

Ramavtal - eID 2004

Vägledning

Version 1.0

Innehåll

1	Inledning	3
1.1	Allmänt	3
1.2	Statskontorets uppdrag	3
1.3	Upphandlingsområdet	3
1.4	Angränsande upphandlingsområden	4
1.5	Avropsberättigade	4
2	Ramavtalen	5
3	ID-tjänster	5
3.1	Tjänsteerbjudande	5
4	Köparprogramvara och Infratjänsten	7
4.1	Förutsättningar	7
4.2	Köparprogramvara	8
4.2.1	Avrop av generell köparprogramvara från eID-avtalet	8
4.3	Infratjänst	12
5	Prissättning, personlig e-legitimation	13
5.1	Användaren väljer – myndigheten betalar	13
5.2	Betalning per transaktion	14
5.3	Alternativa prismodeller	15
5.3.1	Nordea – Spärrkontroll mot spärrlista (CRL)	15
5.3.2	TeliaSonera – Fast årsavgift per användare och år (flat rate)	15
5.3.3	Steria	15
5.3.4	Övrigt	16
5.4	Kommunpaket	16
5.5	Startpaket	17
5.5.1	Föreningssparbanken	17
5.5.2	Svenska Handelsbanken	17
5.5.3	Nordea	17
5.5.4	TeliaSonera	17
5.5.5	Steria	18
5.6	Kostnadsexempel	18
5.7	Intern användning inom myndigheten	18
6	Prissättning – generell köparprogramvara	19
6.1	Teleca	19
6.2	Nexus	20
6.3	TietoEnator	21
7	Beräkningsstöd via kalkyl på Statskontorets webb	22
8	Begrepp och definitioner	23

1 Inledning

1.1 Allmänt

Arbetet med 24-timmarsmyndigheter handlar om utveckling av elektroniska tjänster för att uppnå förenklade rutiner, snabbare beslut, bättre tillgänglighet och ökad insyn. Privatpersoner och företag ska få tillgång till e-tjänster som sparar tid och pengar och som låter dem utföra tjänsterna när de vill. Det ska vara lätt att nå fram till myndigheterna och få sitt ärende utträttat. Man ska också kunna hitta rätt utan att känna till tider, platser, namn, telefonnummer, adresser osv. Medborgaren ska inte behöva hålla reda på hur ansvaret är fördelat mellan olika myndigheter. Målet är ”ett ärende – en kontakt”. Det ska också vara lätt att få en samlad information om vilket tjänsteutbud myndigheterna tillhandahåller oavsett vilken myndighet som är ansvarig.

En förutsättning för att myndigheter¹ ska kunna tillhandahålla mer avancerade e-tjänster för allmänheten och företag är att det finns möjligheter att säkert identifiera privatpersoner elektroniskt samt hantera elektroniska underskrifter. Privatpersoner ska, snabbt och enkelt, kunna skaffa sig en elektronisk legitimation (e-legitimation) för att få tillgång till förvaltningens alla e-tjänster.

I statens målbild ligger att en privatperson eller ett företag, med en och samma e-legitimation, ska kunna identifiera sig elektroniskt och skapa en underskrift åtminstone i alla offentliga e-tjänster.

Ramavtalet är ett led i Statskontorets arbete med att främja utvecklingen av 24-timmarsmyndigheter.

1.2 Statskontorets uppdrag

Statskontoret har regeringens uppdrag att svara för inköpssamordning inom offentlig förvaltning, bland annat inom IKT²-området. För att skapa bättre villkor och lägre kostnader för den offentliga förvaltningen genomför Statskontoret som ett led i detta arbete upphandlingar och tecknar ramavtal med leverantörer. Ramavtalen används i Statskontorets arbete med att utveckla IT-infrastrukturen för informationsutbyte mellan statliga myndigheter, kommuner, landsting samt i deras dialog med medborgare och företag. Med stöd av tecknade ramavtal kan sedan enskilda förvaltningar göra avrop, utan att genomföra egen upphandling.

1.3 Upphandlingsområdet

Ramavtalet avser tjänster så att den offentliga sektorns olika aktörer kan hantera e-legitimation för identifiering och underskrift vid kontakter med privatpersoner och företag över Internet.

¹ Myndighet är i detta dokument ett gemensamt begrepp för myndigheter, landsting och avropsberättigade kommuner

² Informations- och Kommunikationsteknik-området

2005-02-22

Ramavtalet omfattar också tilläggstjänster inom olika områden bl.a. att på uppdrag utfärda e-legitimationer till en riktad grupp t.ex. myndighets anställda eller en kundgrupp, att utfärda s.k. webbserverlegitimation, att utfärda s.k. legitimation för myndighetens elektroniska stämpel samt utfärdande och tjänster i samband med olika former av tjänstelegitimationer. Vissa begränsade konsulttjänster för etablering av tjänsten hos myndigheten ingår också i upphandlingsområdet.

1.4 Angränsande upphandlingsområden

Infratjänst 2003 är ett ramavtal med koppling till eID 2004.

Syftet med Infratjänst 2003 är att underlätta och sänka kostnaderna för myndigheternas utveckling och drift av e-tjänster och att stödja standardiserade lösningar för ett säkert och effektivt informationsutbyte. Statskontorets ambition med infratjänsten är bl.a. att en kund till infratjänsten endast ska behöva ha kontakt med infratjänstleverantören för att den vägen kunna kontrollera e-legitimationer från alla ramavtalsknutna leverantörer av eID-tjänster. För information om Infratjänst 2003, se Statskontorets avtalswebb.

1.5 Avropsberättigade

Avropsberättigade till ramavtalet eID 2004 är samtliga statliga myndigheter, 20 landsting och regioner, 229 kommuner, försäkringskassorna samt 26 offentliga organ, förbund, stiftelser etc. Mer exakta uppgifter finns i ramavtalet, dokumentet Avropsberättigade – eID 2004.

2 Ramavtalen

Ramavtal har tecknats med följande fem leverantörer:

- Föreningssparbanken AB (FSB)
- Nordea Bank AB
- Steria AB
- Svenska Handelsbanken AB (SHB)
- TeliaSonera Sverige AB

Avtalen är giltigt t.o.m. 2006-06-30 med möjlig förlängning med upp till 24 månader.

Bankernas ID-tjänst (BID) representeras i avtalet av Föreningssparbanken och Svenska Handelsbanken. I bankernas ID-tjänst ingår Danske Bank, Föreningssparbanken, Ikanobanken, Länsförsäkringar Bank, Skandiabanken, Sparbanken Finn, Sparbanken Gripen, Svenska Handelsbanken. E-legitimationer utfärdade av dessa åtta banker täcks in genom att myndigheten ingår ett avtal med Föreningssparbanken eller Svenska Handelsbanken.

3 ID-tjänster

3.1 Tjänsteerbjudande

Användningsområden för de i ramavtalen ingående ID-tjänsterna omfattar

- Personlig e-legitimation
- Personlig e-legitimation för riktad grupp
- Webbserverlegitimation
- E-legitimation för myndighetens elektroniska stämpel
- Tjänstelegitimation

Endast Personlig e-legitimation är obligatorisk och erbjuds från samtliga leverantörer.

I avtalet erbjuds både så kallade mjuka och hårda e-legitimationer. Begreppen ”hård” respektive ”mjuk” avser sättet att lagra den privata nyckeln. Den privata nyckeln är grundläggande för säker identifiering och underskrift och skall förvaras på ett betryggande sätt. En ”mjuk” e-legitimation (mjukt certifikat) innebär att den privata nyckeln finns lagrad som en krypterad datafil. Med ”hård” e-legitimation (hårt certifikat) menas oftast att den privata nyckeln finns lagrat på ett eID-kort.

2005-02-22

Nedanstående tabell visar respektive leverantörs erbjudanden av ID-tjänster.

	Personlig e-legitimation		Riktad grupp		Webbserver	E-leg för myndighetens stämpel		Tjänstelegitimation
	Mjukt	Kort	Mjukt	Kort	Mjukt	Mjukt	Kort	Sekundär
Föreningssparbanken	X							
Nordea	X	X						
Steria	X	X	X	X	X	X	X	X
Svenska Handelsbanken	X							
TeliaSonera	X	X		X				X

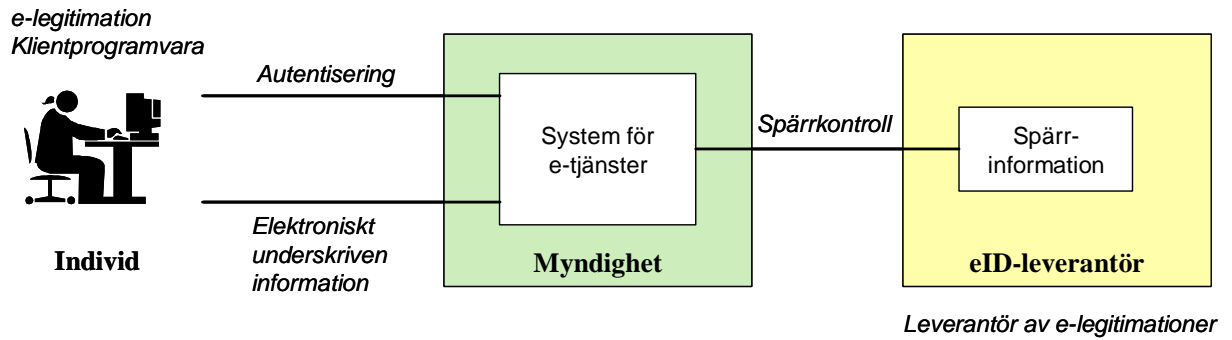
- *Personlig e-legitimation* används av personer när de kommunicerar elektroniskt med myndigheter, i egenskap av privatperson eller som företrädare för en juridisk person som inte är en myndighet. Inom en myndighets verksamhet kan också en personlig e-legitimation användas som tjänstelegitimation. Flertalet leverantörer tillhandahåller personlig e-legitimation gratis för användaren. En eventuell kostnad för anskaffning av e-legitimationen (t ex kortbaserad e-legitimation) får annars användaren bekosta.
- *Personlig e-legitimation för riktad grupp* har samma användning som *personlig e-legitimation* enligt ovan. Eventuell kostnad för anskaffning av e-legitimationer (t ex kortbaserad e-legitimation) bekostas vanligen av myndigheten. Den riktade gruppen kan bestå av myndighetens egen personal eller viss kundgrupp kopplad till myndigheten.
- *Webbserverlegitimation* används av myndigheten för att individer och myndigheter ska kunna identifiera en myndighets webbplats eller e-tjänst med vilken de kommunicerar samt skydda denna kommunikation mot obehörig insyn.
- *E-legitimation för myndighetens elektroniska stämpel* används av myndigheter för elektroniska handlingar som skall skyddas mot förfalskning och förnekande. Den som tar emot en myndighetshandling med myndighetens elektroniska stämpel kan förvissa sig om att den elektroniska handlingen har upprättats av myndigheten, eller inom ramen för ett visst verksamhetsområde inom myndigheten samt att den inte har förvanskats eller ändrats.
- *Tjänstelegitimation* används av handläggare vid myndigheter när de kommunicerar elektroniskt inom myndigheten, med andra myndigheter och med privatpersoner och privaträttsliga organ, i egenskap av anställd eller uppdragstagare hos myndigheten. Tjänstelegitimation som sekundärcertifikat innebär att en e-legitimation för tjänstebruk kopplas till individens befintliga eID-kort. Detta görs så att kortets publika nyckel även kan användas för tjänstelegitimationen.

4 Köparprogramvara och Infratjänsten

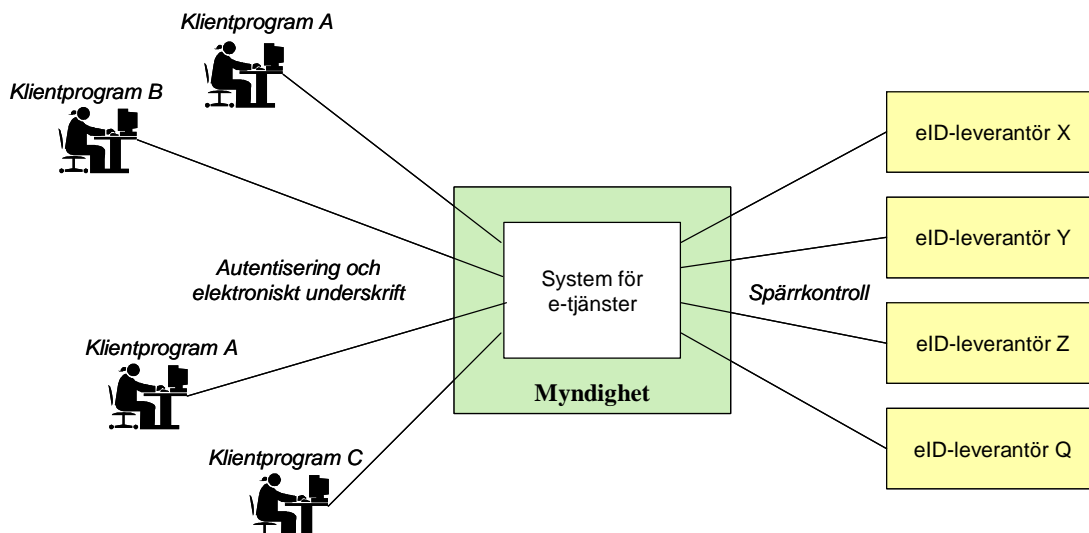
4.1 Förutsättningar

Några grundläggande funktioner som myndighetens e-tjänst måste kunna hantera vid användning av en e-tjänst baserad på PKI är:

- Autentisering av individen med hjälp av dennes e-legitimation
- Verifiering av information som har undertecknats elektroniskt av en person
- Verifiering av giltighet för individens e-legitimation, vilket bl a sker genom att kontrollera om e-legitimationen är spärrad (jfr kreditkort).

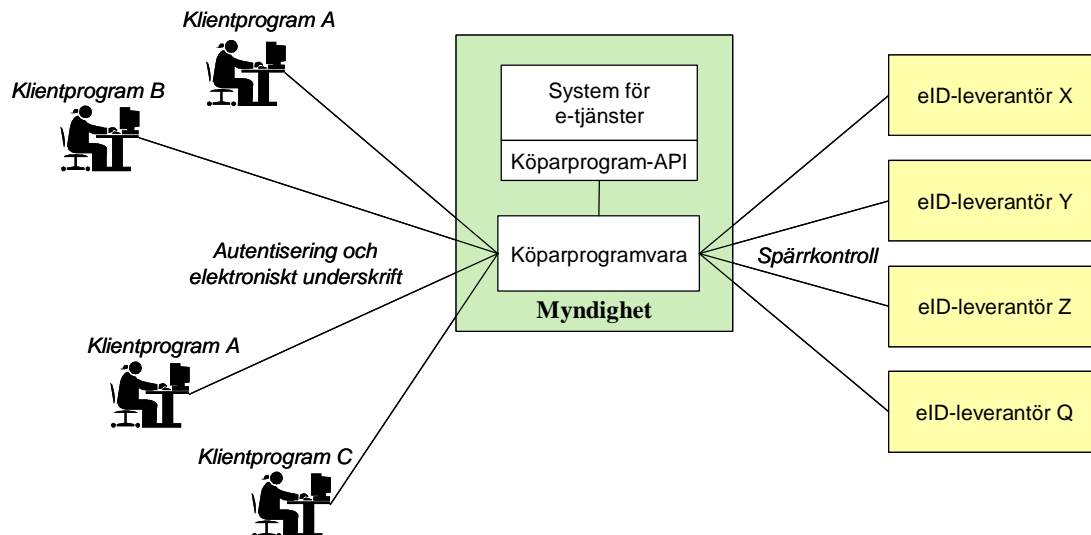


Sättet att göra spärrfråga skiljer sig åt mellan de olika leverantörerna. Användarens val av utfärdare av e-legitimationen medför även indirekt ett val av den klientprogramvara som ska sköta kontakten med myndigheternas e-tjänster. Olika eID-leverantörer kan kräva olika klientprogramvaror. Varje klientprogramvara kan ha sitt sätt att identifiera användare och skapa sitt format på den elektroniska underskriften. Detta innebär att en myndighet som inför e-tjänster måste kunna autentisera individer, verifiera elektroniska underskrifter samt göra spärrkontroll utifrån krav från respektive eID-leverantör och dess klientprogramvara.



4.2 Köparprogramvara

För att underlätta anpassningen mellan myndighetens e-tjänster och respektive eID-leverantörs IT-miljö (inklusive användarens klientprogramvara) ingår i ramavtalen möjligheter att köpa speciell programvara för detta ändamål. Denna programvara benämns köparprogramvara. Genom denna är tanken att myndighetens e-tjänst via ett gränssnitt (API) ska kunna hantera autentisering, elektronisk underskrift och spärrkontroll mot den aktuella köparprogramvaran oavsett vilken eID-leverantörs miljö som avses. Tanken är alltså att köparprogramvaran är generell programvara, där myndigheten endast ska behöva anskaffa *en* köparprogramvara för att klara alla de eID-leverantörer som individerna valt för sina e-legitimationer. Myndigheten bör innan köp av programvaran stämma av med leverantören för att få en exakt bild över vad den aktuella köparprogramvaran stödjer. En översikt ges även i avsnitt 4.2.1.



Myndigheten ansvarar själv för införande, test och drift av köparprogramvaran.

4.2.1 Avrop av generell köparprogramvara från eID-avtalet

Med generell köparprogramvara menas här köparprogramvara som kan användas mot alla eller flertalet av de eID-leverantörer som omfattas av ramavtalet eID 2004. Generell köparprogramvara som kan avropas via ramavtalet tillverkas av Teleca, Nexus och TietoEnator.

Tillverkare	Programvarans namn
Teleca	Teleca Security Server
Nexus	Nexus MultiID server
TietoEnator	TECS – TietoEnator Certificate Services

2005-02-22

Den generella köparprogramvaran finns i ramavtalen för Föreningssparbanken, Svenska Handelsbanken och TeliaSonera. För Föreningssparbanken och Svenska Handelsbanken är tillverkarna återförsäljare och kontakter tas direkt med dessa angående köparprogramvaran. TeliaSonera återförsäljer däremot själva köparprogramvaran.

Nedanstående sammanställning ger en övergripande bild av de generella köparprogramvarorna. Stödet för eID-miljön avser endast stödet hos eID-leverantörer med avtalsrelation. Visst stöd finns idag även för tjänsteutbudet från Nordea och Steria.. Kontakt med återförsäljare/tillverkare av den generella köparprogramvaran krävs för att få en exakt bild över vad som vid en viss tidpunkt täcks in av programvaran.

4.2.1.1 Teleca

Programvara: Teleca Security Server 2.3.0

Stöd för eID-miljöer hos eID-leverantörer med avtalsrelation

E-leg	Miljö		Status			Kommentar
	Spärr	Klient	Aut	Sign	Spärr	
BID						
Mjuk	OCSP	CBT	2	2	2	Inkluderar stöd för CBT-klient version 3.2.0
TeliaSonera						
Mjuk	OCSP	Verisign PTA	2	2	2	
Telia standard-kort	CRL	Smart Trust Personal	2	2	2	
Teila SIS-kort	CRL	Smart Trust Personal	2	2	2	

För statuskolumnerna gäller: *Aut*: Stöd för autentisering av individen, *Sign*: Stöd för validering av individens underskrift, *Spärr*: Stöd för spärrkontroll

2: Alternativet stöds

1: Arbete pågår med att införa stöd för detta alternativ

Programmiljöer som stöds

Teleca Security Server, TSS, exekverar i en Java-miljö på något av de operativsystem som stödjer Java. TSS har testats i olika konfigurationer och via olika API:er i miljöer med JDK 1.3.1 och JDK 1.4 på operativsystemen Windows NT 4, Windows 2000, Windows Server 2003, SUN Solaris 8 och IBM AIX 4.3.3.

TSS kan köras i någon av följande konfigurationer:

- Webbapplikation på förkonfigurerad Apache Tomcat 4.1 applikationsserver vilken medföljer i leveransen.
- Webbapplikation på annan applikationsserver med stöd för Servlet API 2.2 eller senare som exempelvis IBM WebSphere och BEA WebLogic.
- Integrerad direkt i existerande Java-applikation.

Loggning av transaktioner i TSS kan göras till fil eller databas via JDBC. De databaser som testats med TSS är:

- MySQL (MySQL ConnectorJ 3.0)
- Microsoft SQL Server 2000 (Microsoft SQLServer 2000 Driver for JDBC)
- IBM DB2 (IBM DB2 Universal Driver for JDBC 1.0)
- Oracle 9i (Oracle JDBC Driver 1.2)

API:er som stöds

Följande API:er finns inkluderade i produkten:

- Java klient-API för anrop via HTTP/XML till TSS på applikationsserver
- COM klient-API för anrop via HTTP/XML till TSS på applikationsserver
- HTTP/XML API för anrop till TSS på applikationsserver
- TSS WebService API för anrop till TSS på applikationsserver
- OSIF WebService API för anrop till TSS på applikationsserver (se www.sveid.se för mer information kring detta API)
- Java API för direkt integration med lokal Java-applikation

4.2.1.2 Nexus

Programvara: Nexus MultiID Server 2.1

Stöd för eID-miljöer hos eID-leverantörer med avtalsrelation

Miljö			Status			Kommentar
E-leg	Spärr	Klient	Aut	Sign	Spärr	
BID						
Mjuk	OCSP	CBT	2	2	2	
TeliaSonera						
Mjuk	OCSP	Verisign PTA	2	2	2	
Telia standard-kort	CRL	Smart Trust Personal	2	2	2	Autenticering m.h.a ssl gäller för denna klient, Vår server har stöd för att verifiera certifikaten.
Teila SIS-kort	CRL	Smart Trust Personal	2	2	2	Autenticering m.h.a ssl gäller för denna klient, Vår server har stöd för att verifiera certifikaten.

För statuskolumnerna gäller: *Aut*: Stöd för autentisering av individen, *Sign*: Stöd för validering av individens underskrift, *Spärr*: Stöd för spärrkontroll

2: Alternativet stöds

1: Arbete pågår med att införa stöd för detta alternativ

Programmiljöer som stöds

Java JDK/JRE 1.4.2. Solaris, Win32, Linux. AIX 5.2 under övervägande. Andra plattformar kan erbjudas på kundbegäran.

API:er som stöds

SOAP/WebServices enligt OSIF, Java Online API (förenklar aktivering av säkerhets-plugin), Java API.

4.2.1.3 Tieto Enator

Programvara: TECS 2.1

Stöd för eID-miljöer hos eID-leverantörer med avtalsrelation

Miljö			Status			Kommentar
E-leg	Spärr	Klient	Aut	Sign	Spärr	
BID						
Mjuk	OCSP	CBT	2	2	2	
TeliaSonera						
Mjuk	OCSP	Verisign PTA	2	2	2	
Telia standard-kort	CRL	Smart Trust Personal	2	2	2	
Teila SIS-kort	CRL	Smart Trust Personal	2	2	2	

För statuskolumnerna gäller: *Aut*: Stöd för autentisering av individen, *Sign*: Stöd för validering av individens underskrift, *Spärr*: Stöd för spärrkontroll

2: Alternativet stöds

1: Arbete pågår med att införa stöd för detta alternativ

Programmiljöer som stöds

Windows 2000/2003, Sun Solaris 9 64-bit.

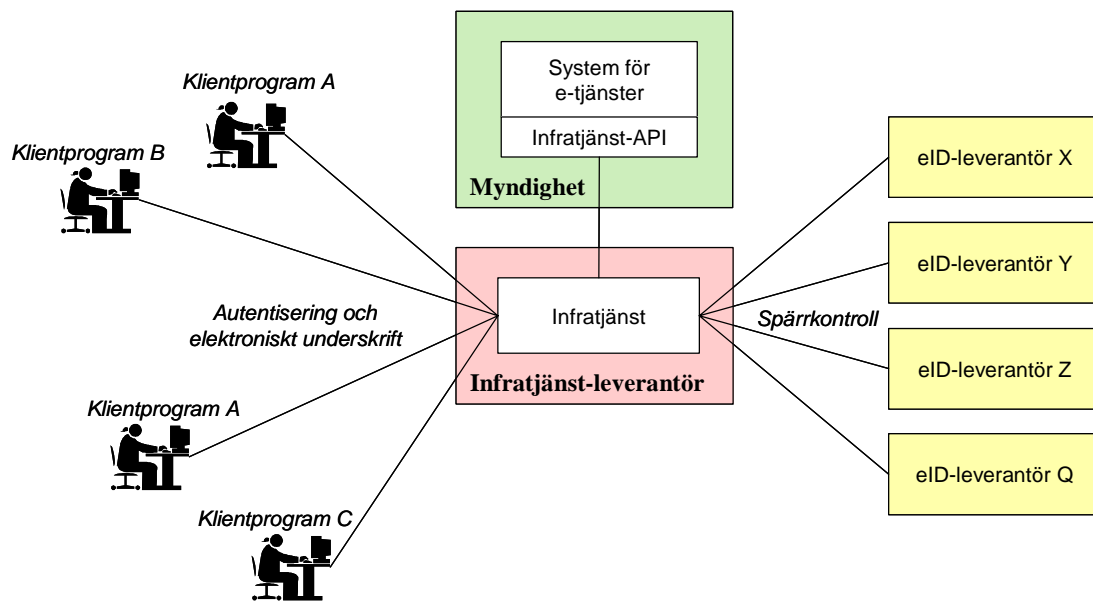
API:er som stöds

TECS Native Protocol, OSIF

Alla miljöer som stöder HTTP och SOAP.

4.3 Infratjänst

Som ett alternativ till köparprogramvaran kan köparprogramfunktionerna fås via Statskontorets ramavtal för Infratjänster (upphandlat under 2003). Infratjänster tillhandahålls av TietoEnator och WM-data. Genom att avropa Infratjänster får myndigheten dessutom driften av köparprogramvaran som en tjänst.

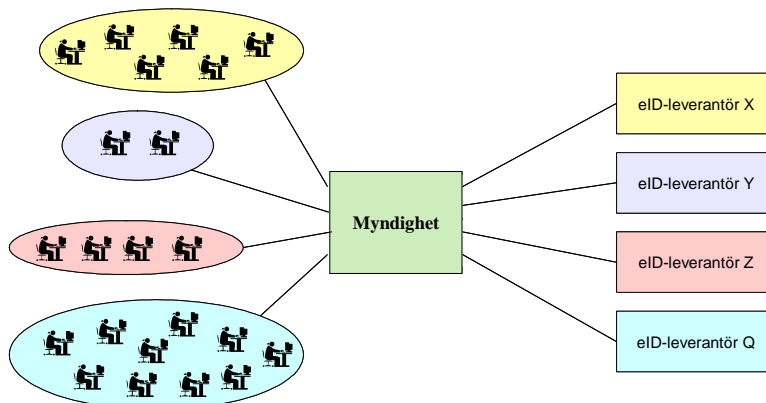


5 Prissättning, personlig e-legitimation

Att hantera ett ärende manuellt kostar i många branscher 100-tals kronor. I vissa fall kan det minskas till en hundradel om elektronisk hantering införs. En låg skattning av den manuella ärendekostnaden motsvarar ett 5-kronors brevporto. Säker identifieringen samt verifiering av underskrift är en del av e-tjänstens totala kostnad. Som framgår i detta avsnitt kommer kostnaden per transaktion mot eID-leverantörerna enligt ramavtalet för eID att ligga på en betydligt lägre nivå (t ex 40 öre per transaktion i kommunexemplet i avsnitt 5.6)

5.1 Användaren väljer – myndigheten betalar

Användaren väljer själv utfärdare, bland dem som har ramavtal, för att få sin e-legitimation. Den vanligaste lösningen är att användaren, i regel gratis, erbjuds ladda ner en e-legitimation från sin Internetbank. Myndigheten betalar dock en avgift till den som utfärdat e-legitimationen varje gång legitimationen används för någon av myndighetens 24-timmars tjänster. Man kan säga att myndigheten betalar en avgift för hjälpen med att kontrollera att det är rätt person som får tillgång till tjänsterna. Till detta kommer en särskild avgift för hjälpen med att kontrollera en elektronisk underskrift om användaren väljer att skriva under ett formulär, ett dokument etc. som sänds till myndigheten. Genom sitt val av utfärdare avgör användaren till vilken leverantör myndigheten skall betala, och därmed vilken leverantörs prislista som ska gälla. Idag har åtta banker gått samman om en utfärdare, Bankernas ID-tjänst (BID). Detta gör att en myndighet kan kontrollera kundernas e-legitimationer från alla dessa åtta banker via en tjänst och ett avtal. Två banker har rollen av leverantör av eID-tjänster baserade på dessa åtta bankers kunder, Föreningssparbanken och Svenska Handelsbanken.



När e-legitimationer användes för inkomstdeklarationen under våren 2004 var enligt Skatteverket 68 procent av de e-legitimationer som användes (totalt något mer än 100 000) utfärdade av BID-bank, 18 procent kom från Nordea och 14 procent från TeliaSonera. Denna typ av fördelning styr hur stort inflytande leverantörernas prislistor får på de avgifter myndigheterna måste betala för eID-tjänsten.

Myndigheten betalar samma pris till eID-leverantören för spärrkontroll oavsett om användaren har en mjuk eller hård e-legitimation.

5.2 Betalning per transaktion

Kostnader i nedanstående tabell är uttryckta i SEK.

Månadsavgifter betalas kvartalsvis i efterskott.

Kostnader för kontroll av e-legitimation är styckekostnader per transaktion.

Beräkning av kontrollkostnaden sker månadsvis genom skiktvis summering av transaktionsintervall i tabellen.

Exempel (FSB): Vid förbrukning av 50 000 transaktioner på en månad blir kostnaden för detta:

$300 * 0,50 + 700 * 0,50 + 2\ 000 * 0,5 + 7\ 000 * 0,50 + 20\ 000 * 0,50 + 20\ 000 * 0,45 = 24\ 000$ kr i kontrollkostnader för månaden. Till detta tillkommer abonnemangskostnader för månaden.

		FSB ³	SHB ⁴	Nordea	TeliaSonera
Anslutningsavgift (engångs)		10 000	0	10 000	10 000
Abonnemangavgift per månad		500	1 000	2 000 ⁵	5 00
Kontroll av e-leg avseende identitet (månadsvolym)	1 – 300	0,50	0,70	0,80	0,45
	301 – 1 000	0,50	0,70	0,70	0,45
	1 001 – 3 000	0,50	0,70	0,60	0,45
	3 001 – 10 000	0,50	0,60	0,50	0,45
	10 001 – 30 000	0,50	0,60	0,30	0,45
	30 001 – 100 000	0,45	0,50	0,20	0,30
	100 001 – 300 000	0,40	0,40	0,15	0,20
	300 001 – 1 000 000	0,35	0,35	0,12	0,10
	1 000 001 – 3 000 000	0,30	0,30	0,10	0,05
	3 000 001 – 10 000 000	0,10	0,25	0,08	0,05
10 000 001 –	0,07	0,15	0,06	0,05	
Kontroll av e-leg avseende underskrift (månadsvolym)	1 – 300	2,75	3,00	4,00	5,50
	301 – 1 000	2,75	3,00	3,50	4,50
	1 001 – 3 000	2,75	3,00	3,00	4,50
	3 001 – 10 000	2,75	2,75	2,50	4,00
	10 001 – 30 000	2,50	2,75	1,50	3,00
	30 001 – 100 000	2,25	2,75	1,00	2,50
	100 001 – 300 000	1,90	2,25	0,75	2,00
	300 001 – 1 000 000	1,40	1,75	0,60	1,00
	1 000 001 – 3 000 000	1,10	1,25	0,50	0,50
	3 000 001 – 10 000 000	0,45	0,75	0,40	0,40
10 000 001 –	0,35	0,50	0,30	0,25	
Tak för avgiftsuttag, år 2005 ⁶		10 000 000/år	Erbjuds ej	10 000 000/år	700 000/mån
Tak för avgiftsuttag, år 2006		20 000 000/år	Erbjuds ej	15 000 000/år	700 000/mån
Tak för avgiftsuttag, år 2007		20 000 000/år	Erbjuds ej	20 000 000/år	700 000/mån

Tabell 2 – Transaktionsavgifter utan garanterad volym

Beträffande Steria se avsnitt 5.3.3 nedan.

³ FSB = Föreningssparbanken

⁴ SHB = Svenska Handelsbanken

⁵ För Nordea gäller att transaktionsavgifter för kontroll av e-legitimationer får avräknas mot abonnemangavgiften

⁶ Taken för år 2005, 2006 och 2007 gäller avrop från enskild avropande part.

5.3 Alternativa prismodeller

5.3.1 Nordea – Spärrkontroll mot spärrlista (CRL)

Anslutningsavgift (engångs), kr	10 000
--	--------

Antalet användare per myndighet	Kr per månad
1 – 100	2 000
101 – 500	4 000
501 – 1 000	10 000
1 001 – 10 000	18 000
10 001 –	36 000

Prismodellen kan endast avropas när eID-tjänsten används för myndighetsinternt bruk. Tak för avgiftsuttag framgår av tabell 2 ovan och avser den sammanlagda kostnaden för de båda betalningsmodellerna.

5.3.2 TeliaSonera – Fast årsavgift per användare och år (flat rate)

Avtalsperiod, månader	Abonnemangsavgift per månad, kr
12	2 490
36	1 990

Avgift per användare och år, kr	45
--	----

För användare utöver avtalat antal under året är avgiften 60 kr/år. Detta regleras årsvis. Avgiften inkluderar obegränsat antal I- och U-transaktioner. Avgifter betalas kvartalsvis i förskott.

För att begränsa risken för eskalerande kostnadsutveckling gäller att maxuttaget av total årsavgift är 8 400 000 kr för denna prismodell. Taket gäller endast för enskild avropande part.

5.3.3 Steria

Prislistorna 1-3 är alternativa prislistor som fritt kan väljas.

Prislista 1

Anslutningsavgift (engångs), kr	50 000
--	--------

Abonnemangsavgift per månad, kr	
Antal användare	Totalt, kr
1 – 500 000	4 500
500 001 – 1 000 000	9 500
> 1 000 000	14 500

Prislista 2

Anslutningsavgift (engångs), kr	5 000
--	-------

Abonnemangsavgift per månad, kr	
Antal användare	Totalt, kr
1 – 20 000	2 500
20 001 – 100 000	4 000
100 001 – 500 000	6 000
500 001 – 1 000 000	11 000
> 1 000 000	16 000

Prislista 3

Anslutningsavgift (engångs), kr	50 000
--	--------

Abonnemangsavgift per månad, kr	
Antal användare	Totalt, kr
Oberoende av antal användare	11 000

5.3.4 Övrigt

I avtalet erbjuder Föreningssparbanken och TeliaSonera under vissa villkor lägre avgifter vid garanterade volymer. Svenska Handelsbanken erbjuder även ett s k "Årskort med rabatt" som under vissa villkor kan ge lägre avgifter.

För ytterligare information, se respektive leverantörs avtal.

5.4 Kommunpaket

Via kommunpaket ger flera eID-leverantörer gynnsamma fastprisvillkor till små och medelstora kommuner.

Kommunpaket erbjuds av Föreningssparbanken via fyra paket utifrån antal invånare (10 000, 25 000, 50 000 respektive 100 000). Nordea och TeliaSonera har även kommunpaket (20 000 respektive 25 000 invånare).

Genom att bankernas ID-tjänst (BID) idag står för en stor del av eID-användarna (68 % enligt Skatteverkets inkomstdeklaration) får Föreningssparbankens kommunpaket stort genomslag i prisbilden då Föreningssparbanken väljs.

eID-leverantör	Max antal invånare vid avropstillfället	Avtalstid (månader)	Förlängning (månader)	Årsavgift, kr	Månadsavgift, kr
Föreningssparbanken	10 000	24	12	9 500	-
Föreningssparbanken	25 000	24	12	14 500	-
Föreningssparbanken	50 000	24	12	23 000	-
Föreningssparbanken	100 000	24	12	33 000	-
Nordea	20 000	24	12	10 000	1 000
TeliaSonera	25 000	24	12	20 000	-

5.5 Startpaket

5.5.1 Föreningssparbanken

Avgift 30 000 kr för ett startpaket.

Avtalet gäller för användning under högst 12 månader och inkluderar anslutning, abonnemang samt sammanlagt 40 000 identifierings- och underskriftstransaktioner. Efter 12 månader eller när max antal transaktioner uppnåtts gäller priser enligt tabell 2 ovan. Avgiften erläggs vid avtalstecknandet.

5.5.2 Svenska Handelsbanken

Avgift för ett startpaket	Kr/månad
Fast avgift	1 000
Avgift per 1 000 användare	1 000 (avrundat till närmaste tusental uppåt)

Avtalet gäller för användning under högst 6 månader. Användarantalet skall vara begränsat till 10 % - 20 % av det potentiella kundunderlaget. Ingen begränsning finns av antalet transaktioner. Avgiften erläggs månadsvis i efterskott.

5.5.3 Nordea

Anslutningsavgift (engångs), kr	10 000
---------------------------------	--------

Abonnemangavgift per månad, kr	1 000
--------------------------------	-------

Avtalet gäller för användning under högst 12 månader. Ingen begränsning finns av antalet transaktioner.

5.5.4 TeliaSonera

Anslutningsavgift (engångs), kr	10 000
---------------------------------	--------

Abonnemangavgift per månad, kr	500
--------------------------------	-----

Avtalet gäller endast en gång per avropande part för användning under högst 12 månader. Avgiften inkluderar sammanlagt 20 000 identifierings- och underskriftstransaktioner. Efter 12 månader eller när max antal transaktioner uppnåtts gäller priser enligt tabell 2 (eller speciella villkor vid garanterade volymer).

2005-02-22

5.5.5 Steria

Steria erbjuder avropande myndigheter ett startpaket för test och utvärdering av e-legitimationer som innebär att ingen anslutningsavgift eller abonnemangsavgift utgår för myndigheten under en pilotfas som kan vara av valbar tidslängd, dock maximalt 12 månader. Beställaren betalar under pilotfasen endast för utställda e-legitimationer enligt respektive legitimations prislista. Priset för ett startpaket är 15 000 kr. Avgiften erläggs endast om myndigheten bestämmer sig för att inte övergå i produktion.

5.6 Kostnadsexempel

Exempel 1: Kommun med 20 000 invånare och 6 500 användare

Kostnad - ca 7 - 9 kr per användare och år oavsett intensiteten i användning (första året dyrare på grund av startavgifter).

Exempel 2: Kommun med 80 000 invånare och 26 000 användare

Varje användare tar del av information en gång i veckan med identifiering via eID.

Varje månad krävs även en underskrift via eID. Kostnad - ca 23 - 24 kr per användare och år (första året dyrare på grund av startavgifter). Räknat som transaktionskostnad hamnar avgiften på ca 0,40 kr per transaktion (spärrfråga).

Exempel 3: Skatteverket får in 100 000 inkomstdeklarationer under april och maj där e-legitimation används för identifiering och underskrift. Kostnad - 4 kr per användare och år.

Kostnaderna i exemplen bygger på en summering av förvaltningens kostnader mot respektive leverantör av eID-tjänster. Skatteverkets statistik från användning av e-legitimationer för inkomstdeklarationerna har använts för att fördela eID-volymer mellan leverantörerna. Föreningssparbanken har valts som BID-bank.

5.7 Intern användning inom myndigheten

Den transaktionsbaserade prissättningen i avtalet lämpar sig för det mesta inte för internt bruk där anställda använder förvaltningens egna system och gör ett stort antal identifieringar och underskrifter per dag. Ramavtalet erbjuder dock bland annat tjänste-legitimationer från TeliaSonera och Steria lämpade för dessa ändamål.

6 Prissättning – generell köparprogramvara

Med generell köparprogramvara menas här köparprogramvara som kan användas mot alla eller flertalet av de eID-leverantörer som omfattas av ramavtalet eID 2004. Till de generella köparprogramvarorna räknas programvara från Teleca, Nexus och TietoEnator.

6.1 Teleca

		År 1		År 2		År 3		År 4	
		Licenser	Underhåll & Support	Licenser	Underhåll & Support	Licenser	Underhåll & Support	Licenser	Underhåll & Support
Licensavgift per licens	1-2 licenser	75 000							
	Licens nr 3 och uppåt.	50 000							
Supportavgift 1-5 licenser ¹⁾			23 000		46 000		46 000		46 000
Support per licens, 6-10			3 000		6 000		6 000		6 000
Kommun ²⁾ (upp till 3 licenser)	< 25 000	24 960		24 960		24 960			
	25 000-50 000	28 020		28 020		28 020			
	50 000-100 000	32 520		32 520		32 520			
Startpaket ³⁾		Giltigt 12 månader till 30 % av totala licenskostnaden + underhållskostnad (80 % licens vid fortsättning)							
Testpaket ⁴⁾		Gratis utvärderingslicens giltig i 2 månader (kan förlängas i 2-månaders perioder)							

1) Supportavgift 1-5 licenser är en paketavgift för upp till 5 licenser (d v s samma avgift oavsett om det är 1 eller 5 licenser).

2) Teleca erbjuder kommunkunder möjligheten att hyra upp till tre licenser av Teleca Security Server under en treårsperiod. Licensavgiften varierar beroende på kommunens storlek (antalet kommuninvånare).

Hyresavgiften faktureras årsvis i förskott. Efter hyresperiodens slut kan kommunen välja att övergå till ett traditionellt licensavtal, till vid den tidpunkten gällande prislista, alternativt att avsluta användandet av programvaran.

Kommunpaketet innehåller rätt till nya utgåvor av eID funktionen i Teleca Security Server. Eventuell felrapportering kan ske via e-post. Teleca AU-System kan efter beställning medverka vid utredning och felsökning kring problem i Kundens tjänst och kringliggande system på konsultbasis.

Kommunpaketet kan inte kombineras med andra erbjudanden.

3) Teleca AU-System erbjuder myndighet möjlighet att under en period om 12 månader genomföra pilotdrift med ett begränsat antal unika användare.

Under pilottiden erbjuder Teleca AU-System myndigheten att hyra Teleca Security Server till en kostnad motsvarande 30 % av den totala licenskostnaden.

Om Myndigheten efter genomförd pilot väjer att inte gå vidare till skarp drift kan myndigheten utan extra kostnader utöver hyreskostnaden lämna tillbaka licenserna för Teleca Security Server.

Väljer Myndigheten att efter pilottidens slut övergå till skarp drift erlägger myndigheten 80 % av den totala licenskostnaden.

Supportavgift tillkommer enligt gällande prislista.

4) Testlicens för Teleca Security Server avser användning i testmiljö under en tvåmånadersperiod. För att göra det enkelt för kunder att komma igång levererar Teleca AU-System mjukvaran med exempelkod och tillgängliga testcertifikat.

Testperioden kan efter båda parter godkännande förlängas i två månadersperioder.

Testlicensen erbjuds kostnadsfritt.

6.2 Nexus

		År 1		År 2		År 3		År 4	
		Licenser	Underhåll & Support	Licenser	Underhåll & Support	Licenser	Underhåll & Support	Licenser	Underhåll & Support
Myndighet	Små	25 000	12 500	50 000	25 000		25 000		25 000
	Stora ¹⁾	50 000	25 000	100 000	50 000		50 000		50 000
Kommun ²⁾	<30 000	10 000	5 000	20 000	10 000		10 000		10 000
	30 000-80 000	25 000	12 500	50 000	25 000		25 000		25 000
	>80 000	50 000	25 000	100 000	50 000		50 000		50 000
Landsting ³⁾	< = 50 000	25 000	12 500	50 000	25 000		25 000		25 000
	> 50 000	50 000	25 000	100 000	50 000		50 000		50 000
Startpaket		Startpaketetspris motsvarar pris för licens och underhåll & support år 1							
Testpaket		Gratis utvärderingslicens giltig i 3 månader							

1) Skatteverket och motsvarande.

2) Antal kommuninvånare.

3) Antal landstingsinvånare.

Priser för Nexus MultiID Server inkluderar hantering av valfritt antal certifikatutgivare och möjlighet att använda servern för flera tjänster. Licensen tillåter även installation på flera servrar. Priserna gäller för en kund, men täcker flera av denna kunds tjänster. I support- och underhållsavgiften ingår nya releaser och servicereleaser.

Kund med giltigt support- och underhållsavtal har rätt till nya versioner till rabatterat pris, för närvarande 50 % av i varje stund gällande prislista.

Tidsbegränsad (3 månader) utvärderingslicens finns tillgänglig kostnadsfritt.

Observera att normala supportkanaler ej kan användas för utvärderingslicenser.

Observera att certifikatutfärdare kan ta ut avgifter för kontroll av certifikatstatus eller användning av certifikat. Dessa avgifter är inte inkluderade i denna prislista.

6.3 TietoEnator

		År 1		År 2		År 3		År 4	
		Licenser	Underhåll & Support	Licenser	Underhåll & Support	Licenser	Underhåll & Support	Licenser	Underhåll & Support
Myndighet	Liten ¹⁾	45 000	7 200		11 250		11 250	11 250	11 250
	Mellan ²⁾	75 000	12 000		18 750		18 750	18 750	18 750
	Stor ³⁾	190 000	30 400		47 500		47 500	47 500	47 500
Kommun ⁴⁾	<50 000	45 000	7 200		11 250		11 250	11 250	11 250
	50 000-200 000	75 000	12 000		18 750		18 750	18 750	18 750
	>200 000	190 000	30 400		47 500		47 500	47 500	47 500
Landsting ⁵⁾	<300 000	45 000	7 200		11 250		11 250	11 250	11 250
	300 000-650 000	75 000	12 000		18 750		18 750	18 750	18 750
	>650 000	190 000	30 400		47 500		47 500	47 500	47 500
Startpaket		3 500 kr/mån under maximalt 6 månader							
Testpaket		Inget separat utvärderingspaket. Dock demokörning möjlig. Även startpaketet kan användas vid test							

- 1) Myndigheter med högst 100 anställda.
- 2) CSN, PRV och motsvarande.
- 3) AMS, RFV, RPS, Skatteverket och motsvarande.
- 4) Antal kommuninvånare.
- 5) Antal landstingsinvånare.

Licens avser 36 månader med möjlighet till förlängning 12 månader vid erläggande av 25 % av grundlicenspris.

Försöksverksamhet/Pilotlicens

I syfte att bedriva försöksverksamhet/pilot med TECS BankID kan nyttjandet av programprodukten gälla under begränsad tid till en begränsad avgift.

Leveransavtalet reglerar den fullständiga licensen samt den avgift som skall erläggas under försöksverksamheten för nyttjandet av programprodukten. Avgiften erlägges vid tecknandet av leveransavtalet.

Normalt sex månader efter effektiv leverans av försöksverksamhetens installation faktureras resterande nyttjandeavgift och underhållsavgift. Därvid får 80 % av till försöksverksamheten erlagd nyttjandeavgift tillgodoräknas Beställaren vid fakturering av total nyttjandeavgift och underhållsavgift.

Hyra

För att möjliggöra för exempelvis en uppstart av ett projekt eller för att tillfredsställa ett behov av finansiering erbjuds hyresalternativ av produkten TECS BankID. Prissättning av detta sker utifrån behovsbilden och med samma förmånliga prisnivåer som engångslicenserna.



2005-02-22

Rabatter

Ett samordnat avrop av flera organisationer kan ge upphov till mängdrabatt/samordningsrabatt.

En sådan bedömning kan göras från fall till fall och införas i aktuellt Leveransavtal.

7 Beräkningsstöd via kalkyl på Statskontorets webb

Förvaltningar som vill göra prognoser för sina eID-kostnader kan nu få hjälp. Statskontoret har tagit fram en Excel-kalkyl för uppskattning av eID-kostnader. Kalkylmodellen kan nås via adressen www.statskontoret.se/eidkalkyl

Modellen kan även inkludera kostnaden för köparprogramvara och Infratjänst.

8 Begrepp och definitioner

Begrepp	Förenklad beskrivning	Definition
e-legitimation Elektronisk legitimation (e-leg) Elektronisk identitets-handling (eID)	En elektronisk motsvarighet till en vanlig legitimation. Innehavaren använder den för att legitimera sig och att skriva under.	Intyg i elektronisk form av en utfärdare som kopplar ihop en publik nyckel med en innehavare och bekräftar vem innehavaren är samt en privat nyckel som förvaras tillsammans med intyget. Utfärdaren förser intyget med sin avancerade elektroniska stämpel.
Certifikat	Den del av en e-legitimation som används för att identifiera innehavaren och kontrollera om det är innehavaren som undertecknat.	Ett av en utfärdare stämplat intyg i elektronisk form som innehåller den publika nyckeln i ett nyckelpar och som kopplar ihop ett nyckelpar med en innehavare och bekräftar vem innehavaren är.
e-legitimation för myndighets elektroniska stämpel		e-legitimation som utfärdas för att det ska kunna kontrolleras att stämplade elektroniska handlingar är äkta.
e-tjänst (Elektronisk) självbetjäningstjänst	En elektronisk tjänst där användaren kan utföra sina ärenden.	En tjänst där kommunikation sker elektroniskt mellan t.ex. myndighet och privatperson. Tjänsten kan innefatta funktioner för legitimering och undertecknande med stöd av en ID-tjänst.
Förlitande part	Den som litar på en elektronisk underskrift, en elektronisk stämpel eller en e-legitimation.	Den som tar emot en e-legitimation, en annan undertecknad eller stämplad elektronisk handling eller data för identifiering av privatpersoner, handläggare eller myndigheter och som svarar för vissa kontroller samt avses lita på den elektroniska handlingen eller data för identifiering. Förlitande part kan vara såväl en privatperson som en myndighet eller en utfärdare.
Hårdvarubaserad bärare		En säker nyckelförvaringsplats för den privata nyckeln med beräkningskapacitet för basala kryptologiska beräkningar så att den privata nyckeln aldrig behöver lämna bäraren. Exempel på hårdvarubaserade bärare är aktivt kort, SIM-kort, USB-enhet med aktivt chip (där privata nyckeln aldrig lämnar chipet).
(Elektronisk) identifiering Elektronisk ID-kontroll	Kontroll av vem som legitimerar sig med en e-legitimation.	Kontroll av att en viss privatpersons, handläggares eller myndighets privata nyckel för legitimering har använts. Den privata nyckeln för legitimering ska a) vara knuten uteslutande till en fysisk person eller en myndighet, och b) ha använts i en process som gör det möjligt att identifiera personen eller myndigheten genom att kontrollera vissa elektroniska data; normalt ett av motparten signerat slumptal. Data som kontrolleras ska ha skapats med en nyckel som endast innehavaren har under sin kontroll.
ID-tjänst	En tjänst för att ut-	En tjänst som en utfärdare av e-legitimationer

2005-02-22

	färda, stödja och kontrollera e-legitimationer.	tillhandahåller för att stödja elektroniska underskrifter och legitimationer
Personlig e-legitimation Medborgarcertifikat		E-legitimation som tilldelas en enskild i egenskap av privatperson.
Personlig e-legitimation för riktad grupp		E-legitimation som tilldelas en enskild i egenskap av privatperson där tilldelningen erbjuds på uppdrag av myndigheter som subventionerar eller bekostar leverantörers kostnader i samband med tilldelningen.
Privat nyckel	Dina hemliga data som du aktiverar med din säkerhetskod och använder för att underteckna eller legitimera dig elektroniskt.	Den hemliga delen av ett nyckelpar för kryptering där det som krypteras med den ena nyckeln kan dekrypteras med den andra.
Privatperson Medborgare		Fysisk person som innehar en personlig e-legitimation och använder den för egen räkning eller som företrädare för en fysisk person eller en juridisk person som inte är en myndighet ⁷ .
Publik nyckel	Uppgift i din e-legitimation som förlitande part använder för att identifiera dig eller att kontrollera din underskrift.	Den publika delen av ett nyckelpar för kryptering där det som krypteras med den ena nyckeln kan dekrypteras med den andra.
Spärr		En markering om att en e-legitimation inte längre bör anses tillförlitlig. Spärrarna distribueras i form av spärrlistor eller görs tillgängliga via en tjänst för giltighetskontroll.
Spärrkontroll		Kontroll som förlitande part gör av att en e-legitimation inte har spärrats. Spärrkontroll kan göras gentemot en spärrlista eller mot en tjänst för transaktionsbaserad giltighetskontroll
Spärrlista		En elektroniskt undertecknad eller stämplad lista över e-legitimationer som har spärrats.
(Elektronisk) stämpel Avancerad elektronisk stämpel e-stämpel	Ett elektroniskt bevis, som motsvarar en elektronisk underskrift och intygar vilken organisation som har ställt ut handlingen.	Elektronisk signatur som a) är knuten uteslutande till en myndighet eller en annan organisation, b) gör det möjligt att identifiera myndigheten eller organisationen, c) är skapad med hjälpmedel som endast myndigheten eller organisationen har kontroll över, och d) är knuten till andra elektroniska data ⁸ på ett sådant sätt att förvanskningar av dessa data kan upptäckas
(Elektronisk) tjänst-legitimation Tjänstecertifikat	E-legitimation för handläggare vid en myndighet.	E-legitimation som tilldelas en person i egenskap av anställd eller uppdragstagare.
(Elektronisk) underskrift Avancerad elektronisk	En elektronisk motsvarighet till en	Elektronisk signatur som a) är knuten uteslutande till en undertecknare,

⁷ I äldre versioner av riktlinjerna användes begreppet "medborgare", vilket kan missförstås så att endast svenska medborgare skulle innefattas. Begreppet privatperson skulle istället kunna missförstås så att personen inte kan underteckna som företrädare för en juridisk person. Genom att använda begreppet privatperson tydliggörs emellertid att den elektroniska underskriften och e-legitimationen hör till en viss individ, oberoende av om denne agerar för egen eller för annans räkning (se 1.4.1).

⁸ Med "andra elektroniska data" menas data som representerar texten i dokumentet.

2005-02-22

signatur	namnteckning.	b) gör det möjligt att identifiera undertecknaren, c) är skapad med hjälpmedel som endast undertecknaren har kontroll över, och d) är knuten till andra elektroniska data ⁹ på ett sådant sätt att förvanskningar av dessa data kan upptäckas
Utfärdare (av e-legitimation) Certifikatutfärdare Utgivare	Den som ger ut e-legitimationer.	Den som utfärdar e-legitimationer; här beteckning på utfärdare som uppfyller kraven enligt dessa riktlinjer.
Webbserverlegitimation Webbservercertifikat		E-legitimation som utfärdas för att medborgare och myndigheter ska kunna identifiera en myndighets e-tjänst som de kommunicerar med och skydda denna kommunikation mot obehörig insyn. (Beteckningen <i>webbserverlegitimation</i> kommer från SAMSET och används här främst för att behålla sambandet med SAMSETs rapporter. Webbserverlegitimation är här synonymt med olika typer av <i>serverlegitimation</i> , <i>funktionslegitimation etc.</i>)

⁹ Se not 8.