Universitetet i Oslo
IN2120 Informasjonssikkerhet
Høst 2023
Teoretiske oppgaver

Teori 4: (Del 4): Nøkkelhåndtering og PKI

Oppgave 1: Sertifikater

a. Hvorfor er det viktig å ha relativt begtrensede kryptoperioder for nøkler, og også hvorfor kryptoperioden for noen nøkler heller ikke bør være for kort ? Nevn fire grunner for å ha begrenset kryptoperiode, og en grunn for å ha lang kryptoperiode.
b. Hva menes med periodene for beskyttelse og prosessering ved bruk av kryptonøkler? Gå til nsm.no med din favorittnettleser. I de fleste nettlesere kan du klikke på hengelåsen på adresselinjen for å se serversertifikatet (X.509-sertifikat for offentlig nøkkel). (I Edge må du trykke på knappen med tre horisontale prikker øverst til høyre, deretter trykke på knappen (Settings/Innstillinger), deretter trykke på knappen (privacy, search and services) i venstre marg, og til slutt skrolle ned til «Security» og «Manage certificates». Finn sertifiseringskjeden og klikk på rotsertifikatet. Sjekk detaljer for rotsertifikatet for å se gyldighetsperioden, som tilsvarer kryptoperioden for den offentlige nøkkelen.
c. Hva er gyldighetsperioden (fra/til) for rotsertifikatet?
d. Den private signaturnøkkelen for rotsertifikatet ble brukt til å signere det mellomliggende CA-sertifikatet. Sjekk datoen for utstedelsen av det mellomliggende CA-sertifikatet. Vil du si at gyldighetsperioden for den private signaturnøkkelen i rotsertifikatet følger anbefalingene for beskyttelsesperioden (OUP) for private signaturnøkler i henhold til NIST SP800-57?
e. Hvis man antar at kraftige kvantekomputere vil være praktisk tilgjengelig rundt 2030, er gyldighetsperioden av rotsertifikatet fornuftig? Hva måtte gjøres med rotsertifikatet hvis kraftige kvantecomputere ble tilgjengelig rundt 2030?
f. Bruk tjenesten på https://www.ssllabs.com/ssltest/ til å teste kvalitet på sertifikat og TLS-tjener på nettstedene **nsm.no** og **universitetsforlaget.no**. Sammenlign resultatene.

Oppgave 2: Tillitsmodell

a. Beskriv tillitsmodellen for PKI'en som brukes av nettlesere.
b. Nevn fordeler og ulemper ved denne modellen.
c. Man sier at nøkkelsertifikater og PKI skaper tillit. Hva menes med dette?

Oppgave 3: Sikkerhet for kryptonøkler

a. Nevn faktorer som bestemmer styrken på kryptografiske sikkerhetsløsninger.
b. Hvorfor er nøkkelhåndtering viktig for kryptografiske sikkerhetsløsninger?
c. Tre viktige nøkkelkategorier er: i) symmetriske hemmelige nøkler, II) asymmetriske offentlige nøkler og III) asymmetriske privatnøkler. Forklar hvilken type sikkerhet tjenester/beskyttelse (dvs. konfidensialitet, integritet og autentisitet) som kreves for hver nøkkelkategori.
d. Beskriv sikkerhetstiltak som kan brukes til å beskytte kryptografiske nøkler.

Oppgave 4: Nøkkeltyper

Se på de 19 nøkkeltypene beskrevet i Tabell 1, s.45,46,47 i NIST SP800-57
https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final

a. Hva er en nøkkeltransportnøkkel (key-transport key) (for nøkkelinnkapsling) ?
b. Nøkkeltypene 10 og 11 kalles henholdsvis privat nøkkel-transportnøkkel og offentlig nøkkel-transportnøkkel. I hvilken type kryptosystem (illustrert i figur 4.10 i læreboka) brukes disse nøkkeltypene?
c. Hva er fremoverhemmelighold, og kan kryptosystemet i b) gi «fremoverhemmelighold»?

Diagrammet for nøkkeltilstander og overganger mellom tilstander i figur 3, s.80, NIST SP800-57 (også vist i figur 5.2 i læreboka) indikerer at når en nøkkel er i aktiv tilstand, kan den angis til bare beskytte, bare prosessere eller begge deler.

d. Hvilke nøkkeltyper er kun ment for å beskytte?
e. Hvilke nøkkeltyper er kun ment for å prosessere?
f. Hvilke nøkkeltyper er ment for både å beskytte og prosessere?

Oppgave 5: CA-autorisering

a. Hvilket problem er løst med CA-autorisering (CAA) og sertifikat-transparens?
b. Hvor lagres CA’ens autoriseringspolicy?
c. Hva er OSCP-sertifikater, og hva menes med «must staple»?

Oppgave 6: Sertifikater og tillit

a. Forklar hvordan offentlig-nøkkel sertifikater kan garantere autentisitet av offentlige nøkler.
b. Hvilke betingelser bør man sette for å ha tillit til et digitalt sertifikat? Begrunn ditt svar.
c. Rotsertifikater er selvsignert. Gir det tillit, eller hvordan skal man få tillit til rotsertifikater?

Oppgave 7: Sertifikater i nettlesere

Tilgang til lagrede rotsertifikater i nettleseren din(e) er via nettlesermenyene. Se gjennom rotsertifikater som er installert i webleseren for å se deres utløpsdatoer.
Metode for å inspisere rotsertifikater

Chrome: Select «Update»  in the top right corner. → Settings → Privacy and Security → Security → Manage Certificates → Trusted Root Certification.

Microsoft Edge: Se fremgangsmåte i oppgave 1.

Firefox: Select «Menu button»  in top right corner. → Settings → Security & Privacy → Scroll down to Certificates → View Certificates → Authorities → View

a. Hvor mange rotsertifikater er installert? Variere for eksempel mellom Firefox og Chrome?
b. Hvilke sertifikater har kort levetid?
c. Kan du finne sertifikater med utløpsdato i overkant av ti år fra nå?
d. Kan du finne sertifikater som allerede har utløpt? Hva skjer når du inspiserer dem?

Oppgave 8: Sertifikatrevokering

a. Hvorfor er det nødvendig å tillate revokering / tilbakekallelse av sertifikater?
b. Hvilke problem er løste med «must-staple protokollen»?