Digitaaliset allekirjoitukset mobiiliympäristössä

Taneli Virkkala

Kandidaatin tutkielma
HELSINGIN YLIOPISTO
Tietojenkäsittelytieteen laitos

Helsinki, 21. helmikuuta 2014

HELSINGIN YLIOPISTO — HELSINGFORS UNIVERSITET — UNIVERSITY OF HELSINKI

Tiedekunta — Fakultet — Faculty	Laitos — Institution — Department
Matemaattis-luonnontieteellinen	Tietojenkäsittelytieteen laitos

Tekijä — Författare — Author
Taneli Virkkala

Työn nimi — Arbetets titel — Title

Digitaaliset allekirjoitukset mobiiliympäristössä

Oppiaine — Läroämne — Subject
Tietojenkäsittelytiede

Työn laji — Arbetets art — Level	Aika — Datum — Month and year	Sivumäärä — Sidoantal — Number of pages
Kandidaatin tutkielma	21. helmikuuta 2014	4

Tiivistelmä — Referat — Abstract

Tiivistelmä.

Avainsanat — Nyckelord — Keywords
avainsana 1, avainsana 2, avainsana 3

Säilytyspaikka — Förvaringsställe — Where deposited

Muita tietoja — Övriga uppgifter — Additional information

Sisältö

1 Johdanto

Digitaalisten allekirjoitusten käyttö on noussut huomattavasti mobiililaitteilla nykypäivänä. Mobiiliympäristössä turvallinen yhteys on varmistettava, koska tietoturvariskit langattomissa verkoissa ovat erittäin suuret [SY13]. Teknisen kehityksen ansiosta allekirjoitusten luonti mobiililaitteilla on yleistynyt, ja erityistä tietoturvaa vaativat toimenpiteet ovat tulleet mahdollisiksi. PC:llä käytettävät protokollat kuten PKI-malli ovat siirtyneet mobiiliympäristöön sellaisenaan, eivätkä nämä protokollat ole tarvinneet suuria muutoksia toimiakseen. Kehittyneemmän laskentatehon ansiosta monet algoritmit kuten RSA ja Diffie-Hellman ollaan pystytty ottamaan käyttöön kannettavilla laitteilla [SY13]. Palvelimille voidaan silti delegoida operaatiot, joita laitteella ei pystytä suorittamaan. Huolimatta siitä tehdäänkö allekirjoitus palvelimella vai asiakkaan laitteessa, tulee allekirjoituksen täyttää kaikki sille asetetut ehdot tietoturvaa koskien. Palvelinpohjaisen allekirjoituksen yleensä luo välissä oleva kirjautumispalvelin eikä lopullinen palveluntarjoaja [SSA10].

Digitaalisten allekirjoitusten käyttö mobiiliympäristössä tulisi olla nopeaa ja turvallista. Monet nykyaikaiset sovellukset voivat vaatia jokaisen viestin lähetyksen yhteydessä uuden allekirjoituksen. Esimerkkinä tästä voisi toimia eräänlainen huutokauppasovellus, jossa jokaisen huudon on oltava kiistaton ja todennettu. Lisäksi viestin sisältämän datan tulee olla yhtenäistä. Varmenteet eivät voi siis kokonaan korvata asiakkaan tunnistamista. Sen sijaan jokainen allekirjoitus tarvitsee varmenteen toimiakseen [SSA10].

Schwabin ja Yangin mukaan mahdollisia tietoturvariskejä mobiiliympäristössä ovat urkinta, mies välissä -hyökkäys, datan muuntaminen, toisena osapuolena esiintyminen ja laitteen kadottaminen [SY13]. Näitä riskejä vastaan tulee mobiililaitteen sisäisen toiminnan ja verkkoviestinnän olla turvallista. Jos palvelun tarjoajan ja asiakkaan välissä on välityspalvelin, siihen tulee myös muodostaa luotettava yhteys. Koska digitaaliset allekirjoitukset perustuvat julkisen avaimen protokollaan, on äärimmäisen tärkeää pitää salainen avain mahdollisimman piilossa. Laitteen SIM-kortti on turvallinen paikka säilyttää salaista avainta, sillä silloin se ei paljastu laitteen käyttöjärjestelmälle. Laitteen prosessorin luoma avain sekä allekirjoitus paljastuvat aina käyttöjärjestelmälle. Sen sijaan prosessorilla laskenta on nopeampaa kuin SIM-kortilla [SSA10].

Sekä RSA että Diffie-Hellman käyttävät jakojäännösmenetelmää salauksessa. Diskreetin logaritmin avulla ulkopuolinen tunkeutuja ei voi tietää puuttuvaa alkulukua. Luvun arvaamiseen kuluisi polynomisen ajan verran nykyaikaisilla algoritmeilla. Diffie-Hellmanin algoritmia käytetään julkisen avaimen vaihtoon ja RSA puolestaan perustuu yksityisen avaimen luontiin asymmetrisen salauksen mahdollistamiseksi. Digitaalisessa allekirjoituksessa sekä datan että salauksen tiivisteen tulee olla samat, jotta voidaan varmistaa allekirjoituksen pätevyys. Tiivisteen laskemiseen käytetään erilaisia tiivistefunktioita kuten SHA-2 tai MD5 [LCJ04].

2 Digitaalisen allekirjoituksen määritelmä

Digitaalinen allekirjoitus on menetelmä, jolla voidaan todentaa tietyn lähettäjän lähettäneen viestin vastaanottajalle muuttumattomana. Allekirjoituksen ja datan tiivisteestä voidaan varmentaa tiedon muuttumattomuus ja todentaa lähettäjän kiistämättömyys [Cam03]. Jos tieto allekirjoituksessa tai tiivisteessä muuttuu, vastaanottajan avaimella purettu viesti ei ole ymmärrettävässä muodossa enää. Seuraavien ehtojen on oltava voimassa allekirjoituksessa: uskottavuus, muuttumattomuus, kertakäyttöisyys ja kiistattomuus [TX10]. Digitaalisella allekirjoituksella voidaan siis todentaa vain yksi viesti kerrallaan ja jokaiselle viestille on luotava uusi allekirjoitus.

2.1 PKI-malli

Julkinen ja salainen avain muodostavat PKI-mallin. Digitaalinen allekirjoitus perustuu tähän malliin ja siksi salaisen avaimen on pysyttävä vain lähettäjän hallussa. Sen sijaan julkinen avain annetaan vastaanottajalle, joka voi purkaa salatun viestin ja laskea tiivisteet. Koska avainten luomiseen käytetään monimutkaisia algoritmeja kuten RSA, on toisen identtisen avainparin syntyminen erittäin epätodennäköistä. Allekirjoitus voidaan liittää viestiin tai lähettää erillisenä [Cam03].

2.2 RSA

Menetelmän kehittäjien sukunimien mukaan nimetty RSA on salausalgoritmi, joka jakojäännöksen avulla hoitaa salauksen ja purkamisen. Aluksi valitaan kaksi alkulukia p ja q, jotka eivät saa olla samat. ksens

Lähteet

[Cam03] Campbell, S.: *Supporting digital signatures in mobile environments.* Teoksessa *Enabling Technologies: Infrastructure for Collaborative Enterprises, 2003. WET ICE 2003. Proceedings. Twelfth IEEE International Workshops on*, sivut 238–242, June 2003.

[LCJ04] Lei, Yu, Chen, Deren ja Jiang, Zhongding: *Generating Digital Signatures on Mobile Devices.* Teoksessa *Proceedings of the 18th International Conference on Advanced Information Networking and Applications - Volume 2*, AINA '04, sivut 532–, Washington, DC, USA, 2004. IEEE Computer Society, ISBN 0-7695-2051-0. `http://dl.acm.org/citation.cfm?id=977394.977538`.

[SSA10] Samadani, Mohammad Hasan, Shajari, Mehdi ja Ahaniha, Mohammad Mehdi: *Self-Proxy Mobile Signature: A New Client-Based Mobile Signature Model.* Teoksessa *Proceedings of the 2010 IEEE 24th International Conference on Advanced Information Networking and Applications Workshops*, WAINA '10, sivut 437–442, Washington, DC, USA, 2010. IEEE Computer Society, ISBN 978-0-7695-4019-1. `http://dx.doi.org/10.1109/WAINA.2010.125`.

[SY13] Schwab, David ja Yang, Li: *Entity Authentication in a Mobile-cloud Environment.* Teoksessa *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop*, CSIIRW '13, sivut 42:1–42:4, New York, NY, USA, 2013. ACM, ISBN 978-1-4503-1687-3. `http://doi.acm.org/10.1145/2459976.2460024`.

[TX10] Tianhuang, Chen ja Xiaoguang, Xu: *Digital signature in the application of e-commerce security.* Teoksessa *E-Health Networking, Digital Ecosystems and Technologies (EDT), 2010 International Conference on*, nide 1, sivut 366–369, April 2010.