A2003:015

IT och tillit

Delrapport till ITPS utvärdering av den svenska IT-politiken

Claudio Aguirre-Bianchi,
Metamatrix Development & Consulting AB

itps INSTITUTET FÖR TILLVÄXTPOLITISKA STUDIER

IT och tillit

Delrapport till ITPS utvärdering av den svenska IT-politiken

Claudio Aguirre-Bianchi

INSTITUTET FÖR TILLVÄXTPOLITISKA STUDIER

ITPS, Institutet för tillväxtpolitiska studier
Studentplan 3, 831 40 Östersund
Telefon 063 16 66 00
Telefax 063 16 66 01
e-post info@itps.se
www.itps.se
ISSN 1652-0483

Förord

Institutet för tillväxtpolitiska studier har haft i uppdrag av regeringen att genomföra en utvärdering av den svenska IT-politiken. ITPS har därför gett Metamatrix Development & Consulting AB i uppdrag att analysera IT och tillit som ett av många underlag för analysen och slutsatserna i institutets huvudrapport.

Rapportens huvudslutsatser är: Tillit är svårdefinierat i IT-sammanhang och tolkats huvudsakligen som IT-säkerhet. Det behövs ett konkret och hanterbart IT-politiskt instrument, tillförlitlighet: en kvalitetsdimension som omfattar även säkerhet.

Sveriges IT-säkerhet är bra, men landet kan bli världens säkraste IT-land, inte minst som ett investeringsincitament. Informationssamhället måste studeras i sin relation till demokrati, välfärd, livskvalité och hållbar tillväxt.

Föreliggande rapport har utförts av Claudio Aguirre-Bianchi vid Metamatrix Development & Consulting AB. Dessa svarar ensamma för analyser och slutsatser i föreliggande underlagsrapport.

Ansvarig chef vid Institutet för tillväxtpolitiska studier har varit Hans-Olof Hagén medan Kurt Lundgren har varit projektledare.

Stockholm i oktober 2003

Sture Öberg,
Generaldirektör

Innehåll

1 Tillit och IT-politiken

Enligt regeringens andra IT-proposition[1] har tillit en central roll i IT-politiken. Riksdagen har bekräftat denna bedömning genom sitt beslut. Tillit utgör därmed ett av de tre centrala IT-politiska instrumenten.[2]

Det är däremot svårt att utröna innebörden av tillit i det svenska IT-politiska sammanhanget och därefter utvärdera IT-politiken ur ett tillitsperspektiv. Vi har därför gjort en analys av IT-propositionen, diskussionerna i Sveriges riksdags trafikutskott, Näringsdepartementets skrivelser, samt Budgetpropositionen 2002 med syfte att finna de konstituerande elementen i innebörden av tillit i svensk IT-politik, såsom den har konkretiserats av regeringen och riksdagen.[3]

1.1 Vad säger IT-propositionen

Trots att tillit är, enligt IT-propositionens text, en av de tre uppgifterna som staten prioriterar för IT-politiken, finns det inte i propositionen någon definition av vad som menas med tillit. Termens tydning överlämnas därmed till allmän språkkompetens.

IT-propositionen fastställer däremot att:

> Informationssamhället bygger på användarnas **förtroende för den nya tekniken**. Exempelvis bygger förutsättningarna för att utveckla elektronisk handel **i hög grad på den tillit till säkerheten** som köpare och säljare känner på denna framväxande marknad. För att främja *tilliten* bör **lagstiftningsåtgärder och åtgärder i syfte att underlätta branschöverenskommelser** prioriteras."[4]

En tillbakablick på IT-utvecklingsagendan under 1990-talet, hjälper till att förstå rollen av den odefinierade tilliten i svensk IT-politik.

Tillit till IT-baserade tjänster och system betraktades under 1990-talet som en grundläggande förutsättning för att få fart på e-handeln. E-handeln sågs ofta som en faktor som kunde i sig göra ekonomin mer dynamisk och säker samtidigt ge en hög tillväxt.[5] De finansiella kostnaderna och riskerna underskattades och **.com**-fenomenet blev ett högriskområde där investerarna agerade med överdriven tilltro på teknikens självvärde. För att kunna uppnå de överdrivna förväntningarna, blev det

---

[1] *Prop. 1999/2000:86, Ett informationssamhälle för alla.*

[2] *Jfr Prop. 1999/2000:86. IT-propositionen fastslår att IT-politikens tre centrala uppgifter är Tillgänglighet, Tillit och Kompetens. Dessa uppgifter döptes av ITPS om till* ***IT-politiska instrument****; Jfr ITPS (A2002:009), En lärande IT-politik – förslag till utvärdering, 2002. Online: http://www.itps.se/pdf/A2002_009.pdf (per 2003-03-15).*

[3] *En detaljerad redovisning av innehållsanalysen finns i Claudio Aguirre-Bianchi, Tillit i svenska IT-politiska dokument – En innehållsanalys, 2003. Dokumentet (PDF) kan beställas från cab@metamatrix.se.*

[4] *Jfr Prop. 1999/2000:86, s 22, (fetstil, ca-b).*

[5] *Denna övertro på teknikens förmåga att accelerera cirkulationen i ekonomin genom snabbare handel och därmed ge ökad tillväxt, har visat sig orealistisk. Däremot dominerade denna föreställning bland näringslivstoppar och ledande politiker i början på 1990-talet och gav upphov till en tillväxtdiskurs präglad av kommersialism.*

nödvändigt att överföra tillit på resten av marknaden (konsumenterna). På det sättet överfördes även en stor del av ansvaret för att lyckas eller misslyckas till individerna. På det finansiella planet finns det likheter med 1980-talets överskattning av fastighetsmarknaden.

Denna föreställning gjorde sig gällande inom EU, som lanserade flera initiativ med syfte att befrämja e-handeln. Fortfarande idag har e-handeln inte levererat de resultat som utlovades för ca femton år sedan: I USA ligger hushållens onlineinköp på samma nivå som förra året.[6] Den ansedda tidningen E-week ställer sig, i 12 september, 2003 upplaga n, frågan om e-handeln ”äntligen har börjat leverera”, efter att konstatera att ”since the mid-1990s, e-business has been *the next big thing*.”[7]

Det är intressant att konstatera att den allmänna inriktningen för tillit inom IT-politiken[8] och informationssäkerhetsperspektivet[9] är inte riktigt välintegrerade i en sammanhållen syn på tillit i IT-propositionen. En möjlig förklaring för den spänningen som uppstår mellan dessa två perspektiv i IT-propositionen är att informationssäkerheten var mer omedelbar som angelägenhet och att regeringen hade Statskontorets rapport om **En sammanhållen strategi för samhällets IT-säkerhet** (1999:118) som underlag för konkreta åtgärder kring informationssäkerheten. Däremot saknade regeringen konkreta åtgärder för att realisera den allmänna inriktningen.

En innehållsanalys av de legislativa IT-politiska dokumenten[10] visar med tydlighet att IT-propositionen betraktar tillit som en direkt effekt av informationssäkerhet: tillit skapas och stärks genom att höja säkerheten. En följd av denna betraktelse är att tillit förutsätter att medborgarna skall ha kännedom om de komplexa säkerhetsåtgärder som vidtas. Denna kännedom blir följaktligen nödvändig för att skapa en tillitsfull attityd i samband med användningen av IT-baserade tjänster och produkter.

Tillit kan sägas vara uttryck för individens förtroende för de agenterna (människor, institutioner, system, maskiner) hon förlitar sig på, med förväntan att minska osäkerheten beträffande resultatet av dennes handlingar. Följaktligen, förväntar individen sig en reducering av ovissheten inför komplexa operationer och abstrakta system. Detta innebär att kompetens, kunnande och insikt är centrala förutsättningar för tillit. Det borde då finnas en korrelation mellan kompetens och tillit till IT.[11]

IT-politiken, hävdar IT-propositionen, är således inte i grunden ett tekniskt utan ett demokratiskt projekt som handlar om att ge alla människor tillgång till den nya teknikens möjligheter, samt utnyttja dessa möjligheter för att förbättra samhället

---

[6] Jfr Buying Online. Frilling Down. The New York Times, 2003-08-04. Online: http://www.nytimes.com/2003/08/03/business/media/04MOSTWANTED.html (per 2003-08-04).
[7] Editors of CIO Insight, ”E-business: Is it finally Starting to Deliver?”. E-week, 2003-09-12. Online: http://www.eweek.com/print_article/0,3048,a=103299,00.asp (per 2003-09-20).
[8] Jfr Prop. 1999/2000: 86, Kap. 5.3.1. Allmän inriktning.
[9] Jfr Prop. 1999/2000:86, Kap 5.3.2. Informationssäkerhet,
[10] Jfr Fotnot 3, s 5 i denna rapport.
*[11] Detta syftar på det vi kallar **kompetensparadoxen**. Jfr Claudio Aguirre-Bianchi, Paradoxer vid IT-användning: Behovet av ett operationellt användbarhetsbegrepp. 2003. Dokumentet (PDF) kan beställas från cab@metamatrix.se.*

och välståndet. Denna intention har dock så småningom tolkats annorlunda av regeringen. På Näringsdepartementets webbplats heter det:

> Tillit till den nya tekniken är avgörande för att uppnå en ökad användning. Regeringen prioriterar särskilt områdena skydd mot informationsoperationer, ett säkrare Internet samt elektroniska signaturer och annan säkerhetsteknik.[12]

1.2 Vad säger riksdagen om tillit

Riksdagens Trafikutskott lade stor vikt vid tillitsperspektivet och, i enlighet med propositionen, fokuserade tillitsfrågorna huvudsakligen kring säkerhetsproblematiken, både gällande informationssäkerhet och gällande nationalsäkerhet.

Trafikutskottets betänkande redogör för statens tre prioriterade uppgifter i IT-politiken och skriver:

> Tillit till IT skall inte förutsätta hög teknisk kompetens eller dyr utrustning, utan förtroende att använda IT för kommunikation, handel och höjd livskvalitet skall kunna skapas hos alla användare.[13]

Trafikutskottet pekar på en väsentlig aspekt av visionen *ett informationssamhälle för alla* genom att koppla tillit till en höjning av livskvalitén. Den väsentliga kopplingen har däremot inte införts i de åtgärder som vidtagits inom ramen av IT-politiken.

Diskussionen kring informationssäkerhetsarbete och åtgärder för elektronisk kommunikation har präglats av säkerhetsteknisk inriktning. Även perspektivet nationalsäkerhet har haft stort prägel i diskussionen.

Trafikutskottet efterlyste en översyn av betalningssystemen på Internet med syfte att underlätta betalningen i samband med e-handeln.

1.3 Vad säger Näringsdepartementet om tillit

Näringsdepartementet har i ett redigerat utdrag ur Budgetpropositionen för 2002,[14] fastslagit att ”det finns många olika sätt att undersöka tillit till IT. Ett är att titta på den elektroniska handelns utbredning som måttstock även på konsumenternas förtroende för Internet och den nya tekniken.”[15]

---

[12] *Jfr http://naring.regeringen.se/fragor/it/ (per 2003-09-10).*
[13] *Jfr Riksdagens trafikutskott, Betänkande 1999/2000: TU9, s 17.*
[14] *Näringsdepartementet, Uppföljning av Regeringens IT-politik. Online: http://www.naring.regeringen.se/pressinfo/infomaterial/pdf/uppdatering01.pdf.*
[15] *A. a. s 26. Detta innebär att tilliten skulle kunna, enligt Näringsdepartementets idé, mäta i själva användningsgraden av tjänsterna.*

När det gäller IT-säkerhet målas det upp en ljus bild, nämligen:

> Regeringens bedömning är att arbetet med att öka informationssäkerheten, både inom Sverige och internationellt, tagit fart. Det är dock tydligt att det fortfarande finns stora behov av åtgärder på detta område. De undersökningar som gjorts pekar på att förtroendet och tilliten till tekniken och till dem som ansvarar för systemen påverkar Internetanvändningen.
>
> Huvudansvaret för informationssäkerheten bör fortsatt ligga hos respektive systemägare, men regeringen måste fortsatt arbeta för att skapa förutsättningar för en hög säkerhet.[16]

1.4 Vad säger regeringen i Budgetpropositionerna 2002

Det IT-politiska instrumentet tillit, har formulerats i IT-propositionen och i Näringsdepartementets skrifter med en innebörd som har hållit sig konsekvent inom regeringen: tillit handlar om säkerhet och säkerhet är huvudsakligen en teknisk fråga. Även tillitens objekt är tekniken. Detta återbekräftas i Budgetpropositionen 2002. I propositionens text för Utgiftsområde 22: Kommunikationer, heter det:

> ***Tillit*** till den nya tekniken är avgörande för att uppnå en ökad användning. Regeringens insatser på informationssäkerhetsområdet inriktas på att skapa förtroende för den nya tekniken genom att bidra till bättre generella förutsättningar för informationssäkerhetsarbetet. Sverige skall även vara aktivt i det internationella arbetet inom informationssäkerhetsområdet. Regeringen prioriterar särskilt områdena skydd mot informationsoperationer, ett säkrare Internet samt elektroniska signaturer och annan säkerhetsteknik.[17]

I det fortsatta arbetet med tillit prioriterar alltså regeringen informationssäkerheten, med fokus på:

- Skydd mot informationsoperationer.
- Ett säkrare Internet.
- Elektroniska signaturer och annan säkerhetsteknik.

Följande åtgärder nämns:

- Uppdrag till PTS att senast den 31 december 2002 inrätta en Rikscentral för IT-incidentrapportering. Rikscentralens uppgift är att arbeta med skydd mot IT-incidenter via ett system för att snabbt kunna sprida information om sådana inträffar. Rikscentralen skall också kunna lämna information och råd om förebyggande åtgärder samt ge ut statistik som underlag för kontinuerliga förbättringar i det förebyggande arbetet.
- Underlag från PTS om rättsliga och organisatoriska förändringar för att säkerställa oberoende drift har lämnats till Utredningen om elektronisk kommunikation (dir. 2001:32). Från och med budgetåret 2001 är medel avsatta för upprätthållande av en säker nationell tidsangivelse på Internet. En säker

[16] *A. a. s 30.*
[17] *Jfr Prop. 2002/03:1 Utgiftsområde 22: Kommunikationer, s 116.*

svensk tidsangivelse för Internet finns att tillgå för operatörerna och kan användas i till exempel säkerhetstillämpningar.

- PTS har på regeringens uppdrag utvärderat den verksamhet som bedrivs med stöd av lagen (2000:832) om kvalificerade elektroniska signaturer och finansieringen av denna verksamhet. PTS föreslår bl.a. att avgiftsfinansieringen av kostnader hänförliga till tillsynsverksamheten enligt lagen avskaffas tills vidare och att verksamheten huvudsakligen finansieras genom anslag. Rapporten Information till Internetanvändare har remissbehandlats och bereds för närvarande inom Regeringskansliet.
- Riksskatteverket, som under ett inledningsskede givits ett sammanhållande ansvar för administration av certifikat för elektronisk identifiering och elektroniska signaturer inom statsförvaltningen, har publicerat riktlinjer för myndigheternas användning av elektroniska signaturer och certifikattjänster. Statskontoret har upphandlat tjänsten elektronisk identifiering och tecknat ramavtal med ett antal leverantörer av elektroniska certifikat.
- För att göra en samlad översyn av formkrav i lagar och förordningar i syfte att undanröja onödiga hinder mot en ökad elektronisk kommunikation och elektronisk dokument- och ärendehantering har en särskild arbetsgrupp inrättats. Arbetsgruppen skall samordna den genomgång av formkrav som skall göras departementsvis.
- Regeringen har också deltagit i bl.a. EU: s och OECD: s arbete på informationssäkerhetsområdet.[18]

Vidare under rubriken *Tillit till informationsteknik* heter det: ”Frågorna berörs även inom området försvarspolitik. Under hösten 2001 och våren 2002 föreslog regeringen bl.a. en strategisk inriktning på arbetet och en ansvarsfördelning mellan myndigheter som arbetar med informationssäkerhetsfrågor.”[19]

Regeringen påpekar att:

> ”Vad gäller ***tilliten*** så har den ansvarsfördelning mellan myndigheterna avseende informationssäkerhetsfrågor som regeringen presenterat inte ändrat på den tidigare principen, utan huvudansvaret för informationssäkerheten ligger fortfarande hos respektive systemägare.” Detta vill säga att nya uppdrag, som till exempel en rikscentral för IT-incidentrapportering och omvärldsbevakning inom informationssäkerhetsområdet, ”förväntas ytterligare förbättra möjligheterna till att skapa höjd informationssäkerhet.”[20]

Användarnas eget ansvar beträffande det avgörande informationssäkerhetsarbetet fastställs: ”Säkerhetsfrågor som till exempel datavirusspridning behandlas i massmedierna vilket bidrar till att höja allmänhetens medvetenhet om informationssäkerhetsfrågor. På marknaden finns en god tillgång av produkter och tjänster inom

[18] *A.a. s 119-120.*
[19] *A.a. s 122.*
[20] *A.a. s 132.*

området. Fler leverantörer erbjuder eller inkluderar idag säkerhetstjänster vid leverans av nya datorer och vid försäljning av Internet- och bredbandsabonnemang."[21]

Till sist heter det:

> Den pågående översynen av formkrav i lagar och förordningar i syfte att undanröja hinder för elektronisk kommunikation bör på sikt också innebära en ökad användning av elektroniska signaturer.[22]

Propositionen bekräftar gång på gång en de-facto definition av tillit som en effekt av informationssäkerhet.

1.5 Realisering av IT-politiken ur tillitsperspektiv

IT-propositionen prioriterade följande områden för realiseringen av det IT-politiska instrumentet Tillit under den aktuella cykeln av IT-politiken:

I sin bedömning för **Informationssäkerhetsarbetet** anger regeringen följande prioriteringar för den närmaste framtiden:

- Skydd mot informationsoperationer,
- Ett säkrare Internet samt
- Elektroniska signaturer och annan säkerhetsteknik.
- En tvärsektoriell samordning för IT-säkerhet och skydd mot informationskrigföring.[23]

Bland åtgärderna som bör vidtas nämns i IT-propositionen:

- Att främja att den svenska delen av Internet skall kunna drivas oberoende av funktioner utomlands.
- Att tillhandahålla en säker och korrekt nationell tidsangivelse för Internet via riksmätplatsen för tid och frekvens.
- Att ta initiativ till en bred samverkan mellan de viktigaste aktörerna på leverantörs- och användarsidan i syfte att få till stånd en samsyn om hur man kan stimulera och utveckla en gemensam infrastruktur för elektroniska signaturer, till exempel genom en lösning baserad på s.k. smarta kort.
- Att på grundval av betänkandet Ds 1999:73 under våren 2000 föreslå riksdagen en lag om elektroniska signaturer med syfte att underlätta användningen av sådana.[24]

När det gäller skydd för den personliga integriteten i samband med datoranvändning, är IT-propositionen fåordig. Den enda konkreta åtgärden som tas upp är **Skyddet av den personliga integriteten i arbetslivet**.[25] I denna punkt redogörs för regeringens beslut i september 1999 att tillkalla en särskild utredare för att se över behovet av lagstiftning eller andra åtgärder för att stärka skyddet av den enskildes personliga integritet i arbetslivet (dir. 1999:73).

---

[21] *A.a.*
[22] *A.a.*
[23] *Jfr Prop. 1999/2000:86, s 36.*
[24] *A.a., s 32-33.*
[25] *A.a., s 122-123.*

IT-propositionen saknar fokus på den personliga integriteten i samband med IT-användningen. Förklaringen till detta är att frågeställningarna kring den personliga integriteten anses reglerade i Personuppgiftslagen (PUL, SFS 1998:204). Däremot tar IT-propositionen upp frågan om personlig integritet i arbetslivet, vilken hanteras som ospecificerat krav på informationshantering, utan att ange ramar eller normer för integritetsskyddande åtgärder.

1.6 Tillitsbegrepp inom IT-branschen

Tillit har ofta använts inom IT-branschen som synonym för eller komponent av informationssäkerhet eller teknisk säkerhet. Nyligen har relationen mellan säkerhet och tillit börjat bli mer och mer operationell, även inom IT-branschen.

Meta Group[26] har, exempelvis föreslagit ett nytt sätt att hantera tillit (trust) genom att generera någon slags ”säkerhetsgrammatik” eller grundspråk (Baseline Language).

Meta Group ser tillit (trust) som en egenskap av tjänster och affärsprocesser som måste säkras genom informationssäkerhet och så småningom rent systemtekniska åtgärder (IT). De tre relevanta aktörer för att utforma och definiera tilliten (trust) är, enligt Meta Group:

- Verksamhetsansvariga
- Informationssäkerhetsansvariga
- IT-ansvariga

Den av Meta Group föreslagen process för att hantera tillit (trust) är huvudsakligen inriktat på att skapa förståelse mellan olika nivåer inom ett företag/organisation. Tillit (trust) betraktas som en egenskap av de tjänster och system som företaget/organisationen levererar. Tillit (trust) skulle kunna uppnås genom att:

A. De verksamhetsansvariga i företaget/organisationen identifierar olika tillitsnivåer (trust levels) som är nödvändiga för olika tjänster eller verksamhetsprocesser. Betingande behov för definitionen av dessa tillitsnivåer (trust levels) är: sekretess, integritet, tillgänglighet.

B. De verksamhetsansvariga viktar graden av tillit (trust) som skall säkras för dessa tjänster/processer genom att optimera relationen mellan behov och kostnader; tillit (trust) skall sedan levereras genom olika säkerhetsmekanismer. Detta närmande möjliggör, enligt Meta Group, ett positivt sätt att instrumentalisera tillit (trust) och översätta det i termer av säkerhetsåtgärder.

I botten för detta sätt att operationalisera tillit (trust) finns det ett behov av att erkänna att det finns någon slags ”grammatik” för IT-säkerhet som grundas på tillit. En sådan grammatik skall användas, enlig Meta Group, för att formalisera definitioner för säkerhet, genom att använda olika ”tillitsnivåer” (trust levels) som kan definiera verksamhetens behov av säkerhet.

[26] *Meta Group är en av världens ledande företag för undersökningar och analyser av IT, samt strategikonsultationer.*

Meta Groups begreppskonstruktion kring tillit (trust) som grunden för en IT-säkerhets grammatik är ett viktigt bidrag med tanke på behovet att skapa operationella tillitsbegrepp som kan översättas i informationssäkerhetsdefinitionen som betingar IT-säkerhetsåtgärder.

Trots att Meta Groups schema för ***trust*** onekligen är ett viktigt bidrag för att operationalisera tillitsproblematiken inom ett företag eller organisation, lider detta bidrag av brister. Den huvudsakliga bristen är att **trust** begränsas till säkerhet och syftar till att omsättas i tekniska lösningar, därför söks en **grammatik** för att skapa förståelse mellan tre olika funktioner inom ett företag eller organisation: Från verksamhet, till information, till teknik.

Tillit kan inte avgränsas till interna processer som betingar egenskaperna i utbudet av tjänster och produkter till de brukande personerna (fysiska eller juridiska). Personerna och huvudsakligen människan är egentligen tillitens huvudagenter och kan därmed inte vara externa till de nödvändiga preciseringarna av processerna för att konstruera tillit. Ett holistiskt perspektiv behövs för att förstå tillitens väsen och roll i samhälliga processer.

När det gäller tillit för IT-baserade produkter och tjänster bör tilliten betraktas som en egenskap i användningsrelationen som uppstår mellan brukaren och tjänsten eller produkten vid användningen. I denna användningsrelation ingår: människan (i centrum), verksamheten, informationssystem, ledning och regelverk, processer och teknik (IT).

I denna studie kommer vi att betrakta Meta Groups sätt att förstå tillit (trust) som en mycket intressant utgångspunkt, dock inte en färdig begreppskonstruktion. I avsnittet **3. Begreppsrekonstruktion: Om tillit och tillförlitlighet**, kommer detta begrepp att diskuteras vidare.

1.7 Tillit i svenska språket

Ordet tillit är ett mångtydligt ord, inte minst pga. dess tämligen svårdefinierade betydelse. I IT-sammanhang används tillit huvudsakligen som översättning för trust, vilket bidrar till att minska precisionen i ordets betydelse.[27] Ännu en komplikation är att inom IT-engelska har tillit ofta används – och det görs fortfarande – som modeord (buzzword) för en brokig blandning av säkerhets- och anseendes och marknadsföringsåtgärder som paketeras ihop i olika produkter och plattformar.

Svenska akademiens ordbok har ännu inte publicerat artikeln om ordet tillit.[28] I Svenska Akademiens ordlista[29] anges *förtroende* och *förtröstan* som betydelse för tillit; likaså anges denna betydelse i Strömbergs synonymordbok.[30]

---

[27] Trust täcker ett större semantiskt fält på engelska än tillit på svenska.

[28] Ordboken, såsom den är publicerad, slutar per oktober 2003 vid ordet Talkumera; de ord som följer efter Talkumera bearbetas vid ordbokens redaktion i Lund. (Jfr http://www.svenskaakademien.se/saob/, kontrollerat per 2003-10-05). Inom ramen för denna studie har en telefon- och e-postintervju hållits med Annika Karlholm, vid Svenska akademiens ordboksredaktion och fått förhands upplysning om ordets betydelse i den kommande artikeln om tillit.

[29] Svenska Akademiens ordlista över svenska språket. Tolfte upplagan, fjärde tryckningen, 1998 (ISBN 91-7227-032-2).

Nationalencyklopedin saknar ordet tillit i annan bemärkelse än den geologiska.

Enligt Svenska Akademiens ordboksredaktör, kommer artikeln om ordet tillit att bygga på att tillit:

- Är en sammansättning av *lita* och *till*.
- Betyder att lita på någon, dvs. en oreserverad eller trygg förtröstan och förlitande på någons pålitlighet, uppriktighet och/eller sannfärdighet.
- Åsyftar en känsla av trygghet.
- Har före i tiden syftat på: stöd, hjälp.

När det gäller att lita på eller räkna med att någonting fungerar, är inte tillit det rätta ordet i svenska språket: tillförlitlighet är mer adekvat.

Tillförlitlighet (dependability) är ett väldefinierat begrepp inom svenska och internationella standarder, bl. a. inom el-industrin, och datakommunikation; tillförlitlighet är även ett väsentligt begrepp för kvalitet inom logistiken.

Enligt Nationalencyklopedin är tillförlitlighet en ”kvalitetsdimension hos ett system som speglar dess förmåga att fungera på ett tillfredsställande sätt med ett minimum av störningar, fel och reparationer.”[31]

1.8 Tillit och IT-politiken

IT-propositionen ger ingen definition av tillit. Ordet används som samlingsbegrepp för ett antal föreslagna åtgärder som pekar på nödvändiga infrastrukturella säkerhetsbehov.

IT-propositionen saknar strategier för att uppnå tillit, eftersom tillit betraktas som ett samlingsbegrepp och inte ett operationellt begrepp. Generella visioner är svåra att operationaliseras och omsättas i politik. Dessa generella visioner tenderar att förbli retoriska istället för strategiska.

[30] *Alva Strömberg, Strömbergs synonymordbok. Femte upplaga, elfte tryckningen, 1976. (ISBN 91-7148-300-4).*
[31] *Nationalencyklopedin, Artonde bandet. Bokförlaget Bra Böcker AB, 1995 (ISBN 91-7024-621-1), s 268.*

Ovanstående har lett till att tillit har förblivit en abstrakt retorisk konstruktion i den svenska nationella IT-politiken, som finner konkreta uttryck enbart när den reduceras till tekniska lösningar och lagregleringsåtgärder. Denna frånvaro av ett holistiskt perspektiv är en brist som kännetecknar det begränsade sättet på hur tillit betraktades och hanterades under 1990-talet inom IT-industrin i hela världen. Tillit var då huvudsakligen en förutsättning för att säkra användningen av IT-baserade tjänster och system, i synnerhet för e-handeln, och som syftade omväxlande på tre olika områden:

- Informationssäkerhet för tjänste- eller processleverantörer (företag eller myndighet).
- Integritetsskydd för individer.
- Säkra affärstransaktioner.

Individens tillit till maskiner och system i sig (att lita på att datorn fungerar som det förväntas) har inte förekommit som ett påtagligt behov varken i Sverige eller internationellt. Den abstrakta och emellertid retoriska användningen av ordet tillit i svensk lagstiftning och i IT-politiken har inte omfattat tillit till datorn. I ett större perspektiv kan ”datorn” även betraktas som individens instrument[32] för att komma åt digitala tjänster via Internet och/eller andra kommunikationsnät. Detta instrument består av datorn, system- och programvara, kommunikationskanal och Internet-serviceleverantör. Man kan då säga att exempelvis ett robust Internet ingår i tillit till datorn (nätverksapparaten) då maskinen som individen använder är en del av ett större sammanhang och instrumentet för tillgänglighet till informationssamhällets infrastruktur. En sådan tolkning finner stöd i konvergensfenomenets framväxt.

[32] *I det avseende kan tillit på maskinerna kopplas med regeringens och PTS’ idé om användarens ansvar för sin egen utrustnings säkerhet. Jfr s 11 och 25.*

2 Kan svenskarna lita på IT baserade tjänster?

Det finns inget tydligt svar på denna fråga, eftersom frågan i sig bygger på antagandet att IT är en entitet som har eget värde. Frågan kan formuleras om till huruvida svenska befolkningen litar på Sveriges myndigheters och näringslivets förmåga att prestera korrekta, kvalitativa, säkra och integritetsskyddande IT-baserade tjänster och produkter. En sådan frågeställning har inte förekommit i de undersökningar som har gjorts. Detta är en allvarlig brist i perspektivet och omfattningen av de utvärderingar av IT-relaterade företeelser som görs: de tenderar att bli alltför snäva och att förbise att det finns ett konceptuellt och, sociologisk och politisk skillnad mellan *informationssamhälle* och *IT-samhälle*.

Bland de aktörer vi har intervjuat under denna studie finns stor samstämmighet i att betrakta tillit som en egenskap av användningen och inte av själva tekniken eller av de IT-baserade tjänsterna. Många har uttryckt detta genom att säga att ”folk har tillit till myndigheterna, företagen eller till personerna och inte till IT”. Andra har sagt att den främsta tillitsfrämjande faktorn för en myndighet är sak- och processkompetensen hos tjänstemännen som handhar medborgarna i en tjänsterelation. På det sättet tillskrivs medborgarnas förtroende för institutioner och myndigheter som en avgörande faktor för att skapa tillit för respektive institutions IT-baserade tjänster. Inom näringslivet brukar detta kallas för anseende (reputation).

Det kan sägas att medborgarnas förtroende för myndigheten betraktas mycket ofta som tillräcklig och därmed blir tillitsperspektivet ointressant för dem som ansvarar för beslut om och utveckling av IT-baserade tjänster hos myndigheterna. Detta sker huvudsakligen hos de myndigheter för vilka medborgarna hyser största förtroende och för de myndigheter som har närmare kontakter med medborgarna, vilket är fallet med de kommunala myndigheterna.

Förtroendet för organisationer (företag eller myndighet), samt kvalitén i processen anses av många av de aktörer som intervjuades vara de mest avgörande faktorerna för att skapa den nödvändiga tilliten för att framhäva personernas benägenhet att använda IR-baserade tjänster. Det bör tilläggas att synligheten av nyttan samt enkelhet i processerna och handhavande är minst lika viktiga i sammanhanget.

Flera intervjuade har påpekat att detta förtroende måste motsvaras med kvalité i processerna och kompetens bland personalen. Informations- process- organisatorisk- och teknisksäkerhet tillhör kategorin egenskaper av ett samlat kvalitetsbegrepp som finns implicit i tankarna hos många av de aktörer som har intervjuats för denna studie: flera intervjuade har påpekat att det är viktigt att basera ett ökat förtroende på en reell kvalitetsökning i tjänsterna och processerna.

Vidare, bekräftar flera av de intervjuade att myndigheterna (både statliga, regionala och kommunala) inte tänker på tillit och tillitsfrämjande åtgärder när de utvecklar nya IT-baserade tjänster. Deras tankar och krav fokuseras istället på skilda områden såsom:

- Teknisk säkerhet.
- Användarvänlighet i användargränssnittet.
- Tydlighet i processerna.
- Kundnytta.

Utvecklingsstrategierna inom den offentliga sektorn har inte nått sådana mognadsnivåer som underlättar holistiska perspektiv. Utvecklingsstrategierna och metoderna är fragmenterade och saknar funktionell, processmässig och systematisk integration.

2.1 e-Handel och tillit

Tillitens betydelse för elektroniska tjänster har huvudsakligen framhävts i samband med användningen av e-handel. Under 1990-talet rådde stora förväntningar om e-handeln som en faktor som skulle öka ekonomins dynamik, en föreställning som fångades av EU vid ett tidigt stadium.

En förväntning om e-handelns tillväxtfrämjande effekter kan spåras i andemeningen av IT-propositionens användning av begreppet tillit. Tillit betraktades då som en förutsättning för ökad e-handel, varför tillit förknippades till IT-säkerhet. I innehållsanalysen av IT-propositionen och andra lagtexter relevanta för Sveriges IT-politik som har gjorts för denna studie, har vi funnit att tillit pekar alltid på teknisk säkerhet. IT-propositionens treenighet *Tillit-Tillgänglighet-Kompetens* kunde väl ha varit *Säkerhet-Tillgänglighet-Kompetens* istället. Denna studie kommer att föreslå att IT-politikens fokus bör inriktas på ett kvalitetsstandardiseringsarbete kring tillförlitlighet, vilket utvecklas senare i rapporten.

E-handeln sker huvudsakligen genom två olika typer av köparesäljare relationer:

- Detaljhandel eller B2C (Business to Consumer) och
- Interföretagshandel eller B2B (Business to Business).

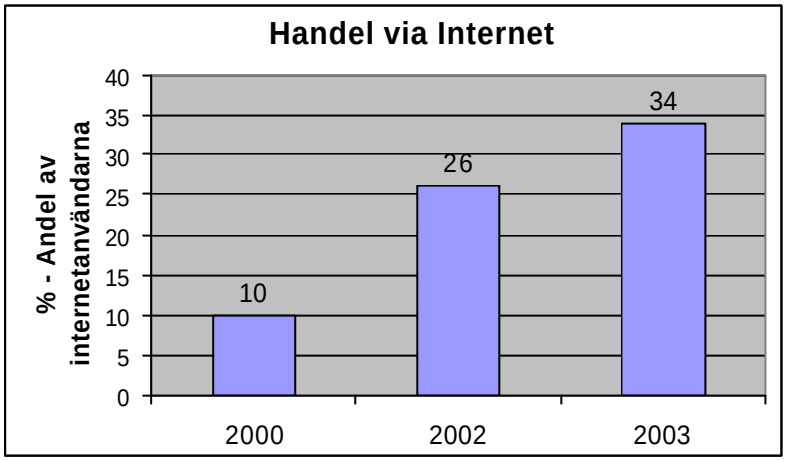
2.1.1 Detalj e-handel och tillit

De kvalitetskrav som de intervjuade aktörerna anser vara tillitsfrämjande och som redovisas i inledningen av det här avsnittet är synnerligt relevanta för e-handeln. Allt tyder på att e-handeln kan komma att lyfta inom den närmaste tiden. Det har gått ganska trögt på e-försäljning till slutkonsumenter (B2C). Betydligt bättre har det gått för e-handeln mellan företag (B2B). De befintliga siffror för att mäta e-handelns volym skiljer sig avsevärt, vilket försvårar jämförelser.

De senaste siffrorna om detalj e-handel i Sverige visar en tydlig uppgång. Undersökningsresultat som kommer att redovisas i den kommande World Internet Institutets årliga rapport **Svenskarna och Internet 2003** visar att 34 procent av Sveriges Internetanvändare (18 år eller äldre) har köpt varor och tjänster via Internet, här räknas även de som bara har provat någon enstaka gång (8 procent av Internetanvändarna). Detta är en markant ökning från 26 procent år 2002 och 10 procent år 2000.

DIAGRAM1

Andel av Internetanvändare som har handlat via Internet



Källa: World Internet Institute[33]

Sverige är trots trögheten ledande när det gäller detalj e-handeln. World Internet Institutet har i sitt internationella program fått jämförbara aktuella siffror för användning av Internet för att handla varor eller tjänster.

Dessa siffror visar att 41,3 procent av svenskarna som har Internetanslutning, som är 66 procent av befolkningen, har handlat via Internet, man bara 38,2 av USA: s befolkning med Internetanslutning har gjort det. Tyskland ligger högre än Sverige med 48,3 procent. Sydkorea har 30,9 procent, Italien 22,8 procent, Kina 20,5 procent och Japan 18,6 procent.[34]

Trots ökningen och den ledande positionen, har detalj e-handeln ännu inte riktigt lyft i Sverige. Detta har förklaringar som inte nödvändigtvis bör förknippas med tillit, till exempel:

- E-handeln innebär en förändring i vanor som hör till vardagslivet, dessa är tämligen långsamma förändringsprocesser.
- Det kan även sägas att e-handeln är en läroprocess där många faktorer medverkar, inte minst betalningssystem som fortfarande är det största hindret.

[33] *Data ur kommande rapport Svenskarna och Internet 2003, World Interntet Institute, http://www.worldinternetinstitute.org.*

[34] *Dessa siffror har inte publicerats ännu. De kommer att publiceras först i USA i november 2003 och därefter i Sverige.*

- Det finns e-butiker som har lyckats rejält och som ofta har sitt ursprung i postorderverksamheten, där det finns etablerade processer, hållbara och beprövade affärsmodeller, köpmönster, mm.
- Andra e-butiker har misslyckats eller har överlevt en trög utveckling. Bland dessa förekommer olika typer av förhastade affärsmodeller eller otillräckligt utvecklade processer.
- Det finns traditionella branscher där det inte kan identifieras ett succémönster för e-handeln, exempelvis etablerade varuhus, där några företag lyckas väl och andra misslyckats.

När det gäller detalj e-handeln och tillit bör problematiken fokuseras på individens benägenhet att använda den elektroniska handeln som transaktionsföreteelse och inte bara på tekniken. Bland tillitsobjekten i relation till detalj e-handeln finns:

- Internet som kanal för transaktionen eller medium: dvs. att Internet är robust.
- Det säljande företaget – där företagets anseende är avgörande.
- Tredje parten (oftast osynlig men ändå viktig i individens riskbedömning inför transaktionen) som hanterar betalningsförfarandet.
- Relationen med den egna datorn och de system individen når via datorn; det handlar huvudsakligen om individens föreställning om sin kompetens för att hantera de system och tjänster som kan uppnås genom den egna datorn.

Post- och telestyrelsen fick regeringens uppdrag att utreda de faktorer som kan förhindra e-handeln. Under hösten 2001 överlämnade PTS sin första rapport för detta uppdrag. Där spaltades det upp de tillitsrelaterade hindren efter företagets perspektiv och konsumentens perspektiv:

Tillitsrelaterade hinder för e-handeln ur företagens perspektiv:

- **Brister i leveranssäkerhet.** Normalt är leveranssäkerheten en betydelsefull parameter vid val av leverantör. Detta kan bli ännu viktigare vid tillämpning av e-handel, då ett motiv för att satsa på e-handel ofta är att korta ledtiderna och att effektivisera processerna. Samtidigt upplevs e-handel inte sällan vara mer anonym än traditionell handel och nya e-handelsaktörer kan mötas av misstänksamhet från branschen. Blotta aningen om att leveransen inte kan genomföras i tid kan vara ett tillräckligt skäl för att välja en annan leverantör. Detta gäller e-handel mellan företag, men även konsumenter har blivit mer försiktiga.
- **Brister i lättillgänglig information.** Genom bl.a. systemintegration, ökar mängden tillgänglig information som kan användas till olika ändamål. Det krävs ett förtroende för dem som får ta del av uppgifter om företaget. Misstanken om att offentliggjord information skapar ett mindre gynnsamt konkurrensläge, kan medföra att vissa företag inte deltar i portaler, marknadsplatser eller på andra ställen på Internet, där priser och villkor kan jämföras på ett direkt och öppet sätt.
- **Brister i sekretess.** Vid mer djupgående affärssamarbeten genom e-handel, där tillgång till varandras system skapar en insikt och kunskap om bl.a. den

andra partens ekonomiska förhållanden och strategier, kan bristande sekretess skapa stora problem.

- **Problem med säkerhet i betalningssystem.** Existerande betalningsslösningar för e-handel anses ibland inte vara tillräckligt säkra och användarvänliga för att vara godtagbara alternativ till traditionella metoder. Komplexiteten ökar när användaren behöver hålla reda på olika betalningssystem och sätt att identifiera sig hos olika leverantörer (till exempel nätbutiker), till skillnad mot i den "fysiska världen", där exempelvis körkort och andra godkända identitetshandlingar är accepterade som legitimation för individer i de flesta sammanhang. Dessutom kan i vissa fall kunskap om regelverk saknas, och medvetenheten är på sina håll låg om att elektroniska signaturer i de flesta fall är tillåtet som identifiering. En viktig uppgift för e-handelsleverantören är förutom att utnyttja säkra tekniska lösningar, att också förmå skapa trygghet och tillit hos kunderna.
- **Virus.** Okunskap om hur systemen ska skyddas mot virus och andra typer av dataintrång, utgör ett problem. Öppen e-handel exempelvis via marknadsplatser och portaler kan vara sårbara för angrepp.[35]

Tillitsrelaterade hinder för e-handeln ur konsumentens perspektiv

PTS studien omfattade även konsumentperspektivet i tillitsrelaterade hinder för e-handeln.

- Betalning. Kunden vill ha ett enkelt, säkert och billigt sätt att betala sina varor. E-handel blir mindre attraktivt om det saknas en smidig betalningslösning till rimlig uppoffring för kunden. Här är ett ställningstagande var risken ska ligga någonstans. Idag står kontokortsföretagen risken om kontokortet skulle utnyttjas på ett bedrägligt sätt på nätet, med en lösning som bygger på smarta kort och certifikat, blir kunden den ansvarige.
- Lågt utnyttjande av kryptering. Säkerhetsproblematiken är påtaglig ur konsumentens perspektiv, och tas inte alltid på allvar av leverantören. Säkra betalningar är en del, och många konsumenter tvekar inför att skicka till exempel kontonummer över en okrypterad förbindelse. Det är vanligt att även annan information avkrävs köparen i okrypterade webbformulär eller via e-post, som personnummer, adress, intressen och beställningsinformation.
- Bristande sekretess och integritet. Även om kundinformationen sänds över säkra förbindelser, kan den användas på ett sätt som kunden inte önskar, exempelvis säljas till andra företag eller lagras av säljaren för framtida behov. Detta är inte unika problem för e-handel, men i och med att det blir mycket enklare att samla in uppgifter om kundens beteende från olika källor och kombinera dem, utgör e-handel ett större hot mot den personliga integriteten.
- Känsla av otrygghet. Även leverantören har vidtagit åtgärder för att skapa en tekniskt säker miljö och värnar om den personliga integriteten, är det också

[35] *Jfr Post- och telestyrelsen (Diarienr. 01-25818/23),Hinder för e-handel, 7 november 2001, s 13. Online: http://www.pts.se/Archive/Documents/SE/Hinder%20for%20e-handel.pdf. (per 2003-05-05).*

> viktigt att en känsla av trygghet kan förmedlas till kunden. En bristande tillit till leverantören, oavsett vilka rationella skäl som finns för ett stort förtroende eller avsaknad av förtroende, är en betydelsefull faktor för e-handel.[36]

De brister och problem funna av PTS överensstämmer med de resultat som redovisas i en studie om kvalitén i Internethandeln över ländernas gränser i Europa som genomfördes av European Consumer Centre's Network under år 2002.[37] Studien fann att:

> The result of our shopping exercise showed that the consumer's situation in cross-border e-commerce is rather unfavourable. Frequently, orders were not delivered, key information regarding the consumer's rights was missing and returned products were not reimbursed. These are just examples of the obstacles a consumer will encounter and they are also reasons why a lot of consumer may refrain from, or be reluctant to engage in cross-border e-commerce.
>
> A worrying fact is that our results, in many aspects, are even more negative than the results found in Consumers Internationals study, "Should I buy?"[38] One explanation for this might be that Consumer Internationals study included both national and international purchases, whereas our project dealt exclusively with cross-border transactions. That indicates that consumers, who buy from foreign web traders are more likely to encounter problems than those who buy from domestic companies.[39]

Bristerna som studien fann var relaterade huvudsakligen till:

- Leveranser (bara 75 procent av de beställda produkterna levererades).
- Återbetalning (31,5 av de returnerade varorna återbetalades inte).

[36] *A.a. s 16.*

[37] *European Consumer Centre's Network, Realities of the European online marketplace. Online: http://www.konsumenteuropa.se/Documents/Engelska/EEC_e-commerce_report.pdf (per 2003-09-02). Studien fann allvarliga brister i e-handeln över nationella gränser inom Europa, beträffande: tydlig kostnadsinformation, kontraktvillkoren, leverans, retur och återbetalning av returnerade varor.*

38 *En studie genomförd år 2001 av Consumers International Jfr Consumers International, Should I buy?, 2001 (ISBN 1 902391 36 5). Online: http://www.consumersinternational.org/document_store/Doc250.pdf. (per 2003-09-02).*

[39] *Jfr. European Consumer Centre's Network, Realities of the European online marketplace, s 6.*

2.1.2 Det riskfyllda nätet

Statistiska centralbyråns undersökningar bekräftar i stort sett dessa hinder. SCB redovisade 2000 att:

Av dem som använder Internet i hemmet anger ungefär 71 procent att tvånget att lämna kreditkortsnummer vid beställning av varor eller tjänster är ett hinder i användningen. Ungefär hälften uppger att osäkerheten kring hur personuppgifter används är ett hinder. Ungefär 44 procent anser att långsam anslutning till Internet är ett hinder och ungefär 35 procent anger att kostnaden är ett hinder i användningen av Internet.

> När det gäller lämnandet av kreditkortsnummer och personuppgifter finns det ingen större skillnad i inställning mellan män och kvinnor. Det är inte heller någon större skillnad i inställning mellan arbetare, tjänstemän och egna företagare. I olika åldersgrupper finns det dock en skillnad i inställning till att lämna kreditkortsnummer och personuppgifter.
>
> Andelen som anger att lämnandet av kreditkortsnummer är ett hinder ökar med stigande ålder. I åldersgruppen 16–19 år anger hälften att tvånget att lämna kreditkortsnummer är ett hinder. I åldersgruppen 55–64 år är andelen närmare 80 procent. Yngre personer uppger i mindre utsträckning att osäkerheten om hur personuppgifter används är ett hinder än äldre personer. Knappt 40 procent av personerna mellan 16 och 19 år uppger att lämnandet av personuppgifter är ett hinder medan cirka 56 procent av personerna mellan 45 och 54 år ser detta som ett hinder.[40]

Trots dessa tillitsrelaterade hinder, har detalj e-handeln vuxit. Enligt Statistiska centralbyråns undersökningar om svenska befolkningens användning av IT och Internet, växer användningen av e-handelstjänsterna stadigt.

Näringsdepartementet i sin tur beskriver år 2002:s läge för tillit till IT, särskilt till e-handeln på följande sätt:

- Fortfarande är utvecklingen av elektronisk handel förhållandevis långsam. De köpmönster som råder idag verkar motsvara dem hos traditionella postorderkunder, där det främst är personer i glesbygd som utnyttjar e-handel för att komma åt varor och tjänster på ett enklare sätt. I en Demoskopundersökning sade 62 procent av de tillfrågade att de ansåg att säkrare alternativ för betalning skulle göra att de handlade mer över Internet. Färre av de tillfrågade ansåg att lägre priser var det som skulle öka deras e-handlande. En under våren utförd Sifoundersökning visade att endast Internetanvändare i åldersgruppen 18-25 år känner sig relativt trygga från eventuella hot på Internet. I övriga åldersgrupper finns en betydande oro för virus, elektroniska spår, dataintrång, avlyssning med mera.
- En europeisk jämförelse pekar på att användare i Sverige i vissa avseenden finner det svårare att lita på Internet än övriga européer. Trots att Internetpe-

[40] *Statistiska centralbyrån, IT i hem och företag – En statistisk beskrivning, 2001. (ISBN 91-618-1094-0), s 37. Online: http://www.scb.se/publkat/Filer/X96ÖP0101.pdf. (per 2003-04-15)* .

netrationen är hög i Sverige och att andelen som handlar on-line ligger över medelvärdet i Europa, kan endast 18 procent av Internetkunderna i Sverige tänka sig att också betala direkt över Internet. Detta är den lägsta andelen i Europa. I Finland är motsvarande siffra 21 procent, i Tyskland 25 procent och i Norge 26 procent.[41] Som skäl för tveksamheten att sköta betalningar över Internet nämns särskilt integritetsaspekter och oro för e-handelsföretag med finansiella problem och att dessa skall släppa vidare känslig information om kunderna.

- Företagen möter också allvarliga hot mot IT-säkerheten. På senare tid har hotet från externa aktörer ökat, men de interna hoten är fortfarande de som överväger. Småföretagarna är en grupp som inte känner sig tillräckligt informerade om säkerhetsfrågor trots att dessa ofta kan vara centrala för verksamheten.
- Bristen på kompetent personal är ett problem. Enligt Högskoleverkets rapport Högskoleutbildade inom IT är det enligt de tillfrågade arbetsgivarna inte brist på utbildad personal, utan snarare på personal som också har praktisk erfarenhet av informationssäkerhetsfrågor.
- Myndigheter och andra offentliga organisationer beskriver hotbilden som mångfasetterad, där allt från hot mot system och känslig information till Internetberoende nämns.
- Ett ökat internationellt samarbete rörande informationssäkerhet är nödvändigt, inte minst på grund av Internets gränsöverskridande natur. Aktuella områden är virus, informationsoperationer och IT-relaterad brottslighet. Här har Sverige varit aktivt under ordförandeskapet i EU:s ministerråd första halvåret 2001 vilket resulterat till exempel i en rådsresolution om Informations- och nätsäkerhet och att arbetet på cyberbrottsområdet drivits vidare.[42]

[41] *Källan till dessa uppgifter har dessvärre inte kunnat identifieras. Därför bör uppgifterna betraktas som validerade av Näringsdepartementet.*

[42] *Näringsdepartementet,* ***Uppföljning av Regeringens IT-politik (utdrag ur Budgetspropositionen för år 2002), s 26-27.*** *Online: http://www.naring.regeringen.se/pressinfo/infomaterial/pdf/uppdatering01.pdf. (per 2003-04-15).*

I PTS senaste rapport om e-handeln påpekas vikten av och olika problem relaterade med tillit och säkerhetsmedvetenhet.[43]

> ”Användarnas tillit och säkerhetsmedvetenhet har betydelse för e-handelns utveckling. De som e-handlar har större behov av att lämna ut personliga uppgifter via Internet. Studien visar att en knapp fjärdedel av dem som har e-handlat har lämnat kredit- eller kontokortsnummer via e-post eller webbplatser. Av dessa är det bara 17 procent som endast lämnar ut personliga uppgifter om webbplatsen är säker (d.v.s. att förbindelsen är krypterad).
>
> Säkerhetsmedvetenheten, finner PTS studie är högre hos bredbandsanvändare än hos dem med uppringd access i bostaden, ”ändå saknade hälften av dem med bredbandsaccess brandvägg och en tredjedel saknade uppdaterat virusskydd. Nio av tio av dem med uppringd access saknade brandvägg och hälften saknade uppdaterat virusskydd.”
>
> PTS fastslår att det ”finns behov av att informera allmänheten om relevanta säkerhetsåtgärder och att genom information om risker minska onödig oro. Staten kan bidra till ett säkrare Internet, bl.a. genom att inom statsförvaltningen tillämpa säkra webbplatser och e-legitimation.” Det läggs dock till att ”PTS, och staten överhuvudtaget, har begränsade möjligheter att påverka förutsättningar och undanröja hinder. Marknadskrafterna avgör utvecklingen (…)”.

PTS anger i sin rapport att staten bör:

- Utreda och analysera marknader, ta fram underlag för beslut om eventuella åtgärder för att konkurrensen ska fungera bättre.
- Lagstifta för att skapa förutsättningar för en konkurrens på lika villkor för marknadens aktörer.
- Analysera Internetanvändarnas informationsbehov och informera om säkerhetsrisker vid e-handel och andra aktiviteter på Internet.
- Fungera som en pådrivande kraft genom att använda och erbjuda elektroniska tjänster inom den egna förvaltningen och i kontakten med företag och medborgare samt genom att använda elektroniska certifikat där så är lämpligt.[44]

Individernas tillit i samband med e-handeln, sammanfattas av PTS på följande sätt:

> Två problem som har uppmärksammats i den allmänna debatten är användarnas bristande tillit till Internet, respektive en låg säkerhetsmedvetenhet. Flera aspekter är knutna till betalning för och leverans av varan eller tjänsten, bl.a. hur användarens personliga data överförs och hanteras hos e-handlaren och eventuella mellanhänder. Här har e-handelsföretagen ett ansvar både vad gäller att

[43] *Redogörelse nedan bygger huvudsakligen på en studie som genomfördes första gången under hösten 2002, och kan betraktas som en pilotstudie. Enkäten kommer att utvärderas och vidareutvecklas; en ny studie kommer att genomföras under år 2003. Jfr Post- och telestyrelsen (Rapportnr: PTS-ER-2003:4), E-handel - fem förutsättningar, 19 februari, 2003. (ISSN 1650-9862). Online: http://www.pts.se/Archive/Documents/SE/E-handel%20-%20fem%20forutsattningar.pdf. (per 2003-04-15).*

[44] *A.a. s 8.*

hantera kunddata på ett säkert inom företaget, att tillämpa säkra webbplatser samt att erbjuda säkra sätt att betala på.

Från kundens sida är exempel på riskabelt agerande i samband med bl.a. e-handel över Internet, att lämna ut känslig information via ej krypterade förbindelser och att lämna ut personlig information utan att ha möjlighet att verifiera mottagarens identitet.[45]

PTS pekar på ytterligare en risk som blir alltmer påtaglig i samband med användning av Internet och speciellt med e-handeln: Identitetsstöld. Rapporten anger att enligt den amerikanska Federal Trade Commission, sker idag hälften av alla bedrägerier på Internet. Ett exempel på hur bedragare kan gå tillväga för att stjäla identiteter, [46] är att via falska kopior av seriösa webbplatser lura användaren att lämna ut personliga uppgifter.

Det sker även andra online bedrägerier och inskränkningar i den personliga integriteten, exempelvis:

- Auktionsplatser
- Via e-post (s.k. Nigeriabrev)
- PayPal bedrägeriet
- Modem (uppkopplings) stöld
- Oönskad exponering till kränkande material (porr mm)
- Riktad eller slumpmässig massmarknadsföring (spam)
- Kontokorts (betalningsformation) stöld
- Bankkonto informationsstöld
- Olaga registrering

Listan kan göras nästan intill oändlig.[47] Det finns både brottsliga missbruk av Internet och icke brottsliga men besvärliga missbruk. Gränsen är ofta otydlig och missbruket placeras i en grå zon, inför vilken finns det foga skydd.

---

[45] *A.a. s 32. Se även Tillit till IT vid Internetanvändning; PTS-ER-2002:24.*

[46] *Identitetsstöld har blivit ett av de största IT-relaterade brott som drabbar individer. I USA har detta brott fått okontrollerbara proportioner: År 2002 drabbades 3,3 miljoner personer i USA av identitetsstöld, enligt en rapport af Federal Trade Commission, vilket orsakade kostnader för nästan 37 miljarder USD, varav nästan 4 miljarder USD i kostnader för de drabbade individerna. Mellan juni 2002 och juni 2003 drabbades 7 miljoner personer i USA av identitetsstöld, enligt analysföretaget Gartner. I Storbritannien ökade identitetsstölden från 27 270 under 2001 till 42 029 under 2002, med en kostnad för de drabbade personerna på 62,5 miljoner £, enligt Fraud Advisory Panel, en organisation skapad av Revisorförbundet i England och Wales.*

[47] *En genomgång av Internetrelaterade brott finns i Katarina Ritkets Promemoria om Självsanering av Internet (Ds 2003:25) till Justitieminister av 2003-02-07. Online: http://justitie.regeringen.se/propositionermm/ds/pdf/ds2003_25.pdf (per 2003-04-15).*
En annan viktig informationskälla för online brottslighet är den årliga Computer Crime and Security Survey. Studien genomförs varje år av Computer Security Institute i samarbete med San Francisco Federal Bureau of Investigation's Computer Intrusion Squad. Jfr CSI/FBI, Computer Crime and Security Survey. Eight Annual Survey, 2003. Rapporten kan beställas online från http://www.gocsi.com/forms/fbi/pdf.jhtml (per 2003-10-01).

Allmänhetens information om de olika typer av missbruk är inte tillräcklig, vilket gör att många avstår från riskerna genom att inte använda Internet, vilket motverkat visionen om *ett informationssamhälle för alla*.

2.1.3 Att skydda sig: ett medborgaransvar

PTS påpekar vikten för individernas säkerhet av att vidta åtgärder för att skydda informationen på sin dator och av ha kunskap om hur man kan skydda sina personliga uppgifter för att minska individernas risktagande. Läget är bekymmersamt på detta område. Rapporten konstaterar:

> Det är en stor del av Internetanvändarna som inte vidtar åtgärder för att skydda sin dator och sina data. Bredbandsanvändarna är generellt något mer säkerhetsmedvetna, men även i denna grupp tas i stor utsträckning risker. Av de Internetanvändare som har uppringd access, har knappt 30 procent svarat att de inte vidtar några åtgärder för att skydda sin dator eller sina data. Denna siffra kan jämföras med dem som har bredbandsaccess, där 15 procent inte vidtar skyddsåtgärder.

När det gäller de olika sätt att skydda information på den egna datorn, rapporterar PTS:

- *Säkerhetskopior:* Det få personer som enligt undersökningen har tagit regelbundna säkerhetskopior, för att kunna återskapa information om datorns hårddisk skulle bli förstörd, genom olyckshändelse eller ont uppsåt. Siffran för Internetanvändare med uppringd access är åtta procent och för dem med bredbandsaccess tio procent.
- *Inloggningsfunktion:* 16 procent av de tillfrågade med uppringd access hade en inloggningsfunktion på datorn, något som 20 procent av dem med bredbandsaccess hade.
- *Brandväggar:* Av de tillfrågade med uppringd access hade 13 procent en brandvägg installerad. Motsvarande siffra för dem med bredbandsaccess var 52 procent.
- *Virusskydd:* Av bredbandsanvändarna hade 67 procent ett virusskydd som är uppdaterat under det senaste halvåret, vilket 50 procent av dem med uppringd access hade. Bland de tillfrågade i undersökningen kan det finnas de som har svarat nekande på frågan om uppdaterat virusprogram, vilka utan att vara medvetna om det har ett virusprogram som automatiskt uppdateras med jämna mellanrum eller när behov föreligger. Gissningsvis finns en stor grupp användare som har äldre och föråldrade virusprogram, vilket leda till en falsk trygghet hos användaren.

TABELL 1

Andel Internetanvändare som vidtar olika typer av åtgärder för att skydda sin dator och information på hårddisken, redovisat efter accessform, 2002

Typ av säkerhetsåtgärd	Andel av Internetanvändare med uppringd access (procent)	Andel av Internetanvändare med bredbandaccess (procent)
Säkerhetskopior	8	10
Inloggningsfunktion	16	20
Brandvägg	13	52
Uppdaterat virusprogram	50	67

Källa: PTS, E-handel fem förutsättningar, Tabell 7, s 33.

PTS finner ”remarkabelt” att bara en tredjedel av de tillfrågade med bredbandsaccess och hälften av dem med uppringd access saknar ett uppdaterat virusskydd och att nästan hälften av bredbandsanvändarna saknar en brandvägg på den privata datorn samt att det är ovanligt att kryptera information på datorns hårddisk.

Symantec, antivirusföretaget som nyligen har börjat erbjuda säkerhetskonsulttjänster i Sverige har låtit undersöka svenskarnas och skandinavernas datorskyddsvanor och kommit fram till dystra resultat när det gäller små och medelstora företag och betydlig mer uppmuntrande resultat för seniorer i Sverige.

En undersökning i april 2002 omfattande drygt 800 små och medelstora företag i Norden[48] visar att:

- 20 procent saknar virusskydd.
- 56 procent saknar brandvägg.
- 83 procent saknar intrångsdetektering (IDS).
- 17 procent använder sig av kryptering.
- 27 procent har förlorat information eller haft driftstopp p.g.a. virus eller intrång.
- 37 procent anser att de har datasäkerheten i sitt företag under egen kontroll.
- 50procent har en policy för IT-säkerhet.
- 64 procent saknar en konkret uttalad katastrof- och incidentplan.

En undersökning i april 2002, omfattande 1 200 seniorer (över 55 år) som är Internetanvändare[49] visar att:

- 84 procent använder antivirus program
- 45 procent har någonsin haft något virus på sin dator
- 67 procent är rädda för dataintrång eller virus på sin dator
- 36 procent använder brandvägg
- 11 procent har haft intrång på sin dator
- 13procent har förlorat information p.g.a. virus eller intrång
- 35 procent vet inte om de har haft intrång på sin dator

[48] *Jfr http://www.symantec.se/region/se/press/n030520_se.html. (per 2003-05-25).*
[49] *Jfr http://www.symantec.se/region/se/press/n030507_se.html. (per 2003-05-25).*

2.1.4 Personinformation i samband med E-handel och e-post

En annan riskfaktor när det gäller personinformation är att lämna ut information via e-post i samband med e-handel. PTS rapporterar att undersökningen

> (…) visar att det är dubbelt så vanligt bland dem som har e-handlat någon gång, att via Internet ha lämnat sin hemadress, privat telefonnummer eller kontonummer (bank eller postgiro), jämfört med dem som aldrig har e-handlat. Skillnaderna är större när det gäller att lämna ut personnummer eller nummer till konto- eller kreditkort.

TABELL 2

Andel av Internetanvändare som har lämnat personliga uppgifter via Internet

Typ av personlig uppgift	Andel Internetanvändare som aldrig e-handlat men lämnat personliga uppgifter	Andel av Internetanvändare som e-handlat och lämnat ut personliga uppgifter
Hemadress	34 procent	75 procent
Privat telefonnummer	29 procent	65 procent
Privat e-postadress	51 procent	80 procent
Eget personnummer	14 procent	41 procent
Eget bankkonto/pg-kontonr.	4 procent	9 procent
Eget konto/kreditkortsnr.	2 procent	23 procent

Källa: PTS, E-handel fem förutsättningar, Tabell 10, s 35.

Säkerhetsmedvetenheten är större dock bland Inom de personer som e-handlar (oavsett accessform). PTS anger att:

> Av de tillfrågade i denna grupp lämnar 17 procent endast ut uppgifter om det är en säker webbplats. Motsvarande siffra för den grupp som aldrig har e-handlat är nio procent. (Andelen av dem som e-handlar och som krypterar e-post, är för liten för att ha statistisk signifikans, varför den ej redovisas här) Alltså är det 91 procent av dem som lämnar ut personliga uppgifter på webbplatser och aldrig har e-handlat, som *inte* tar hänsyn till om det är en säker webbplats eller ej, till vilken uppgifterna överförs. Av dem som e-handlar är det 83 procent som *inte* tar hänsyn till om webbplatsen är säker eller ej.

PTS drar följande slutsatser av sin undersökning:

- En stor del av Internetanvändarna vidtar inte några åtgärder alls för att skydda sin dator och sina data.
- Bara en tiondel av dem med uppringd access har en brandvägg, något som drygt hälften av bredbandsanvändarna har.
- Hälften av Internetanvändarna med uppringd access ett virusprogram som är nytt eller uppdaterat de senaste sex månaderna, medan 67 procent av bredbandsanvändarna har ett aktuellt virusprogram. Att sakna ett adekvat virusskydd är inte ett problem endast för den enskilde användaren, utan också för alla dem som virus kan spridas vidare till. Även vad gäller andra säkerhetsåtgärder är bredbandsanvändare mer aktiva.

- De som e-handlar har av naturliga skäl i större utsträckning lämnat ut personliga uppgifter på nätet, och enligt denna studie så finns det i denna grupp en något större säkerhetsmedvetenhet, jämfört med den grupp som aldrig har e-handlat.
- En stor andel Internetanvändare tar risker och kan bli offer för olika typer av bedrägerier, att få data förstörda eller på annat vis råka illa ut i onödan, till följd av bristfälliga säkerhetsåtgärder.
- Även andra Internetanvändareutsätts för risker, när en enskild Internetanvändare inte skyddar sig mot till exempel virus eller dataintrång.
- Det framgår inte av studien hur många Internetanvändare som av olika skäl skulle vilja lämna ut känsliga uppgifter via Internet, men som inte vågar av säkerhetsmässiga skäl. Det är troligt att många av dessa skulle kunna lämna ut personliga uppgifter utan att känna oro, med ökade kunskaper om faktiska risker och lämpliga säkerhetsåtgärder.

Undersökningarna säger ingenting om orsaken till att så relativt få vidtar olika skyddsåtgärder. Det kan exempelvis vara bekvämlighet, okunnighet om risker eller okunnighet om hur olika säkerhetsåtgärder vidtas och vilka risker som kan minskas eller undanröjas. Det kan vara besvärligt för konsumenten att sätta sig in i hur olika säkerhetsprodukter och -funktioner fungerar och veta vilken produkt som ska väljas, och det kan vara lätt att glömma bort att uppdatera produkterna.

Vad gäller att lämna ut uppgifter via webbplatser, är det ett problem att många e-handelsföretag inte tillämpar säkra webbplatser. Därmed måste kunden välja mellan att lämna ut uppgifter över en okrypterad förbindelse och att inte genomföra köpet.

2.1.5 Affärsmodeller

Det finns skäl att fråga sig om bristande tillit till IT är verkligen orsaken till den relativ låga användningsnivå av e-handeln i Sverige. Om det vore så, skulle Internetbankerna drabbas av samma relativt låga intresse. Men detta är inte fallet.

World Internet Institute finner i sin undersökning Svenskarna och Internet för året 2003 att medan online bankaktiviteter är den fjärde vanligaste Internetaktiviteten (med 56 procent av Internetanvändarna), ligger e-handeln på 14:4 plats, med 26 procent.[50]

[50] *I denna redovisning har World Internet Institute inte medräknat den 8 % av användarna som bara har provat e-handeln någon enstaka gång. 26 % motsvarar andelen av Internetanvändarna som köper varor eller tjänster online med regelbundhet, dock minst några gånger om året. I tabell 1, sida 17 redovisas att 34% av Internetanvändarna har handlat via Internet: denna tabell inkluderar de som bara har provat någon enstaka gång (8% av användarna).*

Internetbankerna har idag 4,4 miljoner kunder som loggar in ca 30 miljoner gånger i månaden. Under året 2002, ökade antalet kunder med 13 procent.[51] En Demoskop enkätundersökning i september 2002[52] visar att bara 19 procent av de1 261 svarande aldrig har gjort bankärenden på Internet och 5 procent gör bankärenden mer sällan än en gång i månaden. Alltså 76 procent av svaranden gör sina bankärenden på Internet, minst en gång i månaden.

Det ter sig rimligt att tolka intresseskillnaden för e-handel vis-a-vis Internet bankaktiviteter som inte beroende på bristande tillit till tekniken. Förklaringen bör undersökas snarare i affärsmodellerna, vilket gör att problemet ligger utanför IT-politiken och hör snarare till konsumentpolitiken.

2.1.6 Företag-till-företags e-handel och tillit

Den största andelen av all elektronisk handel består av interföretags transaktioner (och interna transaktioner inom stora koncerner), den s.k. B2B (Business to Business).

B2B kan ske med hjälp av diverse verktyg, såsom:

- **E-post** – som används som komplement för traditionell marketing och försäljningskommunikation.
- **Företags webbplats** – Det handlar om online butiker drivna av leverantörsföretag. Detta verktyg har visat sig kräva mer resurser än vad som hade tänkts i början, då man fokuserade bara på de tekniska lösningarna och förbisåg de organisatoriska förändringar som fordrades.
- **Direkt kommunikation** – Fungerar som en direkt länk mellan ett företag och sina affärspartners. EDI är ett exempel av direkt kommunikation.
- **Elektroniska marknadsplatser/eMarknader**[53] – Dessa är många-till-många relationer som i princip är öppna till alla leverantörer och/eller köpare inom en bransch eller ett område. Eftersom dessa är öppna platser råder i dessa huvudsakligen relationer av utbud/efterfråga karaktär för prisbestämningar.
- **Privat utbyte** (**Private Exchanges)** – Dessa är e-markets bestående av en leverantör och flera köpare eller en köpare och flera leverantörer (en till många relation). Benämning privat betecknar att en aktör kontrollerar eMarknaden vare sig i sin egenskap av leverantör eller också köpare.

---

[51] *Jfr Svenska bankföreningen. Internetkunder i Bankföreningens medlemsbanker. Enkätundersökning per december 2002. Online: http://www.bankforeningen.se/pdf/Internetbank%20dec%202002%20aggregerad.pdf. (per 2003-05-03).*

[52] *Jfr Demoskop, Framtidens bankaffärer. Nyhetsbrev Opinionen November 2002.*

[53] *För en utförlig definition och genomgång av verktyget electronic marketplaces, se Marija Popovic, B2B e-Marketplaces. Bryssel, June 2002: European Commission's Electronic Commerce Team (Information Society Directorate General. Online: http://europa.eu.int/information_society/topics/ebusiness/ecommerce/3information/keyissues/documents/doc/B2Bemarketplaces.doc. (per 2002-10-20).*

Exportrådet har låtit analysera B2B: s utveckling efter *hypen*,[54] som visar att

- 45 procent av företagen inte bedriver B2B e-handel i någon form.
- 52 procent av de som bedriver B2B handel gör det genom EDI.
- 42 procent av dem som bedriver B2B handel köper genom leverantörernas hemsidor.
- Drygt 60 procent av dem som bedriver sluten e-handel uppger att mindre än 1 procent av inköp sker via e-handel. Knappt 30 procent uppger att e-handel står för 10-50 procent av deras inköp
- E-market är ett tämligen okänt verktyg bland svenska företag.[55]

Denna dominans av sluten e-handel och den blyga framväxt av eMarknader aktualiserar frågan om tillit och e-handel ur perspektivet B2B. IT-propositionen gör däremot ingen koppling mellan B2B och tillit. Propositionen konstaterar däremot att ”De stora fördelarna med att handla elektroniskt torde emellertid finnas inom området elektronisk handel mellan företag och organisationer” [56], och uttrycker sin tilltro på självreglering och branschöverenskommelser på detta område.

Det finns dock tillitsrelaterade hinder för eMarknads affärer. Dessa har identifierats i en öppen konsultation som EU: s Directorate General Enterprise gjorde till handelskammare, branschorganisationer, företag, e-marknadsoperatörer, tillitsoperatörer, samt e-handelsplattformar under mars-juni 2002. Konsultationen finner följande hinder för användning av eMarknader:

Identifierade hinder för B2B online försäljning:

- Ovisshet beträffande säker hantering av känslig information (data) (54 procent).
- Ovisshet beträffande konfliktlösning (50 procent).
- Ovisshet beträffande informations- och kommunikationssäkerhet (46,9 procent).
- Ovisshet beträffande onlinebetalningar (43,8 procent).
- Övriga brister (26,5 &) till exempel höga startkostnader, höga användningsavgifter, även för att komma i kontakt med redan kända kunder (1,5 procent).

[54] *Silf kompetens AB & Exportrådet (eMarket Service), Inköp och e-handel efter hypen – En undersökning av svenska inköpares inställning till och erfarenheter av elektroniska affärsverktyg i affärsprocessen. Stockholm, September 2001. Online: http://www.emarketservices.com/reports_facts/pdf/Inkop_e-handel_efter_hypen.pdf. (per 2002-10-20).*
[55] *Mellan 60 % och 75 % av respondenterna känner inte till någon eMarknad. Jfr A.a. s 26.*
[56] *Prop. 1999/2000: 86, s 106.*

Identifiera hinder för B2B online inköp:

- Ovisshet beträffande skydd av känslig data (59,4 procent).
- Ovisshet beträffande informations- och kommunikationssäkerhet (57,8 procent).
- Brister i informationstydlighet när det gäller avtalsmässiga villkor (till exempel tillämplig lagstiftning, jurisdiktion, mm) (56,3 procent).
- Ovisshet beträffande konfliktlösning (50 procent).
- Ovisshet beträffande onlinebetalningar (48,4 procent).
- Brister i informationstydlighet när det gäller stegen för att sluta ett avtal (42,2 procent).
- Brister i informationstydlighet när det gäller företagens identitet (37,5 procent).
- Brister i informationstydlighet när det gäller rätten att träda ur ett avtal (35,9procent).
- Brister i informationstydlighet när det gäller retur av beställda varor och återbetalning (34,4 procent).
- Övriga informationsbrister, till exempel: produkttillgång och leveranstider (29,7 procent); betalningsmetoder (25 procent); certifiering av produkter/tjänster (23.4procent); varupriser, tilläggskostnader inkl. (20.3procent); varuförsäkringar (18,8 procent); leveranskostnader (15,6 procent); transaktionsspråk (14,1 procent).[57]

Konsultationens resultat aktualiserar frågar om en tillitsmärkning för e-handelsaktörer, samt självreglering och etiska koder. Dessa frågor får det bestämda stödet av respondenterna i konsultationen.

2.1.7 Tillit i Lagen om elektronisk handel

I lagstiftningen om e-handel som följde IT-propositionen föll tillitsfrågan bort. Det förefaller som att regeringen och riksdagen under tiden har nedvärderat tillitens centrala roll i IT-politiken eller som att elektronisk handel inte skulle behöva harmoniseras med IT-politiken.

[57] *Jfr Open consultation on Trust barriers for B2B e-marketplaces. Presentation of the main results. Online: http://europa.eu.int/comm/enterprise/ict/policy/b2b-consultation/b2b-trust-cons-sum.pdf. Denna sammanställning är en översättning av Helen Lassen, eMarket Places: Trust Barriers and Trust Marks. eMarket Services (www.emarketservices.com), okt. 2002, uppdaterad i jan. 2003.*

Den 1 juli 2002 trädde lagen om elektronisk handel i kraft.[58] Propositionen nämner tillit bara en gång och i samband med elektroniska signaturers utformning.[59] Lagutskottets betänkande tar inte heller upp tillitsfrågan.[60] Detta ter sig paradoxalt eftersom direktivet baserade behovet av lagstiftning i frågan på tillit och förtroende.

Näringsdepartementet förklarar denna till synes paradoxala situation genom att hänvisa att lagstiftningen om e-handel byggde på ett EG-direktiv och att föra in en så stor fråga som tillit i det svenska genomförandet av lagen torde sig inte varit möjligt. Vidare förklarar Näringsdepartementet att propositionen *Samhällets säkerhet och beredskap* (Prop. 2001/02: 158) tar upp frågorna om informationssäkerhet och ansvarsfördelning.[61] Återigen hänvisas tillitsproblematiken till informationssäkerhetsfrågor.

2.2 Integritet och personinformation

Sedan Personuppgiftslagen (PUL) trädde i kraft, har diskussionen kring dess effektivitet och tillämplighet varit animerad i Sverige.

PUL etablerar en princip, dock implicit i texten. Varje person äger sina personliga uppgifter och därmed bör användning av dessa personuppgifter i IT-baserade system och tjänster vara kända och godkända av de aktuella individerna. Det är många som anser att PUL har detaljreglerat till en punkt som motverkar sitt syfte eller sätter hinder för processer som prioriteras i IT-politiken.

I samband med framvästen av Internet, i synnerhet ***www***, blir konflikten mellan lagskyddad personlig integritet och offentlighetsprincipen mer tydlig. Denna konflikt var redan tydliggjort i förarbete av PUL.[62]

Samtidigt känner sig svenskarna otrygga när det gäller den personliga integriteten i samband med IT-baserade tjänster.

Inom de statliga myndigheterna råder en föreställning om att PUL är ett hinder för att förverkliga 24-timmarsmyndigheten[63], som i sin tur betraktas av regeringen som det främsta sättet för att staten skall bli en förebild när det gäller IT-användningen.

---

[58] *SFS 2002:562, Lag om elektronisk handel och andra informationssamhällets tjänster. Den bygger på Prop. 2001/02: 150. Lagen är den svenska responsen till harmoniseringskrav som uttrycks i Europaparlamentets och rådets direktiv 2000/31/EG av den 8 juni 2000 om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden ("Direktiv om elektronisk handel"), som trädde i kraft den 17 juli 2000.*

[59] *Jfr Prop. 2001/02: 150, s 84.*

[60] *Jfr Lagutskottets betänkande 2001/02: LU29. Lag om elektronisk handel och andra informationssamhällets tjänster, med mera.*

[61] *Dessa förklaringar framfördes 2003-10-09 i ett e-postmeddelande från Enheten för IT, forskning och utveckling, Näringsdepartementet till denna studies författare.*

[62] *Konflikten mellan integritetsskyddet och offentlighetsprincipen kan få allvarliga konsekvenser för demokratin i Sveriges offentlighet. Den banbrytande studien som Lars Ilshammar gjorde i sin doktorsavhandling bör tas till grund för vidare forskning och för att skapa agila varningssystem då det uppstår grundläggande principiella konflikter i samband med omvandlingen till informationssamhället. Jfr Lars Ilshammar, Offentlighetens nya rum – Teknik och politik i Sverige 1969-1999. Örebro Studies in History, DemocrIT nr. 1, 2002 (ISBN 91-7668-302-8).*

IT-propositionen saknade tydlighet och konkreta förslag beträffande skydd för integriteten och den efterkommande lagstiftningen har inte tagit upp denna fråga.[64]

PTS rapporterar i E-handel – fem förutsättningar beträffande individernas skydd av sin personinformation följande:

- *Elektroniska signaturer:* Det är en liten andel av Internetanvändarna som i enkäten har angivit att de utnyttjar elektroniska signaturer (e-signaturer), knappt tre procent av de tillfrågade med uppringd access och knappt fyra procent av dem med bredbandsaccess. Det kan förmodas att det i verkligheten är fler som använder e-signaturer, men som inte själva är medvetna om det, till exempel vid kontakter med en Internetbank. I en undersökning från PTS[65], avseende bl.a. hur allmänheten betalar räkningar, visas att det i januari år 2003 var 39 procent som betalade sina räkningar över Internet, att jämföra med 32 procent i januari år 2002. En större andel än fyra procent av dessa, torde utnyttja elektroniska certifikat vid sina bankkontakter.
- *Lämnar information på säkra webbplatser:* Det är nio procent av dem med uppringd access som har uppgivit att de endast lämnar information på säkra webbplatser (vilket innebär att informationen som skickas mellan användarens dator och webbplatsen är krypterad). Motsvarande siffra för dem med bredbandsaccess är 12 procent.
- *Krypterar e-post:* Endast två procent av dem med uppringd access krypterar viktig information innan den skickas över Internet med e-post, något som en andel om fem procent av bredbandsanvändarna gör.

TABELL 3

Andel Internetanvändare som har uppgivit att de vidtar åtgärder för att skydda data som överförs via Internet, redovisat efter accessform, 2002

Säkerhetsgrad	Andel av Internetanvändare med uppringd access (procent)	Andel Internetanvändare med bredbandsaccess (procent)
Använder e-signatur vid överföring av viktiga dokument	3	4
Lämnar information endast på säkra webbplatser	9	12
Krypterar information som skickas via Internet	2	5

Källa: PTS, E-handel fem förutsättningar, Tabell 8, s 34.

[63] *Exempelvis, angav flera deltagare i ett Statskontorsseminarium den 27 november 2002 att ett av de främsta hindren för att implementera 24-timmarsmyndigheten var PUL. Alla deltagare i seminariet var företrädare för myndigheter och arbetar direkt med IT eller organisations- eller tjänsteutveckling.*

[64] *Lagen om elektronisk kommunikation, som trädde i kraft den 25 juli 2003, etablerar att alla som besöker en webbplats med cookies skall få information om att webbplatsen innehåller cookies, vad dessa cookies används till och hur cookies kan undvikas. Detta, även om det är viktigt, är marginell när det gäller de integritetsskyddsproblem som är olösta och som orsakas eller förvärras av IT-baserade system och elektronisk kommunikation. Detta har både Konvergensutredningen och Formelutredningen förbisett.*

[65] *Postens service – kassatjänst, PTS 2003.*

TABELL 4

Andel av Internetanvändare som under de senaste sex månaderna har lämnat ut olika typer av personliga uppgifter på Internet, redovisat efter accessform, 2002

Typ av personlig uppgift	Andel av alla Internetanvändare (procent)	Andel av Internetanvändare med uppringd access (procent)	Andel av Internetanvändare med bredband (procent)
Hemadress	56	53	65
Privat telefonnummer	49	46	59
Privat e-postadress	68	65	81
Eget personnummer	27	25	33
Eget bankkonto/pg-kontonr.	7	6	10
Eget konto/kreditkortsnr.	13	9	22

Källa: PTS, E-handel fem förutsättningar, Tabell 9, s 34.

De brister hos användarna som redovisas ovan tyder på att det inte räcker med att skapa instrument och säkra infrastrukturen eller vidta åtgärder från staten eller den offentliga sektorn. Medvetenhet, mognad och kompetens hos användarna måste höjas.

Datainspektionen genomförde ett tillsynsprojekt under våren och hösten 2002 för att kontrollera hur kunders personuppgifter hanteras vid e-handel. Tillsynen utövades på 50 slumpvis utvalda företag.

I projektet kom Datainspektionen fram till:

- Att det råder en okunskap om vem som har yttersta ansvaret för de personuppgiftshandlingar som utförs. Enligt PUL är den personuppgiftsansvarige i ett företag eller organisation också huvudansvarig för IT-säkerheten, som är en mycket viktig del av det skyddet
- Att Informationen till de registrerade uppfyllde sällan PUL:s krav.
- Att rutiner för gallring saknades i de flesta fall.
- Att flera av företagen inte hade gjort någon säkerhetsanalys av den egna IT-miljön.

Det förefaller tydligt att tillämpningen av PUL är svår, att både myndigheternas tjänstemän och företagens personal saknar kunskap och förståelse för PUL, att PUL hamnar i konstant konflikt med offentlighetsprincipen.

Det ter sig rimligt att tolka situationen som olöst när det gäller IT-politiken och personlig integritet. Detta är inte förvånansvärt, eftersom själva problemområdet är fullt av konflikter, däribland:

- Ideologiska konflikter mellan individperspektiv och statens perspektiv.
- Kommersiella konflikter mellan företagens kundhantering och individens skyddsbehov.
- Processrelaterade konflikter mellan effektivitet (genom informationsspårbarhet) och personlig integritet.
- Kulturella konflikter mellan öppenhet och integritetsskydd.
- Säkerhetsrelaterade konflikter mellan statens behöv av skydd och individens behov av skydd.[66]

I grunden för dessa konflikter finns den omvandling som samhället genomgår i samband med framväxten av det s.k. informationssamhälle i form, bl. a. av en utsuddning av de traditionellt tydliga sfärerna för det offentliga, det privata och det intima. En särskild svårighet i det IT-politisk sammanhanget är att realisera en politik som ramas in i visionen *ett informationssamhälle för alla*, utan att lagstiftaren har ens skissera vad det är för samhälle som betecknas av termen *informationssamhälle*.

2.3 Förtroende som grund för institutionell tillit

Sveriges befolkning är ett förtroendefolk. Diverse undersökningar om socialkapital har, till exempel, visat att Sverige, tillsammans med Norge och Finland befinner sig högst i frågan om tillit bland de länder som har studerats. Sveriges befolkning utmärker sig i sitt förtroende för myndigheterna.

2.3.1 Medborgarundersökningen (Statskontoret)

Statskontoret genomför på uppdrag av regeringen en medborgarundersökning i samarbete med Statistiska centralbyrån.[67] Denna undersökning ger intressanta indikationer på medborgarnas förtroende för och nöjdhet med samhällets institutioner.

Undersökningen har under året 2002 mätt medborgarnas förtroende för förvaltningen genom att fråga om tolv verksamheter. Resultatet redovisas i tabellen nedan.[68]

[66] *Jfr Datainspektionen (Rapport 2003:2), Behandling av kunders personuppgifter vid elektronisk handel. Stockholm, april 2003, s 3.*

[67] *Statskontoret (2002:12) Att ta reda på vad folk tycker. En pilotundersökning om medborgarnas syn på offentlig förvaltning. (ISBN 91-7220-489-3).*

[68] *Rapporten varnar: ”Tänk på följande vid läsning av tabellerna. Svarsbortfallet är högt – speciellt för domstolar och åklagare – och skillnaderna mellan myndigheter och olika grupper av svarande är ofta marginella. Det bör vara en skillnad på mer än ett skalsteg för att det ska vara värt att kommentera.” Jfr A.a. s 33.*

TABELL 5

Förtroende för tolv offentliga verksamheter 2002, medelvärden

Myndigheter/verksamheter	Förtroende
Universitet/högskolor	7,0
Förskolan	6,6
Polisen	6,3
Sjukvården	5,9
Skattemyndigheterna	5,9
Domstolarna	5,9
Åklagarna	5,8
Grundskolan	5,7
Försäkringskassan	5,5
Vägverket	5,5
Äldreomsorgen	4,6
Arbetsförmedlingen	4,1
Medelvärde (oviktat)	5,7

Anmärkning. De svarande har fått ange en siffra mellan 1–10, där 1 är mycket lågt förtroende och10 mycket högt.

Källa: Statskontoret (2002:12).[69]

Det genomsnittliga förtroendet för de tolv verksamheter som ingick i undersökningen är **”medelmåttig”**.[70] Detta förklaras i Statskontorets rapport på följande sätt:

> Det genomsnittliga förtroendet för de tolv verksamheterna är medelmåttigt. Korrekt behandling, tjänster med god kvalitet och god service är de aspekter som för förvaltningen i stort får det bästa betyget. Myndigheternas förmåga att samarbeta med varandra och reglernas lättbegriplighet var de områden där förvaltningen fick det sämsta omdömet.
>
> Tittar man på de myndighetsspecifika frågor som berör de förvaltningspolitiska värdena, är kvalitet och service de delar som medborgarna och brukarna är mest nöjda med. Lägst omdöme fick inflytande.
>
> Undersökningen visar också på en mer negativ inställning till förvaltningen som helhet än till enskilda myndigheter. Förklaringen kan vara att det är lättare att vara negativ till något som är stort och abstrakt än till specifika verksamheter, som det är lättare att se nyttan med.[71]

[69] *A.a. s 34.*
[70] *A.a. s 16.*
[71] *A.a.*

Medborgarundersökningen tar inte upp frågan om tillit, vilket kan betraktas som en brist, särskilt med tanke på tillitens centrala roll i den nationella IT-politiken. Detta kan förklaras med att den allmänrådande föreställningen inom statsförvaltningen på hög nivå är att tillit är en fråga om teknisk säkerhet. Relevansen av att mäta medborgarnas tillit för myndigheterna, dess tjänster och IT-baserade system är hög med tanke på att tillit är en grundläggande förutsättning för att harmonisera 24-timmarsmyndigheten med det förvaltningspolitiska programmet En förvaltning i medborgarnas tjänst, samt regeringens PM om En förvaltning i demokratins tjänst. Denna harmonisering är av central vikt för att uppnå visionen *ett informationssamhälle för alla*.

2.3.2 Riksskatteverket

Riksskatteverket har redovisat en studie om medborgarnas förtroende för myndigheten som genomfördes i slutet av 2002. Studien visar att 48 procent av medborgarna har förtroende för skattemyndigheten och 10 procent saknar det, vilket är en förbättring i jämförelse med tidigare år. 10procent fler medborgare har förtroende för skattemyndigheten än de som har förtroende för myndigheterna i allmänhet.[72]

Riksskatteverket har samtidigt upplevt en besvikelse med det som betraktades som en låg användning av onlinedeklarationen i år, då ca en halv miljon personer deklarerade online. Samtidigt uppger RSV att tillit inte har varit ett prioriterat område vid definitionen av online-deklarationstjänsten.[73]

En uppföljning som gjordes av e-deklarationen visar att bara 13 procent av de personer som fick erbjudande om att deklarera på Internet eller telefon, använde onlinedeklarationen. 7 procent av dem som fick erbjudandet angav att de inte litar på Internet som skäl för att inte ha deklarerat online, medan 27 procent i samma grupp avstod från att deklarera online, eftersom de upplevde det som krångligt, komplicerad eller svår.[74]

Riksskatteverket kan betraktas som en föregångare när det gäller implementering av IT-baserade tjänster inom staten, både när det gäller omfattning och kvalitet. Därför är det intressant att konstatera att tillit inte har varit något prioriterat område. Mycket talar för att tolka detta som att det stora förtroende som medborgarna har för myndigheten betraktas som tillräcklig grund för att myndighetens IT-baserade tjänster skall ha bred acceptans. Online deklarationen år 2003 är en tankeställare som kan leda till att större uppmärksamhet läggs till de tillitsfrämjande faktorerna i samband med ny- eller vidareutveckling av online tjänster.

[72] *Jfr RSV (Rapport 2003:2) Allmänhetens synpunkter på skattesystemet, skattefusket och myndigheternas kontroll. April 2003.*
[73] *Information per telefon av Riksskatteverkets chefredaktör, Björn Thärnström den 22 augusti 2003.*
[74] *Jfr NFO Infratest, Riksskatteverket – Uppföljning av e-deklaration. Projekt 14130. Göteborg 2003-06-10 (stencil).*

2.3.3 Socialförsäkringssystemet

Mer abstrakta system som socialförsäkringssystemet lider av brist på befolkningens förtroende. I en undersökning som Statistiska centralbyrån har gjort på uppdrag av Riksförsäkringsverket redovisas att:

- Enbart 12 - 22 procent av de intervjuade gav högt betyg tillsocialförsäkringssystemet, medan 21–29 procent gav ett lågt betyg.
- Försäkringskassorna får högre betyg än socialförsäkringssystemet, men inte ett högt betyg: Klart godkänt – men inget överbetyg,
- Bara hälften av de intervjuade litar på sekretessen vid Försäkringskassorna, medan ca 15 procent inte litar på det.

Den kritiska hållningen till socialförsäkringssystemet gäller också för offentlig verksamhet i övrigt.[75]

2.3.4 Förtroende räcker inte för att öka användningen

Det finns fog för att påstå att förtroende till myndigheten eller organisationen inte är en avgörande faktor för att skapa tillit till IT-baserade tjänster.

Vikten av anseendet (reputation) kan inte nekas som en faktor som påverkar personernas benägenhet att lita på en agent eller organisation. Men det vore felaktigt att betrakta anseendet som tillräckligt: anseendet kan konstrueras på tom PR och annan institutionell reklam.

Tillit däremot förutsätter rejäl kvalitetssäkring i system och tjänster, vad enligt vår mening inbegrips i tillförlitligheten.

[75] *Jfr SCB, Rapport för undersökningen som genomfördes våren 2003 som en postenkät riktad till ett slumpmässigt urval av befolkningen i åldrarna 25-74 år, 2003. (PDF, online: http://www.rfv.se/press/pm/2003/docs2003/pm34_03.pdf)(Per 2003-08-25).*

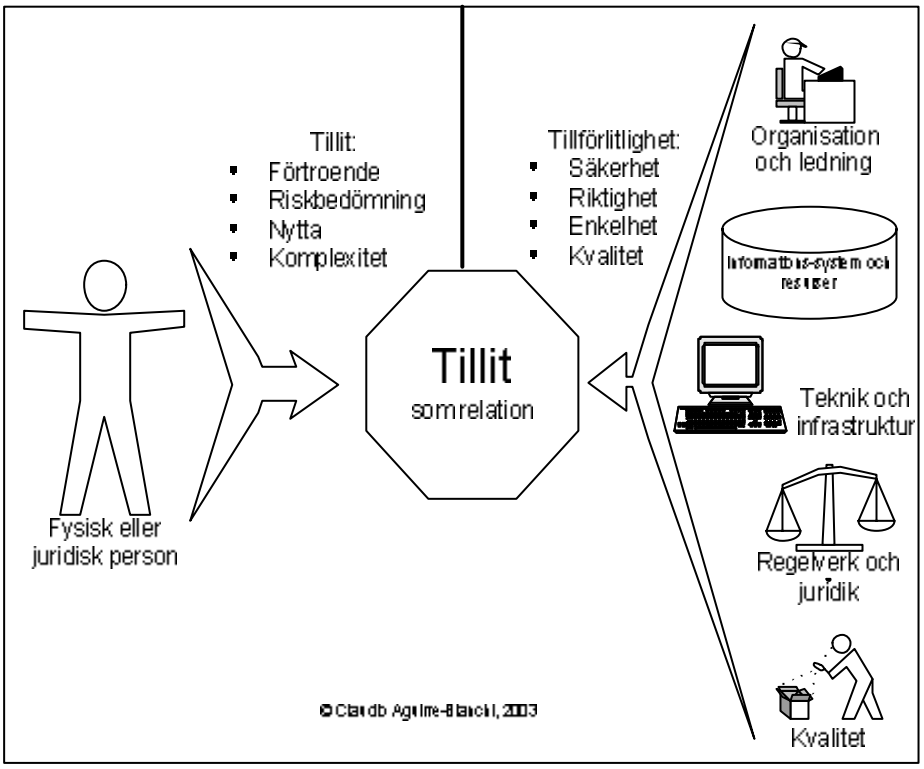
3 Begreppsrekonstruktion: Om tillit och tillförlitlighet

Detta kapitel kommer att bygga på den här rapportens tidigare avsnitt ur två olika perspektiv som samverkar med varandra:

- Teori- och metodutveckling (begreppsrekonstruktion) och
- Individens status i realisering av IT-politiken.

Syftet med detta avsnitt är att lägga upp grunderna för ett nytt sätt att omsätta tillitsproblematiken i politik. Detta nya sätt bygger på att betrakta tillit som en relation mellan subjektiva företeelser, och kvalitetsegenskaper i organisationer, tjänster och processer i samhället. Tillit kommer i detta avsnitt att behandlas som en relation mellan fysiska eller juridiska personers benägenhet att ta risker (eller betala priser) för att använda sig av en tjänst eller delta i en process och organisationernas förmåga att prestera kvalitativa tjänster och säkra processer. Tillit till IT-baserade tjänster och produkter kommer att betraktas som en flerdimensionell företeelse där relationen mellan å ena sidan risk och totalkostnad för den brukande personen och å andra sidan sannolikheten av att få det förväntade resultatet är betingande.

Figuren nedan representerar tillit som relation mellan en brukande person och flera kvalitetsdimensioner som är egenskaper av IT-baserade tjänster och produkter:



Tillit är följaktligen en angelägenhet som i sig inte kan operationaliseras i politik, om politiken skall bedrivas inom ramen av demokratiska processer med respekt för individens åsiktsfrihet och valfrihet i samspel med samhällets institutionella och organisatoriska grundvalar.

Genom tillit sammansvetsas samhället i en ständig kommunikationsprocess som bygger på att man bildar det informella (reella) samhället genom att kommunicera det i gemenskap.[76]

Det politiska rummet för de tillitsrelaterade frågorna kommer i enlighet med vår begreppsrekonstruktion att koncentreras på tillförlitligheten, d v s en kvalitetsdimension bestående av egenskapar tillhörande system och tjänster och som säkerställer:

- Säkerheten.
- Riktigheten.
- Enkelheten.
- Kvalitén.

Tillförlitlighetsbegreppet har definierats som en kvalitetsdimension i svenska och internationella standarder. Dessa standardinriktade definitioner och relaterade operationaliseringar bör revideras med syfte att omfatta IT-baserade tjänster och system i ett minimalistiskt standardiseringsperspektiv som bygger på absolut nödvändiga krav som måste uppfyllas men som är samtidigt tillräckligt flexibla att de kan anpassas efter samhällets förändring.

3.1 Från tillit till tillförlitlighet

När det gäller begreppet tillit, har vi utgått från den operationalisering som Meta Group nyligen har utvecklat, som redovisas i kapitel **1.6 Tillitsbegrepp inom IT-branschen**, sida13.

Meta Groups hantering av tillit (trust) fungerar bra för tjänsteproducenterna och huvudsakligen för att översätta säkerhetsbehoven såsom de upplevs av de verksamhetsansvariga i ett företag eller organisation som ansvarar för verksamheten till nivåer av säkring som ett IT-baserat system eller process behöver för att uppfylla de kvalitetsvillkoren (tillförlitlighet) som systemet eller tjänsten måste kunna garantera till brukarna. Det handlar om att översätta kvalitetsvillkor i informationssäkerhetsåtgärder och följaktligen omsätta dessa åtgärder i tekniska lösningar.

Meta Groups operationalisering är inte lika tillämpningsbar när det gäller brukarnas vilja eller benägenhet att använda eller acceptera dessa system eller tjänster. Meta Group fokuserar på producentsidan och omfattar inte brukarsidan.

---

[76] Detta är en mycket viktigt idé om det demokratiska, människocentrerade samhället som utvecklades av John Dewey i sin bok Democracy and Education: "There is more that a verbal tie between the words common, community, and communication. Men live in a community in virtue of the things which they have in common; and communication is the way in which they come to possess things in common. What they must have in common in order to form a community or society are aims, beliefs, aspirations – a common understanding – like-mindedness…" skrev Dewey 1916. Jfr John Dewy, Democracy and Education, Macmillan Company, 1916. Citerad ur Colliers första Free Press Paperback Edition, 1966. Macmillan Canada, Ldt., s 4. (ISBN saknas).

Meta Groups modell för *trust* skapar förutsättningar för rätt hantering av tillförlitlighet inom en organisation i samband med utformning, införande, genomförande och förvaltning av IT-baserade tjänster och system.

Vi har valt att översätta *trust* i Meta Group till *tillförlitlighet*, istället för *tillit*. Tillförlitlighet är en egenskap av objekten IT-baserade tjänster och system. Tillförlitlighet betecknar med större precision än tillit de processer som så väl beskrivs av Meta Group.

Vår ambition i detta avseende är inte att ge svar på dessa problem, utan att föra fram ett resonemang som kan belysa vägar och därmed bidra till att utveckla lämpliga metoder för att stärka:

- Medborgarnas tillit för IT-baserade offentliga tjänster.
- Konsumenternas tillit för e-handeln.
- Individens trygghet beträffande skyddet av den personliga integriteten.

Tillit är inte ett begrepp som kan operationaliseras i samband med IT-relaterade tjänster i produkter om inte dessa skapar efter ett holistiskt utvecklingsperspektiv. Det är nödvändigt att tjänstedesign och tjänsteutveckling för informationssamhället görs efter ett utvecklingsperspektiv som ser på alla de medverkande processer, aktörer och resurser som medverkar i en tjänst.[77]

Att konkretisera tillitsbegreppet så att det kan bli operationellt för att definiera, formulera, bedriva och utvärdera IT-politik förutsätter en tydligare definition av:

- Tillitens subjekt – förutsättningar för brukarens benägenhet att lita på IT-baserade tjänster och system.
- Tillitens objekt – egenskaper hos IT-baserade tjänster och system som gör dem tillförlitliga.
- Tillit och användning – användningsfaktorer som påverkar tilliten och som hör till kvalitetsegenskaper i användningen.

3.1.1 Tillitens subjekt

Både Meta Groups trustbegrepp (tillförlitlighet i vår översättning) och innebörden av tillit i de IT-politiska dokumenten som har analyserats i den här studien, placerar tilliten på tjänsteleverantörsidan, genom att likställa trust/tillit med säkerhet. Fokus är i detta perspektiv att identifiera de åtgärder, processer och tekniker som kan skapa den säkerhetsnivån som betraktas av tjänsteproducenter och systemägare som tillräcklig för att brukarna skall kunna utöva en befogad tillit till dessa. Denna infallsvinkel är angeläget och bör utvecklas vidare, dock bör inte betraktas som den enda, ens den viktigaste, dimensionen av tillit.

Det är inadekvat att förvänta sig att enbart genom säkerhetsåtgärder för infrastrukturen, processer och tjänster, i kombination med lagstiftning, kan tillit för de nya tjänsterna skapas. En sådan föreställning kan dessutom leda till en betraktelse av

[77] *Denna studie syftar inte till att presentera en utvecklingsstrategi, därför kommer vi inte att fördjupa oss i detta resonemang. Figuren i början på det här kapitlet (sidan 40) är en bra utgångspunkt för att tänka på tillit i utvecklingstermer.*

personerna (medborgare, företag och organisationer i det civila samhället) som objekt av staten. Aktiva medborgare, dynamiska företag och välfungerande nätverk av frivilliga och intresseorganisationer – som är socialkapitalets infrastruktur – kommer att bedöma, tolka och utvärdera den graden av tillförlitlighet som IT-tjänsterna och systemen erbjuder, inför en användningssituation som förutsätter brukarens tillit. Dessa sociala aktörer kan inte underordnas tekniska eller organisatoriska system: de är samhällets kärna, och existerar i den informella sektorn.

Tillit är inte en egenskap av IT, IT-infrastrukturen eller av IT-baserade tjänster eller system. Tillit är en egenskap av användningen, en relation eller interaktion mellan brukarna och IT-produkter och tjänster. Därmed måste fokus på individen som tillitens subjekt göra sig gällande i varje försök att operationalisera tillitsbegreppet.

Tillitens subjekt är personer. Fysiska eller juridiska personer som brukar de IT-baserade tjänster, produkter eller system som, i sin tur, är tillitens främsta objekt.

Den gängse och dominerande betraktelse av tillit som en direkt översättning av det ganska löst använda engelska begreppet ***trust*** inom IT-industrin, ställer fler och allvarligare problem än de som syftas att lösas.

När det gäller subjektets benägenhet att utöva tillit, bör det kvarstå som fri från reglering och statlig inblandning: tillit utgör en grundläggande förutsättning för det sociala livet och den existerar på samhällets informella sektorn.

3.1.2 Tillitens objekt

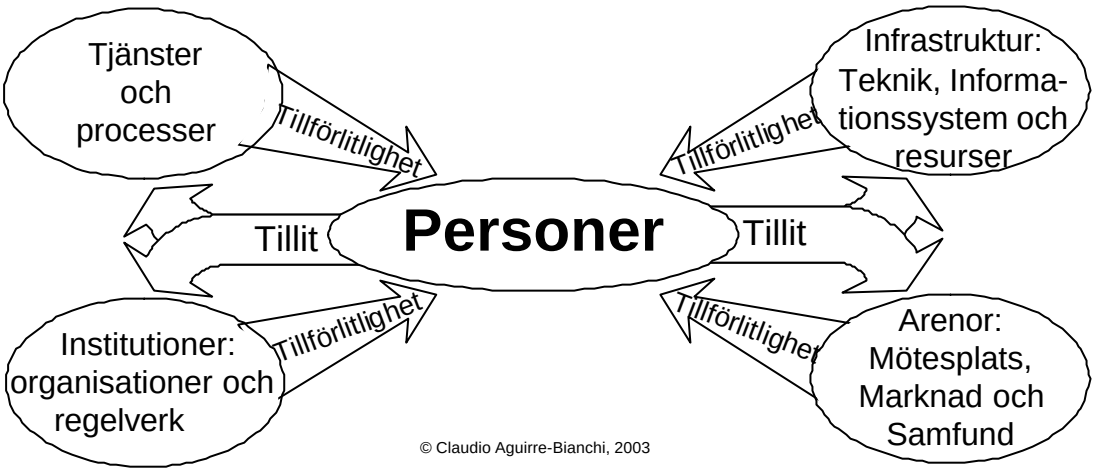
Tillit, betraktad som en relation mellan de fysiska eller juridiska personernas attityder och benägenhet att förlita sig på andra aktörer eller företeelser (såsom IT-baserade tjänster och produkter) kan riktas mot olika typer av agenter eller objekt. I sammanhanget av denna studie har vi identifierat följande relevanta objekt för tillit, nämligen:

- Tjänster och processer (tjänsteprocesser, såsom den årliga inkomstdeklarationen, eller e-handel).[78]
- Institutioner: organisationer (både myndigheter, företag och andra tjänste- eller informationsförmedlande organisationer), inkluderar andra samhällsinstitutioner, såsom regelverk, mm.

[78] *Denna kategorisering har vi gjort med utgångspunkten i konvergensfenomenet, som ligger som grundförutsättning för IT-politiken. Jfr Claudio Aguirre-Bianchi, Konvergens, integration och omvandling av den publika sfären, 2003. Documentet (PDF) kan beställas via e-post från cab2@metamatrix.se.*
Det vore rimligt att argumentera att tillit på en process som den årliga inkomstdeklarationen tillhör egentligen kategorin Tillit till organisationer (skattemyndigheten), eftersom det finns en tydligt ansvarig myndighet för processen. Vi har ändå valt att särskilja en tillitskategori för processer och tjänster som är så legitimerade att individen inte bryr sig om vilken den ansvariga organisationen är. Detta har en intressant bäring i definitionen av informationsstrategier som har i syfte att öka och/eller stärka individens tillit för nya former eller kanaler för realisering av legitimerade och grundläggande samhälliga processer. Vi vill påpeka att inom ramen av s.k. 24-timmarsmyndigheten är visionen "ett ärende, en myndighetskontakt" central och den riktar medborgarfokusen på processen istället för myndigheten; ett tydligt exempel för detta är Kontakt-N (samtjänst av RSV och PRV).

- Infrastrukturen, bestående av utrustning, nätverk och system, samt Informationsresurser, som till exempel samhällets grundläggande informationsresurser.
- Arenor, som i sammanhanget syftar på virtuella arenor vart individernas möt och agerar socialt, utbyter varor, tjänster och symboliska värden. Bland arenorna kan räknas de virtuella platserna som underlättar personernas tillgång till maskinella processer, såsom tjänsteportaler.

Tillitsrelationen och dess objekt representeras grafiskt som nedan:



3.1.3 Tillit och användning av IT-baserade tjänster

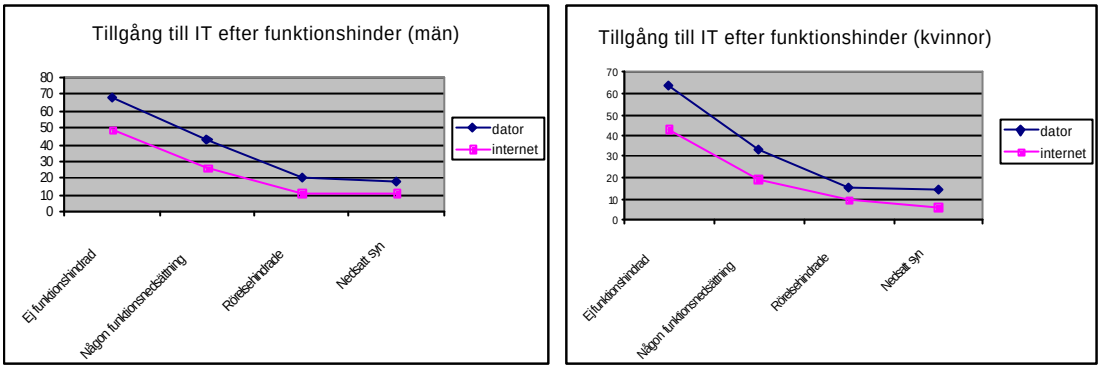
Tillit till IT är en egenskap av användningen av IT-baserade tjänster.

Användningen är interaktionen mellan det institutionella objektet (leverantörsidan: myndigheter och företag) och det personliga subjektet (både fysiska och juridiska personer). För att operationalisera ett sådant begrepp är det viktigt at fokusera på tillitens objekt och på konvergensfenomenet. Därmed är tillförlitligheten det centrala element för att operationalisera tillit till IT och för att omsätta denna tillit i politik.

Brukarens första och främsta upplevelser av någon IT-baserade tjänst sker vid kontaktytan (medium och användargränssnitt) och bestäms sedan i en kombination av minnesbilden av den första upplevelsen och användarens värdering tjänstens nytta och utformning (tjänstedesign) i relation till tjänstens kostnad (i tid och ansträngning) och de risker som kan vara aktuella för användaren.

Eftersom den första kontakten med ett medium eller ett informationsgränsnitt är avgörande för individens tillit till den aktuella tjänsten, är det angeläget att kartlägga och tydliggöra relationen mellan tillit och användbarhet av en IT-baserad tjänst.

Ett bra sätt att synliggöra denna relation är att analysera frågan om tillgängligheten till IT för funktionshindrade. En studie genomfört av H@handikapp.se/Funka Nu[79] år 2000 visar ett tydligt samband mellan funktionshinder och minskad användning av IT. Studien visar även att ju gravare funktionshindret är desto mindre används IT av den aktuella personen.



Källa: H@andikapp.se (2000).[80]

Det sambandet funnen i studien genomfört av H@ndikap.se/Funka Nu är högsta grad relevant, eftersom användbarhet och tillgänglighet ur perceptionsförmåga och kulturellt perspektiv lär vara otillfredsställande i de statliga IT-baserade tjänster.[81]

Tillförlitligheten stärks med bra användbarhet och tillgänglighet i tjänsterna och system. Därför bör dessa betraktas som element i det samlade kvalitetsdimension som betecknas av tillförlitlighet.

[79] *H@andikapp.se var handikapprörelsens samarbetsorganisation för IT. Funka Nu är ett företag som föddes som ett projekt inom handikappsrörelsen och vars verksamhet fokuserar på att underlätta IT-användningen hos människor med funktionshinder.*

[80] *H@ndikapp.se, Användning av dator och Internet för personer med funktionshinder - kartläggning 2000. Rapporten finns i pdf-format och kan beställas genom e-post till Stefan Johansson [stefan.johansson@funkanu.se].*

[81] *Jfr Riksrevisionsverket (RRV 2003:11), Ett informationssamhälle för alla? Användbarhet och tillgänglighet hos statliga webbplatser. (ISBN 91-7498-510-8). Online: I den nya myndigheten Riksrevisions webbplats: http://www.riksrevisionen.se.*

3.1.4 Tillitens rimlighet i IT-politiskt sammanhang

Tillit är i sig inte alltid en önskvärd egenskap. Beroende på relationen mellan den litande personen och det litade objektet, samt de risker och nyttoförväntningar som finns inblandade i relationen, kan tillit (och dess motsats misstro) klassificeras enligt följande kvadrant:

	Befogad	**Obefogad**
Tillit	Befogad tillit	Obefogad tillit
Misstro	Befogad misstro	Obefogad misstro

Denna kvadrant har vi lånat från professor Cecilia Magnusson-Sjöberg[82], och ter sig lämplig för att klassificera tillit till IT-baserade tjänster.

Var ambition har varit att använda denna modell för analys av tillitsdata, men de disponibla data är inte av den karaktär som lämpar sig för en sådan analys. Matrisens potential för angelägna analyser av tillit i relation till IT-baserade tjänster, system och produkter kvarstår, även om avsaknad av relevant data omöjliggör dess tillämpning i denna studie.

3.1.5 Problematisering av IT-propositionen och dess tolkningar

IT-propositionen definierar inte tillit. Däremot uttrycker propositionen en tydlig säkerhetsfokusering på tillit med betoning i lagstiftning och tekniska samt infrastrukturella åtgärder. Eftersom säkerhetshantering består av ytterst komplexa tekniska och administrativa procedurer, förskjuts ansvaret för att skapa tillit till säkerhetsspecialister, med tydligt avgränsning av ett brett deltagande av medborgarna och det civila samhällets organisationer i utformningen av tillit.

Ovanstående innebär en intressant paradox där det sociala kapitalets utformning i ett samhälle i omvandling mot *informationssamhället* förlitar sig på specialister (där den avgörande kontrollen ligger i slutna privata företag) och samtidigt skall det omvandlande samhället vara **för alla**. Detta resonemang är angeläget, men dessvärre kan inte utvecklas vidare i denna rapport.[83]

Den inbäddade faran i denna paradox är att de instrument och arenor där medborgaren kommer i vardagskontakt med *informationssamhället* uppträder som främmande företeelser och förblir abstrakta system[84] där medborgaren blir tvungen, på brist av alternativ, att förlita sig på experterna. Detta resulterar i att socialkapital reduceras till tillit till IT, och tillit till IT reduceras till förtröstan till experterna.

---

*82 Jfr Cecilia Magnusson Sjöberg, **Tillit till 24-timmarsmyndigheten: Förvaltningspolitisk och juridik**. Föredrag till Swedish Information Resource Network (SIRNET), mars 2003. Materialet finns i form av nedladningsbar PowerPoint-presentation på http://sirnet.metamatrix.se/moten2003.html.*

83 Resonemanget utvecklas däremot i annat arbete: Claudio Aguirre-Bianchi, Tillit, samhälle, information och IT: en begreppsrekonstruktion. Stockholm, 2003 (PDF, kan beställas från cab@metamatrix.se).

84 Anthony Giddens, The Consequences of Modernity, Cambridge: Polity Press (1991).

Det uppstår i detta en intressant spänning mellan den nödvändiga öppenheten som förutsätts av demokratimålen, av tillgänglighet som prioriterad uppgift och av ökad insyn som kännetecknar det öppna samhället som skall stärkas med IT:s hjälp och en tillistskapande strategi som baseras på specialister som arbetar huvudsakligen inom organisationer och företag som kännetecknas inte för sin öppenhet.

Vi anser det angeläget att breda begreppet tillit och föreslå utgångspunkter och förutsättningar för utformningen av en skalbar och iterativ tillitsfrämjande strategi för övergången mot *informationssamhället*. Tillit är en multidimensionell företeelse som inte låter sig operationaliseras i specifika politiska definitioner. Tillit är, enligt en av dess främsta, tillitsexperter, *a basic fact of life*[85].

[85] *Jfr Niklas Luhmann,* ***Trust and Power****, Chichester: Wiley, 1979, s 4.*

4 Slutsatser och förslag

Det IT-politiska instrumentet tillit är illa definierat och har präglats på ett obalanserat sätt av en inriktning på informationssäkerhet. Denna obalans har flera möjliga förklaringar. I det lärande perspektivet som detta uppdrag har, har vi valt att inte fokusera på möjliga förklaringar som pekar på aktörernas ansvar, utan på lärande inför kommande iterationer i IT-politiken.

Inom IT-politiken har regeringen etablerat myndighetsansvarsprincipen för IT-säkerheten: varje myndighet ansvarar för sin egen IT-säkerhet. De myndigheter vi har tittat närmare på under denna studie har en stor medvetenhet beträffande den mer tekniska aspekten av säkerheten (brandväggar, accesskontroll, mm). Det finns dock tydliga brister. Utan att göra anspråk för att punkterna nedan kan valideras, kan vi peka på några områden där bristerna förefaller uppenbara:

- Krypterad e-post
- Den mjuka säkerheten; eller säkerhetskultur: utformningen av verksamhetsprocesserna med inbyggda säkerhetsegenskaper istället för att ha bara policydokument och slussar.
- Säkerhetsstruktur i samhällets grundläggande informationsresurser. Här brister regelverkets i enhetlighet och även konsistens (exempelviss PUL i relation till säkerhetsföreskrifter)

Sitic är ett bra instrument som skulle kunna skapa grunder för att revidera hotbilden och skapa en flexibel strategi för IT-säkerhet. Ett stort problem i sammanhanget att Sitic informerar för lite; den modesta incidentstatistiken som Sitic publicerar (se http://www.sitic.se/dokument/Sitic-Statistikrapport2003Q2.pdf) räcker inte till. Det finns även olösta problem som minskar incidentrapporteringsintensiteten och som PTS har uppmärksammat regeringen om, exempelvis i relation med hinder till incidentrapportering och behovet att se om sekretesslagen.

En flexibel strategi för skydd – och detta har blivit ännu tydligare under den gångna sommarens virusintensiva händelser – förutsätter en beredskap som bygger på ”konjunkturanalyser”, ”early-warningssystem” och långsiktiga trendanalyser. Sitics effektivitet går inte att utvärdera utifrån den publika informationen.

Det går dock att de-facto konstatera att de offentliga institutionernas informationssystem och även de privata företagens har ”klarat” sig utan kända allvarliga skador, dock med förmodligen stora kostnader, mycket möda och manuellt arbete samt ovisshet under sommarens intensiva virusattacker.

De informationssäkerhetsåtgärderna som har vidtagits inom ramen av den nationella IT-politiken har varit adekvata och lär ha varit effektiva, dock utvärderingar av de enskilda satsningarna har inte kunnat analyseras inom ramen av detta uppdrag.

En övergripande och integrerande utvärdering av dessa informationssäkerhetsinsatser bör göras inom kort.

4.1 Tillförlitlighet

Vår slutsats är att det är angeläget att precisera vad som menas med tillit och särskilja tillförlitligheten som ett IT-politiskt instrument, medan tillit tillhör ett bredare samhällsperspektiv än IT-politiken och bör inte vara föremål för lagstiftning eller politiska beslut.

I kapitel **3: Begreppsrekonstruktion: Om tillit och tillförlitlighet**, utvecklar vi teoretiska, samhälleliga och metodmässiga grunder för att operationalisera tillitsproblematiken kring tillförlitlighet som en kvalitetsdimension för IT-baserade tjänster, system och produkter.

Vårt förslag är att FoU arbete kring denna operationalisering genomförs med medverkan av VINNOVA, Satens kvalitets- och kompetensråd och Sveriges standardiseringsinstitut med syfte att utveckla en samling minimalistiska och flexibla standarder för IT-tillförlitlighet som kan utgöra en grund för en kvalitetssatsning i den nationella IT-infrastrukturen (både den tekniska och den mjuka infrastrukturen).

Vi föreslår också att ett projekt genomförs med syfte att skapa förutsättningar för att göra Sveriges IT-infrastruktur till världens mest tillförlitliga. Detta projekt bör genomföras med deltagande av Sveriges exportråd, Invest in Sweden Agency och Institutet för tillväxtpolitiska studier (omvärldsbevakningsfunktion). Projektet bör ha trå syfte: att göra Sveriges IT-miljö tillförlitlig och högkvalitativ som en led till att skapa generella förutsättningar för tillit till IT och samtidigt skapa nya incitament för att investera i Sverige som det landet som erbjuder största IT-tillförlitlighet till företag och e-handel.

Vi föreslår även av tillförlitlighets perspektiv för IT-infrastruktur läggs i de regionala tillväxtavtalen (RTA), som ett sätt att öka incitament för nyetablering av företag i de regioner som kan erbjuda bättre tillförlitlighet. En regional konkurrens kring IT-infrastrukturens tillförlitlighet kan även vara ett effektivt sätt att få igång dynamiska regionala satsningar på området, vilken kan resultera i en generell höjning an tillförlitligheten i hela landet. Näringsdepartementet bör ge Verket för näringslivsutveckling i uppdrag att undersöka detta förslags genomförbarhet.

4.2 Demokrati

De brister i begreppsapparaten denna studie har synliggjort beträffande tilliten och beträffande informationssamhället rör vid större sammanhang än IT-politiken. Dessa problem är nära relaterade till frågor om demokrati, välfärd, livskvalitet, hållbar tillväxt, mm.

Vi föreslår att en studie över tillit och samhällets nya skede genomförs med interdisciplinär karaktär. Studien skulle antingen kunna organiseras i form av ett program till vilket olika forskningsinstitut kan ansluta sig eller i form av ett koncentrerat projekt, exempelvis inom ramen av Institutet för framtidsstudier och/eller Örebros universitets DemocrIT-program.

Det vore även önskvärt att Sveriges riskdag organiserade en hearing om tillit och informationssamhället, med syfte att initiera en bred samhällsdebatt kring detta begrepp och dess samband med demokrati, välfärd, livskvalité och tillväxt.

4.3 Märkning

Ett hinder för e-handelns snabbare tillväxt och utveckling är den diversiteten av aktörer som finns tillgängliga och svårigheten för individerna att forma sig en uppfattning av aktörernas tillförlitlighet, affärsmodeller, mm.

Vi föreslår att arbete kring en tillförlitlighetsmärkning genomförs med deltagande av Konsumentverket, E–handelskammaren, Gemenskapen för elektroniska affärer, LO: s UsersAward, TCO (märkning) och någon FoU institut, exempelvis Centrum för användarorienterad IT-design (KTH/NADA).

Syfte med arbete skulle vara att sammanställa de kvalitetskriterier som kan läggas till grund för en tillförlitlighetscertifiering eller märkning.

Arbetet borde även genomföras med ett europeiskt perspektiv och bör syfta till att en sådan märkning kan bli en europeisk kvalitetsmärkning.

4.4 Metodutveckling

Ett stort problem i de flesta säkerhetsstrategier som tillämpas på IT-området är den svaga kopplingen till utvecklingsprocesser och metodik.

Ett holistiskt perspektiv som syftar till att betrakta säkerhet som en kvalitetsegenskap förutsätter att samlingsbegreppet IT-säkerhet analyseras och operationaliseras även ur ett utvecklingsperspektiv.

Metodutveckling för tjänstedesign och e-tjänsteproduktion bör vara ett ämne som läggs till de olika yrkesutbildningar som syftar till att göra IT säkrare och att höja tilliten till IT-baserade tjänster, produkter och system.

Satsningarna bör göras inte para på universitet och högskolor, utan även på de kvalificerade yrkesutbildningarna (KY).

VINNOVA skulle kunna få uppdraget att undersöka förutsättningarna för en samlad insats i holistisk metodutveckling för IT-tjänstedesign och produktion. Ett sådant uppdrag borde genomföras i samarbete med de relevanta utbildningsmyndigheterna.

Ett sådant initiativ kan bli en katalysator för kunskapsutvecklingen och för framsteg när det gäller att skapa yrkesprofiler för IT-utvecklingsrelaterade professionerna. Det kan även bidra till att skapa bättre kommunikation och samsyn mellan verksamhetsfolk och teknikfolk i samband med tjänstedesign och implementering.

4.5 Information och kompetens för ökad tillit

Vetskap om de reella risker vid IT-användning och hur dessa kan undvikas eller minimeras är väsentlig för att lita. Samtidigt är det mycket viktigt att kunna urskilja mellan verkliga och fiktiva risker.

Informationsinsatser är minst lika viktiga som datautbildning för att skapa medvetna användare.

Det finns myndigheter som utmärker sig i sina tillitsfrämjande informationsinsatser, exempelvis Konsumentverket. Staten borde finna en lämplig agent som har förmåga och förutsättningar för att informera allmänheten om IT-baserade risker och om opålitliga rykten.

En organisation kapabel att tillämpa källkritik, att göra rimliga bedömningar och att informera effektivt om risker och skydd på ett enkelt och begripligt sätt vore en av de mest effektiva tillitsfrämjande insatser som staten kan göra.

Informationstjänsten skulle kunna samarbeta med forskningsinstitutioner, myndigheter, företag och branschorganisationer för att prestera en samlad insats.

Informationsinsatserna är viktiga även för att öka medborgarnas säkerhetskompetens och därmed förbättra tillitens förutsättningar.

En möjlighet är att inrätta en IT-ombudsman eller Internetombudsman som kan samordna insatser för att:

- Skydda den personliga integriteten.
- Förebygga IT-relaterade brottslighet som drabbar individerna.
- Införa kvalitetstänkande och kriterier för IT-baserade tjänster, produkter och system.
- Ombesörja IT-inriktad information för att höja användarkulturen.

Denna ombudsman skulle kunna placeras hos en befintlig myndighet som har kompetens och resurser för denna typ av aktiviteter, exempelvis Konsumentverket eller Post- och telestyrelsen.

5 Intervjuer och konsultationer

Följande aktörer har intervjuats och/eller konsulterats under denna studiens gång:

- Håkan Bystedt – Föreståndare, Kooperativa institutet
- Annika Bränström - Projekt samordnare – Patent- och registreringsverket
- Lars Emerius - Utvecklingskontroller, Försvarsmakten, Högkvarteret
- Lars Flintberg - IT-strateg, Sandvikens kommun
- Håkan Färm - Departementsråd, Enheten för förvaltningsutveckling, Finansdepartementet
- Yvonne Gustafsson - Generaldirektör, Ekonomistyrningsverket
- Lars Ilshammar - Forskare, Örebro universitet, DemokrIT
- Annika Karlholm - Redaktör Svenska Akademiens Ordbok
- Stefan Johansson – Utvecklare och tillgänglighetsexpert, Funka Nu
- Simon Lindgren - IT-direktör, Ekonomistyrningsverket
- Nicklas Lundblad – Verkställandedirektör, E-handelskammaren
- Jarl Magnusson – Strategispecialist, Försvarets materialverk
- Christoffer Nilsson – Verkställandedirektör World Internet Institute
- Fredrik Sand - Kansliråd, Enheten för IT, forskning och utveckling, Näringsdepartementet
- Bengt Svensson - IT-strateg Kommun- och landstingsförbundet
- Björn Ternström –Informationschef Riksskatteverket
- Siv Torstensson - IT-strateg Uddevalla kommun
- Ingwar Åhman-Eklund - Samordningschef för kultur och kommunikation – Kista stadsdelsnämnd

ITPS, Institutet för tillväxtpolitiska studier
Studentplan 3, 831 40 Östersund
Telefon: 063 16 66 00
Fax: 063 16 66 01
info@itps.se
www.itps.se
ISSN 1652-0483

INSTITUTET FÖR TILLVÄXTPOLITISKA STUDIER