Understøttelse af LSS til NemID i organisationen

Table of contents

1 Dette dokuments formål og målgruppe 3

2 Introduktion til LSS til NemID 4
2.1 Forudsætninger hos organisationen 5
2.1.1 SSL og lokal trust 5

3 Krav til implementeringen.....6

Version history

Dec 16th 2016	Version 2.0	MSP
4th April 2014	Version 1.1	MSP
28th March 2014	Version 1.0	MSP
13th March 2014	Version 0.9	BS
4th februar 2014	Version 0.5	MSP

1 Dette dokuments formål og målgruppe

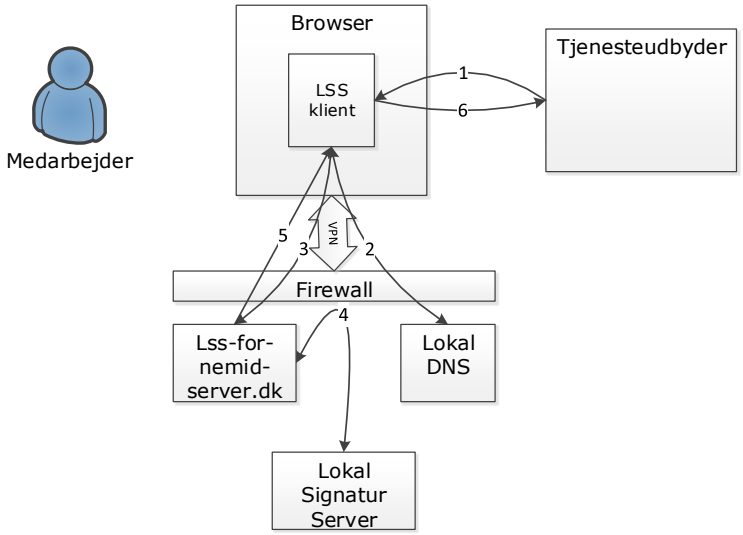
Dette dokument beskriver forhold omkring sikkerhed og skalering af LSS til NemID løsninger som implementeres i den enkelte organisation.

Dette dokument henvender sig til projektleder og IT-sikkerhedsansvarlige i den enkelte organisation.

2 Introduktion til LSS til NemID

LSS til NemID-løsningen muliggør, at organisationer der opbevarer deres medarbejdersignaturer på en lokal signatur server, som understøtter LSS til NemID, kan understøtte medarbejdernes anvendelse af disse medarbejdersignaturer fra mobile devices imod de tjenesteudbydere, som understøtter LSS til NemID. LSS understøttelse er en del af den generelle NemID TU pakke fra Nets fra efteråret 2016.

Løsningen fungerer som illustreret i nedenstående figur.



Figur: Medarbejderens anvendelse af medarbejdersignatur via LSS til NemID

1. Tjenesteudbyder sætter en iFrame op som kalder enten en logon eller en signeringsfunktion hentet fra adressen https://lss-for-nemid-server.dk.

2. Brugerens devices oversætter via den sikre netværksforbindelse til den lokale DNS server på organisationens netværk adressen for lss-for-nemid-server.dk til IP adressen på den lokale LSS for NemID server.

3. iFrame henter Javascript implementeringen af den kaldte logon eller signeringsfunktion, som modtager logon eller signeringsdata fra tjenesteudbyderen

4. Den lokale lss-for-nemid-server.dk autentificerer brugeren og påfører brugerens digitale medarbejdersignatur på logon eller signeringsdata.

5. Logon eller signeringsdata returneres til brugerens device

6. Logon eller signeringsdata returneres til tjenesteudbyderen, som herefter kan fortsætte dialogen med brugeren.

2.1 Forudsætninger hos organisationen

Organisationer som ønsker at understøtte løsningen for sine medarbejdere skal opfylde følgende forudsætninger.

Organisationen skal have de relevante medarbejdersignaturer installeret på et signaturserver-produkt, som understøtter LSS til NemID-løsningen.

Organisationen skal have etableret en lokal lss-for-nemid-server.dk.

Organisationen skal etablere en lokal DNS, som oversætter adressen lss-for-nemid-server.dk til IP adressen på den lokale lss-for-nemid-server.dk.

Organisationen skal tilvejebringe en sikker netværksopkobling til organisationens netværk for de enheder, hvorfra LSS til NemID-løsningen skal anvendes.

Disse enheder skal anvende organisationens lokale DNS, når de er opkoblet, således at lss-for-nemid-server.dk oversættes til IP adressen på den lokale signaturserver.

2.1.1 SSL og lokal trust

Den lokale lss-for-nemid-server.dk bliver kontaktet igennem brugerens browser på adressen https://lss-for-nemid-server.dk.

Det er derfor en nødvendighed, at de brugere, som skal bruge denne service, har tillid til det aktuelle SSL certifikat på denne server.

Dette gøres lettest ved at I får udstedt et certifikat til denne adresse fra jeres egen CA eller jeres LSS leverandørs CA. Derefter skal I etablere i tillid til denne CA i de devices som skal anvendes.

3 Krav til implementeringen

Krav 1	Den sikre netværksforbindelse fra de relevante mobile devices til organisationens netværk skal etableres med anvendelse af to-faktor-autentifikation af brugeren og under opfyldelse af øvrige sikkerhedskrav, som gælder for enheder, der skal tilkobles organisationens sikre netværk.

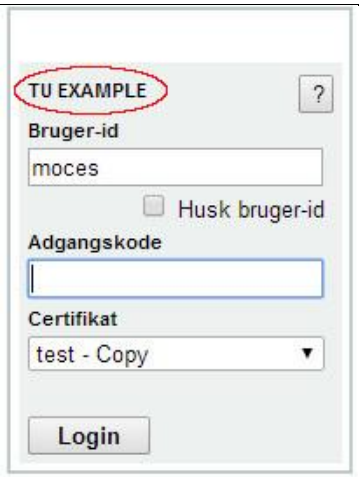
Krav 2	De relevante mobile devices, hvorfra LSS til NemID-løsningen skal anvendes, skal være sikret imod skadelig software og som udgangspunkt være underlagt organisationens mobil device management system for sikring af platform og data. De mobile devices skal konfigureres således at deres SSL trust list kun omfatter nødvendige SSL certifikat udstedere, herunder den udsteder der anvendes til organisationens lss-for-nemid-server.dk.

Krav 3	De relevante krav fra OCES certifikat politikkerne skal opfyldes af den samlede løsning.

Krav 4	Organisationen er selv ansvarlig for, at organisationens installation og netværk understøtter den ønskede skalering og performance for organisationens medarbejdere.

Krav 5	Organisationen skal etablere drift af den lokale lss-for-nemid-server.dk indenfor en perimeterbeskyttelse der opfylder organisationens sikkerhedspolitik for perimeterbeskyttelse. Herunder skal sikkerheds risici ved angreb fra interne privilegerede brugere indgå i en risikoanalyse.

Krav 6	Organisationen skal uddanne sine brugere i almindelig sikkerhed adfærd på nettet og særligt i risici for social engineering og phishing, således at brugerne bliver i stand til at identificere og afvise sådanne typer af angreb. Særligt skal brugerne informeres om at de aldrig må udlevere deres forskellige bruger-id og passwords hørende til den sikre netværksopkobling eller medarbejdersignatur. Brugerne skal instrueres om, at de hurtigt skal informere organisationen hvis et mobil device anvendt til LSS for NemID er stjålet eller tabt. Brugerne skal også informeres om LSS til NemID brugergrænsefladen, herunder at de for at identificere eventuelle svindlere skal validere, at "log on to" teksten stemmer med den tjeneste som brugeren forventer at logge på. Illustreret herunder, hvor brugeren er ved at logge på tjenesten "TU Example".

Krav 7	Organisationen skal implementere en styring af hvilke applikationer brugerne får installeret på deres mobile devices og tilse at disse er sikre. Organisation skal særligt inspicere apps som understøtter NemID til LSS for at validere, at disse virker sikkerhedsmæssigt forsvarligt og understøtter korrekt visning af logon og signeringsforespørgsler.

Krav 8	Såfremt organisationen modtager besked om nødvendige sikkerhedsopdateringer fra sin leverandør af løsningen, eller fra andre software leverandører som anvendes i løsningen, skal organisationen iværksætte disse opdateringer uden unødvendig ophold.