

Håndbog net-ID standard

Version 1.11

17. juli 2007

Synopsis

Dokumentnavn:	Kravbeskrivelse
Konceptnummer:	IO-2162
Konceptnavn:	Håndbog net-ID standard
Version, Versionsdato:	1.11, 17. juli 2007
Versionshistorik	<p>Version 1.0: 26. marts 2004</p> <p>Version 1.1: 4. maj 2004</p> <p>Afsnit om direkte link medtaget</p> <p>Definitioner: net-ID taget fra TU-aftale</p> <p>Indrapportering af data til batchserver:</p> <ul style="list-style-type: none">- Kun logo i GIF-format er tilladt- URL-felt tilføjet <p>Bilag 3: URL ændres til IP-adresse</p> <p>Dokumentbekræftelse request: HDR_KVER netbankens er ændret til tjenesteudbyders certifikater.</p> <p>Dokumentbekræftelse respons: HDR_KVER punktum fjernet fra Keylabel.</p> <p>Certifikatanmodning: Krav om password beskyttet ZIP-fil slettet. Subject Distinguished Name a) og c) Common Name indeholder "net-ID".</p> <p>Version 1.2: 28. maj 2004</p> <p>7.2 Reference til ledelseserklæring inkluderet.</p> <p>8. Skema til indrapportering delt i 2.</p> <p>14. Ledelseserklæring delt i 2.</p> <p>Version 1.3: 18. august 2004</p> <p>5. Tilføjelse af krav om fremvisning af dokumentbekræftelse.</p> <p>6. Tilføjelse af reference til faktureringsgrundlag.</p> <p>7. Kryptering af dokumentbekræftelse ændret til opbevaring i beskyttede biblioteker.</p> <p>Bilag 1: Specifikation af e-Tickets, maks. længde af dokumentbekræftelse ændret til 20 KB.</p> <p>7.3.4 Tilføjelse af anbefaling til TU om pilottest med konkrete netbankbrugere.</p> <p>Version 1.4: 20. september 2004</p> <p>5. Nyt krav, ingen sammenblanding af net-ID og netbank.</p> <p>7.3.2 TU skal kvittere for dokumentbekræftelse.</p> <p>8. Blanket for indrapportering til Batchserver flyttet til bilag.</p> <p>Bilag 1: Note tilføjet om CVR-nummercheck.</p> <p>Bilag 2: Brugerregler inkl. dokumentbekræftelse.</p> <p>Bilag 3: Password slettet i formular.</p> <p>Bilag 4: Nyt - Fremskaffelse af dokumentation i en tvist.</p> <p>Bilag 7: Nyt - PBS kundesupport.</p> <p>Bilag 8: Nyt - net-ID vedligeholdelse</p>

Bilag 9: Nyt - Servicemål

Bilag 10: Nyt - Retningslinjer for kommunikation af net-ID.

Bilag 11: Nyt - TU checkliste for implementering af net-ID.

Version 1.5, 15. november 2004

Kapitel 5: Krav til dokumentbekræftelse, punkt k slettet og der er tilføjet 4 nye punkter m.n.o.p.

Kapitel 7.2.3 Præciseret krav til indrapportering af testrapport.

Kapitel 7.3.2 Præciseret krav med hensyn til:

- Bruger-ID for operatør
- Logisk adgang
- Revisionspsor og logning

Kapitel 7.3.4 Præciseret krav til indrapportering af testrapport.

Kapitel 9: systemtest. Præcisering af test.

Kapitel 21: Testerk læring

Version 1.6, 21. januar 2005

Afsnit 7.2.2 print af dokumentbekræftelse præciseret.

Kapitel 9 systemtest opdateret

Kapitel 15 bilag 6 Indrapportering til batchserver er opdateret med vært for tjenesteudbyder.

Kapitel 22 bilag 13 PI Revisionscheckliste inkluderet.

Version 1.7, 24. maj 2005

Kapitel 4: Ændring af adresseoplysninger for certifikatansøgningsformular og elektronisk ansøgning.

Kapitel 9: Tilføjelse af test hændelse hvor det testes, at man kan håndtere et certifikatskift.

Bilag 1: Tilføjelse af protokol version 1005, samt præcisering af adresseoplysninger.

Bilag 6: Tilføjelse Logo skal angives.

Version 1.8, 21. juli 2005

Generel opdatering så alle krav er blevet nummereret for at lette den årlige systemrevision.

Afsnit 4.3: Præcisering af certifikatformat for filer fra PBS.

Kapitel 22: Inkludering af Revisionschecliste.

Version 1.9, 6. januar 2006

Generelt: Kontaktinformationer ændret.

Kapitel 1.2: Opdatering af referencer.

Kapitel 12: Opsplitning i 2 ansøgningsformularer samt tilføjelse af fuldmagt.

Kapitel 22: Præciseringer af checklister

Nyt kapitel 23: Kontaktinformationer

Version 1.10, 2. juni 2006

Generelt: Kontaktinformationer ændret.

Bilag 6: Supplerende oplysninger indsat for TU der benytter direkte link.

	Version 1.11, 17. juli 2007
	Kap. 3: Tilføjelse af tekst for direkte logon.
	Afsnit 7.3.1: 1) præcisering af krav.
	Afsnit 7.3.2: 3) anbefaling ændret til krav.
	Kap. 9: Præcisering af testhændelser.
	Kap. 10: Inkludering af CVR i KUNDEIDTYPE.
	Kap. 18: Ændring af planlagt servicevindue.
	Kap 21: Opdatering af indhold af testrapport.
	Kap 22: Kontaktinformationer opdateret.
Målgruppe:	PI-sektoren og private tjenesteudbydere
Dokumentejer:	PE 2210
Dokumentstatus:	Officiel udgave
Dokument udarbejdet af:	Peter Fjelbye
Kvalitetssikret af:	PE 2210
Type af kvalitetssikring:	
Fysisk placering:	k:\processer\net-id forvaltning\ni\håndbog\håndbog version 1-11 17072007 officiel.doc
Sikkerhedsklasse:	Uklassificeret
OPUS Skabelon	Kravbeskrivelse (local).dot
Format:	Microsoft Word 10.0
Copyright:	@PBS A/S 2007
	Alle rettigheder tilhører PBS Holding A/S. Det er ikke tilladt at videregive eller på anden måde gøre materialet eller dele heraf tilgængeligt for tredjepart uden tilladelse fra PBS.

Indholdsfortegnelse

1.	Indledning	6
1.1.	Omfang	6
1.2.	Referencer	6
1.3.	Definitioner og forkortelser	8
1.4.	Vedligeholdelse af dokumentet	9
2.	Net-ID	10
2.1.	Generel beskrivelse	10
2.2.	Direkte link	11
2.3.	Dokumentbekræftelse	11
3.	Specifikation af kommunikationsprotokol	12
3.1.	Protokol for logon	12
3.2.	Direkte logon	13
3.3.	Protokol for dokumentbekræftelse	13
3.4.	E-Ticket layout	13
4.	PBS-Certifikater	15
4.1.	Ansøgning om certifikater	15
4.2.	Ansøgningsformular	15
4.3.	Certifikatanmodning (certifikat-request)	15
4.4.	Certifikatfornyelse	17
4.5.	Certifikatspærring/-afmelding	17
5.	Anvisning af pengeinstitutternes kommunikation til brugerne	18
5.1.	Skærmbillede til brug for tilmelding	18
5.2.	Skærmbillede til brug for logon og dokumentbekræftelse	18
5.3.	Indhold i skærmbilleder	20
5.4.	Præsentation af tjenesteudbyders logo	21
6.	Krav til opsamling af faktureringsgrundlag i pengeinstitutterne	22
7.	Sikkerhedskrav	24
7.1.	Kommunikationssikkerhed og krypteringsnøgler	24
7.2.	Sikkerhedskrav til pengeinstitutterne	26
7.2.1.	Sikkerhedskrav til nøgleadministration	26
7.2.2.	Opslag på Batch-server	26
7.2.3.	Interne sikkerhedskontroller i pengeinstitutterne	26
7.2.4.	Test, erklæring og godkendelse	28
7.3.	Sikkerhedskrav til tjenesteudbyder	28
7.3.1.	Sikkerhedskrav til nøgleadministration	28
7.3.2.	Interne sikkerhedskontroller hos tjenesteudbyder	29
7.3.3.	Krav til tjenesteudbyders skærmbilleder	32
7.3.4.	Test, erklæring og godkendelse	33
7.4.	Sikkerhedskrav PBS CA	33
8.	Indrapportering af data til Batchserver	34
9.	Systemtest	35
10.	Bilag 1: Specifikation af e-Tickets	38
11.	Bilag 2: Net-ID-krav til pengeinstituttets aftale med bruger	49
12.	Bilag 3: Ansøgningsformularer PBS-certifikater	52
	Fuldmagt til bestilling af PBS certifikater	54
13.	Bilag 4: Fremskaffelse af dokumentation i en tvist	55
14.	Bilag 5: Ledelseserklæringer	62
15.	Bilag 6: Blanket til indrapportering til Batch-server	64
16.	Bilag 7: PBS kundesupport	70
17.	Bilag 8: Net-ID vedligeholdelse	72
18.	Bilag 9: Servicemål	75
19.	Bilag 10: Retningslinjer for kommunikation af net-ID	76
20.	Bilag 11: TU-checkliste for implementering af net-ID	78
21.	Bilag 12 Testrapport	80
22.	Bilag 13 Revisionschecklister	81
23.	Bilag 14 Kontakt	90

1. Indledning

Formålet med denne håndbog er at angive tekniske standarder og retningslinjer for anvendelse af net-ID. Håndbogen henvender sig både til pengeinstitutter og deres datacentraler samt til de tjenesteudbydere, som ønsker at tilslutte sig net-ID-løsningen. Net-ID-løsningen er en identifikationsløsning, der bygger på den infrastruktur, som danske pengeinstitutter har opbygget gennem en årrække med deres netbankløsninger. Via en standardiseret grænseflade kan tjenesteudbydere nu få adgang til denne infrastruktur. En tjenesteudbyder, der tilslutter sig infrastrukturen, kan hermed få adgang til 2 mio. netbankbrugere, der med deres almindelige netbank-adgangskoder kan logge på hos tjenesteudbydere.

1.1. Omfang

Håndbogen stiller krav til pengeinstitutterne og deres datacentraler samt til tjenesteudbydere. Disse krav omfatter net-ID-protokollen og tekniske standarder for udveksling af net-ID. Endvidere stilles der krav til sikkerhed ved nøgleadministration og til sikkerhedskontroller i de edb-miljøer, hvor logon-komponenten installeres.

Håndbogen indeholder desuden de minimumsbestemmelser, der skal indarbejdes i netbankernes brugerregler.

1.2. Referencer

Love, bekendtgørelser og retningslinjer

- 1) Retningslinjer vedrørende foranstaltninger mod hvidvaskning af penge, Finansrådet juni 1993.
- 2) Kodeks for IT-sikkerhed i selvbetjeningssystemer, Finansrådet 14. januar 2003.
- 3) Vejledning om kontrol- og sikringsforanstaltninger på IT-området i henhold til lov om finansiel virksomhed § 71, stk. 1, nr.4, vejledning nr. 9074 af 23. januar 2004.
- 4) PBS Certifikat Practice Statement (CPS).
- 5) Lov nr. 429 af 31. maj 2000 Lov om behandling af personoplysninger.
- 6) Bekendtgørelse om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning. Sikkerhedsbekendtgørelsen (Bkg. nr. 528 af 15. juni 2000 som ændret ved bkg. nr. 201 af 22. marts 2001).

- 7) Vejledning til bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning. Sikkerhedsvejledning (vejledning nr. 37 af 2. april 2001).
- 8) Transmission af personoplysninger over Internet af den 15. august 2001, Datatilsynet.
- 9) Lov om visse betalingsmidler - Lov nr. 414 af 31/05/2000 (Gældende).

Tekniske standarder

- 10) FIPS PUB 140-1 (1994): Security Requirements for Cryptographic Modules.
- 11) ISO/IEC 9794-8 ITU-T Recommendation X.509 Information Technology – Open systems Interconnects, The Directory: Public Key and Attribute certificate frameworks.
- 12) PKCS #1 [RSA Cryptography Standard](#)
- 13) PKCS #7: [Cryptographic Message Syntax Standard](#)
- 14) PKCS #10: [Certification Request Syntax Standard](#)
- 15) PKCS #12: [Personal Information Exchange Syntax Standard](#)
- 16) [RFC 2246](#): "The TLS Protocol Version 1.0".

Net-ID-specifikationer

- 17) Tjenesteudbyder til Netbank Kommunikationsprotokol, version 2.2, af 19. maj 2005.
- 18) Logon Requester API Installations- og brugsvejledning, version 1.3 af 2. december 2003.
- 19) Logon Requester API Specifikation Version: 2.3, af 28. oktober 2003.
- 20) Test med Vejrtjenesten, version 2.0, 17. august 2004.
- 21) Faktureringsgrundlag fra Datacentraler vedr. Tjenesteudbyders forbrug af Generel Logon, version 3, 25. juni 2004.
- 22) Afvist faktureringsgrundlag til Datacentraler vedr. Tjenesteudbyders forbrug af Generel Logon, version 2, 25. juni 2004

1.3. Definitioner og forkortelser

Definitioner

- *E-Ticket*: En e-Ticket er en specifik protokolmeddelelse, der er signeret med brug af afsenders private krypteringsnøgle. E-Ticket indeholder oplysninger om afsenderen af e-Ticket. Desuden kan en e-Ticket indeholde ID-oplysninger om en netbankbruger og en meddelelse fra tjenesteudbyder, som ønskes bekræftet af brugeren.
- CA: Certification Authority er en betroet tredjepart, der er ansvarlig for udstedelse og administration af certifikater.
- *Certifikat*: Et certifikat er et digitalt visitkort, som indeholder navn, offentlig nøgle og nogle få andre oplysninger. Certifikatet er digitalt underskrevet af en CA, som står inde for, at indehaverens identitet er korrekt, og at indehaveren er i besiddelse af den private nøgle. Certifikater benyttes til at verificere digitale signaturer, som er lavet med den tilhørende private nøgle. Certifikater kan distribueres frit, mens private nøgler aldrig må komme andre i hænde end den retmæssige indehaver.
- *Net-ID*: Ved net-ID forstås en række elementer, der tilsammen sætter tjenesteudbyder i stand til at få oplyst identiteten af brugere og få brugere til at knytte deres identitet til indholdet af et givent dokument;
 - en specifikation af en fælles kommunikationsgrænseflade til pengeinstitutternes sikkerhedssystemer,
 - software til installation hos tjenesteudbyder,
 - et CA-system (nøglecenter) til udstedelse af certifikater med henblik på verifikation af tjenesteudbyder,
 - en batch-server til brug for registrering af tilsluttede tjenesteudbydere og pengeinstitutter,
 - håndbogen, der specificerer procedurer og sikkerhedskrav til tjenesteudbydere og pengeinstitutters edb-installationer,
 - logninger af brugerens opkoblinger til tjenesteudbydere og lagring af de dokumenter, som brugeren har knyttet sin identitet til, og
 - det systembevis og de muligheder for at tilvejebringe de beviseligheder, der godtgør, hvorvidt og hvornår en bestemt kommunikation mellem bruger og tjenesteudbyderen har fundet sted.
- *Tjenesteudbyder*: En tjenesteudbyder er en privat eller offentlig virksomhed, der stiller tjenester til rådighed på internettet.

Forkortelser

- RSA-algoritme: Public Key Cryptosystem opfundet af Rivest Shamir og Adleman.

- SHA-1: Secure Hash Algorithm udviklet af NIST i 1994.

1.4. Vedligeholdelse af dokumentet

Denne håndbog vedligeholdes af PBS A/S.

Net-ID-specifikationerne er PBS A/S' ejendom. Der må ikke foretages ændringer i net-ID-specifikationerne uden godkendelse af PBS A/S.

Ændringsønsker til denne håndbog skal rettes til PBS (se kapitel 23 Kontakt).

Dette dokument er opdelt i en række afsnit, der hver især beskriver delementer af dokumentets kravbeskrivelse.

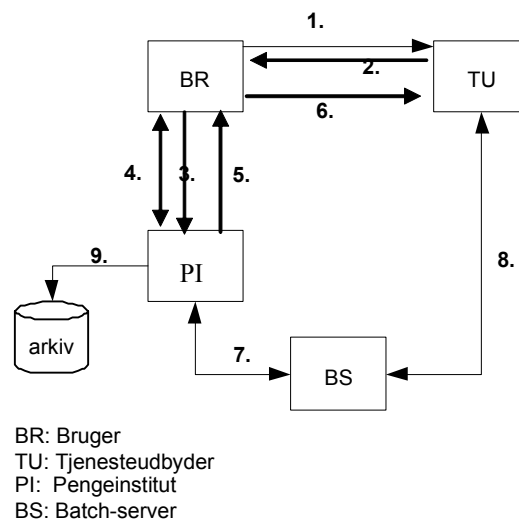
2. Net-ID

2.1. Generel beskrivelse

Net-ID er et identifikationssystem, der på en let og effektiv måde sikrer, at en bruger kan logge på hos en vilkårlig tjenesteudbyder med brug af samme adgangskode, som bruger anvender i sin netbank. Net-ID giver tillige tjenesteudbyder mulighed for at få brugers accept af indholdet af en specifik meddelelse. Meddelelsen signeres og lagres af brugers pengeinstitut, inden den fremsendes i en net-ID til tjenesteudbyder. Denne funktionalitet kaldes en dokumentbekræftelse, idet brugers pengeinstitut gemmer en kopi af meddelelsen til brug for evt. senere bevisførelse.

Funktionaliteten i en logonsekvens er, at bruger kontakter tjenesteudbyders website og anmoder om logon via sit pengeinstitut (1). Tjenesteudbyder dirigerer bruger til eget pengeinstitut sammen med en e-Ticket (2) og (3). Pengeinstituttet verificerer e-Ticket fra tjenesteudbyder. Herefter bliver bruger autentificeret ved brug af pengeinstituttets sikkerhedssystemer (4). Til sidst dirigeres bruger tilbage til tjenesteudbyder med en e-Ticket fra pengeinstituttet, som fortæller tjenesteudbyder, hvorvidt autentifikationen af bruger er gennemført tilfredsstillende (5) og (6). Tjenesteudbyder verificerer e-Ticket fra netbanken og kan dermed logge bruger ind til data, som bruger er autoriseret til. Autorisationen defineres egenhændigt af tjenesteudbyder.

Udvekslingen af e-Ticket mellem tjenesteudbyder og netbank skitseres i følgende tegning:



Systemoversigt net-ID

Den på figuren nævnte "Batch-server" er en server, som er opstillet hos PBS, og som blandt andet rummer en liste med tilsluttede pengeinstitutter og deres da-

tacentraler samt tjenesteudbydere. Pengeinstitutter kan fra Batch-serveren hente en liste med oplysninger om tjenesteudbydere, der er tilsluttet net-ID (7) mens tjenesteudbydere kan hente en liste med tilknyttede pengeinstitutter (8).

2.2. Direkte link

I net-ID er der også mulighed for, at en bruger via et direkte link i netbanken, kan linke direkte til en tjenesteudbyder. Der kan være tekniske forhold, som skal aftales direkte mellem pengeinstitut og tjenesteudbyder i denne forbindelse.

2.3. Dokumentbekræftelse

Net-ID kan tillige benyttes af en tjenesteudbyder til at få en bekræftelse på indholdet af en specifik meddelelse og kan dermed fastholde dette over tid og eventuelt benytte det som bevis, såfremt der måtte opstå en tvist om indholdet af meddelelsen.

Udvekslingen af net-ID for dokumentbekræftelse foregår på samme måde som beskrevet ovenfor i afsnit 2.1. I denne situation medsendes blot den meddelelse, som tjenesteudbyder ønsker, at bruger skal godkende.

Godkendelsen sker ved at bruger bekræfter indholdet af meddelelsen ved brug af sin netbank adgangskode. Pengeinstituttet modtager meddelelsen fra bruger og opbevarer denne til brug for en eventuel senere bevisførelse. Bruger bliver herefter dirigeret til tjenesteudbyder sammen med en e-Ticket fra pengeinstituttet. Tjenesteudbyder vil modtage denne e-Ticket, som indeholder meddelelsen, der er godkendt af bruger.

3. Specifikation af kommunikationsprotokol

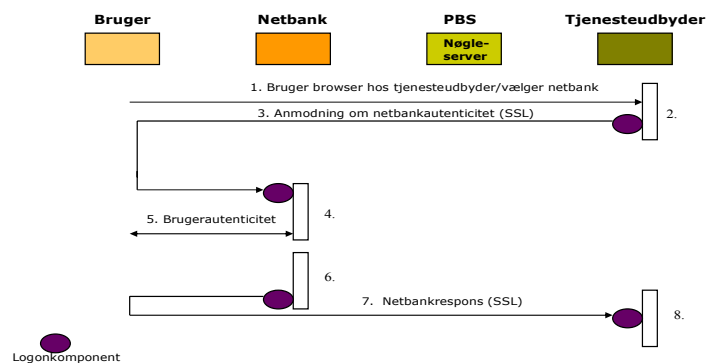
Dette afsnit indeholder en overordnet beskrivelse af protokollen for net-ID og dermed de e-Tickets, der udveksles. Kapitel 10 Bilag 1 specificerer de konkrete e-Tickets, der indgår i net-ID.

Når tjenesteudbyder har fremstillet en e-Ticket sendes den til pengeinstituttet via omdirigering på brugers browser. E-Ticket placeres i en HTML-form i et hidden field med navnet "ETICKET", som med JavaScript sendes til pengeinstituttet i et HTTP POST request. Dette gøres meget let som vist i følgende:

```
<form name="netbank" action="https://bank URL" method="post">  
<input type="hidden" name="ETICKET" value="eticket data"/>  
</form>  
<script>document.netbank.submit( )</script>
```

Teksterne "bank URL" og "eticket data" skal erstattes af rigtige data.

3.1. Protokol for logon



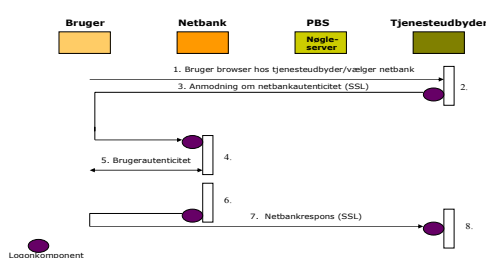
- 1) Bruger browser hos tjenesteudbyder og vælger pengeinstitut.
- 2) Tjenesteudbyder fremstiller autenticitetsanmodning.
- 3) Bruger bliver dirigeret til eget pengeinstitut i en SSL-tunnel.
- 4) Netbanksikkerhedssystemet verificerer anmodningen fra tjenesteudbyder.
- 5) Netbanksikkerhedssystemet anmoder om brugerautenticitet (2-faktor autentitet).
- 6) Netbanksikkerhedssystemet fremstiller respons.
- 7) Bruger bliver dirigeret til tjenesteudbyder i en SSL-tunnel.

- 8) Tjenesteudbyder verificerer respons fra pengeinstitut og giver bruger adgang.

3.2. Direkte logon

Direkte logon er en variant af net-ID logon, hvor brugeren starter sin kommunikation i netbanken, dvs. logger ind i netbanken på almindelig vis og vælger derfra at blive logget på hos en tjenesteudbyder med brug af net-ID. Netbanken fremstiller en e-Ticket der indeholder de nødvendige oplysninger se kap. 10. Protokollen vil derfor kun omfatte hændelserne 5), 6), 7) og 8) ovenfor.

3.3. Protokol for dokumentbekræftelse



- 1) Bruger browser hos tjenesteudbyder og vælger pengeinstitut.
- 2) Tjenesteudbyder fremstiller dokument, der skal godkendes af bruger, og fremstiller en anmodning til brugers pengeinstitut.
- 3) Bruger bliver dirigeret til netbanksikkerhedssystemet i en SSL-tunnel.
- 4) Netbanksikkerhedssystemet verificerer anmodning fra tjenesteudbyder.
- 5) Netbanksikkerhedssystemet præsenterer dokument, der skal godkendes, og anmoder om brugerautenticitet (2-faktor autenticitet).
- 6) Netbanksikkerhedssystemet verificerer brugerautenticitet og gemmer kopi af dokument med tilhørende autenticitetsdata.
- 7) Pengeinstituttet fremstiller en e-Ticket, der indeholder meddelelsen, der blev præsenteret for bruger, og dirigerer bruger tilbage til tjenesteudbyder i en SSL-tunnel.
- 8) Tjenesteudbyder verificerer respons fra pengeinstitut og gemmer kopi heraf.

3.4. E-Ticket layout

Dette afsnit beskriver datalayout for e-Ticket, som anvendes i forbindelse med protokollen mellem tjenesteudbydere og netbanker. E-Ticket-headerens HHDR_ALG felt sættes altid til PKCS#7 med SHA1 svarende til værdien 13. Det

betyder, at de efterfølgende dele af e-Ticket (Auth Ticket og Context Ticket) er indlejrede i headerens HDR_TICKET i form af PKCS#7 ContentInfo.

1. Der skal anvendes e-Ticket i henhold til kapitel 10 bilag 1. Alle e-Ticket skal indeholde et certifikat, selv om det ifølge PKCS#7 standarden er valgfrit.

I kapitel 10 bilag 1 er specificeret følgende e-Ticket:

- Logonanmodning fra tjenesteudbyder til pengeinstitut.
- Logonresponse fra pengeinstitut til tjenesteudbyder.
- Dokumentbekræftelsesansøgning fra tjenesteudbyder til pengeinstitut.
- Dokumentbekræftelsesresponse fra pengeinstitut til tjenesteudbyder.

E-Ticket-formatet består af 3 dele, en Header, en Auth Ticket og en Context Ticket:

Felt	Beskrivelse
Header	Beskriver format og sikkerhed for den e-Ticket, der følger.
Auth Ticket	Indeholder information til brugeridentifikation.
Context Ticket	Indeholder supplerende information om bruger.

4. PBS-Certifikater

4.1. Ansøgning om certifikater

I Net-ID-løsningen skal anvendes SSL-certifikater og net-ID-certifikater, se kapitel 7.1.

Net-ID-løsningen er et "lukket system", som kræver, at der indgås en tilslutningsaftale til infrastrukturen. Der kan kun udstedes certifikater til de parter, der har indgået denne aftale eller til edb-servicevirksomheder, der drifter løsningen på vegne af en part, der har indgået tilslutningsaftalen.

Vejledning

For at få et certifikat, der benyttes i forbindelse med net-ID-løsningen, skal ansøgeren fremsende en ansøgning for hver certifikattype, der skal benyttes. Ansøgningen skal fremsendes til PBS.

Ansøgning om PBS-certifikater foregår som specificeret i 4.2 og 4.3:

4.2. Ansøgningsformular

Ansøger udfylder ansøgningsformular (se kapitel 12) og indsender denne til PBS A/S, Lautrupbjerg 10, 2750 Ballerup, att.: Sikkerhedsadministrationen.

PBS kontrollerer oplysningerne.

4.3. Certifikatanmodning (certifikat-request)

Fremstilling af certifikatanmodning foregår ved brug af standardværktøjer, der giver mulighed for at importere, eksportere og fremstille certifikat-request. De eksisterende scripts i referenceimplementeringen (Open SSL) kan også benyttes til at anmode om SSL-certifikater.

Hver certifikat-request skal opfylde følgende:

- PKCS #10 DER kodet med base 64 + eventuelt PEM header og footer.
- Identificere hvilken type certifikat, der ønskes udstedt (SSL-server-certifikat eller net-ID-certifikat).
- Filnavnet skal overholde følgende format: nnnnnnnn.xxx, hvor nnnnnnnn er et unikt filnavn, der er defineret af ansøgeren, og hvor xxx er enten "der" eller "pem", afhængig af kodningen.
- Nøglefremstillingsalgoritmen skal være RSA med en nøglelængde på 1024 bit, og hash-algoritmen skal være SHA-1.

- Certifikatansøgningen må kun indeholde Subject Distinguished Name-felter, offentlige nøglekomponenter samt en Certificate Extension Request Attribute, som hedder SubjectKeyIdentifier (ref. 14), hvor KeyLabel placeres.

Certifikatfornyelse foregår som specificeret i afsnit 4.1.

Net-ID anvender forskellige typer af certifikater, der skal indeholde tilsvarende forskellige Subject Distinguished Name-oplysninger:

- a) Net-ID certifikat: benyttes til at sikre e-Tickets
- b) SSL-server-certifikat: Benyttes til at identificere en server i en SSL-dialog.
- c) SSL-Klient-certifikat: Benyttes til at identificere en afsender i en SSL-dialog, specielt når en tjenesteudbyder eller en datacentral skal initiere en SSL-dialog med Batch-serveren.

a) Subject Distinguished Name-format (net-ID-certifikat-request)

Country Name	DK for Danmark
State or Province Name	Kommune
Locality Name	By
Organization Name	Firmanavn evt. inkl. CVR-nr.
Organizational Unit Name	Afdeling/division
SerialNumber	CVR-nr. konkateneret med et løbenummer
Common Name	CVR-nr. net-ID (e-Ticket)

b) Subject Distinguished Name-format (SSL-server-certifikat-request)

Country Name	DK for Danmark
State or Province Name	Kommune
Locality Name	By
Organization Name	Firmanavn
Organizational Unit Name	Afdeling/division
Common Name	Serverens domain name

c) Subject Distinguished Name-format (SSL-Klient-certifikat-request)

Country Name	DK for Danmark
State or Province Name	Kommune
Locality Name	By
Organization Name	Firmanavn
Organizational Unit Name	Afdeling/division
Common Name	CVR-nr. net-ID (klient certifikat)

- 1) Ansøger fremsender certifikatanmodning til PBS. Anmodningen kan sendes med e-mail til PBS (se kapitel 23 Kontakt) eller ved brug af diskette, som sendes til adressen anført under ansøgningsformular.
- 2) PBS fremstiller PBS-certifikat X.509v3 (.cer=DER kodet og .crt=PEM kodet) og fremsender dette til ansøgeren i en e-mail.

3) Ansøger verificerer certifikatet med PBS root-certifikat og installerer PBS-certifikat.

4.4. Certifikatfornyelse

Certifikatfornyelse foregår som specificeret i afsnit 4.1.

4.5. Certifikatsspærring/-afmelding

Certifikater kan spærres hele døgnet ved henvendelse til PBS, se kapitel 23 Kontakt.

5. Anvisning af pengeinstitutternes kommunikation til brugerne

Dette afsnit indeholder anvisninger til, hvorledes pengeinstitutterne kommunikerer net-ID-løsningen til bruger. Det omfatter anvisninger til skærmbilleder til tilmeldingsfunktionen, hvor bruger kan tilmelde sig net-ID direkte i netbanken, og til skærmbilleder, hvor bruger tilmelder sig i pengeinstituttets sikkerhedssystem via anmodning fra tjenesteudbyder. Desuden er der anvisninger til skærmbilleder til godkendelsesfunktionen, som bliver aktiveret ved hver logon til en tjenesteudbyder.

Pengeinstitutterne skal efterleve følgende anvisninger:

5.1. Skærmbillede til brug for tilmelding

En bruger bør have mulighed for at tilmelde sig net-ID både direkte i sin netbank og i pengeinstituttets sikkerhedssystem via anmodning fra tjenesteudbyder.

1. Bruger skal have mulighed for at fortryde tilmeldingen efter at have læst betingelserne.
2. Skærmbilleder, hvor bruger kan tilmelde sig, skal inkludere navn og eventuelt logo for net-ID.

Der bør højst benyttes 2 skærmbilleder til at få bruger tilmeldt løsningen; en aktiveringsside og en side med betingelser, hvor brugers accept kan aktiveres.

5.2. Skærmbillede til brug for logon og dokumentbekræftelse

1. Skærmbilleder, hvor bruger indtaster personlige koder eller personlige oplysninger, skal udføres, så bruger er klar over, at bruger kommunikerer med sit pengeinstitut. Skærmbilledet skal indeholde navn og eventuelt logo fra pengeinstituttet. Skærmbilledet skal tillige indeholde navn og eventuelt logo fra tjenesteudbyder, som har foretaget logon-anmodningen, således at bruger tydeligt ved, hvortil der forsøges foretaget logon.

Skærmbilledet bør kun indeholde links, der hjælper brugeren i logon-processen.

2. Skærmbilledet må ikke indeholde reklamer, logoer eller andre meddelelser, der anbefaler andre services eller produkter.
3. Logo og brandbilleder må ikke indeholde animationer.
4. Pengeinstituttet skal gennemføre logon med den kortest mulige brugerdialog - altså færrest mulige skærmbilleder. Logon-processen fra pengeinstituttets

modtagelse af anmodning om logon til bruger kan indtaste oplysninger bør almindeligvis ikke tage mere end 1 minut.

- 5.** Skærbilledet skal give bruger mulighed for at bekræfte, at CPR-nummer, navn, adresse og e-mail-adresse overføres til tjenesteudbyder.

Pengeinstituttet må gerne forhåndsudfylde følgende felter for at smidiggøre autenticitetsprocessen: UserID og en eventuel personlig velkomsthilsen.

- 6.** Den personlige velkomsthilsen må kun defineres af brugere i en sikker dialog med pengeinstituttet, for eksempel i netbanken.
- 7.** Skærbilledet bør være in-line og skal overtage browser-sessionen i det aktuelle vindue. Såfremt det ønskes at benytte pop-up vindue, skal det aktiveres inden for det etablerede inline vindue.
- 8.** Såfremt tjenesteudbyder fremsender en fejlbehæftet e-Ticket til pengeinstituttet, kan pengeinstituttet ikke stole på afsenderen (tjenesteudbyderen) og skal derfor route bruger til en fejl-URL hos pengeinstituttet.
- 9.** Hvis bruger fortryder tilmeldingsbetingelserne for net-ID og kommer direkte fra en tjenesteudbyder, skal bruger returneres til fejl-URL hos tjenesteudbyder.
- 10.** Pengeinstituttet skal sikre, at skærbilledet ikke giver bruger indtryk af, at net-ID har relation til betalingsformidling og netbank. Det betyder, at ordet "netbank" ikke må fremgå sammen med net-ID.
- 11.** I forbindelse med dokumentbekræftelse skal skærbilledet indeholde tekst, der fremhæver overfor bruger, at brugeren med sin accept bekræfter et dokumentindhold overfor tjenesteudbyder, hvilket kan være en forpligtende aftale.
- 12.** Dokumentbekræftelse skal som minimum bekræftes ved at bruger indtaster sin personlige kode(r).
- 13.** I forbindelse med dokumentbekræftelse skal skærbilledet indeholde tekst, der fremhæver overfor bruger, at dokumentindholdet først er modtaget hos tjenesteudbyder, når dette fremgår hos tjenesteudbyder, f.eks. i form af en kvittering.
- 14.** Såfremt bruger afviser et dokumentindhold, skal bruger dirigeres tilbage til en fejl URL hos tjenesteudbyder.

5.3. Indhold i skærbilleder

Tilmeldingsvinduet bør kun indeholde:

- Banknavn og logo
- Dato
- Kort tekst, der beskriver net-ID løsningens muligheder
- Tillæg til netbankaftale
- Acceptknap
- Hjælp link
- Fortryd link

Logon- og godkendekendelsessiden bør kun indeholde følgende:

- Banknavn og logo
- Tjenesteudbydernavn og eventuelt logo
- Eventuel personlig velkomsthilsen
- Dato
- UserID eller andet aftalenummer, der identificerer bruger i pengeinstituttet
- Password eller anden betegnelse for personlig kode, som brugeren skal indtaste
- Kort tekst der specificerer, hvilke oplysninger (CPR-nummer, navn, postadresse eller e-mail-adresse), der overføres til tjenesteudbyder.
- Fremvisning af den tekst, som skal bekræftes af bruger. Skal kun medtages, såfremt tjenesteudbyder har anmodet om dokumentbekræftelse.
- End knap.
- Hjælp link.
- Fortryd link.

5.4. Præsentation af tjenesteudbyders logo

1. Såfremt pengeinstituttet medtager tjenesteudbyders logo skal det have følgende dimension:

Bredde	Højde
120 pixels	90 pixels

2. Baggrunden i billedet skal være transparent.

6. Krav til opsamling af faktureringsgrundlag i pengeinstitutterne

1. Den enkelte netbank skal opsamle faktureringsgrundlag til brug for fakturering af tilsluttede tjenesteudbydere og til brug for afregning af decentral produktion til pengeinstitutterne.
2. Faktureringsgrundlaget skal indeholde følgende oplysninger:

Felt	Type og længde	Værdi	Kommentar
CVR-nummer	CHAR 10	<0..9>	Entydig identifikation af tjenesteudbyder.
RA-ID	CHAR 4	< 0..9 >	ID-angivelse for det pengeinstitut (reg-nr.), der har registreret bruger.
Logontype	CHAR 1	< 0..9 >	Benyttes til at specificere hvilken funktion, der er gennemført. Kan antage værdierne: Netbank: 0 PIN: 1 Certifikat: 2
Tjenestetype	CHAR 1	< 0..9 >	Angiver hvilken tjeneste, der er gennemført. Kan antage værdierne: Logon: 0 Dokumentbekræftelse: 1
Cpr-nummer-request flag	CHAR	< Y/N >	Angiver om pengeinstitut har afgivet CPR-nummer. Afgivet: "Y" Ikke afgivet: "N"
Adresse-request-flag	CHAR 1	< Y/N >	Angiver om pengeinstitut har afgivet adresseoplysninger. Afgivet: "Y" Ikke afgivet: "N"
Mail-request-flag	CHAR 1	< Y/N >	Angiver om pengeinstitut har afgivet mail-adresseoplysninger. Afgivet: "Y" Ikke afgivet "N"
URL-request-flag	CHAR 1	< Y/N >	Angiver om pengeinstitut har afgivet brugers URL-adresseoplysninger. Afgivet: "Y" Ikke afgivet "N"
Tidsstempel	CHAR 32	YYYY: år MM: måned DD: dag HH: time MM: minutter SS: sekunder PGG: tidszone (UTC) RRRRRRRR: 4 tilfældige tal der er hex kodet til 8 tal. NNNNN: sekvensnummer	Angivelse af tidspunkt for hvornår logon eller dokumentbekræftelse er gennemført.

Størrelse	CHAR 3	< 0..9 >	Størrelse i Kbytes på eventuel dokumentbekræftelse. Ved almindelig logon registreres nul som værdi.
SUBID	CHAR 4	< 0..9 >	Angivelse af applikation hos TU. Under opdeling under CVR.

3. Faktureringsgrundlaget skal fremsendes til PBS i et bestemt format, som specificeres særskilt af PBS i ref. (21) og (22).
4. Når pengeinstituttet har autentificeret bruger, fremstillet en net-ID med identitetsoplysninger og signeret den, betragtes autentifikationen som gennemført, og faktureringsgrundlaget skal logges. Tjenesteudbyder køber en autentifikation, og denne transaktion er på dette tidspunkt bindende.

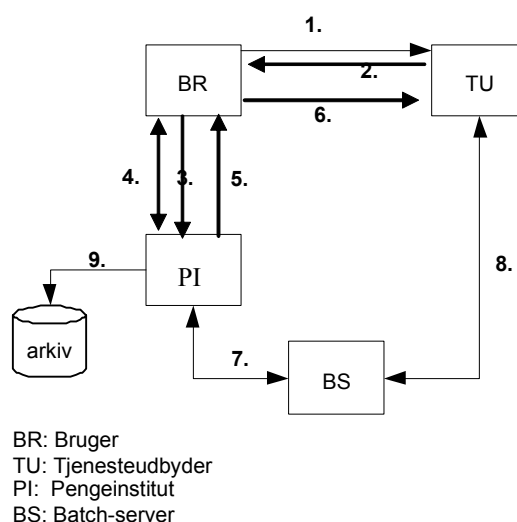
Først herefter bliver brugers browser omdirigeret tilbage til tjenesteudbyder med den signerede net-ID. Da net-ID først sendes til tjenesteudbyder efter logning af faktureringsgrundlaget, vil transaktionen altså være bindende, før tjenesteudbyder modtager net-ID. I princippet vil bruger endda kunne lukke sin browser, inden net-ID bliver sendt til tjenesteudbyder, hvilket vil medføre, at tjenesteudbyder kommer til at betale for en afbrudt logon. Der er desværre ikke mulighed for at undgå dette specialtilfælde, da alle browsere er opbygget efter event-styringsprincipper, der altid giver bruger mulighed for at lukke browseren. Til gengæld er det muligt for pengeinstitutterne at begrænse sandsynligheden for, at det sker ved at konstruere omdirigeringen af brugers browser (og samtidig afsende net-ID), så det sker automatisk efter ganske få sekunder. Denne automatik er uddybet i protokolbeskrivelsen, se ref. (17).

7. Sikkerhedskrav

7.1. Kommunikationssikkerhed og krypteringsnøgler

SSL-certifikater benyttes til at etablere en sikker SSL- forbindelse, hvor både klient og server bliver autentificeret. Net-ID-certifikater benyttes til at styrke autentificeringen udover SSL-autentificeringen mellem de parter, der er tilsluttet løsningen. PBS udsteder disse certifikattyper.

Der anvendes flere forskellige krypteringsnøgler i systemet til understøttelse af Net-ID og dokumentbekræftelse.



Sikkerheden i kommunikationen mellem bruger og tjenesteudbyder (1) defineres af tjenesteudbyder. Der stilles derfor ingen specifikke krav til sikkerheden i denne kommunikation.

Der etableres en SSL-krypteret forbindelse (server-autenticitet) mellem tjenesteudbyder og pengeinstitut (2). Dette sker i to sekvenser. Først etableres en SSL-forbindelse mellem brugers PC og tjenesteudbyder, som benyttes til at overføre net-ID til brugers PC.

1. Der skal etableres en SSL-session (server-autenticitet) mellem brugers PC og det valgte pengeinstitut (3), ref. (8) og (16). E-Tickets sikres med brug af net-ID-specifikke signeringsnøgler, som skal være RSA (asymmetriske nøgler) på minimum 1024 bit. SSL (symmetriske nøgler) skal være på minimum 128 bit.

Sikkerheden i kommunikationen mellem pengeinstituttet og bruger (4) defineres af pengeinstituttet. Alle pengeinstitutter overholder sektorens kodeks for sikkerhed i computerbaserede systemer, ref.(2)(1)(16).

2. Ved omdirigering af bruger tilbage til tjenesteudbyder skal der etableres en SSL-krypteret forbindelse (server-autenticitet) mellem bruger og pengeinstituttet (5), ref. (8) og (16). Denne session benyttes til at fremsende net-ID til brugers PC. Net-ID sikres med brug af net-ID-specifikke signeringsnøgler.

Efterfølgende etableres der en SSL-session (server-autenticitet) mellem brugers PC og tjenesteudbyderen (6). Net-ID fremsendes via denne forbindelse.

3. Kommunikationen mellem pengeinstitutter og Batch-serveren (7) skal sikres med en SSL-krypteret forbindelse (klient-server-autenticitet), ref. (8)(16). Det sikres via certifikatet, at pengeinstituttet kun kan hente oplysninger om tjenesteudbydere.
4. Kommunikationen mellem tjenesteudbydere og Batch-serveren (8) skal sikres med en SSL-krypteret forbindelse (Klient-server-autenticitet). Det sikres via certifikatet, at tjenesteudbyder kun kan hente oplysninger om pengeinstitutter.
5. Dokumenter, der er bekræftet af bruger, som opbevares i pengeinstitutterne eller hos tredjepart (9), skal opbevares i beskyttede biblioteker (se afsnit 7.2.3).

Oversigt over anvendte certifikater

Entitet	Certifikater	Formål	Gyldighed	Udsteder
Bruger	Defineres af PI	Sikring af kommunikation bruger-PI (4)	Defineres af PI	PI
Tjenesteudbyder	SSL-server-certifikat	SSL-sikring af kommunikation til tjenesteudbyder fra bruger (1, 2 og 6), og klient-certifikat til BS. (8)	2 år	PBS CA eller public CA
	Tjenesteudbyders net-ID certifikat	Sikring af net-ID (2+3)	2 år	PBS CA
	PBS rod-certifikat ⁴	Verifikation af PBS-udstedte certifikater	10 år	PBS CA
	PI'ernes net-ID certifikat ⁵	Verifikation af net-ID fra PI	2 år	PBS CA
PI	SSL-servercertifikat	SSL-sikring af kommunikation til PI fra bruger (3, 5), og Klient-certifikat til BS (7).	2 år	PBS CA eller public CA
	PI'ens egen net-ID-certifikat	Sikring af net-ID fra PI (5+6)	2 år	PBS CA
	PBS rod-certifikat ⁶	Verifikation af PBS-udstedte certifikater	10 år	PBS CA
	Tjenesteudbydernes-net-ID- certifikat ⁷	Verifikation af net-ID fra tjenesteudbyderne.	2 år	PBS CA
Batch Server	SSL-servercertifikat (7, 8)	Sikring af kommunikation til Batch-server	2 år	PBS CA

⁴ Hentes via PBS' website eller fremsendes i en e-mail.

⁵ Hentes via via Batch-serveren

⁶ Hentes via PBS' website eller fremsendes i en e-mail.

⁷ Hentes via via Batch-serveren

	PBS rod-certifikat	Verifikation af PBS-udstedte certifikater	10 år	PBS CA
--	--------------------	---	-------	--------

7.2. Sikkerhedskrav til pengeinstitutterne

7.2.1. Sikkerhedskrav til nøgleadministration

Fremstilling og anvendelse af nøgler

1. Pengeinstitutterne må kun fremstille, anvende og opbevare private signeringsnøgler og DES-krypteringsnøgler i sikkert krypteringsudstyr, der er certificeret i henhold til minimum FIPS 140-2 level 3, ref. (10).

Nøgler der anvendes i forbindelse med sikring af SSL-forbindelser behøver ikke at blive opbevaret i hardware-sikrede omgivelser.

2. Såfremt en kryptografisk nøgle bliver eksporteret fra det sikre krypteringsudstyr, for eksempel i forbindelse med backup, skal nøglen transporteres enten krypteret eller ved at anvende "delt viden kontroller". Hvis der anvendes "delt viden kontroller", skal
 - det kryptografiske udstyr autentificere hver operatør, der indlægger/eksporterer nøglekomponenter,
 - en kryptografisk nøgle som minimum opdeles i 2 komponenter.
3. Private signeringsnøgler må kun anvendes til at signere e-Tickets i forbindelse med net-ID.
4. Kryptografiske nøgler må ikke deles eller udveksles mellem produktions- og testsystemer.

Spærring af nøgler

5. Private signeringsnøgler må ikke anvendes efter ophør af gyldighedsperioden eller ved mistanke om kompromittering. Ved kompromittering af nøgler, der relaterer til certifikater, skal anvendelsen af nøglen spærres, og PBS skal straks have meddelelse herom.

7.2.2. Opslag på Batch-server

1. Pengeinstitutterne skal regelmæssigt, minimum hver 24. time, hente de nyeste certifikatoplysninger fra Batch-serveren, der vedligeholdes af PBS.

7.2.3. Interne sikkerhedskontroller i pengeinstitutterne

1. Pengeinstitutterne skal overholde Finanstilsynets sædvanlige praksis for kontrol og etablering af sikringsforanstaltninger på IT-området, ref. (3).

Logning af logon

2. Systemerne skal være indrettet, så alle logon-anmodninger fra tjenesteudbydere registreres og gemmes til brug for senere revision. Disse logs skal gemmes i minimum 6 måneder.
3. Faktureringsgrundlag skal opbevares i løbende år + 5 år.

Opbevaring af dokumentbekræftelse

Følgende elementer udgør en beviskæde:

- En brugers bekræftelse af et dokumentindhold over for pengeinstituttet.
 - Pengeinstituttets net-ID, som sendes til tjenesteudbydere, og som tjenesteudbydere verificerer med pengeinstituttets net-ID certifikat.
4. Pengeinstitutter skal derfor kunne fremvise dokument med tilhørende kontrolkoder, hvilket omfatter:
 - data, som er accepteret af bruger.
 - style-sheets og værktøjer, der blev benyttet til præsentation af XML-data-kontrolkoder eller signaturer og relaterede certifikater/kryptonøgler.
 5. Opbevaringstiden er som udgangspunkt minimum løbende år + 5 år, medmindre anden lovgivning tilsiger noget andet.
 6. Pengeinstituttet skal i denne henseende etablere sikkerhedskontroller, som kan sidestilles med Datatilsynets retningslinjer for opbevaring af fortrolige og følsomme oplysninger, ref. (6)(7).

Det betyder, at almindelige pengeinstitutmedarbejdere - for eksempel brugers bankrådgiver - ikke vil have adgang til disse data.

Hvis en bruger foretager indsigelser mod et givent dokument, kan pengeinstituttet fremvise dokumentet med tilhørende kontrolkoder og sammenholde det med data, der er fremsendt til tjenesteudbydere i en signeret net-ID.

Udskrivning og fremfindning af dokumentbekræftelse

7. Pengeinstituttet skal som minimum give bruger mulighed for at udskrive indholdet af dokumentet i forbindelse med dokumentbekræftelse.

Pengeinstituttet kan eventuelt give bruger mulighed for at fremfinde tidligere bekræftede dokumenter.

7.2.4. Test, erklæring og godkendelse

Test

1. Pengeinstituttets datacentral skal inden ibrugtagning af net-ID gennemføre en test mod PBS' tjenesteudbydersimulator (Vejrtjenesten).
2. Pengeinstituttets datacentral skal inden ibrugtagning af net-ID gennemføre en ekstern test mod:
 - PBS' Batch-server-testsystem i henhold til testspecifikationen indeholdt i ref.(20) og
 - En pilotkunde (tjenesteudbyder) i henhold til kapitel 9.
3. Pengeinstituttets datacentral skal inden ibrugtagning til PBS fremsende:
 - Testrapport (ref. kapitel 21) samt
 - Kopier af anvendte skærbilleder, som dokumenterer, at de i kapitel 5) bestemmelser er overholdt.

Oplysningerne rapporteres med email til PBS (se kapitel 23 Kontakt).

Erklæring

4. Pengeinstituttets datacentral skal inden ibrugtagning af net-ID og én gang årligt fremsende en revisorattesteret ledelseserklæring om, at de i denne håndbog specificerede kontroller er etableret, ref. kapitel 14. Den årlige erklæring skal bekræfte, at de etablerede kontroller er efterlevet i det forløbne år.

Godkendelse

PBS vil godkende pengeinstituttets net-ID implementering, når testrapport og erklæringer er godkendt.

7.3. Sikkerhedskrav til tjenesteudbyder

7.3.1. Sikkerhedskrav til nøgleadministration

Nøglefremstilling

1. Nøglefremstilling skal ske på baggrund af betryggende procedurer og ved brug af "delt viden kontroller" (der skal medvirke minimum 2 personer ved nøglefremstillingen). Den enhed, hvorpå nøglefremstillingen sker, skal være off-line i forbindelse med selve nøglefremstillingen.

2. Private asymmetriske nøgler og datakrypteringsnøgler skal være kryptografisk beskyttet ved lagring.
3. Net-ID private signeringsnøgler må kun anvendes til at signere net-ID til netbanker i forbindelse med net-ID og dokumentbekræftelse.
4. Net-ID private signeringsnøgler må ikke anvendes efter ophør af gyldighedsperioden eller ved mistanke om kompromittering.
5. Kryptografiske nøgler må ikke deles eller udveksles mellem produktions- og testsystemer.

Spærring af nøgler

6. Ved kompromittering af nøgler, der relaterer til certifikater, skal anvendelsen af nøglen spærres, og PBS skal straks have meddelelse herom. PBS kontaktes (se kapitel 23 Kontakt).

7.3.2. Interne sikkerhedskontroller hos tjenesteudbydere

Bruger-ID for operatør

1. Adgang til serveren skal være beskyttet af bruger-ID og password-kontrol. Der skal tildeles en unik bruger-ID til de enkelte operatører, der skal have adgang til serveren. For at sikre tilstrækkelig autentificering skal der anvendes statiske eller dynamiske password.
2. Der skal opretholdes en liste over brugere med historik. Password skal være behørigt beskyttet.
3. Der skal forefindes procedurer for suspension eller inddragelse af bruger-ID. For eksempel bør en bruger-ID inddrages, når denne ikke har været anvendt i 90 dage. Bruger-ID tilhørende personer, som forlader virksomheden, skal inddrages, og disse skal slettes efter 30 dage.

Nød-bruger-ID

4. Såfremt der anvendes nød-bruger-ID (foruddefinerede bruger-ID, som typisk ligger i konvolutter i en reception, hvor operatører kan hente dem i specielle nødsituationer), som giver adgang til installation, ændring eller sletning af softwarefunktioner, tildeling af brugeradgang etc., skal disse så vidt muligt tildeles en individuel bruger eller beskyttes, således at kun foruddefinerede personer kan få adgang til disse bruger-ID. Enhver brug heraf skal logges og kontrolleres dagligt. Password til disse bruger-ID skal ændres efter enhver brug.
5. Et foruddefineret password til en foruddefineret bruger-ID skal ændres.

Logisk adgang

6. Adgang til serveren, hvor net-ID komponenten installeres, skal altid være begrænset til personer med et arbejdsbetinget behov.
7. Bemyndigelser til at sætte programmer/systemer i drift skal administreres restriktivt og kun tildeles personer med et arbejdsbetinget behov. Der skal etableres funktionsadskillelse i bruger- og nøgleadministration, forvaltning og sikkerhedsadministration, som sikrer at ingen enkeltstående person kan udføre alle disse opgaver. Kun autoriserede programmer må benyttes.
8. Administration af firewall skal restriktivt begrænses til autoriserede personer.
9. Kritiske sikkerhedsfunktioner skal deles op på en sådan måde, at ingen enkeltpersoner har mulighed for at påvirke systemets integritet.

Fysisk adgang

10. Servere og andet udstyr, som indeholder net-ID-komponenter, skal fysisk placeres således, at uautoriserede personer ikke har adgang dertil. Dette kan for eksempel ske ved at placere udstyret i et aflåst skab/rum med adgangskontrol.

Viruskontrol

11. Der skal være installeret en effektiv viruskontrol på serveren, hvor net-ID-komponenten er installeret. Viruscheck skal køre kontinuerligt og skal checke nye data.
12. Viruscheck skal altid opdateres med nyeste release/opdatering af drivers/filtre.
13. Software til viruscheck skal være almindeligt tilgængelig på markedet (det vil sige fra en aktiv leverandør).

Netværk og firewall

14. Serveren, hvor net-ID-komponenten er installeret, skal indgå i et sikret, pålideligt netværk, som anvender intern Internet Protokol (IP) adresser, som kun giver adgang til databaser gennem en firewall. Al trafik til og fra databaser, som indeholder serverens private nøgle, skal passere gennem denne firewall.
15. Tjenesteudbyders server-topologi skal være skjult for andre netværk - for eksempel ved at oversætte netværksadresser for at skjule de interne netværksadresser.

16. Der skal etableres sikkerhedskontroller og –procedurer, som sikrer, at der afgives en alarm ved forsøg på uautoriseret adgang, herunder at der sker logning af angreb på firewall.

17. Alle administrative ændringer skal logges/dokumenteres.

18. Firewall skal altid opdateres med nødvendige og effektive ændringer af sikkerhedsmæssig art.

Revisionsspor og logning

19. Der skal føres følgende logs:

- Transaktionslog (typisk i CICS), der registrerer:
 - Gyldige logon respons (inkl. e-Tickets) fra pengeinstitutterne
 - Dato og tidsstempel
- Ændringslog (forvaltningssystemer), der registrerer:
 - Systembrugeridentifikation.
 - Funktioner, ressourcer og data der er anvendt og ændret.
 - Dato og tidsstempel.
- Sikkerhedslog (typisk RACF), der registrerer:
 - Systembrugeridentifikation.
 - Funktioner, ressourcer og data der er anvendt og ændret.
 - Dato og tidsstempel.

20. Revisionsspor skal opbevares i minimum 6 måneder eller i overensstemmelse med gældende lovgivning.

Dokumentbekræftelse

En dokumentbekræftelse er signeret med netbankens private nøgle.

Tjenesteudbyder bør sikre, at bruger får en kvittering for modtagelse af en dokumentbekræftelse. Det kan f.eks. være i form af et skærmbillede, der bekræfter, at dokumentet er modtaget.

21. For at sikre bevisværdien heraf skal tjenesteudbyder gemme:

- Modtagne e-Ticket, som indeholder en dokumentbekræftelse.

- Relaterede certifikater (certifikater, der benyttes til at verificere net-ID) så længe det er nødvendigt i henhold til gældende lovgivning, eller så længe tjenesteudbyder vurderer, at det er relevant i forbindelse med at kunne modgå indsigelser fra brugere.

Hvis der er behov for at opbevare meddelelser i mere end 5 år af hensyn til bevisførelse, skal dette aftales med PBS.

Kommunikation til Batch-server

22. Tjenesteudbyder skal regelmæssigt, minimum hver 24. time, hente de nyeste certifikatoplysninger fra Batch-serveren.

23. Kommunikationen mellem serveren, hvor net-ID-komponenten er installeret, skal være SSL-sikret. Der må kun sendes en transaktion (forespørgsel) i en SSL-session. Serveren skal lukke SSL-sessionen efter hver transaktion.

7.3.3. Krav til tjenesteudbyders skærbilleder

Nedenstående krav verificeres ved at tjenesteudbyder fremsender kopi af anvendte skærbilleder til PBS i henhold til afsnit 7.3.4.

Brug af varemærker/logoer

Tjenesteudbyder skal vise navn og logo for net-ID på deres website, hvor brugeren kan vælge at logge på med brug af net-ID. Navn og logo skal overholde specifikationerne defineret af PBS. Varemærker kan downloades fra PBS' web site eller fås hos PBS.

Brug af sikkerhedsikon "hængelås"

Tjenesteudbyder skal i de sessioner, der etableres mellem bruger og tjenesteudbyder sikre, at sikkerhedsikonet "hængelåsen" er synlig i brugerens browser-vindue, således at bruger kan forvise sig om at linjen er krypteret.

Skærbillede til håndtering af fejlsituationer

Tjenesteudbyder skal sikre, at der eksisterer skærbilleder, som indeholder oplysninger om fejlsituationer, der kan aktiveres ved dirigering af bruger til den af tjenesteudbyder oplyste fejl-URL.

Valg af pengeinstitut i drop-down-menu

Tjenesteudbyder skal sikre, at placering af pengeinstitutter i drop-down-menu er ordnet alfabetisk, første gang en bruger skal vælge pengeinstitut. Ved efterføl-

gende logon skal bruger nemt kunne dirigeres til sidst valgte pengeinstitut, enten automatisk med en "cookie" eller ved at sidst valgte pengeinstitut står øverst i drop-down-menuen.

7.3.4. Test, erklæring og godkendelse

Test

1. Tjenesteudbyder skal inden ibrugtagning af net-ID gennemføre en test mod PBS' netbanksimulator.
2. Tjenesteudbyder skal inden ibrugtagning af net-ID gennemføre en ekstern test mod:
 - PBS' Batch-server-testsystem i henhold til testspecifikationen indeholdt i ref.(20) og
 - Edb-centraler med udvalgte netbankbrugere, der repræsenterer de tilsluttede edb-centraler i henhold til kapitel 9.
3. Tjenesteudbyder skal inden ibrugtagning til PBS fremsende:
 - Testrapport (ref. kapitel 21) samt
 - Kopier af anvendte skærbilleder, som dokumenterer, at de i afsnit 7.3.3 bestemmelser er overholdt.

Oplysningerne rapporteres med email til PBS (se kapitel 23 Kontakt).

Erklæring

4. Tjenesteudbyder skal inden ibrugtagning af logon-komponenten og én gang årligt fremsende en revisorattesteret ledelseserklæring om, at de i denne håndbog specificerede kontroller er etableret, ref. kapitel 14. Den årlige erklæring skal bekræfte, at de etablerede kontroller er efterlevet i det forløbne år.

Godkendelse

PBS vil godkende tjenesteudbyder, når testrapport og erklæringer er godkendt.

7.4. Sikkerhedskrav PBS CA

Sikkerhedskravene til udstedelse og administration af PBS-certifikater er specificeret i ref. (4). PBS' aktiviteter i forbindelse med net-ID er genstand for en revisionsgennemgang 1 gang årligt.

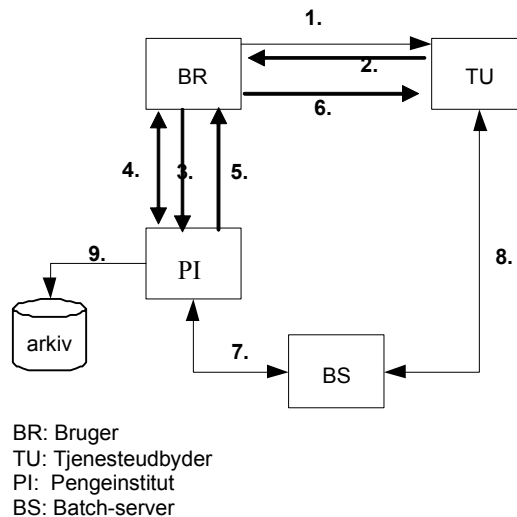
8. Indrapportering af data til Batchserver

Forudsætningen for at net-ID-løsningen fungerer korrekt er, at Batch-serveren er opdateret med tidssvarende oplysninger. Tjenesteudbyder, pengeinstitut og datacentral skal derfor inden produktionsstart og ved enhver ændring i data rapportere med email relevante oplysninger (ref. bilag 6 kapitel 15) til PBS (se kapitel 23 Kontakt).

Data lægges derefter på Batch-serveren.

9. Systemtest

1. Inden produktionsstart skal tjenesteudbydere og datacentraler gennemføre en systemtest, der som minimum indeholder følgende testhændelser:



Logon-sekvens

Reference	Testhændelse	Forventet testresultat
(1) Kommunikation mellem bruger og tjenesteudbyder		
	Defineres egenhændigt af tjenesteudbyder.	Defineres egenhændigt af tjenesteudbyder.
(2) Kommunikation mellem tjenesteudbyder og pengeinstitut (datacentral)		
2.1	Net-ID er OK.	PI-logon-skærbillede.
2.2	Net-ID fejl i signatur. Testcase kun relevant for test af netbank.	Bruger dirigeres til en fejl-URL hos PI (ugyldig henvendelse fra TU).
2.3	Net-ID fejl i timestamp. Testcase kun relevant for test af netbank.	Bruger dirigeres til en fejl-URL hos PI (ugyldig henvendelse fra TU).
2.4	Ingen kontakt med PI.	Time out eller page not available.
(3) Kommunikation mellem pengeinstitut og bruger (brugerautentifikation)		

3.1	Bruger indtaster korrekt bruger-ID og koder. Testcase kun relevant for test af netbank.	Gå til 3.1.1 eller 3.1.2
3.2	Bruger indtaster forkert bruger-ID og koder flere gange end tilladt. Testcase kun relevant for test af netbank.	Bruger dirigeres til en fejl URL hos pengeinstituttet.
3.1.1 Bruger er ikke tilmeldt net-ID		
a)		Bruger præsenteres for aftale om brug af net-ID.
b)	Bruger accepterer tilmelding. Testcase kun relevant for test af netbank.	Bruger præsenteres for skærmbillede hvor det fremgår, hvilke oplysninger der vil blive overført til TU.
c)	Bruger fortryder tilmelding.	Bruger bliver dirigeret til TU uden net-ID.
d)	Bruger trykker "tilbage". Testcase kun relevant for test af netbank.	Bruger præsenteres for aftale igen.
e)	Bruger accepterer overførelse af personoplysninger.	Bruger bliver dirigeret til TU med net-ID.
f)	Bruger afviser overførelse af personoplysninger.	Bruger bliver dirigeret til TU uden net-ID.
g)	Bruger trykker "tilbage". Testcase kun relevant for test af netbank.	
h)	Bruger indtaster forkert kode flere gange end	Bruger bliver dirigeret til TU uden net-ID.

	accepteret af PI. Testcase kun relevant for test af netbank.	
--	---	--

3.1.2 Bruger er tilmeldt net-ID
Denne test skal gennemføres i to tempi med brug af 2 forskellige net-ID certifikater. 1) med brug af det aktuelle net-ID certifikat og 2) med et fornyet net-ID certifikat. Det sikres dermed at man kan håndtere et certifikat skift.

a)		Bruger præsenteres for skærbillede hvor det fremgår, hvilke oplysninger der vil blive overført til TU..
b)	Bruger accepterer overførelse af personoplysninger.	Bruger bliver dirigeret til TU med net-ID.
c)	Bruger afviser overførelse af personoplysninger.	Bruger bliver dirigeret til TU uden net-ID.
d)	Bruger trykker "tilbage". Testcase kun relevant for test af netbank.	
e)	Bruger indtaster forkert kode flere gange end accepteret af PI. Testcase kun relevant for test af netbank.	Bruger instrueres om at kontakte sin bank.

Dokumentbekræftelse

2. Inden dokumentbekræftelse sættes i produktion skal der gennemføres en test i henhold til ref. (20), afsnit 2.3 med tilfredsstillende resultat.

Test mod Batchserver

3. Som minimum skal det testes, at der kan hentes brugbare data fra Batchserveren.

10. Bilag 1: Specifikation af e-Tickets

Logon Requester

Header

Alle felter i headeren, som beskrevet herunder, er påkrævet.

Felt	Type og længde	Værdi	Kommentar
HHDR_ALG	CHAR2	02 = PKCS#7 (MD5) SignedData Streng Ticket 03 = PKCS#7 (SHA1) SignedData Streng Ticket 07 = PKCS#1 (MD5) Streng Ticket 08 = PKCS#1 /SHA1) Streng Ticket 12 = PKCS#7 (MD5) ContentInfo Streng Ticket 13 = PKCS#7 (SHA1) ContentInfo Streng Ticket	13 bruges her, da alle net-ID-layouts benytter PKCS#7 og SHA1 anses for mere sikker end MD5.
HDR_TICKET	VARIABLE	PKCS#7 data indeholdende Auth Ticket og Context Ticket signeret med tjenesteudbyders signatur	Indeholder PKCS#7 ContentInfo, da HHDR_ALG er sat til 13.

Auth Ticket

Auth Ticket anvendes til udveksling af brugerinformationer. Alle felter i Auth Ticket er påkrævet.

Felt	Type og længde	Værdi	Kommentar
HDR_VER	CHAR4	1004 eller 1005	Protokolversion 1004 og 1005 er for net-ID. Begge har samme e-Ticket format, men 1005 tilføjer URL escaping af subfelter.
HDR_STAMP	CHAR 32	YYYYMMDDHHMMSSSSPGGRRRRRRRRNNNNN YYYY year MM month DD day HH hour MM minute SS second SS hundred-part second PGG time zone (UTC) RRRRRRRR 4 random binary digits hex coded, so it becomes a 8 digit string. NNNNN sequence number	Et tidsstempel der angiver, hvornår den pågældende net-ID er fremstillet på afsenderens computer. [YYYYMMDDHHMMSSSS] er fra den lokale tids-server. [PGG] er tidszonen, inklusive sommertid, i forhold til UTC. Eks. Dansk sommertid: "+02". Det er et krav, at HDR_STAMP er unikt mellem en afsender og en modtager.
HDR_KVER	CHAR VARIABLE	SIGRSAX1.APPL.02.CCCCCC.PUBNNNNN X 'S' for test, 'P' for produktion. APPL Applikationsnavn; 'PBSLOGON'. CCCCC Tjenesteudbyders CVR-nummer.	Tjenesteudbyders key-label. Vær opmærksom på at dette CVR-nummer ikke nødvendigvis er det samme som det CVR-

		NNNNN Løbenr til entydig identifikation af tjenesteudbyders certifikater.	nummer der er angivet i DISTRIBID.	
HDR_RCV	CHAR 14	RCVTYPE	CHAR 2	Dette flet angiver modtagerens identitet. RCVTYPE sættes til 02 (request til pengeinstitut). RCVIDENT udfyldes med netbankens registreringsnummer prefixet med 0000; for eksempel 00009388. SUBID benyttes til at angive en specifik applikation hos TU.
		RCVIDENT	CHAR 8	
		SUBID	CHAR 4	
HDR_UID	CHAR VARIABLE	BRANCHEID:<e.g. 'banks'>;DISTRIBID:<e.g. a specific bank Identification>;KUNDEIDTYPE:<'type of KUNDEID field'>;KUNDEID:<'senders identification of a specific user'>	Se beskrivelse nedenfor.	

Detaljer for HDR_UID

Field	Value	Comment
BRANCHEID	01 - Netbanker 02 - Tjenesteudbydere	02 benyttes, da request kommer fra tjenesteudbyder.
DISTRIBID	CCCCCCCC	Tjenesteudbyders CVR-nummer.
NB_AUTH	NNNN	pengeinstitutets registreringsnummer. Udfyldes med den tomme streng, da request er fra tjenesteudbyder.
KUNDEIDTYPE	00 - Unspecified 01 - Social Security Number (CPR). 02 - Internet bank agreement number. 03 - User ID in CAPS 04 - eBoks user identifier 05 - CVR (Central Virksomhedsregister)	00 benyttes.
KUNDEID	Tom	Udfyldes med den tomme streng, da KUNDEIDTYPE er Unspecified.

Context Ticket

Context Ticket bruges til informationer som er nødvendige for modtageren. Alle felter i denne Context Ticket request er påkrævet.

Felt	Type og længde	Værdi	Kommentar
CHDR_VER	CHAR 4	1004 eller 1005	Protokolversion 1004 og 1005 er for net-ID. Begge har samme e-Ticket format, men 1005 tilføjer URL escaping af subfelter.

HDR_LANG	CHAR 2	DK	Landekode (ISO-8859-1) Kun DK er understøttet.	
HDR_LANG2	CHAR 2	DK	Alternativ landekode. Kun DK er understøttet.	
APP_DMID	CHAR 4	1020	Logonservice applikationsid.	
APP_DMVER	CHAR 4	1001	Logonservice request-id.	
APP_DATA	CHAR Variable	CPR: <returner CPR no>;EMAIL: <returner brugers email>;ADR: <returner brugers adresse>;USER_URL: <returner bruger-url>;URL: <returner URL i tilfælde af fejl>;HDR_RCV_SUBID: <tjenesteudbyders subsid>	Felt	Max længde
			CPR	1 ('Y' eller 'N')
			EMAIL	1 ('Y' eller 'N')
			ADR	1 ('Y' eller 'N')
			USER_URL	1 ('Y' eller 'N')
			URL	255
			ERR_URL	255
			HRD_RCV_SUBID	4

Logon response

Header

Alle felter i headeren, som er beskrevet herunder, er påkrævet.

Felt	Type og længde	Værdi	Kommentar
HHDR_ALG	CHAR 2	02 = PKCS#7 (MD5) SignedData Streng Ticket 03 = PKCS#7 (SHA1) SignedData Streng Ticket 07 = PKCS#1 (MD5) Streng Ticket 08 = PKCS#1 (SHA1) Streng Ticket 12 = PKCS#7 (MD5) ContentInfo Streng Ticket 13 = PKCS#7 (SHA1) ContentInfo Streng Ticket	13 bruges her, da alle net-ID-layouts benytter PKCS#7 og SHA1 anses for mere sikker end MD5.
HDR_TICKET	VARIABLE	PKCS#7 data indeholdende Auth Ticket og Context Ticket signeret med tjenesteudbyders signatur.	Indeholder PKCS#7 ContentInfo, da HHDR_ALG er sat til 13.

Auth Ticket

Auth Ticket anvendes til udveksling af brugerinformationer. Alle felter i Auth Ticket er påkrævet.

Felt	Type og længde	Værdi	Kommentar
HDR_VER	CHAR 4	1004 eller 105	Protokolversion 1004 og 1005 er for net-ID. Begge har samme e-Ticket format, men 1005 tilføjer URL escaping af subfelter.
HDR_STAMP	CHAR 32	YYYYMMDDHHMMSSSSPGRRRRRRRRNNNN	Et tidsstempel der angiver, hvornår den pågældende net-ID

		YYYY year MM month DD day HH hour MM minute SS second SS hundred-part second PGG time zone (UTC) RRRRRRRR 4 random binary digits hex coded, so it becomes a 8 digit string. NNNNNN sequence number	er fremstillet på afsenderens computer. [YYYYMMDDHHMMSS SS] er fra den lokale tidsserver. [PGG] er tidszonen, inklusive sommertid, i forhold til UTC. Eks. Dansk sommertid: "+02". Det er et krav at HDR_STAMP er unikt mellem en afsender og en modtager.						
HDR_KVE R	CHAR VARIAB- LE	SIGRSAX1.APPL.01ZZZZ.PUBNNNNN X 'S' for test, 'P' for produktion APPL Applikationsnavn: 'PBSLOGON'. ZZZZ BFCNR. Bogføringscentralens ID som er afgivet af Finansrådet. NNNNN Løbenr. til entydig identifikation af netbankens certifikater.	Bogføringscentralens keylabel						
HDR_RCV	CHAR 14	<table border="1"> <tr> <td>RCVTYPE</td> <td>CHAR 2</td> </tr> <tr> <td>RCVIDENT</td> <td>CHAR 8</td> </tr> <tr> <td>SUBID</td> <td>CHAR 4</td> </tr> </table>	RCVTYPE	CHAR 2	RCVIDENT	CHAR 8	SUBID	CHAR 4	RCVTYPE sættes til 01 (tjenesteudbyder). RCVIDENT udfyldes med tjenesteudbyders CVR-nummer SUBID udfyldes med tjenesteudbyders SUBID. Bemærk! Skal aftales med tjenesteudbyder ved brug af Direkte link.
RCVTYPE	CHAR 2								
RCVIDENT	CHAR 8								
SUBID	CHAR 4								
HDR_UID	CHAR VARIAB- LE	BRAN- CHEID;<e.g. 'banks'>;DISTRIBID:<e.g. a specific bank identification>;KUNDEIDTYPE:<'type og KUNDEID field'>;KUNDEID:<'senders identification of a specific user'>	Se beskrivelse nedenfor.						

Detaljer for HDR_UID

Field	Value	Comment
BRANCHEID	01 - Netbanker 02 - Tjenesteudbydere	01 bruges her.
DISTRIBID	CCCC	Pengeinstituttets registreringsnummer. Den netbank der har signeret denne net-ID.
NB_AUTH	CCCC	Pengeinstituttets registreringsnummer. Den netbank der har autentificeret bruger.
KUNDEIDTYPE	00 - Unspecified 01 - Social Security Number (CPR). 02 - Internet bank agreement number. 03 - User ID in CAPS 04 - eBoks user identifier	00 benyttes såfremt cpr-nummer ikke medsendes. 01 benyttes, når tjenesteudbyder skal have et entydigt bruger-ID tilbage.

	05- CVR (Centrale Virksomhedsregister)	05 benyttes når tjenesteudbydere skal have et entydigt bruger-ID (CVR) tilbage.
KUNDEID	<p>For CPR: DDMMYYZZZX</p> <p>DD Dag MM Måned YY År ZZZ Løbenummer X Checkciffer</p> <p>For CVR: ZZZZZZZX</p> <p>ZZZZZZZ løbenummer X Checkciffer</p>	<p>Hvis requester forespurgte at modtage CPR, angives brugerens CPR-nummer.</p> <p>Hvis respons er et direkte logon med CVR nummer angives brugerens 8 cifrede CVR nummer fra netbanken.</p> <p>Ellers angives "00000000"</p>

Context Ticket

Context Ticket bruges til informationer som er nødvendige for modtageren. Alle felter i denne Context Ticket response er påkrævet.

Felt	Type og længde	Værdi	Kommentar																							
CHDR_VE R	CHAR 4	1004 eller 1005	Protokolversion 1004 og 1005 er for net-ID. Begge har samme e-Ticket format, men 1005 tilføjer URL escaping af subfelter.																							
HDR_LAN G	CHAR 2	DK	Landekode (ISO-8859-1). Kun DK er understøttet.																							
HDR_LAN G2	CHAR 2	DK	Alternativ landekode (ISO-8859-1). Kun DK er understøttet.																							
APP_DMID	CHAR 4	1020	Logonservice applikations-ID.																							
APP_DMVE R	CHAR 4	1002	Logonservice response-ID.																							
APP_DATA	CHAR VARIAB- LE	EMAIL: <brugers email Adr>;FORNAVN: <fornavn>;EFTER NAVN: <efternavn>;CO: <c/o>;GAD E: <gade>;HUSNR: <husnr>;ETAGN R: <etagenr>;POSTNR: <postnr>;B Y: <by>;URL: <url>	<table border="1"> <thead> <tr> <th>Felt</th> <th>Max længde</th> </tr> </thead> <tbody> <tr> <td>EMAIL</td> <td>60</td> </tr> <tr> <td><u>FORNAVN</u></td> <td>34</td> </tr> <tr> <td>EFTER- NAVN</td> <td>34</td> </tr> <tr> <td>CO</td> <td>34</td> </tr> <tr> <td><u>GADE</u></td> <td>34</td> </tr> <tr> <td>HUSNR</td> <td>5</td> </tr> <tr> <td>ETAGENR</td> <td>4</td> </tr> <tr> <td>POSTNR</td> <td>4</td> </tr> <tr> <td><u>BY</u></td> <td>34</td> </tr> <tr> <td><u>URL</u></td> <td>255</td> </tr> </tbody> </table>	Felt	Max længde	EMAIL	60	<u>FORNAVN</u>	34	EFTER- NAVN	34	CO	34	<u>GADE</u>	34	HUSNR	5	ETAGENR	4	POSTNR	4	<u>BY</u>	34	<u>URL</u>	255	
Felt	Max længde																									
EMAIL	60																									
<u>FORNAVN</u>	34																									
EFTER- NAVN	34																									
CO	34																									
<u>GADE</u>	34																									
HUSNR	5																									
ETAGENR	4																									
POSTNR	4																									
<u>BY</u>	34																									
<u>URL</u>	255																									

Bemærk at adressen kan skrives ind i de understregede felter, hvis den angivne opdeling ikke er mulig. Da skal følgende gælde:

- Fornavn indeholder fornavn, efternavn og evt. co.
- Gade indeholder gade, husnummer, etagenummer.
- By indeholder postnummer og by.
- By kan desuden indeholde land og landekode

Hvis der i i POSTNR angives fire nuller betyder det, at personen er udenlandsdanske.

Dokumentbekræftelse request

Meddelelsen, som skal noteres, skal være struktureret efter syntaksen listet i ref. (17). Længden af meddelelsen XML formatering må højst være 20 KB.

Det er op til den enkelte netbank at præsentere meddelelserne. Netbankerne skal gøre det muligt for tjenesteudbydere at se, hvordan en meddelelse fremvises, for eksempel ved hjælp af et standard XSL-dokument, som gøres tilgængelig for tjenesteudbydere.

Header

Alle felter i headeren, som er beskrevet herunder, er påkrævet.

Felt	Type og længde	Værdi	Kommentar
HHDR_ALG	CHAR 2	02 = PKCS#7 (MD5) SignedData Streng Ticket 03 = PKCS#7 (SHA1) SignedData Streng Ticket 07 = PKCS#1 (MD5) Streng Ticket 08 = PKCS#1 (SHA1) Streng Ticket 12 = PKCS#7 (MD5) ContentInfo Streng Ticket 13 = PKCS#7 (SHA1) ContentInfo Streng Ticket	13 bruges her, da alle net-ID-layouts benytter PKCS#7 og SHA1 anses for mere sikker end MD5.
HDR_TICKET	VARIABLE	PKCS#7 data indeholdende Auth Ticket og Context Ticket signeret med tjenesteudbyders signatur.	Indeholder PKCS#7 ContentInfo, da HHDR_ALG er sat til 13.

Auth Ticket

Auth Ticket anvendes til udveksling af brugerinformationer. Alle felter i Auth Ticket er påkrævet.

Felt	Type og længde	Værdi	Kommentar
HDR_VER	CHAR 4	1004 eller 1005	Protokolversion 1004 og 1005 er for net-ID. Begge har samme e-Ticket format, men 1005 tilføjer URL escaping af subfelter.

HDR_STAMP	CHAR 32	YYYYMMDDHHMMSSSSPGGRRRRRRRRRNNNN YYYY year MM month DD day HH hour MM minute SS second SS hundred-part second PGG time zone (UTC) RRRRRRRR 4 random binary digits hex coded, so it becomes a 8 digit string. NNNNN sequence number	Et tidsstempel der angiver, hvornår den pågældende net-ID er fremstillet på afsenderens computer. [YYYYMMDDHHMMSSSS] er fra den lokale tidsserver. [PGG] er tidszonen, inklusive sommertid, i forhold til UTC. Eks. Dansk sommertid: "+02". Det er et krav, at HDR_STAMP er unikt mellem en afsender og en modtager.	
HDR_KEYR	CHAR VARIAB-LE	SIGR-SAX1.APPL.02.CCCCCC.PUBNNNNN X'S' for test, 'P' for produktion APPL Applikationsnavn: 'PBSLOGON'. CCCCCC Tjenesteudbyders CVR-nummer. NNNNN Løbenr. til entydig identifikation af Tjenesteudbyders certifikater.	Tjenesteudbyders keylabel. Vær opmærksom på at dette CVR-nummer ikke nødvendigvis er det samme som det CVR-nummer, der er angivet i DISTRIBID	
HDR_RCV	CHAR 14	RCVTYPE	CHAR 2	Dette felt angiver modtagerens identitet. RCVTYPE sættes til 02 (request til bank). RCVIDENT udfyldes med netbankens registreringsnummer prefixet med 0000, for eksempel 00009388. SUBID benyttes til at angive en specifik applikation hos TU.
		RCVIDENT	CHAR 8	
		SUBID	CHAR 4	
HDR_UID	CHAR VARIAB-LE	BRANCHEID; <e.g. 'banks'>; DISTRIBID: <e.g. a specific bank identification>; KUNDEIDTYPE: <'type og KUNDEID field'>; KUNDEID: <'senders identification of a specific user'>	Se beskrivelse nedenfor.	

Detaljer for HDR_UID

Field	Value	Comment
BRANCHEID	01 - Netbanker 02 - Tjenesteudbydere	02 benyttes, da request kommer fra tjenesteudbyder.
DISTRIBID	CCCCCC	Tjenesteudbyders CVR-nummer.
NB_AUTH	NNNN	Pengeinstitutets registreringsnummer. Udfyldes med den tomme streng, da request er fra tjenesteudbyder.

KUNDEIDTYPE	00 – Unspecified 01 – Social Security Number (CPR). 02 – Internet bank agreement number. 03 – User ID in CAPS 04 – eBoks user identifier	00 benyttes.
KUNDEID	Tom	Udfyldes med den tomme streng, da KUNDEIDTYPE er Unspecified.

Context Ticket

Context Ticket bruges til informationer, som er nødvendige for modtageren. Alle felter i denne Context Ticket request er påkrævet.

Felt	Type og længde	Værdi	Kommentar	
CHDR_VE R	CHAR 4	1004 eller 1005	Protokolversion 1004 og 1005 er for net-ID. Begge har samme e-Ticket format, men 1005 tilføjer URL escaping af subfelter.	
HDR_LAN G	CHAR 2	DK	Landekode (ISO-8859-1). Kun DK er understøttet.	
HDR_LAN G2	CHAR 2	DK	Alternativ landekode (ISO-8859-1). Kun DK er understøttet.	
APP_DMID	CHAR 4	1020	Logonservice applikations-ID.	
APP_DMVE R	CHAR 4	1003	Dokumentbekræftelse request-ID.	
APP_DATA	CHAR VARIAB-LE	CPR:<returner CPR no>;EMAIL:<returner brugers email>;ADR:<returner brugers adresse>;USER_URL:<returner brugers URL>;URL:<retur URL>;ERR_URL:<retur URL i tilfælde af fejl>;HDR_RCV_SUBID:<tje nesteudbyders subid>;BESKED:<meddelelse til notering>	Felt	Max længde
			CPR	1 ('Y' eller 'N')
			EMAIL	1 ('Y' eller 'N')
			ADR	1 ('Y' eller 'N')
			USER_URL	1 ('Y' eller 'N')
			URL	255
			ERR_URL	255
			HDR_RCV_SUBID	4
BESKED	20K (maks.)			

Dokumentbekræftelse response

Header

Alle felter i headeren, som er beskrevet herunder, er påkrævet.

Felt	Type og længde	Værdi	Kommentar
HHDR_ALG	CHAR 2	02 = PKCS#7 (MD5) SignedData Streng Ticket 03 = PKCS#7 (SHA1) SignedData Streng Ticket	13 bruges her, da alle net-ID-layouts benytter PKCS#7 og SHA1 anses for

		07 = PKCS#1 (MD5) Streng Ticket 08 = PKCS#1 (SHA1) Streng Ticket 12 = PKCS#7 (MD5) ContentInfo Streng Ticket 13 = PKCS#7 (SHA1) ContentInfo Streng Ticket	mere sikker end MD5.
HDR_TICKET	VARIABLE	PKCS#7 data indeholdende Auth Ticket og Context Ticket signeret med tjenesteudbyders signatur	Indeholder PKCS#7 ContentInfo, da HHDR_ALG er sat til 13.

Auth Ticket

Auth Ticket anvendes til udveksling af brugerinformationer. Alle felter i Auth Ticket er påkrævet.

Felt	Type og længde	Værdi	Kommentar
HDR_VER	CHAR 4	1004 eller 1005	Protokolversion 1004 og 1005 er for net-ID. Begge har samme e-Ticket format, men 1005 tilføjer URL escaping af sub-felter.
HDR_STAMP	CHAR 32	YYY- YMMDDHHMMSSSSPGGRRRRRRRRNNNN N YYYY year MM month DD day HH hour MM minute SS second SS hundred-part second PGG time zone (UTC) RRRRRRRR 4 random binary digits hex coded, so it becomes a 8 digit string. NNNNN sequence number	Et tidsstempel der angiver, hvornår den pågældende net-ID er fremstillet på afsenders computer. [YYYYMMDDHHMMSS SS] er fra den lokale tidsserver. [PGG] er tidszonen, inklusive sommertid, i forhold til UTC. Eks. Dansk sommertid: "+02". Det er et krav at HDR_STAMP er unikt mellem en afsender og en modtager.

Felt	Type og længde	Værdi	Kommentar	
HDR_KVE R	CHAR VARIAB- LE	SIGRSAX1.APPL.01ZZZZ.PUBNNNNN X 'S' for test, 'P' for produktion APPL Applikationsnavn: 'PBSLOGON'. ZZZZ BFCNR. Bogføringscentralens ID som er angivet af Finansrådet. NNNNN Løbenr til entydig identifikation af netbankens certifikater.	Bogføringscentralens keylabel.	
HDR_RCV	CHAR 14	RCVTYPE	CHAR 2	RCVTYPE sættes til 01. SUBID udfyldes med tjenesteudby- ders subsid.
		RCVIDENT	CHAR 8	RCVIDENT udfyldes med tjenesteudby- ders CVR-nummer.
		SUBID	CHAR 4	SUBID udfyldes med- tjenesteudbyders SUBID.
HDR_UID	CHAR VARIAB- LE	BRAN- CHEID; <e.g. 'banks'>; DISTRIBID: <e.g. a specific bank identifica- tion>; KUNDEIDTYPE: <'type og KUN- DEID field'>; KUNDEID: <'senders identi- fication of a specific user'>	Se beskrivelse ne- denfor.	

Detaljer for HDR_UID

Field	Value	Comment
BRANCHEID	01 - Netbanker 02 - Tjenesteudbydere	01 bruges her.
DISTRIBID	CCCC	Pengeinstituttets registrerings- nummer. Den netbank der har signeret denne net-ID.
NB_AUTH	CCCC	Pengeinstituttets registrerings- nummer. Den netbank der har autentifi- ceret bruger.
KUNDEIDTYPE	00 - Unspecified 01 - Social Security Number (CPR). 02 - Internet bank agreement number. 03 - User ID in CAPS 04 - eBoks user identifier	00 benyttes såfremt cpr- nummer ikke returneres. 01 benyttes, da tjenesteudby- der skal have et entydigt br- ger-ID tilbage.
KUNDEID	DDMMYYZZZX DD Dag MM Måned YY ÅR ZZZ Løbenummer X Checkciffer	Hvis requester forespurgte at modtage CPR, angives bruge- rens CPR-nummer. Ellers angi- ves "000000000"

Context Ticket

Context Ticket bruges til informationer, som er nødvendige for modtageren. Alle felter i denne Context Ticket request er påkrævet.

Felt	Type og længde	Værdi	Kommentar	
CHDR_VE R	CHAR 4	1004 eller 1005	Protokolversion 1004 og 1005 er for net-ID. Begge har samme e-Ticket format, men 1005 tilføjer URL escaping af subfelter.	
HDR_LAN G	CHAR 2	DK	Landekode (ISO-8859-1) Kun DK er understøttet.	
HDR_LAN G2	CHAR 2	DK	Alternativ landekode (ISO-8859-1). Kun DK er understøttet.	
APP_DMID	CHAR 4	1020	Logonservice applikations-ID.	
APP_DMVE R	CHAR 4	1004	Dokumentbekræftelse response ID.	
APP_DATA	CHAR VARIAB- LE	EMAIL: <brugers email Adr>;FORNAVN: <fornavn>;EFTE R NAVN: <efternavn>;CO<c/o>;GAD E: <gade>;HUSNR: <husnr>;ETAGE NR: <etagenr>;POSTNR: <postnr>; BY: <by>;URL<url>;BESKED: <med delelse til notering>	Felt	Max læng- de
			EMAIL	60
			<u>FORNAVN</u>	34
			EFTE- NAVN	34
			CO	34
			<u>GADE</u>	34
			HUSNR	5
			ETAGENR	4
			POSTNR	4
			<u>BY</u>	34
			URL	255
			BESKED	20K Maks.

Bemærk at adressen kan skrives ind i de understregede felter, hvis den angivne opdeling ikke er mulig. Da skal følgende gælde:

- Fornavn indeholder fornavn, efternavn og evt. co.
- Gade indeholder gade, husnummer, etagenummer.
- By indeholder postnummer og by.
- By kan desuden indeholde land og landekode

Hvis der i i POSTNR angives fire nuller betyder det, at personen er udenlandsdanske.

11. Bilag 2: Net-ID-krav til pengeinstituttets aftale med bruger

Net-ID giver pengeinstitutternes tilsammen godt 2 mio. netbankbrugere (brugere) mulighed for at identificere sig entydigt på internettet over for tjenesteudbydere, der udbyder services på internettet.

For at en bruger kan få adgang til at anvende net-ID skal brugeren indgå en aftale med sit pengeinstitut. Med det formål er nedenstående brugerregler udarbejdet.

Reglerne er udformet som et tillæg til brugerens netbankaftale. Aftalerne i de enkelte pengeinstitutter er imidlertid ikke ens, og det har derfor ikke været muligt at udarbejde et tillæg, som kan anvendes umiddelbart af alle pengeinstitutter. Det enkelte pengeinstitut må derfor gennemgå forslaget til brugerregler i sammenhæng med pengeinstituttets egen aftalestruktur.

Det forudsættes, at Pengeinstituttet har indarbejdet den af Finansrådet anbefalede ansvars klausul (udsendt med direktionsskrivelse af 3. juni 2002, løbenr. 2002/065) i aftalegrundlaget med kunden.

Herudover er der en række forhold i de foreslåede brugerregler, som er af afgørende betydning for pengeinstitutternes ansvar i forhold til lov om visse betalingsmidler. De afsnit, som beskriver sådanne forhold, skal indarbejdes i pengeinstituttets aftalegrundlag med brugeren. Disse afsnit er fremhævet med fed skrift. Uanset at afsnittene skal indarbejdes, kan pengeinstituttet tilpasse formuleringerne, så de passer til den måde pengeinstituttet plejer at kommunikere med sine kunder på. Det indebærer eksempelvis, at "du" kan ændres til "De", og at enkelte ord kan erstattes af andre tilsvarende etc. Det juridiske indhold af de obligatoriske afsnit må dog ikke ændres.

Det vil kunne forekomme, at det allerede eksisterende aftalegrundlag med kunden indeholder tilsvarende bestemmelser, og i så fald er dette naturligvis tilstrækkeligt.

Aftale om brug af net-ID

Herved indgår jeg aftale med X-bank om brug af net-ID. Aftalen giver mig mulighed for ved brug af [elektronisk identifikation/min elektroniske underskrift/mit bruger-ID og mine koder] at kommunikere med tjenesteudbydere og bekræfte indholdet af et dokument via internettet. Jeg kan bruge net-ID over for de tjenesteudbydere, som har logoet for net-ID på deres hjemmeside.

En tjenesteudbyder er en virksomhed, som stiller [varer eller] tjenesteydelser til rådighed via internettet.

Anvendelse af net-ID

Net-ID er en sikkerhedsløsning, som gør det muligt for mig at kontakte en tjenesteudbyders hjemmeside og via mit e-bank-sikkerhedssystem

- **at logge på hos tjenesteudbyderen og se mine personlige oplysninger. I den situation oplyser X-bank min identitet over for tjenesteudbyderen.**
- **at bekræfte indholdet af et dokument, f.eks. en aftale, en blanket eller lignende, som jeg ønsker at indgå med eller afgive over for tjenesteudbyderen. I den situation beder tjenesteudbyderen X-bank om at indhente min bekræftelse af dokumentets indhold, hvorefter X-bank oplyser min identitet over for tjenesteudbyderen og meddeler, at jeg har bekræftet indholdet af dokumentet.**

Net-ID kan udelukkende anvendes til de nævnte formål. Net-ID er et selvstændigt produkt, og det har ikke nogen sammenhæng med [de funktioner, der er i] min netbank. Jeg er derfor opmærksom på, at net-ID ikke giver mig mulighed for at foretage betalinger alene ved anvendelse af net-ID.

Når jeg kommunikerer med tjenesteudbyderen og bekræfter indholdet af et dokument, gælder de af tjenesteudbyderen fastsatte regler. Det kan betyde, at jeg bliver forpligtet over for tjenesteudbyderen.

Ansvar for tjenesteudbyder og X-bank

Det er tjenesteudbyderens ansvar, at tjenesteudbyderen overholder lovgivningen, og at de [varer eller] tjenesteydelser, som tjenesteudbyderen stiller til rådighed via internettet, er i overensstemmelse med lovgivningen. X-bank har intet ansvar for tjenesteudbyderens overholdelse heraf.

Idet net-ID ikke selvstændigt kan anvendes som et betalingsmiddel, er jeg i relation til [den bestemmelse i netbank-aftalen, der henviser til ansvarsreglerne i lov om visse betalingsmidler] blevet gjort opmærksom på, at denne bestemmelse ikke er gældende i forholdet mellem X-bank og mig, når jeg bruger net-ID.

Det er tjenesteudbyderens ansvar at gøre mig opmærksom på, hvilke ansvarsregler, der gælder i forholdet mellem tjenesteudbyderen og mig.

X-bank er ikke ansvarlig for andres uberettigede brug af [elektronisk identifikation/min elektroniske underskrift/mit bruger-ID og mine koder]. [Fjernes, hvis dette allerede fremgår af det enkelte pengeinstituts standardbestemmelser for elektronisk identifikation/elektroniske underskrift/bruger-ID og koder.]

Videregivelse og opbevaring af personoplysninger

Hver gang jeg bruger net-ID, skal jeg give samtykke til, hvilke oplysninger X-bank må videregive til tjenesteudbyderen om mig. Oplysningerne kan være navn, personnummer, postadresse og e-mail-adresse.

X-bank videregiver kun oplysninger til tjenesteudbydere, som jeg kontakter ved brug af net-ID.

Al kommunikation mellem mig og X-bank, samt mellem tjenesteudbyder og X-bank foregår i krypteret form med såkaldt stærk kryptering i overensstemmelse med Datatilsynets krav. Det betyder, at oplysningerne ikke umiddelbart vil kunne læses af andre end tjenesteudbyderen.

Oplysninger om mit brug af net-ID opbevares i banken i 6 måneder. Indholdet af det dokument, som jeg bekræfter indholdet af ved brug af net-ID, vil blive opbevaret i X-bank i 5 år udover det år, hvor dokumentet bekræftes. X-bank fungerer kun som arkiv for mig og tjenesteudbyderen. I X-bank vil det alene være systemadministrator, der har adgang til oplysningerne, og disse vil udelukkende blive brugt med henblik på rettelse af eventuelle fejl og vedligeholdelse af net-ID.

Accept af denne aftale

Med min elektroniske identifikation/min elektroniske underskrift/mit bruger-ID og mine koder accepterer jeg indholdet af denne aftale.

[Herudover kan der i de enkelte pengeinstitutter være behov for at redegøre for/beskrive forholdet til det øvrige regelsæt, der gælder vedrørende brugerens netbank og eventuelle aftaler om elektronisk kommunikation med banken, f.eks. i tilfælde af spærring.]

12. Bilag 3: Ansøgningsformularer PBS-certifikater

net-ID certifikat (produktion)	
Firma	
SE-/CVR nummer	
Firmanavn	
Adresse	
Postnummer	
By	
Telefonnummer	
Ansøger	
Navn	
Titel	
Adresse	
Postnummer	
By	
Telefonnummer	
e-mail adresse	
Godkender (tegningsberettiget)	
Navn	
Stilling	
Dato og underskrift	
Indsendes til:	
PBS Lautrupbjerg 10, 2750 Ballerup	
att.: Sikkerhedsadministration	

SSL klient certifikat (produktion)	
Firma	
SE-/CVR nummer	
Firmanavn	
Adresse	
Postnummer	
By	
Telefonnummer	
Ansøger	
Navn	
Titel	
Adresse	
Postnummer	
By	
Telefonnummer	
e-mail adresse	
Godkender (tegningsberettiget)	
Navn	
Stilling	
Dato og underskrift	
Indsendes til:	
PBS Lautrupbjerg 10, 2750 Ballerup	
att.: Sikkerhedsadministration	

Fuldmagt til bestilling af PBS certifikater

Hermed giver vi nedenstående fuldmagt til på < Firma > vegne, at bestille og spærre < Firma >:

- net-ID certifikat
- SSL certifikat

Fuldmagten er gyldig indtil PBS har modtaget en skriftlig tilbagekaldelse fra < Firma >.

Fuldmagt giver

Firmanavn	
Navn på tegningsberettiget	
Telefonnummer	
Sted og dato	
Underskrift	

Fuldmagtshaver

Navn på fuldmagtshaver	
Telefonnummer	
Underskrift	

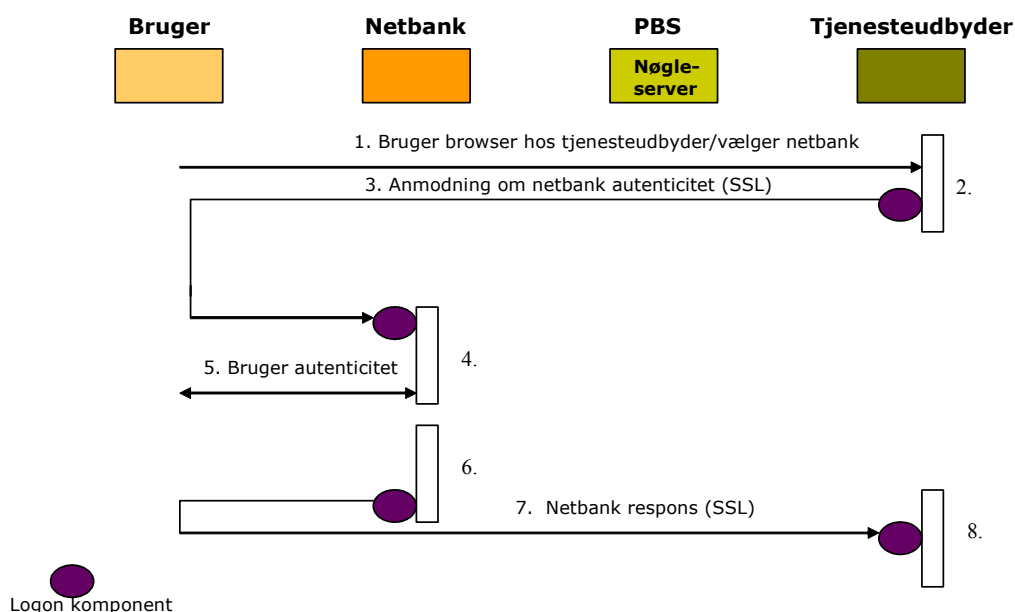
Fuldmagten sendes til PBS Lautrupbjerg 10, 2750 Ballerup att.: Sikkerhedsadministrationen. Fuldmagtshaver beholder kopi af fuldmagten.

13. Bilag 4: Fremskaffelse af dokumentation i en tvist

Fremskaffelse af dokumentation ved tvister mellem tjenesteudbyder og bruger

(a) Hændelsesforløbet i en logon-sekvens

Dette afsnit indeholder en overordnet beskrivelse af net-ID og de hændelser, der ligger bag udvekslingen af data.

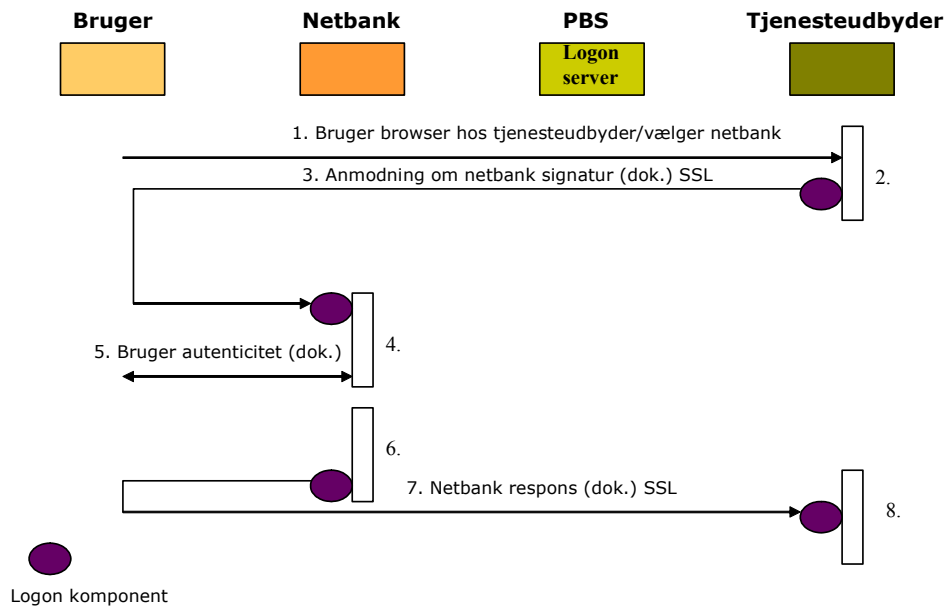


1. Bruger browser hos tjenesteudbyder og vælger pengeinstitut.
2. Tjenesteudbyder fremstiller autenticitetsanmodning. Anmodningen er i håndbogen defineret som en Logon Request.
3. Bruger bliver dirigeret til eget pengeinstitut i en SSL-tunnel, via omdirigering på brugers browser.
4. Pengeinstitutts sikkerhedssystem verificerer autenticitetsanmodningen fra tjenesteudbyder.
5. Pengeinstitutts sikkerhedssystem anmoder om brugerens autenticitet. Alle pengeinstitutterne benytter sig af en 2-faktor autenticitet, som betyder, at det er noget brugeren ved (eks. PIN-kode), og noget brugeren har (eks. CPR-nr.). Brugerens oplevelse er her den samme, som når der logges på netbanken. Hvis ikke brugeren i dette øjeblik har underskrevet en net-ID-tillægsaftale til sin eksisterende netbankaftale, bliver brugeren her præsenteret for vilkårene og har her muligheden for at acceptere dem.
6. Pengeinstitutts sikkerhedssystem fremstiller et svar. Svaret er i håndbogen defineret som en Logon Response.

7. Brugeren bliver dirigeret til tjenesteudbyder i en SSL-tunnel.
8. Tjenesteudbyder verificerer respons fra pengeinstituttet og giver brugeren adgang.

(b) Hændelsesforløbet i sekvens med dokumentbekræftelse

Dette afsnit indeholder en overordnet beskrivelse af net-ID og de hændelser, der ligger bag udvekslingen af data.



1. Brugeren browser hos tjenesteudbyder og vælger pengeinstitut.
2. Tjenesteudbyder fremstiller dokumentet, der skal bekræftes, og fremstiller en anmodning til brugers pengeinstitut. Anmodningen er i håndbogen defineret som en Logon Request.
3. Brugeren bliver dirigeret til eget pengeinstituts sikkerhedssystem i en SSL-tunnel, via omdirigering på brugers browser.
4. Pengeinstituttets sikkerhedssystem verificerer autenticitetsanmodningen fra tjenesteudbyder.
5. Pengeinstituttets sikkerhedssystem præsenterer for brugeren dokumentet, som skal bekræftes og anmoder om brugerens autenticitet. Alle pengeinstitutterne benytter sig af en 2-faktor autenticitet, som betyder at det er noget brugeren ved (eks. PIN-kode), og noget brugeren har (eks. CPR-nr.). Brugeren oplever her den samme, som når der logges på netbanken.
6. Pengeinstituttets sikkerhedssystem verificerer brugerens autenticitet og gemmer kopi af dokumentet (som netop er blevet bekræftet) med tilhørende autenticitetsdata.

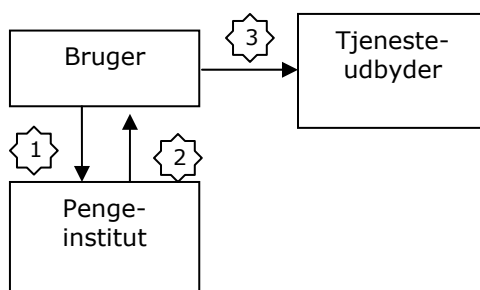
7. Pengeinstituttets sikkerhedssystem fremstiller et svar, der indeholder meddelelsen, der blev præsenteret for brugeren, og dirigerer brugeren tilbage til tjenesteudbyderen i SSL-tunnel.
8. Tjenesteudbyder verificerer respons fra pengeinstituttet og gemmer kopi heraf.

(c) Brugers reaktionsmuligheder ved en tvist

I tilfælde af en tvist imellem bruger og tjenesteudbyder kan der rekvireres dokumentation hos tjenesteudbyderen og i pengeinstituttet (min. 6 måneder tilbage). Se eventuelt håndbogen afsnit 7.2.3 og 7.3.2.

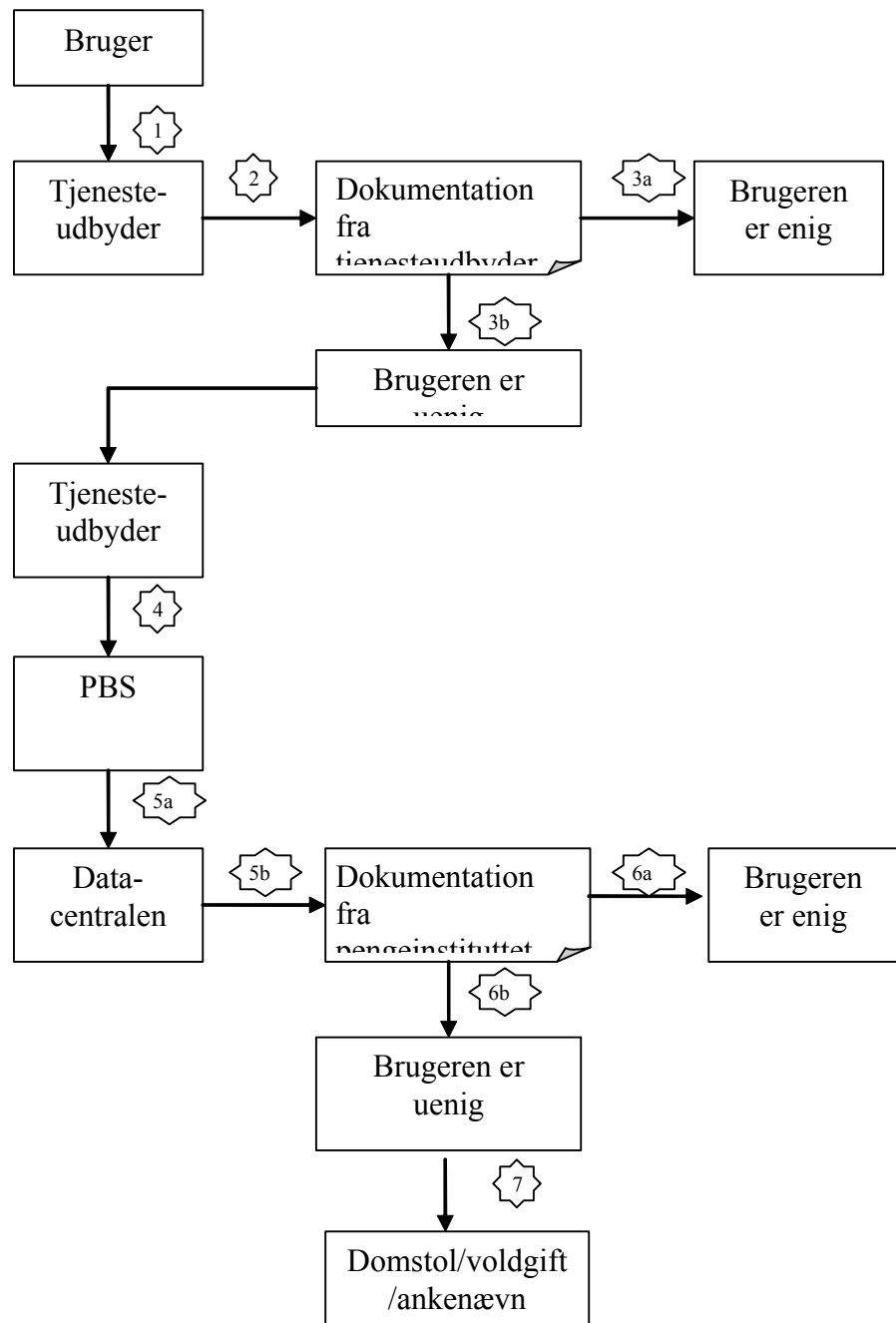
Herunder er proceduren skitseret som et flowdiagram.

1. Brugeren henvender sig i pengeinstituttet



1	Brugeren retter henvendelse til pengeinstituttet i forbindelse med en tvist mellem brugeren og tjenesteudbyderen
1A	Brugeren henvender sig til sit pengeinstitut med mistanke om, at brugers netbankkode/net-ID er blevet kompromitteret. Brugeren er i hht. netbankaftale/net-ID aftale <u>forpligtet</u> til altid at foranledige en spærring af netbankkoden ved mistanke om kompromittering.
2	Pengeinstituttet orienterer brugeren om processen og beder brugeren om at henvende sig til tjenesteudbyderen, da det er denne, som er part i sagen. Et væsentligt sikkerhedselement er, at kun ganske få medarbejdere har adgang til loggede data relateret til net-ID. Fremfinding af data sker kun, når der er tale om en tvist, som begge parter er orienteret om.
2A	Brugeren kan selv spærre netbankkoden elektronisk. Henvender brugeren sig i pengeinstituttet, vil pengeinstituttet straks foranledige en spærring af brugens netbankkode. I tilfælde af en ikke-vedkendelsessag vil der straks blive iværksat en undersøgelse.
3	Brugeren retter henvendelse til tjenesteudbyderen – det videre flow er vist nedenfor.

1. Brugeren henvender sig til tjenesteudbyder



1	Brugeren retter henvendelse til tjenesteudbyderen ifm. en tvist
2	Tjenesteudbyderen fremfinder relevant dokumentation

3a	Brugeren er enig med tjenesteudbyderen, hvorfor der ikke foretages yderligere
3b	Brugeren er ikke enig med tjenesteudbyderen
4	Tjenesteudbyderen retter henvendelse til PBS
5a	PBS retter henvendelse til det relevante pengeinstitut/datacentral
5b	Datacentralen/PI fremfinder relevant dokumentation, jf. pkt. d
6a	Den relevante dokumentation fremlægges for brugeren. Brugeren er enig i indholdet, og der foretages ikke yderligere
6b	Den relevante dokumentation fremlægges for brugeren. Brugeren er ikke enig i indholdet
7	Da brugeren ikke er enig i den dokumentation, som er blevet fremlagt, ender sagen hos domstolen/voldgift/ankenævn

(d) Dokumentation der kan tilvejebringes ved en tvist

"Step"	Dokumentation	Opbevaring
Bruger → Tjenesteudbyder	<p>Der skal føres en log, som viser både gyldige og ugyldige logon responses fra pengeinstituttet*</p> <p><u>Dokumentbekræftelse:</u></p> <p>Der skal føres en log, som viser både gyldige og ugyldige logon responses fra pengeinstituttet*</p> <p>For at sikre bevisværdien skal tjenesteudbyder herudover gemme:</p> <ul style="list-style-type: none"> - Modtagne e-Tickets, 	<p><u>Logon-delen:</u></p> <ul style="list-style-type: none"> - Revisionsspor skal opbevares min. 6 måneder eller i overensstemmelse med gældende lovgivning, evt. persondatalovens rammer <p><u>Dokumentbekræftelse:</u></p> <ul style="list-style-type: none"> - indeværende år + 5 efterfølgende år - Dokument

	<p>som indeholder dokumentbekræftelse</p> <ul style="list-style-type: none"> - Relaterede certifikater (certifikater, der benyttes til at verificere net-ID) 	
Tjenesteudbyder → PBS		
PBS → Pengeinstitut/ Datacentralen	<p><u>Logon-delen:</u></p> <p>Logon-anmodningen (logon request) fra tjenesteudbyderen registreres og gemmes*</p> <p><u>Dokumentbekræftelse:</u></p> <p>Logon-anmodningen fra tjenesteudbyderen + kopi af dokument</p> <p><u>Spærring af netbankkode/net-ID kode</u></p>	<p><u>Logon-delen:</u></p> <ul style="list-style-type: none"> - Min. 6 måneder tilbage <p><u>Dokumentbekræftelse:</u></p> <ul style="list-style-type: none"> - indeværende år + 5 efterfølgende år - Dokument <p>Som anført nedenfor</p>
<p><u>Øvrige dokumenter i tilfælde af tvist</u></p> <p>Tjenesteudbyderen:</p> <ul style="list-style-type: none"> - Bekræftelse af dispositioner (f.eks. faktura, kvittering m.v.) - Brugsmønstre - Mm. <p>PBS (PI):</p> <ul style="list-style-type: none"> - Dokumentation for brugerens indgåelse af netbankaftale + net-ID tilslutning - Spærring af netbankkode - Indsigelser og andet misbrug - Editionspligt i medfør af retsplejeloven 		

Brugerens identitet er i pengeinstituttet fastslået som foreskrevet i lbk. 129 af 23.2.2004 om forebyggende foranstaltninger mod hvidvaskning af penge og

finansiering af terrorisme, der implementerer Rådets direktiv 91/308/EØF af 10.6.1991 om forebyggende foranstaltninger mod anvendelse af det finansielle system til hvidvaskning af penge. Den danske lovgivning trådte i kraft 1.7.1993.

Dette regelsæt foreskriver, at de omfattede virksomheder skal afkræve kunderne legitimation ved etablering af forretningsmæssig forbindelse, åbning af konti eller depoter mv. Legitimationen skal omfatte navn, adresse og CPR-nummer eller CVR-nummer. Disse identitetsoplysninger skal gemmes i mindst 5 år efter, at kundeforholdet er ophørt.

14. Bilag 5: Ledelseserklæringer

Ledelsens erklæring (igangsætning) for «Navn» :

Ledelsen kan i henhold til aftale med PBS erklære:

- at de i den seneste version af net-ID håndbogen krævede skriftlige forretningsgange vedrørende sikkerhed er etableret
- at forretningsgangene samt de etablerede systemer overholder de i net-ID håndbogen (seneste version) opstillede krav
- at forretningsgangene og systemerne er betryggende

Evt. supplerende oplysninger/mangler:

, den / - 200_

Firmastempel og forpligtende underskrift, samt e-mail-adresse.

e-mail:

Revisorattestation

Vi har foretaget revision af «Navn» overholdelse af sikkerheden i overensstemmelse med seneste version af Håndbog net-ID standard jf. ___-Revisionscheckliste kapitel 22.

Vi kan bekræfte:

- at vi har modtaget alle de oplysninger, vi har anmodet om
- at vi har udført revisionen i overensstemmelser med god revisionskik

Vi er enige i/har følgende specifikke forbehold/bemærkninger til ovenstående ledelseserklæring.

Evt. bemærkninger/forbehold

Sted og dato

Stempel og underskrift
Edb-revisor

Indsendes senest 14 dage inden igangsætning til:

PBS A/S, att.: PBS Systemrevision
Lautrupbjerg 10, 2750 Ballerup

Ledelsens erklæring (pr. 31.12) for «Navn» :

Ledelsen kan i henhold til aftale med PBS erklære:

- at de i den seneste version af net-ID håndbogen krævede skriftlige forretningsgange vedrørende sikkerhed er etableret
- at forretningsgangene samt de etablerede systemer overholder de i net-ID håndbogen (seneste version) opstillede krav
- at forretningsgangene og systemerne er betryggende
- at forretningsgangene har været overholdt, og systemerne har fungeret betryggende i det forløbne år

Evt. supplerende oplysninger/mangler:

, den / - 200_

Firmastempel og forpligtende underskrift, samt e-mail-adresse.

e-mail:

Revisorattestation

Vi har foretaget revision af «Navn» overholdelse af sikkerheden i overensstemmelse med seneste version af Håndbog net-ID standard

Vi kan bekræfte:

- at vi har modtaget alle de oplysninger, vi har anmodet om
- at vi har udført revisionen i overensstemmelse med god revisionsskik.

Vi er enige i/har følgende specifikke forbehold/bemærkninger til ovenstående ledelseserklæring.

- at der er udarbejdet forretningsgange/systemer for at sikre de anførte krav.
- at forretningsgangene har været overholdt, og systemerne har fungeret betryggende i det forløbne år (01.01. - 31.12.)

Evt. bemærkninger/forbehold

Sted og dato

Stempel og underskrift
Edb-revisor

Indsendes senest den 31.01 til:
PBS A/S, att: PBS Systemrevision
Lautrupbjerg 10, 2750 Ballerup

15. Bilag 6: Blanket til indrapportering til Batch-server

Tjenesteudbyder

En tjenesteudbyder kan vælge at lade net-ID hoste hos en anden edb-central. Denne edb-central benævnes en "vært". Denne vært skal og også registreres på batchserveren.

Værten skal indrapportere følgende:

Første oprettelse () sæt kryds.

Oplysningerne skal træde i kraft fra den / 200_

Opdatering af eksisterende oplysninger () sæt kryds.

Oplysningerne skal træde i kraft den / 200_

Attribut	Betydning	Validering
CVR-nummer	Værtens CVR-nummer. Er primærnøgle og kan derfor ikke rettes.	Otte cifre. Skal angives.
Navn	Værtens navn.	Skal angives.
URL	Værtens URL.	Skal begynde med http. Skal angives.
Logo	Værtens logo.	Skal være en billedfil af type PNG , JPG eller GIF med en maksimal størrelse på 8 KB. Bredde: 120 pixels Højde: 90 pixels Baggrunden i billedet skal være transparent.
Benyt logo	Angiver om værtens logo skal benyttes for de tilknyttede tjenesteudbydere.	Er enten sat eller ikke sat.

	<p>Hvis check boxen er sat betyder det følgende:</p> <p>I tjenesteudbyderlisten vil alle tjenesteudbydere, som er til knyttet denne vært, have værtens logo og ikke deres eget.</p> <p>Hvis check boxen ikke er sat betyder det følgende:</p> <p>I tjenesteudbyderlisten vil alle tjenesteudbydere, som er tilknyttet denne vært, have deres eget logo.</p>	
Certifikat	Det aktuelle net-ID certifikat, der skal benyttes.	Må ikke være udløbet. Skal angives
Fornyet certifikat	Det net-ID certifikat, der skal afløse det aktuelle ved udløb.	Må ikke være udløbet. Kan angives

Oplysningerne indsendes til PBS (se kapitel 23 Kontakt).

Tjenesteudbyder skal indrapportere følgende:

Første oprettelse () sæt kryds.

Oplysningerne skal træde i kraft fra den / 200_

Opdatering af eksisterende oplysninger () sæt kryds.

Oplysningerne skal træde i kraft den / 200_

Attribut	Betydning	Validering
CVR-nummer	Tjenesteudbyders CVR-nummer. Er primærnøgle og kan derfor ikke rettes.	Otte cifre. Skal angives.

Navn	Tjenesteudbyders navn.	Skal angives.
URL	Tjenesteudbyders URL.	Skal begynde med https. Skal angives.
Logo	Tjenesteudbyderens logo.	Skal være en billedfil af type PNG, JPG eller GIF med en maksimal størrelse på 8 KB. Skal angives.
Direkte link	<p>Angiver om tjenesteudbyderen skal med i listen af tjenesteudbydere, som tilbyder direkte link.</p> <p>Hvis check boxen er sat betyder det:</p> <p>Tjenesteudbyderen er med i tjenesteudbyderlisten for direkte link.</p> <p>Tjenesteudbyderen skal dermed oplyse følgende:</p> <p>Subid (4 cifre) TU ID</p> <p>Reqcpr: (ja/nej)</p> <p>Reqemail: (ja/nej)</p> <p>Reqaddress: (ja/nej)</p> <p>Requserurl: (ja/nej)</p> <p>Protocolvers.: (4 cifre)</p> <p>Description: (streng)</p> <p>Hvis check boxen ikke er sat betyder det:</p> <p>Tjenesteudbyderen er ikke med i tjenesteudbyderlisten</p>	<p>Er enten sat eller ikke sat.</p>

	for direkte link.	
Benyt vært	<p>Angiver om tjenesteudbyderen skal knyttes til en vært.</p> <p>Hvis "Ja" er valgt betyder det:</p> <p>Tjenesteudbyderen knyttes til en vært. I tjenesteudbyderlisten vil værtens URL, net-ID certifikat og (optionelt) logo optræde for denne tjenesteudbyder.</p> <p>Hvis "Nej" er valgt betyder det:</p> <p>Tjenesteudbyderen holder selv alle sine data.</p>	Er enten "Ja" eller "Nej".
Certifikat	Det aktuelle net-ID certifikat, der skal benyttes.	Må ikke være udløbet. Skal angives
Fornyet certifikat	Det net-ID certifikat, der skal afløse det aktuelle ved udløb.	Må ikke være udløbet. Kan angives

Oplysningerne indsendes til PBS (se kapitel 23 Kontakt).

Pengeinstitutter skal indrapportere følgende:

Første oprettelse () sæt kryds.

Oplysningerne skal træde i kraft fra den / 200_

Opdatering af eksisterende oplysninger () sæt kryds.

Oplysningerne skal træde i kraft den / 200_

Attribut	Betydning	Validering
Reg.-nummer	Pengeinstituttets registreringsnummer.	Fire cifre. Skal angives.
Navn	Pengeinstituttets navn.	Skal angives.
URL	Datacentralens URL, hvortil tjenesteudbydere skal dirigere brugere.	Skal begynde med https. Skal angives.
Åbningstid	Datacentralens åbningstid. Hvis der er lukket for eksempel mellem kl. 03 – 04 om natten angives åbningstiden til 04:00 – 03:00.	Tidspunkterne skal have formatet TT:MM eksempelvis 12:56. Skal angives.
Accepterer dokumentbekræftelse	Angiver, hvorvidt pengeinstituttet har implementeret dokumentbekræftelse.	Angives "ja" eller "nej". Skal angives.
Navn datacentral	Angiver den datacentral, som pengeinstituttet benytter.	Skal angives.

Oplysningerne indsendes til PBS (se kapitel 23 Kontakt).

Datacentralen skal indrapportere følgende:

Første oprettelse () sæt kryds.

Oplysningerne skal træde i kraft fra den / 200_

Opdatering af eksisterende oplysninger () sæt kryds.

Oplysningerne skal træde i kraft den / 200_

Attribut	Betydning	Validering
Navn datacentral	Angiver den datacentral, som pengeinstituttet benytter.	Skal angives.
Certifikat	Det aktuelle net-ID certifikat, der skal benyttes.	Må ikke være udløbet. Skal angives.
Forny et certifikat	Det net-ID certifikat, der skal afløse det aktuelle ved udløb.	Må ikke være udløbet. Skal angives.

Oplysningerne indsendes til PBS (se kapitel 23 Kontakt).

16. Bilag 7: PBS kundesupport

Såfremt der opleves driftsproblemer med PBS Batch-server kan henvendelse rettes til PBS driftsovervågning (se kapitel 23 Kontakt).

Fejl og mangler i net-ID Håndbog, implementeringsvejledninger og referenceimplementering kan meddeles til PBS (se kapitel 23 Kontakt).

Helpdesk-procedure

Problem/spørgsmål	Kontakt
-------------------	---------

Bruger

Har brugeren problemer, når han/hun skal indtaste sin netbank adgangskode.	Pengeinstituttet for nærmere information. Åbningstiden varierer fra pengeinstitut til pengeinstitut. <u>Typiske åbningstider:</u> Hverdage 08.00 – 23.00 Søn- og helligdage 10.00 – 23.00
Har brugeren generelle spørgsmål til net-ID.	Pengeinstituttet for nærmere information. Åbningstiden varierer fra pengeinstitut til pengeinstitut. <u>Typiske åbningstider:</u> Hverdage 08.00 – 23.00 Søn- og helligdage 10.00 – 23.00
Har brugeren problemer med net-ID fra tjenesteudbyderens hjemmeside.	Tjenesteudbyderen for nærmere information.

Tjenesteudbyder

Har tjenesteudbyderen spørgsmål eller kommentarer til dokumentationen og referenceimplementering.	PBS for nærmere support. <u>Åbningstid:</u> Hverdage 08.30 – 16.30.
---	---

<p>Har tjenesteudbyderen problemer med at hente de nyeste certifikatoplysninger på Batch-serveren.</p>	<p>PBS for nærmere information (1. level support). Henvendelse til PBS hele døgnet. Såfremt 1. level support ikke kan løse problemet, vil det blive eskaleret til 2. level support.</p> <p>2. Level support via PBS</p> <p><u>Åbningstid:</u></p> <p>Hverdage 08.30 – 16.30.</p>
<p>Har tjenesteudbyderen generelle spørgsmål til net-ID-løsningen.</p>	<p>PBS for nærmere information.</p> <p><u>Åbningstid:</u></p> <p>Hverdage 08.30 – 16.30.</p>
<p>Har tjenesteudbyderen spørgsmål til faktureringen.</p>	<p>PBS</p> <p><u>Åbningstid:</u></p> <p>Hverdage 08.30 – 16.30.</p>
<p>Har tjenesteudbyderen problemer med implementeringen af net-ID i.f.t. egen (tjenesteudbyders) applikation.</p>	<p>Tjenesteudbyderens IT-leverandør</p>
<p>Har tjeneudbyderen eller tjenesteudbyderens IT-leverandør spørgsmål ifm. implementeringen af net-ID.</p>	<p>TietoEnator (2. level support).</p> <p><u>Åbningstid:</u></p> <p>Hverdage 08.30 – 16.30</p>

Adgang til PBS' testserver kan etableres i tidsrummet 8.30 – 16.30 efter forudgående aftale med PBS.

17. Bilag 8: Net-ID vedligeholdelse

Vedligeholdelsesopgaver

PBS har til opgave at vedligeholde net-ID.

Basisversion: Den version af net-ID, som af PBS annonceres som den officielle version.

Opgaver

Vedligeholdelsesopgaven omfatter:

- Fejlrapportbehandling, fejlanalyse og fejlrettelse.
- Vedligeholdelse og aftestning af net-ID basisversioner.
- Vedligeholdelse af dokumentation.

Fejlrapportbehandling, fejlanalyse og fejlrettelse

Ved fejl forstås afvigelser i funktionaliteten i henhold til dokumentationen af de versioner, som vedligeholdes af PBS.

Fejlrapporterne vil af PBS klassificeres i følgende prioriteter:

Prioritet 0:

Bruges til at rapportere fejl i net-ID, som truer driftssystemets stabilitet.

Prioritet 1:

Bruges til at rapportere vitale fejl i net-ID, som forhindrer sikker drift.

Prioritet 2:

Bruges til at rapportere funktionelle fejl i net-ID, som dog ikke truer systemets sikkerhed.

Prioritet 5:

Bruges til at rapportere fremtidige ønsker til nye funktioner i net-ID.

Prioritet 33:

Bruges til at rapportere uhensigtsmæssigheder i net-ID, som ønskes løst inden en bestemt dato eller begivenhed (uden at falde ind under ovennævnte kategorier).

Prioritet 88:

Afvisninger af fejlrapporter (fejl og uhensigtsmæssigheder, som ikke kan klassificeres i ovenstående prioriteter eller som følge af forkert brug af net-ID-systemet).

PBS er eneste kontaktpunkt for levering af fejlrapporter. Levering af fejlrapporter foregår inden for normal arbejdstid 8.30 - 16.30.

Opfølgning på fejlrapporter vil, for den enkelte kategori, være følgende:

Prioritet 0:

Fejlanalyse og efterfølgende fejlrettelse påbegyndes straks og fortsættes uafbrudt til fejlen er rettet og systemet atter fungerer.

Prioritet 1:

Fejlanalyse påbegyndes inden for 8 timer, regnet med udgangspunkt i almindelige arbejdsdage, og fejlrettelse afsluttes i 90% af tilfældene inden for 5 arbejdsdage.

Prioritet 2:

Fejlanalyse påbegyndes inden for 16 timer, regnet med udgangspunkt i almindelige arbejdsdage, og fejlrettelse inkluderes i næste officielle version.

Prioritet 5:

Ønskes behandlet på næste møde mellem PBS og tjenesteudbyder.

Prioritet 33:

Fejlrettelse inkluderes i en af PBS' fremtidige planlagte versioner af net-ID.

Prioritet 88: Fejlrettelse foretages ikke.

Den, der har rapporteret fejlen til PBS, vil blive orienteret om prioriteringen af problemet og om mulige nødforanstaltninger af PBS. For prioritet 0 og 1 inden 1 dag - og for prioritet 2 inden for 10 arbejdsdage.

PBS skal om nødvendigt have mulighed for at foretage fejlanalyse, fejlreproduktion og fejlaftestning på tjenesteudbyders system. Dette skal dog ske med mindst mulig gene for tjenesteudbyder.

Tjenesteudbyder implementerer selv nye net-ID programversioner i egne applikationer. PBS bistår i fornødent omfang og vederlagsfrit, hvis konstaterede problemer kan henføres til net-ID-programversionen.

Vedligeholdelse og test af programversioner:

Net-ID-programmel vedligeholdes i seneste (basisversion) og næstsensete version. Første officielle basisversion, som vedligeholdes, er version 1.0.0. Nye net-ID-basisversioner annonceres over for tjenesteudbyder med 6 måneders varsel.

Net-ID basisversion testes i specificerede afviklingsmiljøer inden frigivelse til tjenesteudbyder.

Net-ID-programmel vedligeholdes, således at der er kompatibilitet med de specificerede versioner af systemprogrammet – men dog således at net-ID-programmet skal være kompatibelt med markedsgængs systemprogrammet senest 12 mdr. efter, at det er markedsført (i nyeste højre version - i modsætning til nye patches eller releases, f.eks. fra version 1.2 til version 1.3).

PBS er ikke forpligtiget til at rette fejl, som kan henføres til fejl i standardsystemprogrammet.

PBS er ikke forpligtiget til forlods at afteste net-ID-programmet ved versionskift af systemprogrammet hos tjenesteudbyder. Versionskift skal i denne sammenhæng betragtes og behandles som prioritet 5 (ønsker til fremtidige nye funktioner).

Kun PBS og de af PBS antagne underleverandører må ændre i net-ID.

Vedligeholdelse af dokumentation

PBS vedligeholder net-ID-dokumentationen i takt med og senest samtidig med, at nye net-ID-basisversioner frigives og som følge af ændrede forretningsgange. PBS forbeholder sig ret til at omstrukturere dokumentationen, hvis det ud fra et vedligeholdelsessynspunkt vil lette brugen af dokumentationen.

Ændringsønsker

Ændringsønsker skal sendes skriftligt (papir eller e-mail), til PBS.

18. Bilag 9: Servicemål

Batch-server

Målsætningen for den planlagte service-tilgængelighed for systemet er 24 timer ugens 7 dage. Servicestop kan dog ikke undgås som følge af hardware- og software fejl, kommunikationsproblemer samt planlagte præventive vedligeholdelsesforanstaltninger.

Periode	Åbningsvindue	Tilgængelighed
Hverdage	08:00 – 16:00	99,5 %
Hverdage	16:00 – 08:00	99,5 %
Weekends og helligdage	00:00 – 24:00	99,5 %

Den anførte tilgængelighed er udregnet over en måned og er eksklusiv planlagt nedetid som følge af regelmæssig vedligeholdelse.

Planlagt servicevindue

Servicevinduet ligger første mandag i måneden (som ikke er en helligdag eller Grundlovsdag) mellem kl. 02.00 - 08.00. Dette servicevindue anvendes primært ved større ændringer med længerevarende utilgængelighed.

Ved mindre ændringer til applikationen, hvor kortvarig utilgængelighed (under 1 time) er aftalt med kunderne, kan disse foretages på tirsdage mellem kl. 18.00 og 19.00

Endvidere er der vedligeholdelsesvinduer på firewall'en (mandag morgen 02.00 - 05.00 samt switch-over tirsdag aften 19.00 - 22.00 (et par minutters utilgængelighed).

Datacentraler

Det planlagte servicemål for datacentralerne er en driftseffektivitet på mindst 99,5 % inden for den oplyste åbningstid. Hver af de seks datacentraler har forskellig åbningstid. Åbningstiden fremgår af oplysninger på Batch-serveren.

19. Bilag 10: Retningslinjer for kommunikation af net-ID

I dette bilag kan tjenesteudbydere og pengeinstitutter finde retningslinjer for deres kommunikation af net-ID over for egne kunder.

Net-ID med logo

Net-ID logoet ser således ud:



Logoet består af farverne rød, hvid og sort. For at logoet også kan bruges på farvet baggrund, har logoet en hvid ring uden om den røde ring.

I al skriftlig kommunikation skrives net-ID med små bogstaver i 'net' og store bogstaver i 'ID' forbundet med en bindestreg. Efter et punktum eller som start på nyt afsnit skrives det første bogstav med stort: 'Net-ID'. Net-ID udtales 'net', pause 'I' pause 'D' - alt med dansk udtale.

Net-ID-logoet kan downloades fra PBS' hjemmeside under punktet 'Billedarkiv, Grafik og logoer'.

Net-ID-sprogbrug

For at sikre en ensartet beskrivelse af net-ID anbefales følgende ord brugt i al kommunikation:

Ord	Ordforklaring
Net-ID	Net-ID er et identifikationssystem. Net-ID er en nem og sikker måde for en netbankbruger elektronisk at identificere sig over for en virksomhed på internettet.
Identifikation	Net-ID giver mulighed for at en virksomhed/tjenesteudbyder, der tilbyder services via internettet, kan kontrollere en brugers identitet, inden virksomheden/tjenesteudbyderen giver brugeren adgang til f.eks. personoplysninger. Identifikationen sker via pengeinstitutternes sikkerhedssystem og med den adgangskode, som brugeren normalt bruger til at logge på sin netbank. Dette svarer til, at brugeren logger sig på netbanken og får adgang til egne kontooplysninger.

Ord	Ordforklaring
Adgangskode	Adgangskode er en fælles betegnelse for de koder, som netbankbrugeren bruger til logge på sin netbank.
Netbankbruger/bruger	Alle personer med en netbank kan bruge net-ID efter at have accepteret en aftale med sit pengeinstitut.
Virksomhed/ tjenesteudbyder	En virksomhed/tjenesteudbyder udbyder services mm. på internettet og kan – efter at have indgået aftale med PBS - tilbyde net-ID.
Brugerbetaling	Pengeinstitutterne tilbyder net-ID til netbankbrugeren uden omkostninger. Ordet gratis bruges ikke .

Net-ID spørgsmål & svar

På www.PBS.dk/it-services/net-id kan tjenesteudbyder bl.a. finde opdaterede spørgsmål/svar, der relaterer sig til henholdsvis brugerne og virksomhederne.

20. Bilag 11: TU-checkliste for implementering af net-ID

Reference	Beskrivelse
1	Underskrift på tilslutningsaftale (eller hensigtserklæring)
2	PBS fremsender programmel + dokumentation til TU inkl. Vejrtjeneste (=demo af anvendelse af API og testværktøj til TU)
3	TU implementerer net-ID. PBS yder support i forbindelse med spørgsmål vedr. indhold i net-ID dokumentation og software-pakke.
4.	<p>Test:</p> <p><u>Forberedelse:</u></p> <ul style="list-style-type: none">- TU fremsender IP-adresser til PBS, som skal benyttes for at kommunikere med test Batch-server.- TU fremsender certifikatansøgning (test) for SSL-klient og net-ID til PBS. (<i>For begge certifikater husk keylabel skal med i SubjectKeyIdentifier</i>).- TU fremsender TU-oplysninger, der skal registreres på Batch-server. <p>Indlæggelse af PBS-certifikater:</p> <ol style="list-style-type: none">a) PBS root certifikat (DER format) import i keystore ca.ksb) PBS CA Admin certifikat (DER format) import i keystore ca.ks.c) Import af eget certifikat (DER). Dette certifikat skal verificere indlæggelse med brug af scriptet PBS CertChain.pem. <p><u>Gennemførelse af test</u></p> <ul style="list-style-type: none">- TU gennemfører test mod Batch-server.- TU foretager intern test med brug af netbanksimulator.

5.	<p>Pilotproduktion (i "skjult produktion")</p> <ul style="list-style-type: none"> - <u>Forberedelse:</u> - TU fremsender IP-adresser til PBS, som skal benyttes for at kommunikere med (prod) Batch-server. - TU fremsender certifikatansøgning (prod) for SSL-klient og net-ID til PBS. - TU fremsender TU-oplysninger der skal registreres på Batch-server. <p><u>Gennemførelse af pilotproduktion:</u></p> <ul style="list-style-type: none"> - TU gennemfører test mod (prod) Batch-server. - TU gennemfører systemtest (ref. kap. 9) med brug af udvalgte netbankkunder.
6.	<p>Certificering af TU</p> <ul style="list-style-type: none"> - TU fremsender skærbilleder til PBS. - TU fremsender testrapport til PBS. - TU fremsender ledelseserklæring og revisorattest til PBS.

21. Bilag 12 Testrapport

Undertegnede firma/edb-central har gennemført en ekstern test mod:

- a) PBS' Batch-server-testsystem i henhold til testspecifikationen indeholdt i ref.(20) og
- b) Minimum en netbank i henhold til kapitel 9. (gældende for Tjenesteudbyder)
- c) Minimum en tjenesteudbyder i henhold til kapitel 9. (gældende for PI).

med tilfredsstillende resultat og kan bekræfte at vores net-ID implementering fungerer, som specificeret under forventet testresultat.

Firma:

Navn på system-/udviklingsansvarlig:

Dato:

Testrapport fremsendes til PBS (se kapitel 23 Kontakt).

22. Bilag 13 Revisionschecklister

Revisionscheckliste for pengeinstitutternes edb-centraler

Dette dokument indeholder en checkliste til brug for edb-revision/ledelsen i pengeinstitutterne, som skal kontrollere om en edb-central overholder Håndbog for net-ID standard.

Checkliste

Reference til kapitler i net-ID Håndbogen	Krav	Kravet overholdes	Kravet overholdes ikke	Kommentar
3.3	e-Ticket layout Krav 1			
5.1	Skærbillede for tilmelding Krav 1 Krav 2			

5.2	Skærmbil. for logon og dok.b.			
	Krav 1			
	Krav 2			
	Krav 3			
	Krav 4			
	Krav 5			
	Krav 6			
	Krav 7			
	Krav 8			
	Krav 9			
	Krav 10			
	Krav 11			
	Krav 12			
	Krav 13			

	Krav 14			
5.4	Præsentation af TU's logo Krav 1 Krav 2			
6.	Krav til faktureringsgrundlag Krav 1 Krav 2 Krav 3 Krav 4			
7.1.	Kom. Sikkerhed og kryp. nøgler Krav 1 Krav 2 Krav 5			

7.2.1	Sikkerhedskrav nøgleadm. Krav 1 Krav 2 Krav 3 Krav 4 Spærring af nøgler Krav 5			
7.2.2	Opslag på Batchserver Krav 1			
7.2.3	Interne sikkerhedskontroller Krav 1 Logning af logon Krav 2 Krav 3			

	Opbevaring afdokumentbekt. Krav 4 Krav 5 Krav 6 Udskrivning og fremf. af dok. Krav 7			
7.2.4	Test, erklæring og godkendelse Krav 1 Krav 2 Krav 3 Krav 4			

Revisionscheckliste for tjenesteudbydere

Dette dokument indeholder en checkliste til brug for edb-revision/ledelsen, som skal kontrollere om net-ID installationen for en tjenesteudbyder overholder Håndbog for net-ID standard.

Checkliste

Ref. til kapitler i Håndbogen	Krav	Kravet overholdes	Kravet overholdes ikke	Kommentar
3.3	e-Ticket layout Krav 1			
7.3 7.3.1	Sikkerhedskrav til TU Nøglefremstilling Krav 1 Krav 2 Krav 3 Krav 4			

	Krav 5 Spærring af nøgler Krav 6			
7.3.2	Bruger-ID for operatør Krav 1 Krav 2 Krav 3 Nød-bruger ID Krav 4 Krav 5 Logisk adgang Krav 6 Krav 7 Krav 8			

	<p>Krav 9</p> <p>Fysisk adgang</p> <p>Krav 10</p> <p>Viruskontrol</p> <p>Krav 11</p> <p>Krav 12</p> <p>Krav 13</p> <p>Netværk og firewall</p> <p>Krav 14</p> <p>Krav 15</p> <p>Krav 16</p> <p>Krav 17</p> <p>Krav 18</p> <p>Revisionspor</p>			
--	--	--	--	--

	Krav 19 Krav 20 Dokumentbekræftelse Krav 21 Kommunikation til Batchserver Krav 22 Krav 23			
7.3.4	Test, erklæring og godkendelse Test Krav 1 (Kun opstartserklæring) Krav 2 (Kun opstartserklæring) Krav 3 (kun opstartserklæring) Erklæring Krav 4			

23. Bilag 14 Kontakt

Test

- Net-ID_teksup@pbs.dk:

Benyttes til alle henvendelser vedrørende implementering af net-ID i test.

Produktion

- Net-ID_certificering@pbs.dk:

Benyttes til alle henvendelser vedrørende igangsætning af net-ID på produktions-systemer, dvs. IP-adresser, certifikatansøgninger, testrapporter, oplysninger til batchserver og skærbilleder.

- PBS Lautrupbjerg 10

2750 Ballerup

Att.: PE 1110 Corporate Affairs

Benyttes til indsendelse af formular og evt. disketter til ansøgning om produktionscertifikater.

- PBS Lautrupbjerg 10, 2750 Ballerup

Att.: PE 1110 Corporate Affairs

Benyttes til indsendelse af ledelses- og revisionserklæringer.

Driftsproblemer

- Tlf. 4489 2530

Benyttes til driftsproblemer på PBS Batchserver og til spærring af certifikater.

- Net-ID_teksup@pbs.dk:

Fejl og mangler i net-ID Håndbog, implementeringsvejledninger og referenceimplementering.

Info om net-ID

- www.pbs.dk/it-services/net

Generel information om net-ID.