

## Dokumentliste med parter og bilag

Sagsnummer	Sagstitel	
Aktnummer	Dokument ID <i>Title</i>	
Brevdato	Type	
Oprettet	Gruppe	Tekst
Svarfristdato	Eventuelle bilag og henvisninger	

### Dokumentets parter

2016-632-0186	Sker der ændringer i NemID, og hvilke konsekvenser har det - Dt af egen drift	
1	384919	<i>Høring</i>
12-05-2016	U	
02-05-2016	TO	

#### Bilag:

384919	384919
--------	--------

Til/Fra	4	Digitaliseringsstyrelsen
---------	---	--------------------------

2016-632-0186	Sker der ændringer i NemID, og hvilke konsekvenser har det - Dt af egen drift	
3	387968	<i>Afsluttende udtalelse</i>
02-06-2016	U	
31-05-2016	TO	

#### Bilag:

387968	387968
--------	--------

Til/Fra	4	Digitaliseringsstyrelsen
---------	---	--------------------------

2016-632-0186	Sker der ændringer i NemID, og hvilke konsekvenser har det - Dt af egen drift	
2	388040	<i>Besvarelse af høring [5 vedhæftede filer]</i>
30-05-2016	I	
31-05-2016	SV	

#### Bilag:

388040	388045
388040	388044
388040	388043
388040	388042
388040	388041
388040	388040

Til/Fra	4	Digitaliseringsstyrelsen
---------	---	--------------------------



Digitaliseringsstyrelsen  
Landgreven 4  
Postboks 2193  
1017 København K

Sendt via Digital Post

12. maj 2016

### Vedrørende den sikkerhed, der opnås ved brug af NemID

Datatilsynet  
Borgergade 28, 5.  
1300 København K

CVR-nr. 11-88-37-29

Telefon 3319 3200  
Fax 3319 3218

E-mail  
dt@datatilsynet.dk  
www.datatilsynet.dk

J.nr. 2016-632-0186  
Sagsbehandler  
Anders Petersen  
Direkte 3319 3221

Datatilsynet er via medieomtale blevet bekendt med, at der tilsyneladende er planer om at ændre på login ved brug af NemID. Der henvises til artiklen på Finans.dk den 28.04.2016 ”Nu bliver det endnu nemmere at bruge dit NemID”<sup>1</sup>. Ifølge artiklen vil man fra juni måned ændre mulighederne i forhold til den personlige kode, så brugerne fremadrettet kan vælge, at den personlige kode kun skal bestå af fire talcifre. I artiklen er bl.a. anført, at den nye kode gælder alle de steder, man plejer at bruge NemID.

Datatilsynet vurderer umiddelbart, at ændringen af sikkerheden omkring login kan have betydning, når NemID anvendes i bl.a. offentlige myndigheders løsninger, hvor sikkerheden skal leve op til persondatalovens krav om datasikkerhed og datakvalitet, dvs. persondatalovens § 41, stk. 3, og § 5, stk. 4.

I den anledning skal Datatilsynet anmode Digitaliseringsstyrelsen om en redegørelse. Det bedes i den forbindelse oplyst:

1. Om der også er tale om en NemID også til offentlig forvaltning (OCES), og i givet fald,
2. hvilke overvejelser der er gjort om ændringens betydning for sikkerheden ved brug af løsningen, herunder i de tilfælde, hvor den anvendes til at give adgang til følsomme personoplysninger hos offentlige myndigheder,
3. om den påtænkte ændring er i overensstemmelse med den gældende certifikatpolitik, eller om denne vil skulle ændres.

Der henvises i øvrigt til tidligere korrespondance mellem IT- og Telestyrelsen/ Digitaliseringsstyrelsen og Datatilsynet om OCES II /NemID-løsningen.

Digitaliseringsstyrelsens udtalelse bedes være tilsynet i hænde senest den 30. maj 2016.

Med venlig hilser

Lena Andersen  
Kontorchef

<sup>1</sup> <http://finans.dk/live/it/ECE8616408/nu-bliver-det-endnu-nemmere-at-bruge-dit-nemid/>

**Fra:** Simon Bruun Hervik [sibrh@digst.dk]  
**Sendt:** 30. maj 2016 22:42  
**Til:** Datatilsynet  
**Cc:** Anders Petersen  
**Emne:** NemID - Henvendelse fra Datatilsynet vedr. ændring i login (DIGST Id nr.: 575887)  
**Vedhæftede filer:** Svar fra Digitaliseringsstyrelsen.pdf; nets-vurdering af risiko vurdering{PwC-GR1xRPI}.pdf; Risikoanalyse password 6 til 4 cifre Final 22082014.pdf; Udleveret til aktindsigt - Risikovurdering + ekstern vurdering.pdf

Til Datatilsynet,

Att. Anders Petersen.

Vedlagt er Digitaliseringsstyrelsen svar på Datatilsynets henvendelse d 12. maj 2016 vedrørende ændringer i krav til adgangskode ved NemID. Samt relevant materiale ift. information undtaget aktindsigt.

Mvh

Simon Bruun Hervik



**Simon Bruun Hervik**  
Fuldmægtig

Mobil +45 41 78 23 45  
[sibrh@digst.dk](mailto:sibrh@digst.dk)

Digitaliseringsstyrelsen  
Landgreven 4  
1017 København K  
[www.digst.dk](http://www.digst.dk)



## Nets – DanID

### Vurdering af "Risikoanalyse for ændring af password i NemID"

#### Baggrund

I forbindelse med etablering og udrulning af en Java Script-baseret klient til NemID er det blevet praktisk muligt at anvende standardklienten på mobile enheder og på sigt på en række ikke pc-orienterede devices. Fælles for disse er, at det kan være meget besværligt eller upraktisk at indtaste et password, der lever op til de nuværende regler for kompleksitet.

Der er derfor i den finansielle sektor et ønske om at genvurdere kravet til passwords, således at der kunne anvendes et firecifret password i stedet for et password på seks karakterer.

PwC er blevet bedt om at vurdere den risikovurdering, som Nets har udarbejdet for ændringen i password-kompleksitet: "Risikoanalyse for ændring af password i NemID" af d. 22. august 2014. I nærværende notat vil vi redegøre for vores vurdering.

Vi har baseret vores vurdering på det udleverede notat. Vi har således ikke haft mulighed for at vurdere styrken og effektiviteten af de foreslæde kompenserende tiltag.

#### Sammenfatning af vores vurdering

Ved vores gennemgang af notatet har vi særligt lagt vægt på den ændring i arkitektur, der er sket siden 1. generation af OCES. Oprindeligt var løsningen baseret på lokalt opbevarede private nøgler, som skulle beskyttes på brugerens pc, og hvor sikkerheden i høj grad var en funktion af passwordet og beskyttelsen af den enkelte maskine, som var uden for NemID's kontrol.

Password-kompleksiteten var derfor den vigtigste beskyttelsesfaktor i den oprindelige løsning.

I dag anvendes der centralt opbevarede private nøgler, hvor både password og nøglekort<sup>1</sup> bidrager til den samlede sikkerhed, men bliver yderligere forstærket af muligheden for sikker programmatisk kontrol med password-afgivelsen samt løbende overvågning og alarmering. Dette giver mulighed for at mindskе password-kompleksiteten, da der er etableret andre sikkerhedsmekanismer, som tilsammen kan give en tilstrækkelig sikkerhed.

Det tilbageværende spørgsmål er derfor, om den foreslæde kompleksitet på fire cifre er tilstrækkelig til at supplere de øvrige tiltag, således at den samlede sikkerhed niveau vil være det samme eller højere, efter de foreslæde kompenserende tiltag er implementeret.

<sup>1</sup> Ved anvendelse af NemID i f.eks. den finansielle sektor kan gives adgang til funktionalitet uden anvendelse af Nøglekort, men denne er begrænset til ikke kritisk læseadgang. Dette er dog ikke relevant for OCES.



Dette er der redegjort for i notatet, hvor der er fremhævet ti væsentlige risikoområder.

Vi har vurderet om disse ti områder dækker alle relevante risici, hvorvidt disse er tilstrækkeligt belyste, og om vi er enige i konklusionen på hvert område. Vi vil nedenfor redegøre for vores vurdering.

***Dækkes alle relevante risici (fuldstændighed)***

Der er udvalgt risici, som direkte bliver påvirket ved ændring af password-kompleksitet, og fravalgt risici, som er ens uanset password-kompleksitet. Dog er der medtaget tre risici (g, h, i), som ikke vil blive påvirket, men som er password-relevante.

Hvad angår angreb mod en bruger, er vi af den opfattelse, at der ikke er udeladt væsentlige risici.

***Er risiciene tilstrækkeligt grundigt belyste***

Det vores opfattelse, at risiciene er tilstrækkeligt grundigt belyste, når de enkelte beskrivelser ses i sammenhæng med risikovurderingens indledende afsnit omkring "Password-styrke" og "Statistik og sandsynlighed for brugervalgte passwords".

***Vurdering af konklusionen for de enkelte områder***

Vi har vurderet, at konklusionerne for de enkelte områder er retvisende, såfremt de foreslæde kompenserende tiltag implementeres med en tilstrækkelig styrke og kvalitet.

**Konklusion**

Vi har ved vores vurdering ikke fundet anledning til at tro, at notatets konklusion ikke er retvisende, såfremt de foreslæde kompenserende tiltag implementeres med en tilstrækkelig styrke og kvalitet.

<b>Notat</b>	Risikoanalyse for ændring af password i NemID	Nets Denmark A/S Lautrupbjerg 10 P.O. 500 DK-2750 Ballerup  T +45 44 68 44 68 F +45 44 86 09 30 www.nets.eu
<b>Til</b>	Digitaliseringsstyrelsen og DanID-udvalget	CVR-nr. 20016175  [REDACTED]
<b>Review</b>	CA-Assurance og IT-solutions.	22. august 2014

**Baggrund** I forbindelse med den forestående levering af NemID JavaScript (JS)-klient, [REDACTED] der i de seneste måneder været drøftelser [REDACTED] [REDACTED] den manglende brugervenlighed ved indtastning af password i NemID JS i forhold til bankernes eksisterende proprietære løsninger på de mobile platforme.

[REDACTED] om ændring af regler for password fra de nuværende minimumskrav om seks karakterer med alfanumeriske værdier til en 4-cifret talkode. Digitaliseringsstyrelsen har som følge heraf bedt Nets DanID udarbejde en risikoanalyse og anbefaling i forhold til dette ændringsforslag.

Dette notat indeholder en analyse af ændringsforslagets eventuelle påvirkning på sikkerheden, samt de tiltag Nets DanID anbefaler at der implementeres i NemID for at opveje den reducerede længde af password, således at det samlede aktuelle sikkerhedsniveau for NemID fastholdes.

**Nuværende politik** Ifølge Nets DanID's gældende password politik "User Id and policy, v.1.3" skal brugeren specificere et password til NemID, som er mellem 6 og 40 karakterer. Password'et kan bestå af en kombination af 26 mulige bogstaver, tallene fra 0 til 9 samt 24 specialetegn og skal indeholde mindst et tal og et bogstav. Der skelnes ikke mellem store og små bogstaver. [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

**Forslag til** Ændringsforslaget fra bankerne går ud på at nedsætte minimumskravet til længden

**ny politik** og kompleksiteten af det brugervalgte password til et 4-cifret tal.

**Konklusion** Det er væsentligt både for Digitaliseringsstyrelsen, bankerne og Nets DanID, at den høje sikkerhed omkring NemID bibeholdes. Borgernes og omverdenens tillid til håndtering af sikkerheden omkring NemID er afgørende.

Ændringen vil givetvis skabe debat omkring sikkerheden om NemID. Nogen vil forventeligt hævde, at der er tale om en forringelse af sikkerheden, idet best practice er at have lange komplekse password i selvbetjeningsløsninger. Specielt når passwordet udgør den eneste adgangsgivende sikkerhedsforanstaltning. Nets DanID vurderer, at ændringen i krav til password kan opvejes af kompenserende tiltag, som er tilstrækkelige til at bibeholde samme sikkerhedsniveau.

Både bankerne og Digitaliseringsstyrelsen er jævnfør persondataloven forpligtet til at beskytte personfølsomme data med fornødne sikkerhedsforanstaltninger. Selvom det samlede tekniske sikkerhedsniveau opretholdes med kompenserende tiltag, er der risiko for kritik og bekymring, som skal imødegås.

#### Analyse af password styrke

Menneskers evne til at huske gode passwords med høj tilfældighed er begrænset. Det betyder, at passwords i praksis ikke er tilfældige.

Entropi<sup>1</sup> er et mål for tilfældighed, som kan bruges til udtale sig om kvaliteten af brugervalgte passwords, og dermed hvor svære de er for en angriber at gætte. Jo højere entropi des stærkere password. For den nuværende password politik er den beregnede entropi<sup>2</sup> 14 bit. Det betyder, at man i gennemsnit<sup>3</sup> skal søge gennem  $2^{13} = 8192$  password for at ramme brugerens password. Tilsvarende har en selv-valgt 4-cifret talkode 10 bits entropi, hvilket medfører at man i gennemsnit skal søge gennem  $2^9 = 512$  password for at finde en brugers password. Til sammenligning skal man for en tilfældig valgt 4-cifret talkode, som eksempelvis en Dankort PIN kode, gennemsøge  $10^{4/2} = 5000$  talkombinationer for at finde frem til den

<sup>1</sup> Entropi er et mål for tilfældighed af en stokastisk variabel. Entropien af password kan bruges til at beregne hvor mange password man forventer at skulle teste for at finde frem til det rigtige password.

<sup>2</sup> Entropi beregningerne er baseret på appendix A i NIST sp-800-63-2: "Electronic Authentication Guidelines"

<sup>3</sup> I gennemsnit skal man søge gennem halvdelen af mængden af passwords før end man finder det rigtige pw. Når entropien er 14 bit forventer man at skulle teste  $2^{(14-1)} = 2^{13}$  passwords.

rette.

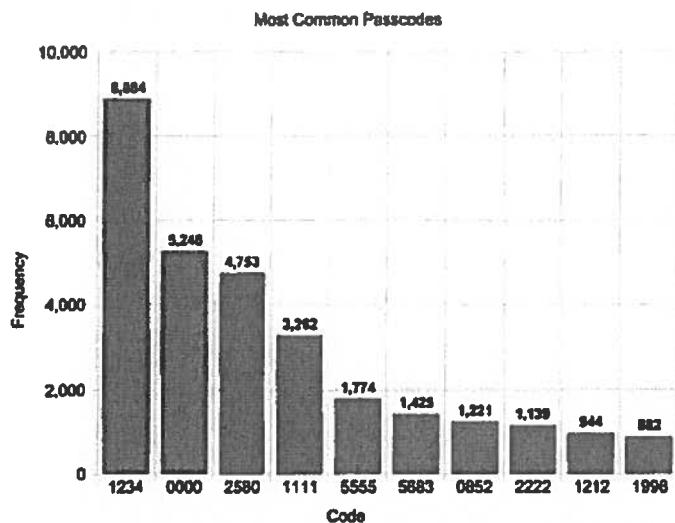
Entropi-beregningen tager imidlertid ikke højde for, at nogle password har en klar overrepræsentation, hvilket man i stedet kan belyse med password statistikker.

#### Statistik og sandsynlighed for brugervalgte password

Der findes forskellige undersøgelser som blandt andet baserer sig på lækkede og crackede password. Nedenfor er angivet to eksempler på sådanne statistikker. Første eksempel er taget fra [www.lifehacker.com](http://www.lifehacker.com). Statistikken grundlag er en lækket password database bestående af 3,4 millioner 4-clfrede passwords. Statistikken viser at password "1234" repræsenterer 10,713% af samtlige passwords i databasen. Det næstmest frekvente password er "1111" og repræsenterer 6,016% af databasens passwords. Samlet set repræsenterer de 5 mest brugte passwords 20,552% af hele databasen. Ved systematisk at gætte på disse fem passwords for alle brugere vil man finde frem til det rette password for hver femte bruger.

#	PIN	Freq.
#1	1234	10,713%
#2	1111	6,016%
#3	0000	1,861%
#4	1212	1,197%
#5	7777	0,745%
#6	1004	0,646%
#7	2000	0,613%
#8	4444	0,526%
#9	2222	0,516%
#10	6660	0,512%
#11	9999	0,451%
#12	3333	0,419%
#13	5555	0,395%
#14	6666	0,391%
#15	1122	0,366%
#16	1313	0,344%
#17	8888	0,333%
#18	4321	0,293%
#19	2001	0,290%
#20	1010	0,285%

Næste eksempel er taget fra [www.danielamitay.com](http://www.danielamitay.com), som er et projekt baseret på 204.508 iPhone passwords, registreret via en applikation. Statistikken begrænser sig ikke til 4-clfrede talkoder, hvilket sandsynligvis er grunden til de lavere procentuelle værdier.

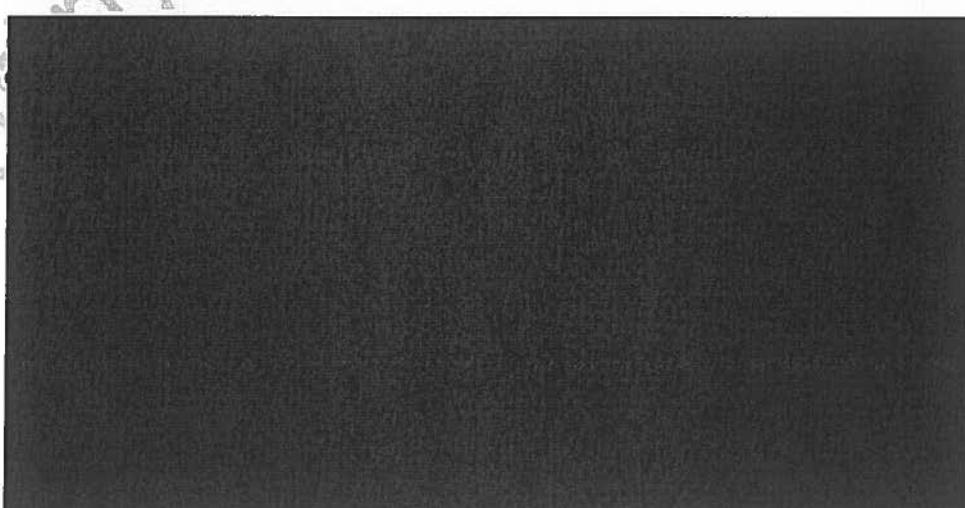


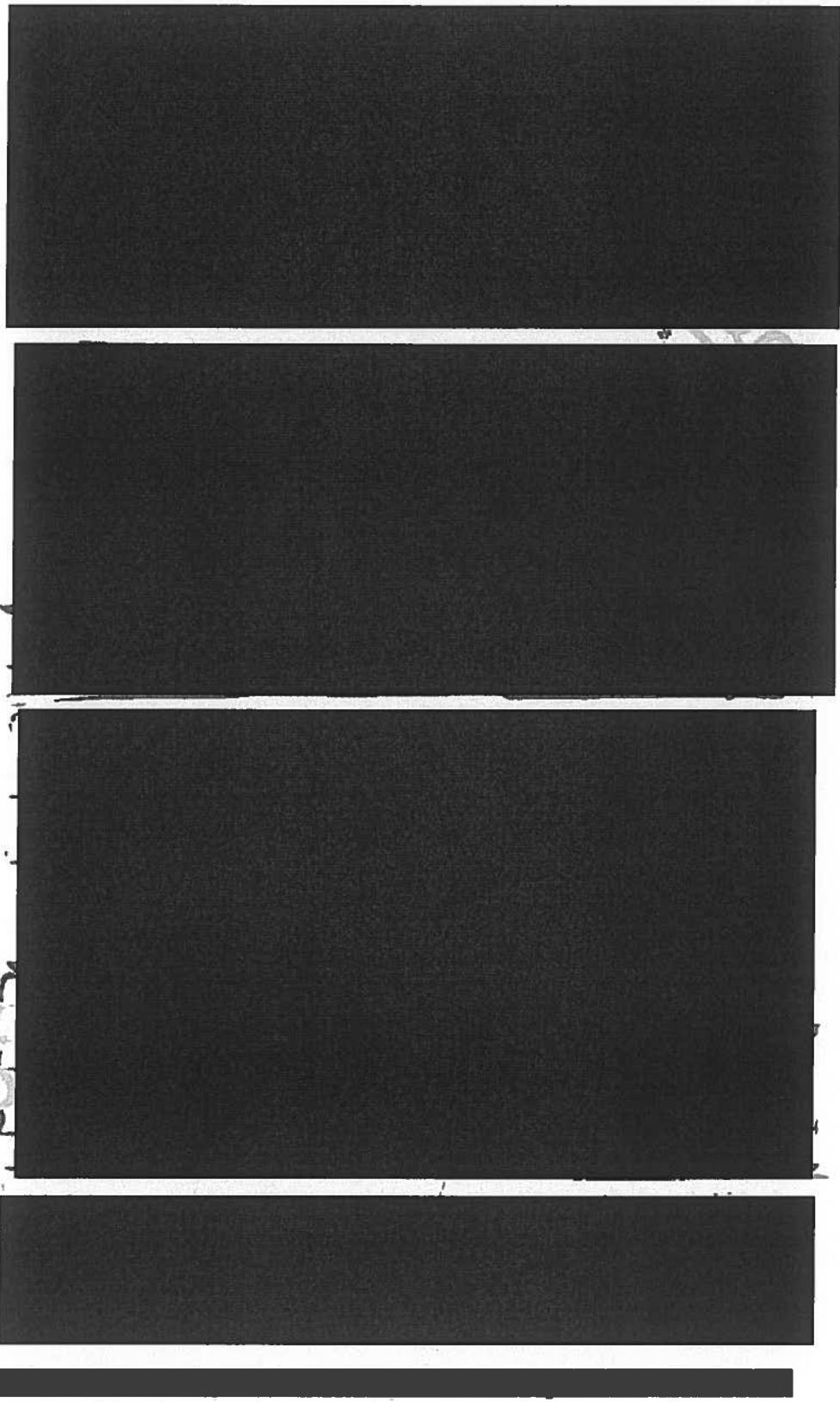
Statistikken viser, at de ti mest brugte iPhone passwords samlet set repræsenterer 15% af alle registrerede passwords.

**Risikoanalyse**

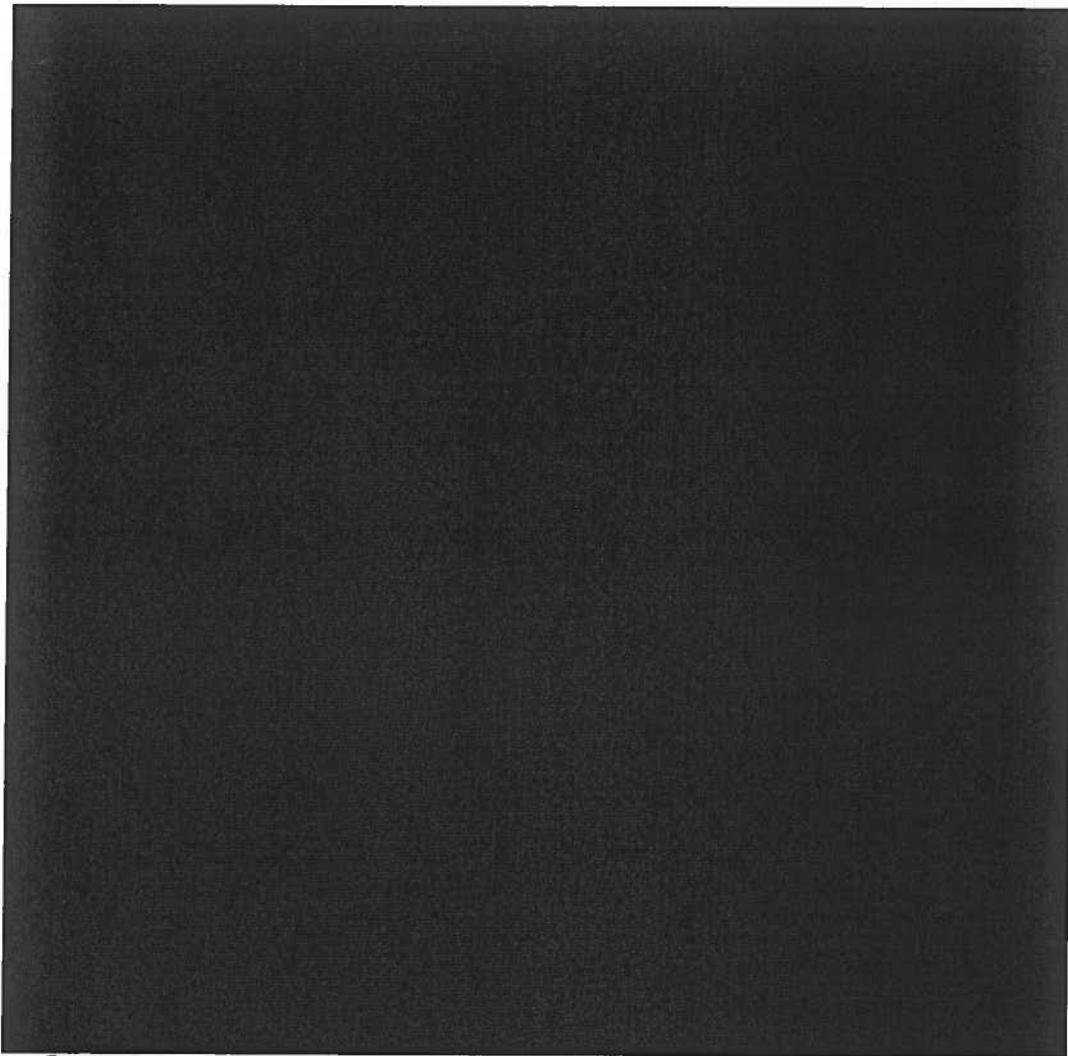
**Trusselsaktører**

Trusselsaktørerne vil være de samme aktører som kendes fra det generelle trusselbillede i NemID. Det vil primært være personer med intention om økonomisk kriminalitet og aktivister med interesse i at udstille sikkerheden omkring NemID som utilstrækkelig. Dertil kommer trusler som stammer fra betroede medarbejdere (Insider) samt spionage og efterretningsvirksomhed.

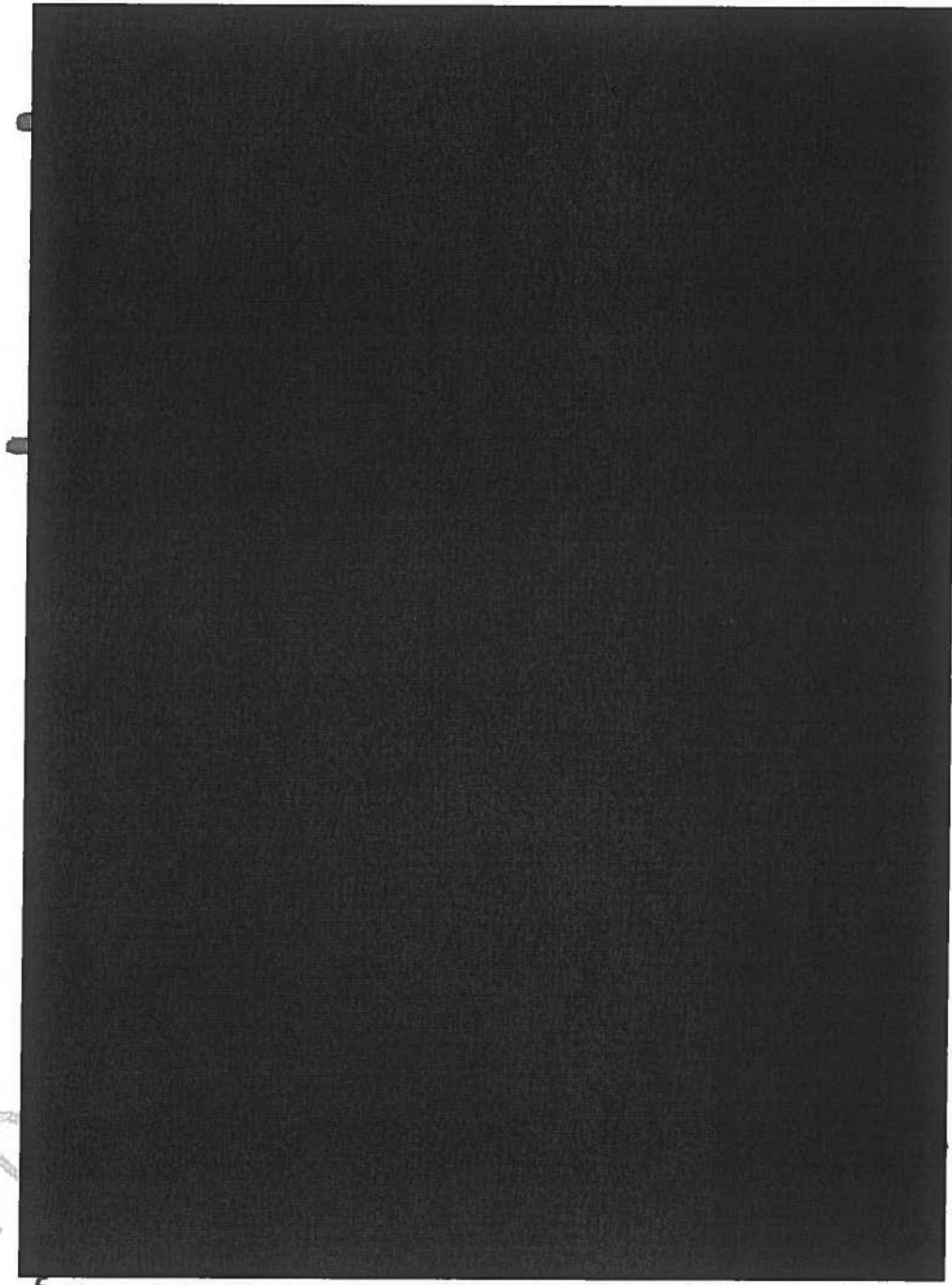


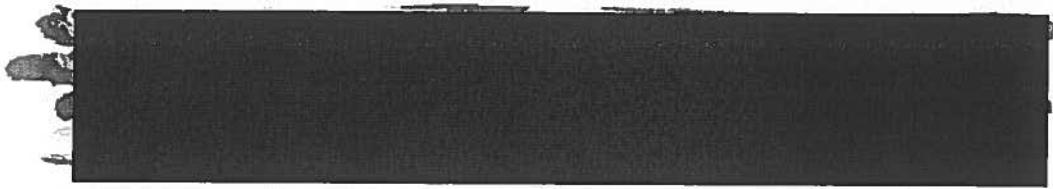


 nets



**8 nets**



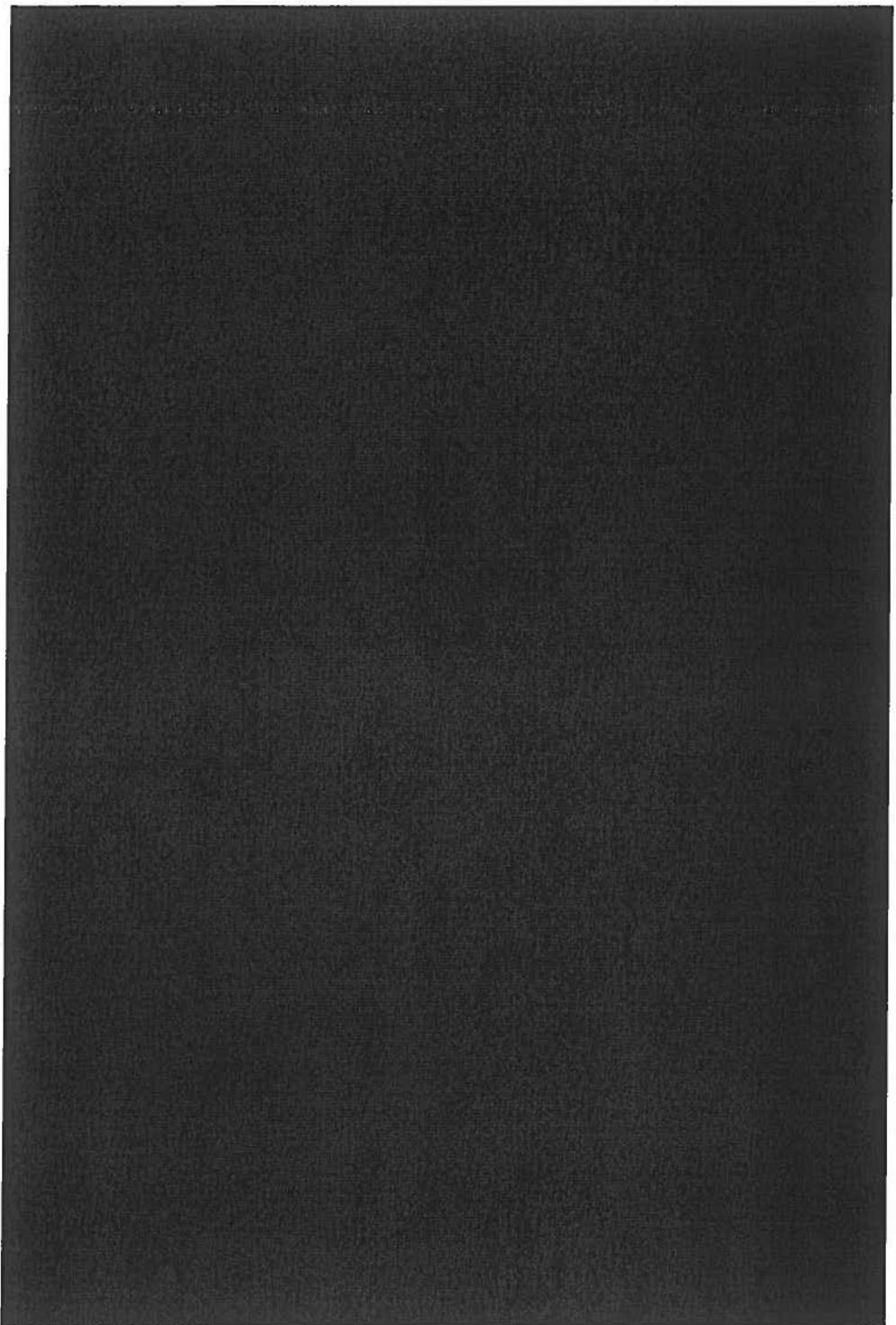


### Opsumming

Nets DanID har i de ovenstående afsnit analyseret risici ved ændrede krav til password og givet anbefalinger til sikkerhedsmæssige tiltag for at opretholde det høje sikkerhedsniveau som NemID er kendtegnet ved. Nets DanID anbefaler på denne baggrund, at det fremlagte ændringsforslag, herunder de kompenserende tiltag, vedtages, idet det samlede sikkerhedsniveau for NemID kan opretholdes.

Tabellen nedenfor giver et overblik over ændring i risici som følge af ændring af krav til password, Nets DanID's forslag til kompenserende tiltag og de heraf resulterende risici.

**Intern brug**



p. 9 - 10

 **e-nets**

The logo consists of a stylized lowercase 'e' enclosed within a circle, followed by the word 'nets' in a bold, lowercase sans-serif font.