

Digitaaliset allekirjoitukset mobiiliympäristössä

Taneli Virkkala

Kandidaatin tutkielma
HELSINGIN YLIOPISTO
Tietojenkäsittelytieteen laitos

Helsinki, 17. helmikuuta 2014

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	17. helmikuuta 2014	2	
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	1
2	Digitaalinen allekirjoituksen määritelmä	2
2.1	PKI-malli	2
2.2	RSA ja Diffie-Hellman	2
2.3	Mobiilikaupankäynti	2
3	Laitepohjaiset allekirjoitukset	2
3.1	SIM-kortilta luonti	2
3.2	Laitteen prosessorilta luonti	2
3.3	Tunnistautuminen laitteella	2
4	Palvelinpohjaiset allekirjoitukset	2
4.1	Välityspalvelin	2
4.2	NRS ja NRR	2
4.3	Varmenteet	2
5	Vertailu	2
5.1	Tietoturva	2
5.2	Tehokkuus	2
5.3	Nyky aikaisten menetelmien käyttö	2
6	Yhteenveto	2

1 Johdanto

Digitaalisten allekirjoitusten käyttö on noussut huomattavasti mobiililaitteilla nykypäivänä. Mobiiliympäristössä turvallinen yhteys on varmistettava, koska tietoturvariskit langattomissa verkoissa ovat erittäin suuret. 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. 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. Palvelin pohjaisen allekirjoituksen yleensä luo välissä oleva kirjautumispalvelin eikä lopullinen palveluntarjoaja.

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.

Schwabin ja Yangin mukaan mahdollisia tietoturvariskejä mobiiliympäristössä ovat urkinta, mies välissä -hyökkäys, datan muuntaminen, toisena osapuolena esiintyminen ja laitteen kadottaminen. Näitä riskejä vastaan tulee mobiililaitteen sisäinen 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.

Sekä RSA että Diffie-Hellman käyttävät jakojäännös menetelmää 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.

2 Digitaalisen allekirjoituksen määritelmä

2.1 PKI-malli

2.2 RSA ja Diffie-Hellman

2.3 Mobiilikaupankäynti

3 Laitepohjaiset allekirjoitukset

3.1 SIM-kortilta luonti

3.2 Laitteen prosessorilta luonti

3.3 Tunnistautuminen laitteella

4 Palvelinpohjaiset allekirjoitukset

4.1 Välityspalvelin

4.2 NRS ja NRR

4.3 Varmenteet

5 Vertailu

5.1 Tietoturva

5.2 Tehokkuus

5.3 Nykyaikaisten menetelmien käyttö

6 Yhteenveto