilagor.....	20
5.1. Teknisk utredning	20
5.1.1. Test 1	20
5.1.2. Test 2	21
5.2. Domäner.....	23
5.2.1. skanetrafiken.se	23
5.3. Skärmsklipp.....	24
5.3.1. skanetrafiken.se	24
5.3.2. Inloggning till skanetrafiken.se.....	25
5.3.3. Trafikdata skanetrafiken.se - personuppgifter	26
5.3.4. Spårningsanalys https://skanetrafiken.se/	27
5.4. Utredare André Catry	28