Innspill til videre arbeider med strategi for eID og e-signatur i offentlig sektor

---

NovaSecure AS

Skrevet: 21 Mai, 2007

Forfatter: Kåre Langedrag

Innledning

Selskapet NovaSecure AS er et privat selskap som besitter flere års erfaring med rådgivning, systemutvikling og etablering av løsninger basert på PKI i Norge.

Med bakgrunn i erfaringer og kompetanse som vi har opparbeidet gjennom nåværende og tidligere arbeidsgivere så har vi gått gjennom kravene som stilles til dagens PKI-løsninger i Norge, og vurdert disse kravene opp mot internasjonale kryptotekniske anbefalinger.
.
I vår konklusjon så anbefaler vi krav om sikker tidsstempling av signerte dokumenter, og vi anbefaler at kravene til nøkkellengder for digital signatur og kryptering økes.

Bakgrunn

I 2001 så leverte Arbeids og Administrasjons-departementet utredningen Uten penn og blekk [NOU 2001:10] som markerte starten på tilretteleggingen for bruk av elektronisk kommunikasjon i offentlig forvaltning. SEID-prosjektet startet i november 2003, initiert av Nærings- og handelsdepartementet og var et samarbeid mellom 16 aktører i privat og offentlig sektor. SEID utarbeidet standarder for PKI-sikkerhetsløsninger i Norge. På bakgrunn av leveransene til SEID så utarbeidet Moderniseringsdepartementet Kravspesifikasjon for PKI i offentlig sektor [KRAV-PKI] som ble levert i Januar 2005.

I mars 2007 så ble dokumentet Strategi for eID og e-signatur i offentlig sektor lagt ut for høring. Mandatet legger til grunn en teknologinøytral forståelse av begrepene ”eID” og ”e-signatur”, men vi har likevel valgt å komme med teknologiske innspill som er direkte knyttet til de-facto løsninger for e-signatur i Norge i dag.

Det er verdt å merke seg at det er vanlig å benytte 1024 bits RSA [RSA] nøkler for å oppnå konfidensialitet ved utveksling av meldinger i dag. I følge den norske Kravspesifikasjonen for PKI i offentlig sektor [KRAV-PKI] så bør bør asymmetriske nøkler være basert på RSA og minst ha en nøkkellengde på 1024 bit. Vi vurderer i denne rapporten disse kravene opp mot eksisterende internasjonale standarder for nøkkellengde i dag og i fremtiden.

Den samme spesifikasjonen setter ikke noe absolutt krav til å tiddstempling av meldinger, og beskriver heller ikke i detalj kravene til en slik løsning. Vi belyser i denne rapporten problemstillinger knyttet til bruk av PKI uten en tiltrodd og sikker tidsstemplingstjeneste.

Konfidensialiteten er tidsbegrenset og avhenger av nøkkellengde

Eksisterende krav og anbefalinger for PKI har stor fokus på e-signatur i forhold til kryptering, til tross for at konfidensialitet er en rammebetingelse for mange som tar i bruk PKI. Begrepet konfidensialitet må alltid knyttes til en tidsperiode. Konfidensiell informasjon er tidsbegrenset i sin natur, og i tillegg er det kryptotekniske begrensninger for hvor lenge vi kan beskytte informasjon. Det er derfor viktig å vurdere konfidensialitetskrav opp mot krav til kryptonøkler (RSA-nøkler).

Nøkkellengden er en viktig sikkerhetsparameter ved bruk av PKI. Det finnes en hel rekke publikasjoner om krav til nøkkellengder som man kan ta utgangspunkt i for sette krav til en løsning. Anbefalingene i publikasjonene varierer noe, men det er likevel enkelt å få et bilde av hva som burde være et minimumskrav ved bruk av PKI i dag. Lesere henvises til eget avsnitt med referanser til publikasjoner som kan benyttes som utgangspunkt for å fastsette krav til nøkkellengder. Tallene som benyttes videre i dette avsnittet har tatt utgangspunkt i disse publikasjonene.

Hvis vi for eksempel tar utgangspunkt i at en kryptert melding skal være beskyttet (eller burde holdes konfidensiell) i tyve år, fra 2007 frem til og med 2027, så vil anbefalingene om nøkkellengde variere enormt. Vi har sett at den anbefalte nøkkellengden varierer helt fra 1600 bit helt opp til ca 3500 bit, mens de fleste ligger rundt 2000 bit. Ut fra dette burde vi kunne trekke konklusjonen at ca. 2000 bit burde være minimum nøkkellengde for kryptering.

Det er verdt å understreke at samtlige av de refererte publikasjonene anbefaler en større nøkkellengde enn 1024 bit ved kryptering av meldinger. Det er også verdt å merke at kravspesifikasjonen til Nasjonal Sikkerhetsmyndighet [NSM Krypto] krever 2048 bits nøkler for å oppnå et moderat sikkerhetsnivå ved kryptering. Det samme gjelder for nøkler som benyttes for signering etter 1. Juli 2008.

Ikke-benekt betinger tiltrodd og sikker tidsstempling

Å kunne realisere ikke-benekt ved bruk av digital signatur som lagres over lengre tid krever spesielle tiltak. Signaturer som utføres med 1024 bits nøkler i dag *kan* i løpet av relativt få år være vanskelige å bevise (Ref. eget avsnitt for beregning av nøkkelstyrke). Selv med nøkkellengder på 2048 bit så vil man måtte basere seg på optimistiske antagelser for å anta at de er tilfredsstillende sikre om 20 år. Videre er ikke de-facto HASH-algoritmen SHA-1 tilstrekkelig til å kunne holde i så mange år. En del av kravene i europeisk standard for signaturformater [ETSI ES 201 733] tar høyde for dette. En viktig del av tiltakene innebærer bruk av en tiltrodd tidsstemplingstjeneste som gjør en ekstra (og sterkere) signatur over hele meldingen og tidsstemplet.

Også på kort sikt kreves det tiltak for å realisere ikke-benekt. Når et sertifikat har gått ut på dato eller blir revokert så kan det være umulig å bevise om en signaturer som er ugyldig(!). Bruce Schenier [RISK-PKI] påpeker denne utfordringen i sitt dokument "Ten risks of PKI". Kort fortalt; hvis en digital ID har gått ut på dato, har kommet på avveie, eller på en annen måte har blitt revokert, så kan man ikke føre et kryptografisk bevis for at en melding faktisk ble signert mens sertifikatet var gyldig – eller motsatt. Bruk av en sikker tidsstemplingstjeneste vil gjøre det umulig å signert et dokument med gammel dato.

Ved å bruke utvidede meldingsstandarder og tiltrodde tidsstempler løser man begge problemene som finnes i dag. Tiddstempling binder signaturen til et tidspunkt (før eller etter gyldighetsperioden) og det forlenger levetiden til den digitale signaturen.

Konklusjon

For å kunne oppnå tilstrekkelig bevisførsel ved ikke-benekt så anbefaler vi at man setter krav til bruk av ***sikker tidsstemplingstjeneste av signerte dokumenter*** så rask som mulig etter mottak og/eller sending av signerte dokumenter.

Vi anbefaler videre at ***nøkkellengde for digital signatur og økes*** og at man så fort som mulig tar i bruk minst 2000 bits nøkler for kryptering.

På sikt burde man kreve sterkere HASH-algoritme, for eksempel SHA-256. Man burde også se på muligheten for å gå over fra 3DES til AES (min 128 bit nøkler) symmetriske nøkler og ECC asymmetriske nøkler.

Referanser

[KRAV-PKI] Moderniseringsdepartementet: Kravspesifikasjon for PKI i offentlig sektor, Versjon 1.02, Januar 2005

[RISK-PKI] By Carl Ellison and Bruce Schneier: Ten Risks of PKI: What Youíre not Being Told about Public Key Infrastructure

[RFC 3161] Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)

[NOU 2001:10] Arbeids- og administrasjonsdepartementet: Uten penn og blekk - Bruk av digitale signaturer i elektronisk samhandling med og i forvaltningen

[NSM Crypto] Norwegian National Security Authority: NSM Cryptographic Requirements

[ETSI ES 201 733] ETSI: Electronic Signature Formats

[RSA] RSA Laboratories: PKCS #1 RSA Cryptography Standard

Referanser for krav til nøkkellengder

[Lenstra] Arjen K. Lenstra and Eric R. Verheul: Selecting Cryptographic Key Sizes, PKC2000: p. 446-465, 01/2000.

[Lenstra Upd] Arjen K. Lenstra: forthcoming Handbook of Information Security, 06/2004.

[ECRYPT] Yearly Report on Algorithms and Keysizes (2005), D.SPA.16 Rev. 1.0, IST-2002-507932 ECRYPT, 01/2006 updated by Yearly Report on Algorithms and Keysizes (2006), D.SPA.21 Rev. 1.1, 02/2007 (Internal Draft).

[NIST] Recommendation for Key Management, NIST Special Publication 800-57 Draft, 05/2006.

[DCSSI] DCSSI - Mécanismes cryptographiques - Règles et recommandations "standard", Rev. 1.02, 11/2004.

[NSA] Fact Sheet Suite B Cryptography, NSA, RSA Conference, 02/2005.

[RFC3766] H. Orman, P. Hoffman, Determining Strengths For Public Keys Used For Exchanging Symmetric Keys, BCP 86, RFC 3766, 04/2004.