Digitaaliset allekirjoitukset mobiilikaupankäynnissä

Tehnyt: Taneli Virkkala
01.02.2014

Nykyään erilaisilla mobiililaitteilla voidaan vaihtaa tärkeää dataa digitaalisten allekirjoitusten ja sertifikaattien avulla. M.H. Samadani, M. Shajari ja M. Ahaniha Amirkabirin teknillisestä yliopistosta esittelevät tieteellisessä artikkelissaan *A Survey on Mobile Digital Signature Models* erilaisia käytäntöjä sopia digitaalisen suojauksen tavoista käyttäjän, välittäjän ja vastaanottajan välillä. Näiden tapojen kaksi pääryhmää ovat palvelinpohjaiset ja käyttäjäpohjaiset mobiiliallekirjoitukset.

Artikkelissa käyttäjä (Client) koostuu laitteesta ja SIM-kortista. Kirjoittajat korostavat SIM-kortin tietosuojaa, koska itse laitteella ei ole pääsyä SIM-kortin tietoihin. Laite puolestaan mahdollistaa tehokkaamman laskentakapasiteetin prosessorin avulla digitaalisten allekirjoitusten luomiseksi. Kirjoittajien mukaan monet kaupankäyntiin tarkoitetut sovellukset nykyaikaisilla mobiililaitteilla vaativat digitaalisen allekirjoituksen rahallisten transaktioiden mahdollistamiseksi. Vastaanottajan on todennettava allekirjoitusten avulla käyttäjä oikeaksi, data yhtenäiseksi sekä tieto kiistattomaksi. Samadani, Shajari ja Ahanina jakavat palvelinpohjaiset mobiiliallekirjoitukset (Server Based Mobile Signatures) kahteen osaan: sertifikaattipohjaiset palvelinpuolen mobiiliallekirjoitukset ja vähemmän sertifikaattipohjaiset palvelinpuolen mobiiliallekirjoitukset. Näiden lisäksi kirjoittajat kertovat käyttäjäpohjaisista mobiiliallekirjoituksista (Client Based Mobile Signatures) ja sen eri malleista.

Sertifikaattipohjaiset palvelinpuolen mobiiliallekirjoitukset

Kirjoittajat esittelevät kolme erilaista mallia sertifikaattipohjaisiin palvelinpuolen mobiiliallekirjoituksiin (Certificate Based Server Side Mobile Signature). Ensimmäisessä mallissa (Server Based Signatures with Client's Certificates) käyttäjä antaa palvelimelle oman salaisen avaimensa, jolla tämä kyseinen palvelin luo allekirjoituksen. Tätä voidaan pitää suurena tietoturvariskinä käyttäjälle, joten artikkelissa torjutaan salaisen avaimen antaminen. Toisessa mallissa (Server Based Signatures with Server's Certificates) käyttäjän ja palvelimen välissä on erillinen kirjautumispalvelin. Kirjautumispalvelimesta on tässä tapauksessa tullut palveluntarjoaja omalla allekirjoituksellaan ja alkuperäisen käyttäjän rooliksi on vain jäänyt pyynnön lähettäminen kirjautumispalvelimelle. Kirjoittajat toteavat tämän periaatteen käyttökelvottomaksi, sillä alkuperäistä pyytäjää palvelulle ei voida varmentaa. Kolmas artikkelissa esitelty malli sertifikaattipohjaisissa palvelinpuolen mobiiliallekirjoituksissa on välityspalvelimen käyttö (Server Based Signatures with Proxy Certificates). Käyttäjä antaa välityspalvelimelle julkisen avaimensa, jolla välityspalvelin allekirjoittaa sertifikaatin omalla yksityisellä avaimellaan. Välityspalvelin muodostaa yhteyden lopulliselle palvelimelle. Lopullinen palveluntarjoaja todentaa välityspalvelimen luoman sertifikaatin. Käyttäjän yksityistä avainta ei siis paljasteta kenellekään osapuolelle. Tähän kolmanteen tyyliin liittyy suuri tietoturvariski väärän käyttäjän olemassaolosta ja mahdollisesta tietomurrosta välityspalvelimelle.

Vähemmän sertifikaattipohjaiset palvelinpuolen mobiiliallekirjoitukset

Artikkelissa todetaan kaksi protokollaa vähemmän sertifikaattipohjaisiin palvelinpuolen mobiiliallekirjoituksiin (Certificate-Less Server Side Mobile Signatures). Nämä protokollat ovat kehittynyt yhdistetty allekirjoitus (IJS) ja palvelimeen pohjautunut allekirjoitus (SBS). Näiden mallien allekirjoitukset eivät perustu yleisiin algoritmeihin kuten RSA:han tai DSA:han. Kirjoittajien mukaan allekirjoituksen luonti perustuu vain yhteistyöhön palvelimen ja käyttäjän kanssa, jolloin käyttäjälle ei jää kuormittavaa laskentaa digitaalisen allekirjoituksen luontiin. IJS on protokolla, jossa käyttäjä lähettää kaksi hajautusoperaatiota (HMAC ja HOAC) palvelimelle. Palvelin ja lopullinen vastaanottaja tekevät kumpikin kaksi julkisen avaimen operaatiota: allekirjoituksen generointi ja vahvistus. IJS ei kuitenkaan käytä digitaalisia sertifikaatteja ja sitä on siis mahdoton käyttää laajalti kirjoittajien mukaan. Artikkelissa käsitelty SBS taas puolestaan perustuu hajautusketjuun, jonka käyttäjä on generoinut. Yleistä julkisen tai salaisen avaimen vaihtoa ei kuitenkaan tapahdu SBS:ssä ja sertifikaattien tuki puuttuu. IJS ja SBS eivät siis ole yleisessä käytössä, sillä kumpikin protokolla vaatii toimiakseen käyttäjän ja palvelimen tuen.

Käyttäjäpohjaiset mobiiliallekirjoitukset

Artikkelissa kerrotaan nykyaikaisten mobiililaitteiden pystyvän luomaan allekirjoituksia perustuen asymmetriseen kryptografiaan. Sen sijaan ensimmäisessä sukupolvessa digitaalisten allekirjoitusten luonti mobiiliympäristöissä oli haastavaa. Käyttäjäpohjaisia mobiiliallekirjoituksia on kolmea eri mallia: SIM-korttiin (SIM Based Signature), laitteeseen (Device Based Signature) tai hybridiin pohjautuva allekirjoitus (Hybrid Signature). Kaikissa näissä kolmessa tapauksessa allekirjoitus luodaan mobiililaitteessa, jossa on sekä SIM-kortti että prosessori. Prosessori on nopeampi luomaan allekirjoituksia, mutta SIM-kortti mahdollistaa avainten turvallisen säilytyksen. SIM-korttiin pohjautuvassa allekirjoituksessa laite ei pääse käsiksi kortilla oleviin tietoihin. Sen sijaan avaimen luonti kestää SIM-kortilla pitkään. Laitteeseen pohjautuvassa allekirjoituksessa avaimen luonti ja varastointi tapahtuu laitteessa. SIM-kortin ei siis tarvitse osallistua operaatioon. Allekirjoituksen luonti on nopeampaa kuin SIM-kortilla, mutta tietoturvariski piilee laitteessa ja sen käyttöjärjestelmässä. Kolmantena mallina Samadani, Shajari ja Ahanina esittelevät hybridimallin. Tässä mallissa avainten säilytys tapahtuu SIM-kortilla mutta avainten luonti laitteessa. Metodi on nopea, mutta allekirjoituksen luonnissa avaimen on poistuttava SIM-kortilta ja paljastuu näin ollen laitteelle. Jos SIM-kortti pystyy vain varastoimaan avaimia, hybridimallin käyttö on suotuisaa. Malli on siis turvallisempi kuin laitepohjainen allekirjoitus, mutta turvattomampi kuin SIM-korttiin pohjautuva malli.

Vertailu

Artikkelissa esitettyjen tutkijoiden mukaan tulevaisuudessa olevien mobiiliallekirjoitusten tulee olla käyttäjäpohjaisia. Suurimmassa osassa mobiilikaupankäynnin sovelluksissa ja palveluissa käyttäjän on luotava yksi tai kaksi digitaalista allekirjoitusta. Tämän määrän perusteella SIM-korttiin pohjautuva allekirjoitus vaikuttaisi olevan paras vaihtoehto. Kuitenkin tarvittavien allekirjoitusten määrän noustessa, kulunut aika vaikuttaa käyttäjän suorituskykyyn. Artikkelissa esitellään huutokauppasovellus, jossa tehdään tarjouksia nopealla aikavälillä. Käyttäjän tulee tehdä tarjouksia nopeasti, ja huutojen on oltava kiistattomia. Tällä hetkellä olevat mobiiliallekirjoitukset kärsivät tietoturvasta tai suorituskyvystä. Kirjoittajien mukaan mikään edellä esitetyistä malleista ei ole sopiva mobiilihuutokauppasovelluksen kaltaisia ohjelmia varten. Artikkelissa mainitaan tulevan SPMS-mallin korjaavan suorituskyvyn ongelman.

Yhteenveto

Mobiilikaupankäynnissä viestien tulee olla turvallisia ja nopeita. Digitaalisen allekirjoituksen on oltava kiistaton, todennettu ja viestin sisältämän datan tulee olla yhtenäistä. Mobiiliallekirjoituksia ovat siis palvelinpohjaiset ja käyttäjäpohjaiset allekirjoitukset. Artikkelissa mainittiin käyttäjäpohjaisten allekirjoitusten olevan palvelinpohjaisia malleja parempia. Tämän hetkisten käyttäjäpohjaisten mallien kerrotaan olevan kuitenkin liian hitaita ja tietoturvariskialttiita mobiilikaupankäyntiä varten. Tulevaisuuden mobiilikauppasovellukset vaativat kehittyneemmät digitaaliset allekirjoitusmenetelmät toimiakseen. Kirjoittajat kuitenkin toteavat tulevaisuuden mallien olevan juuri käyttäjäpohjaisia menetelmiä. He myös korostavat mobiilikaupankäynnin kasvulle digitaalisten allekirjoitusten olevan tärkeitä.

Lähteet:

M. H. Samadani, M. Shajari, M. Ahaniha, *A Survey on Mobile Digital Signature Models*,
ICEC '10 Proceedings of the 12th International Conference on Electronic Commerce: Roadmap for the Future of Electronic Business, sivut: 141-144.