Digitaaliset allekirjoitukset mobiiliympäristössä

Taneli Virkkala

Kandidaatin tutkielma
HELSINGIN YLIOPISTO
Tietojenkäsittelytieteen laitos

Helsinki, 24. 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	24. helmikuuta 2014	7

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. Menetelmä on turvallisimpia tapoja varmentaa luotettava viestinkulku vastaanottajan ja lähettäjän välillä. Sen sijaan allekirjoitus on raskan luoda, joten menetelmä vaatii merkittävää laskentatehoa toimiakseen [SSA10].

2.1 PKI-malli

Julkinen ja salainen avain muodostavat PKI-mallin [RB12]. 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 alkulukua p ja q, jotka eivät saa olla samat. Näiden lukujen tulo on N, jonka jälkeen valitaan kokonaisluku e väliltä $1 < e < N$.

2.3 Mobiilikaupankäynti

Mobiilikaupankäynnillä tarkoitetaan mobiililaitteella tehtäviä maksutransaktioita tai ostotapahtuman vahvistavia viestejä. Menetelmä on siis osa elektronista kaupankäyntiä, jossa käytetään digitaalisia allekirjoituksia [TX10]. Schwab ja Yang toteavat suurten datamäärien varastoinnin olevan yleistä nykyaikaisilla mobiililaitteilla [SY13]. Samadanin, Shajarin ja Ahanihan artikkelissa esitellään huutokauppasovellus, joka vaatii jokaisen huudon varmistuksen lyhyen ajan sisällä [SSA10]. Allekirjoitusten luonti tulee olla siis nopeaa mobiililaitteilla tietoturva huomioon ottaen. Sekä laitepohjaisia että palvelinpohjaisia allekirjoituksia käytetään mobiilikaupankäynnissä [SSA10].

3 Laitepohjaiset allekirjoitukset

Mobiililaite koostuu SIM-kortista ja laitteesta, jossa allekirjoituksen luonti tapahtuu prosessorilla. Tietoturvan kannalta SIM-korttia voidaan pitää parempana vaihtoehtona, mutta nopeudessa allekirjoitusten luontia koskien prosessori on tehokkaampi. Salaisen avaimen säilytyspaikka tulee kuitenkin valita turvallisesti, jotta ulkopuolinen tarkkailija ei saa tietää salaista avainta. Lisäksi on olemassa malli, jossa SIM-kortti ja laitteen prosessori yhdessä osallistuvat allekirjoituksen luontiin (hybridimalli) [SSA10].

3.1 SIM-kortilta luonti

Laitteen SIM-korttia voidaan pitää turvallisimpana paikkana säilyttää salaista avainta. Digitaalisen allekirjoituksen luomisessa kuitenkin avain joudutaan hetkellisesti näyttämään laitteen käyttöjärjestelmälle. Pieni tietoturvariski on siis olemassa käyttöjärjestelmää koskien. Lisäksi SIM-kortin laskentakapasiteetti on huomattavasti pienempi kuin laitteen prosessorin. ??????

3.2 Laitteen prosessorilta luonti

Salaisen avaimen säilytys voi tapahtua myös laitteen muistissa. Digitaalinen allekirjoitus luodaan tällöin laitteen prosessorilla, joka on laskentateholtaan huomattavasti tehokkaampi kuin SIM-kortti. Laitteen käyttöjärjestelmässä voi kuitenkin olla tietoturva-aukko, jota hyväksikäyttäen tunkeutujat voivat saada haltuunsa käyttäjän yksityisen avaimen [SSA10].

3.3 Tunnistautuminen laitteella

Kun käyttäjä haluaa lähettää viestin palvelimelle tai toiselle käyttäjälle, on tärkeä suosia turvallista protokollaa. On turvallista varmistaa myös oikean henkilön käyttävän laitetta, sillä ulkopuolinen varas on voinut anastaa laitteen. Käyttäjän tunnistautuminen voi perustua salasanan syöttämiseen tai visuaaliseen todennukseen. Istunto laitteen ja palvelimen välille voidaan muodostaa Diffie-Hellman protokollaa käyttäen. Yhteisellä avaimella siis hoidetaan viestien salaus. RSA on kuitenkin parempi mies välissä- hyökkäystä vastaan [SY13].

4 Palvelinpohjaiset allekirjoitukset

Palvelin voi luoda digitaalisen allekirjoituksen käyttäjän puolesta, kunhan käyttäjä voidaan todentaa palvelimelle. Palvelinten rooli digitaalisten allekirjoitusten luonnissa oli merkittävä aikana, jolloin laitteessa ei ollut tarpeeksi tehoa allekirjoituksen luomiseen. Nykyään laitepohjaiset allerkijoitukset ovat yleistyneet [SSA10].

4.1 Välityspalvelin

Välityspalvelin toimii siis eräänlaisena kirjautumispalvelimena käyttäjän ja lopullisen palvelimen välissä. Välityspalvelin voi luoda allekirjoituksen, mutta oikean käyttäjän varmenne vaaditaan. Varmennus voi perustua algoritmeihin kuten RSA tai DSA. On myös mahdollista, että käyttäjälle tehdään varmenne, jolla hän on tunnistettavissa jatkossa palvelimelle [SSA10].

4.2 NRS ja NRR

Kiistämättömyys on olennainen osa digitaalista allekirjoitusta. NRS (Non-Repudation of Sender) tarkoittaa, lähettäjä ei voi jälkikäteen kiistää lähettäneensä viestin. NRR (Non-Repudation of Receiver) puolestaan merkitsee vastaanottajan kiistämättömyyttä. Tiivistefunktioilla kuten esimerkiksi MD5:llä. Sekä lähettäjän että vastaanottajan on luotava julkiset avaimet ja merkit kirjautumispalvelimelle tunnistettavaksi. Kirjautumispalvelin pyytää varmenteen varmenneviranomaiselta ja muodostaa oman varmanteen lähettäjälle. Näin ollen kirjautumispalvelin voi jatkossa toimia vahvistavana linkkinä lähettäjän ja vastaanottajan välillä [LCJ04].

4.3 Varmenteet

Varmenteet ovat tapa tunnistaa jokin käyttäjä, välityspalvelin tai lopullinen palveluntarjoaja jatkuvaa yhteydenpitoa varten. Varmenne voi olla voimassa hetken tai pidemmän aikaa, mutta tietoturvan kannalta varmenteiden ei tulisi olla ikuisia. Varmennetta voidaan pitää luotettavana, jos sen tarjoaa ulkopuolinen varmenneviranomainen. Digitaalinen allekirjoitus vaatii toimiakseen aina varmenteen, mutta varmenne voi toimia irrallisena digitaalisesta allekirjoituksesta. PKI-protokollan avulla varmenne voidaan luoda luovuttamalla julkinen avain varmenneviranomaiselle ja lähettämällä pyyntö varmenteelle. Tämän jälkeen käyttäjä vahvistaa vielä itsensä salaamalla viestinsä yksityisellä avaimellaan. Varmenneviranomainen vastaa luovuttamalla varmenteen käyttäjälle. Varmenteesen on yleensä merkitty seuraavat tiedot: voimassaoloaika, sarjanumero, versio ja käyttäjän tunniste [RB12]. Vastaanottajan tulee siis ottaa huomioon vanhentunut varmenne. Koska varmenne on käyttäjäkohtainen, hyökkääjä ei tee varastetulla varmenteella mitään.

5 Vertailu

Tehokkuus ja tietoturva ovat tärkeitä ominaisuuksia koskien digitaalisia allekirjoituksia. Vaikka nämä kaksi seikkaa eivät ole suoraan toisensa poissulkevia, on syytä ottaa huomioon kummankin prioriteetti. Erityisesti mobiililaitteilla tehokkuudesta joudutaan yleensä karsimaan, joten allekirjoituksen luonti voi viedä huomattavan ajan [SSA10].

5.1 Tietoturva

Mobiililaitteilla voidaan havaita seuraavia tietoturvariskejä: urkinta, mies välissä -hyökkäys, datan muuntaminen, toisena osapuolena esiintyminen ja laitteen kadottaminen. Urkinnalla tarkoitetaan viestien kuuntelua, mutta se voidaan torjua helposti viestin salakirjoituksella esimerkiksi väliaikaisella istuntoavaimella. Mies välissä- hyökkäys tarkoittaa kolmannen osapuolen asettumista lähettävän ja vastaanottavan osapuolten väliin. Diffie-Hellmanissa piilee tämä riski mutta ei RSA:ssa. Datan muttaminen voidaan estää salakirjoituksella sekä käyttämällä tiivistefunktioita. Toisena osapuolena tekeytyminen ja laitteen kadottaminen voidaan estää salasanan kirjoittamisella laitteelle tai visuaalisena todennuksena. Julkisen avaimen protokolla eli PKI-malli toimii, jos salainen avain säilyy suojassa. Mikäli on pienikin riski, että salainen avain on jokun muun tiedossa, tulee avainpari vaihtaa heti. Niin kauan kun diskreetin logaritmin ongelmaa ei pystytä ratkaisemaan järkevässä ajassa, ovat RSA ja Diffie-Hellman turvallisia protokollia. [SY13].

5.2 Tehokkuus

Suorituskyky on parantunut vuosien saatossa niin PC- kuin mobiililaitteilla. Prosessorien teknologia on kehittynyt mahdollistaen tiheämmät kellopulssit ja moniydinsuorituksen. Myös tietoliikennenopeuksien nousulla on ollut suuri merkitys digitaalisten allekirjoitusten luonnissa. Tehokkuutta tarvitaan nopeisiin allekirjoituksiin lyhyellä aikavälillä. Artikkelissa Self-Proxy Mobile Signature esitelty huutokauppasovellus tarvitsee jokaiselle huudolle allekirjoituksen lyhyen ajan sisällä. Tietoturvasta on tässä tapauksessa erittäin vaikea tinkiä, joten käyttäjä olisi hyvä luoda allekirjoitus omalta laitteeltaan. Tehokkuudessa tulee ottaa huomioon siis salauksen nopeus, tiivisteen luominen ja varmenteen hankinta [SSA10]. Luonnollisesti myös palvelinpuolella esimerkiksi klusterointi on luonut mahdollisuuden tehokkaisiin allekirjoitusten/varmenteiden luomiseen monelle käyttäjälle samaan aikaan.

5.3 Nykyaikaisten menetelmien käyttö

Laitepohjaiset allekirjoitukset ovat yleistynet kokoajan mobiililaitteiden laskentatehon ansiosta. RSA:n lisäksi elliptiset käyrät ovat yleistyneet niiden paremman tietoturvan ansiosta suhteessa avainten pituuteen bitteinä [RB12]. AES algoritmia voidaan pitää murtumattomana, mutta DSA on murrettavissa jo muutaman bittivuodon avulla [SC12]. Elliptisen käyrän DSA:ta käytetään myös [XDC09].

6 Yhteenveto

Tässä tekstissä olemme tarkastelleet digitaalisia allekirjoituksia mobiiliympäristöissä ja mobiililaitteissa. Menetelmät allekirjoitusten luontiin siis vastaa-

vat tietokoneilla vastaavia menetelmiä. Olemma tarkastelleet PKI-mallia ja RSA algoritmia tarkemmin.

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`.

[RB12] Ray, Sangram ja Biswas, G. P.: *An ECC Based Public Key Infrastructure Usable for Mobile Applications.* Teoksessa *Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology*, CCSEIT '12, sivut 562–568, New York, NY, USA, 2012. ACM, ISBN 978-1-4503-1310-0. `http://doi.acm.org/10.1145/2393216.2393310`.

[SC12] Saxena, Neetesh ja Chaudhari, Narendra S.: *A Secure Approach for SMS in GSM Network.* Teoksessa *Proceedings of the CUBE International Information Technology Conference*, CUBE '12, sivut 59–64, New York, NY, USA, 2012. ACM, ISBN 978-1-4503-1185-4. `http://doi.acm.org/10.1145/2381716.2381729`.

[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.

[XDC09] Xuan, Zuguang, Du, Zhenjun ja Chen, Rong: *Comparison Research on Digital Signature Algorithms in Mobile Web Services.* Teoksessa *Management and Service Science, 2009. MASS '09. International Conference on*, sivut 1–4, Sept 2009.