Sähköinen allekirjoitus ja henkilön tunnistaminen matkapuhelimella

Terveydenhuollon ATK-päivät 30.5.2005

sonera

Mobiilivarmenteet asioinnissa ja työskentelyssä

Sähköinen asiointi, itsepalvelu ja kaupankäynti lisääntyvät

Kustannustehokkaat ja helposti saatavilla olevat palvelut hyödyttävät kuluttajia ja palvelujen tarjoajia

Organisaatiot verkottavat toimintaansa

Etätyöskentely, liikkuvan työn ratkaisut ja yritysten väliset järjestelmät parantavat tuottavuutta ja mahdollistavat joustavamman työskentelyn

Sähköiset henkilöllisyydet / Kansalaisvarmenteet

- Henkilön tunnistaminen
- Käyttäjän todentaminen
- Sähköinen allekirjoitus

Organisaatiovarmenteet

- Käyttäjän todentaminen
- Organisaatioiden välinen tunnistaminen
- Organisaatiotiedot- ja valtuutukset
- Sähköinen allekirjoitus

Matkapuhelin ja SIM-kortti varmennekäytössä

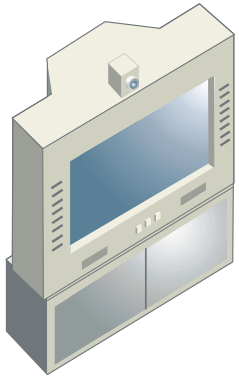
- Matkapuhelin lähes kaikilla henkilökohtaisessa käytössä ja aina saatavilla
- SIM-kortti on murto-, kopio- ja lukusuojattu tunnisteiden ja muiden varmennetoiminallisuuksien sijoituspaikka
- Matkapuhelin toimii kortinlukijana ja -ohjelmistona
- Toimii lähes kaikissa puhelimissa. Vuodesta 1998 kaikki matkapuhelimet ovat tukenneet SIM-kortin sovelluksia GSM-standardina.

Matkapuhelimella varmentaminen monikanavaisessa asiointiympäristössä

…Internetissä tietokoneella

…matka-puhelimessa

…myös puhelun yhteydessä



…Digi-TVssä

…tulevaisuudessa myös fyysisessä asioinnissa

Mobiilivarmenteet sähköisen asioinnin infrastuktuurina

- **Laatuvarmennetoimintaa määrittelee EU-tasoinen ja kansallinen lainsäädäntö**
  - **Viranomaisvalvonta ja -ohjeistus Viestintävirastolla**
- **Mobiilivarmenteet perustuvat kansainvälisiin varmennestandardeihin ja tietoturvateknologiaan**
  - **PKI (Public Key Infrastructure) yleisesti käytössä mm. Internet-istuntojen salaamisessa ja palvelinten tunnistamisessa**
- **Kansallinen yhteistyö**
  - **Henkilön sähköisen tunnistamisen (HST)-infrastruktuuri**
- **Kustannustehokkuus**
  - **Samaa varmennetta voidaan käyttää useissa palveluissa ja palvelukanavissa**

PKI – perustoiminta

- PKI eli julkisen avaimen infrastruktuuri hyödyntää ***julkisen avaimen*** menetelmää.
- Jokaisella viestintään osallistuvalla on **kaksi avainta**: julkinen (*public key*) ja yksityinen (*private key*)
- Julkisella avaimella ja yksityisellä avaimella on sellaisia matemaattisia ominaisuuksia, että julkisella avaimella kryptattu eli salattu viesti voidaan avata selväkieliseksi (vain) salaisella avaimella ja päinvastoin, mutta avaimien suhde keskenään on sellainen, että yksityistä avainta ei voi johtaa julkisesta (ks. esim. yksisuuntaiset funktiot)
- Mobiilivarmenteissa yksityinen avain on suojattuna SIM-kortilla

Tunnistaminen ja sähköinen allekirjoitus julkisen avaimen menetelmällä

Digitaalista allekirjoitusta julkisen avaimen menetelmällä käytetään tunnistamisessa ja sähköisissä allekirjoituksissa

1) Allekirjoitettava viesti kryptataan yksityisellä avaimella. Tunnistamisessa kryptataan tunnistushaaste.
2) Allekirjoitus tarkastetaan julkisella avaimella, joka saadaan allekirjoittajan varmenteesta. Mikäli sekä alkuperäinen että tarkastettu viesti vastaavat tosiaan on allekirjoitus validi. Samalla varmistutaan allekirjoitetun tiedon eheydestä.
3) Allekirjoittajan idetiteetti saadaan julkisen avaimen sisältävän varmenteen tiedoista
4) Varmenne tarkastetaan varmentajan allekirjoituksen perusteella

Varmenne, varmentaja ja sulkulista

- Varmenne eli sertifikaatti (certificate) sitoo julkisen avaimen henkilöön
- Varmentaja eli Certificate Authority (CA) allekirjoittaa sähköisen todistuksen siitä, kenen hallussa ko. julkista avainta vastaava yksityinen avain on. Tästä todistuksesta käytetään nimeä varmenne.
- Varmenteen haltija voi sulkea varmenteen sulkupalvelussa
- Varmenteen status (mahdollinen peruuttaminen) tarkastetaan sulkulistalta, jota varmentaja julkaisee
- Teknisesti ko. lähde on jossakin verkko-osoitteessa sijaitseva hakemisto, usein lukuoptimoitu tietokanta tyyppiä LDAP.

X.509 v3 Varmenne, perusrakenne

version	(versio)
serial number	(varmenteen sarjanumero)
signature algorithm ID	(allekirjoitusalgoritmi)
issuer name	(myöntäjä)
validity period	(voimassaoloaika)
subject name	(varmenteen haltijan nimi)
subject public key info	(haltijan julkisen avaimen tiedot)
issuer unique identifier	(myöntäjän uniikki tunniste)
{extensions}	laajennusosat
Signature	(Varmentajan allekirjoitus)

Tunnusluvut

- Yksityinen avain suojataan yleensä aktivointitiedolla (tunnusluku). Mobiilivarmenteessa tunnusluku syötetään matkapuhelimella SIM-kortille varmennetoiminnallisuuksien aktivoimiseksi.
- Tunnusluku ei siirry puhelimen ulkopuolelle ja sitä on hyvin vaikea kaapata. (Vrt. tietokoneet tai maksupäätteiden lukulaitteet). Varmennetoiminnallisuuksia varten SIM-kortilla on oma selain.
- Two-factor authentication: Vain käyttäjän tiedossa oleva salaisuus (tunnusluku) + vain käyttäjän hallussa oleva esine (yksityinen avain SIM-kortilla)

Transaktioiden ja dokumenttien varmentaminen mobiilisti

- Mobiilivarmenteella voidaan sähköisesti allekirjoittaa transaktioita ja sähköisiä dokumentteja niiden aitouden ja alkuperän todentamiseksi
- Sähköisestä dokumentista allekirjoitetaan sen tiiviste
- Sähköinen allekirjoitus varmentaa
  - allekirjoittajan henkilöllisyyden sekä allekirjoittajan ja allekirjoitetun tietosisällön yhteenkuuluvuuden
  - allekirjoitetun tietosisällön eheyden ja muuttumattomuuden allekirjoituksen elinkaaren ajan
- Potentiaalisia käyttökohteita esim. viralliset asiakirjat, maksutapahtumat, kuitit, reseptit, sopimukset, äänestykset jne.

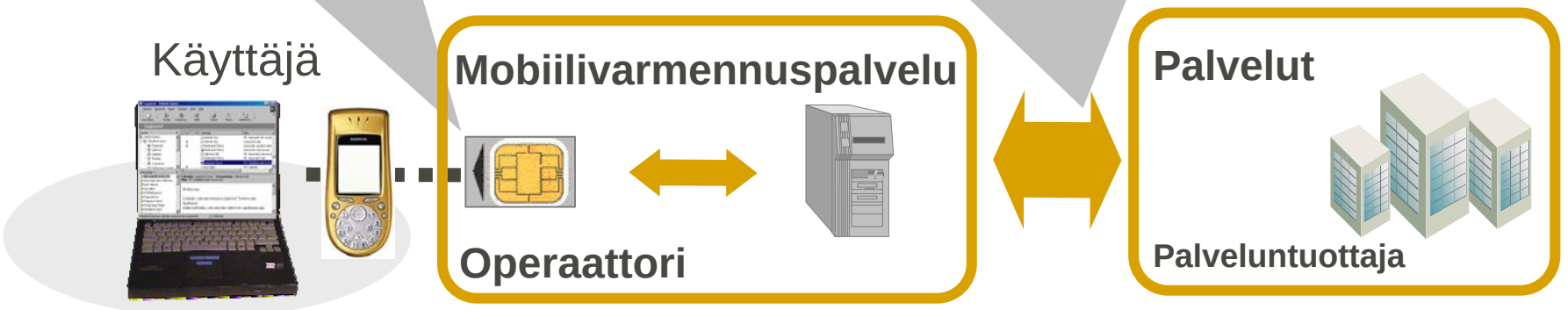
Mobiilikansalaisvarmenne

- Valtion varmentama sähköinen henkilöllisyys, kansalaisvarmenne, matkapuhelinpalveluna
- Samanlainen varmenne kuin sähköisessä henkilökortissa ja Osuuspankin pankkikortilla
- Yhteistyössä ovat mukana kaikki SIM-kortteja liikkeelle laskevat verkko-operaattorit (Sonera, Elisa ja DNA)
- Henkilöllisyys yksilöidään varmenteessa nimen lisäksi väestötietojärjestelmään henkilötunnuksen rinnalle luodulla sähköisellä asiointitunnuksella (SATU). SATU ei henkilötunnuksen tavoin ilmaise varmenteen haltijan syntymäaikaa tai sukupuolta.
- Kansalaisvarmenne on laatuvarmenne, josta on säädetty laissa sähköisestä allekirjoituksessa

Yleiskuva mobiilista kansalaisvarmenteesta

Varmennekortti
Operaattori jakelee käyttäjälle varmenneominaisuuksilla varustetun SIM-kortin ja tunnusluvut.

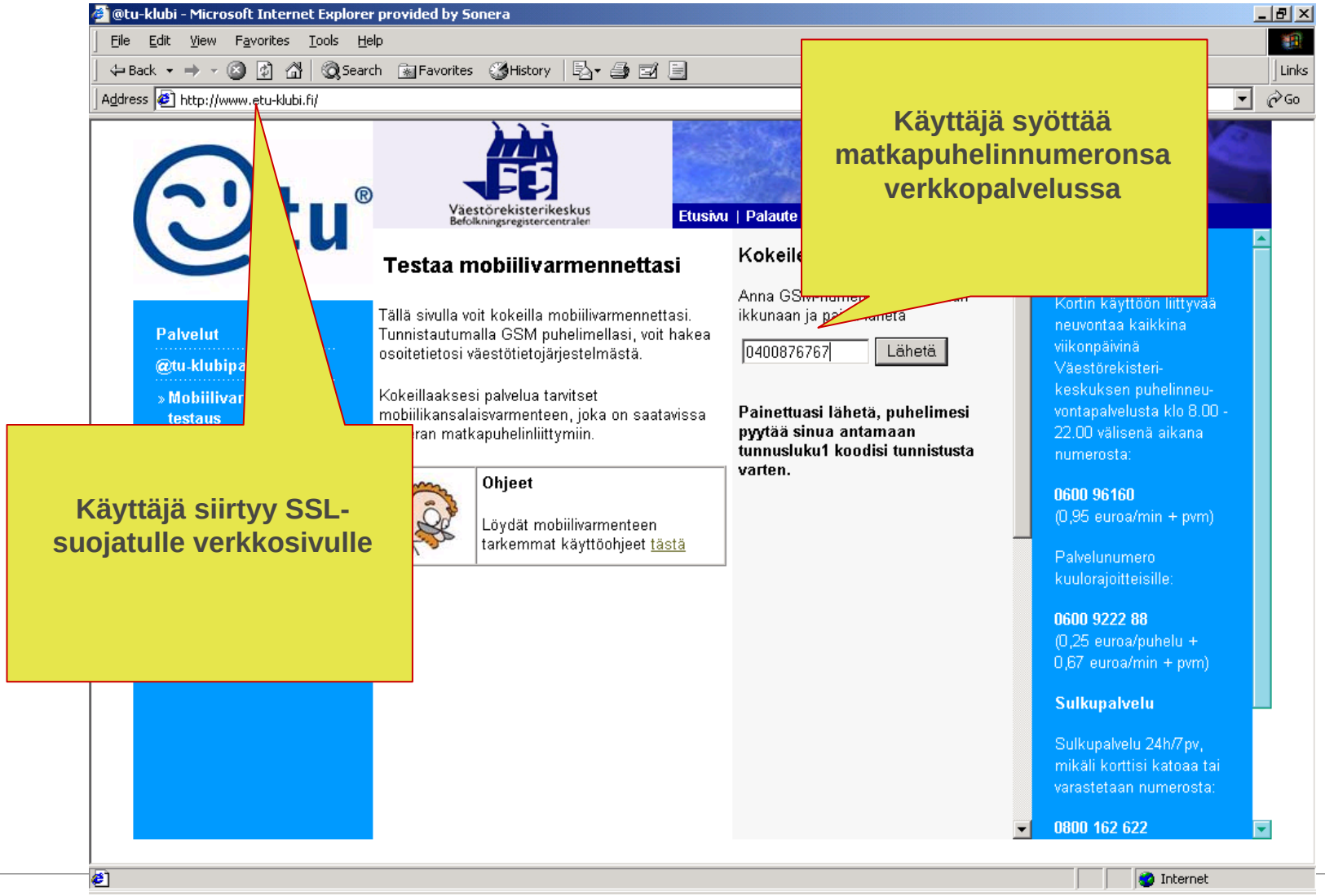
Varmennustapahtuma
Verkkopalvelu liitetään operaattorin rajapintaan, jonka kautta välitetään varmennustapahtumat matkapuhelimen ja palvelun välillä.



Rekisteröinti
Poliisi rekisteröi varmenteet toimipisteissään. Poliisi tarkastaa varmenteen hakijan henkilöllisyyden ja yhdistää henkilöllisyyden SIM-kortin tunnisteisiin.

Kansalaisvarmenne
Kansalaisvarmenteesta vastaa väestötietojärjestelmää ylläpitävä Sisäministeriön alainen Väestörekisterikeskus.
Varmenteeseen kirjataan henkilön nimi ja sähköinen asiointitunnus henkilöllisyyden yksilöimiseksi.
Väestörekisterikeskus ylläpitää sulkupalvelua ja sulkulistoja.

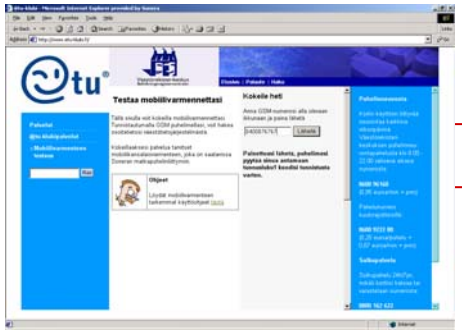
Käyttäjäkokemus internetissä: Tunnistautuminen verkkopalveluun



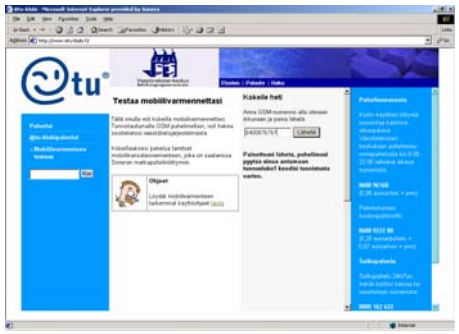
Tunnistautuminen verkkopalveluun - 2

Palvelupyyntö tulee automaattisesti näytölle

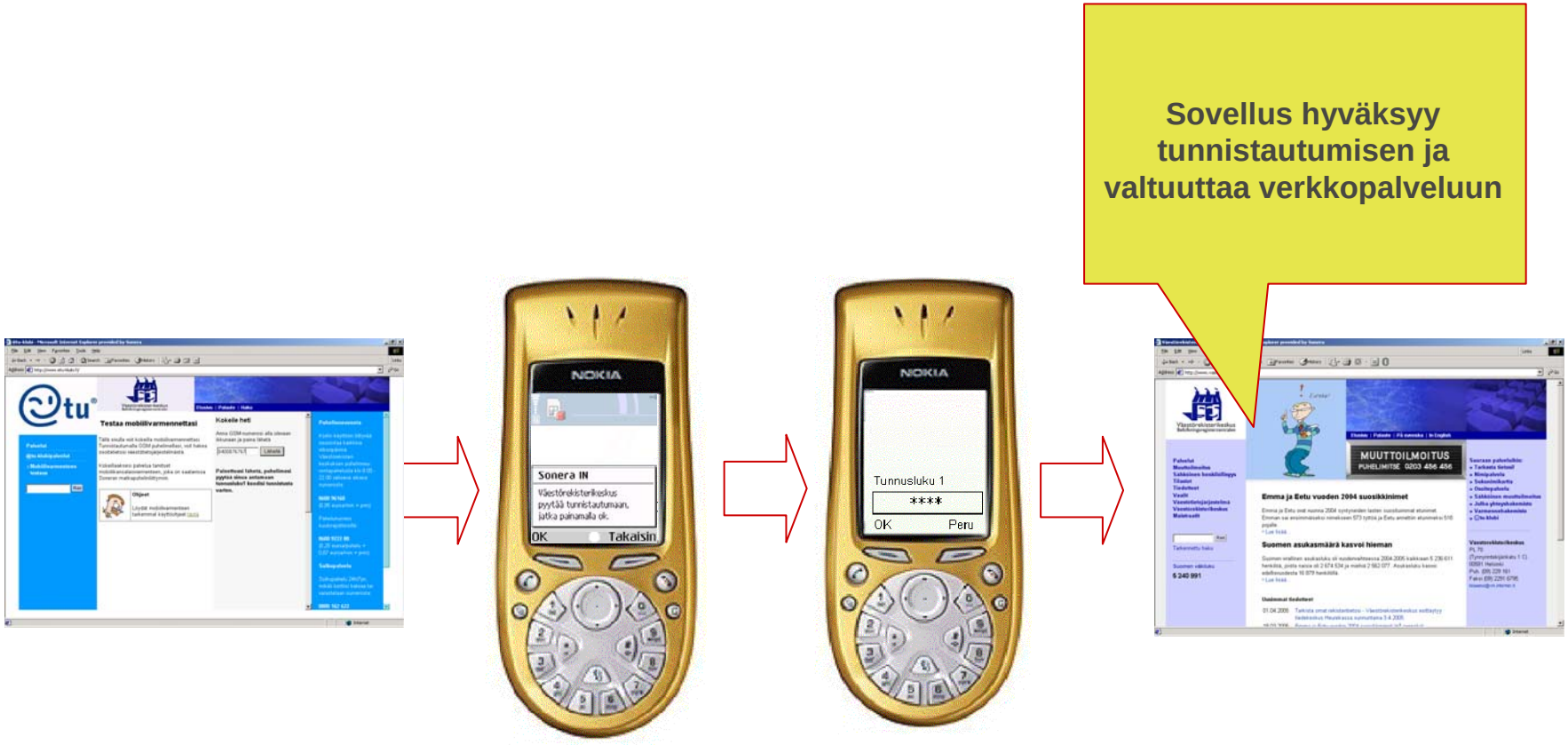
Palveluntuottaja tunnistetaan käyttäjälle sekä kerrotaan palvelutyyppi
•Tunnistautuminen
•Allekirjoitus



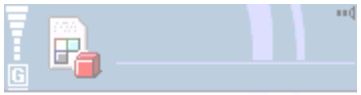
Tunnistautuminen verkkopalveluun - 3

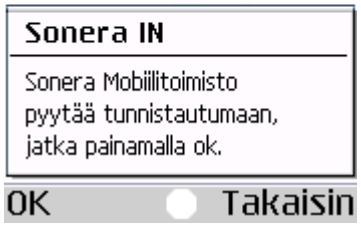


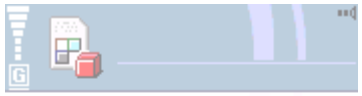
Tunnistautuminen verkkopalveluun - 4

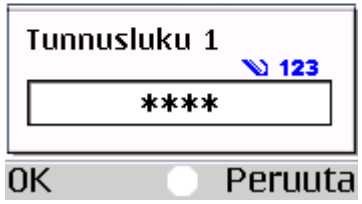


Käyttäjäkokemus Mobiilitoimistoon sisään kirjautumisessa









TLS

Soneran mobiilivarmennepalvelut

Saatavilla olevat palvelut

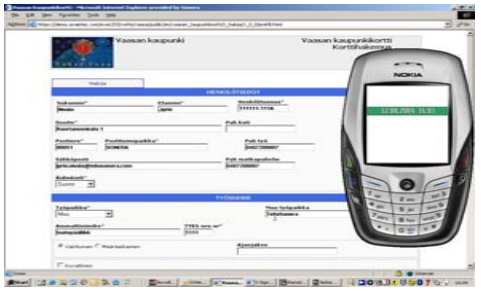
- **Kuluttajaliittymät**: Kansalaisvarmenne voidaan liittää palveluna kaikkiin liittymätyyppeihin prepaid-liittymiä lukuun ottamatta
- **Palveluntuottajat**: Palvelurajapinta Soneran liittymissä tehtäviin varmennuksiin mobiilikansalaisvarmenteella
- **Työliittymät ja organisaatiovarmenteet:** Organisaatiovarmenteet liitetään yritysliittymiin.
- Organisaatiovarmenteelliseen liittymään voidaan maksuttomana lisäpalveluna liittää myös kansalaisvarmenne. Samassa liittymässä työ- ja kansalaisvarmenteet.

Mobiilivarmenteen sovelluksia

VPN: Käyttäjän todentaminen VPN-suojatuissa etä- ja liikkuvan työn yhteyksissä. Myös mobiilit- ja langattomat yhteydet.

SecureWeb: Käyttäjän todentaminen SSL-suojatussa internetistunnossa

Mobiilitoimisto: Sisään kirjautuminen sähköpostiin, verkkokalenteriin ja muihin työsovelluksiin matkapuhelimella tai internetissä

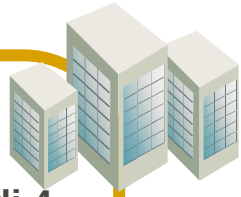


Verkkolomakkeet ja sähköinen asiankäsittely: Lomakkeen sähköinen allekirjoittaminen eSignature-palvelulla

Hyötyjä käyttäjille ja palveluntuottajille

Käyttäjä

- Henkilökohtainen avain sähköiseen asiointiin ja kaupankäyntiin.
- Helppo ja yhtenäinen käyttö
  - Yksi tunnusluku eri palveluissa
  - Yhtenäinen käyttörutiini eri palvelukanavissa
- Ei erillistä välinettä tunnistamista varten. Lähes kaikilla on matkapuhelin ja SIM-kortti.
- Voidaan yhdistää yksityis- ja työkäyttö samaan liittymään ja korttiin



Palveluntuottajat

- Matkapuhelinliittymiin perustuva yli 4 miljoonan käyttäjän potentiaali
- Mahdollista tavoittaa myös käyttäjäryhmiä, joilla ei esim. pankkitunnuksia
- Ei edellytä investointeja omiin tunnistusvälineisiin tai varmenneohjelmistoihin
- Liitettävissä internet-standardeilla sähköisiin palveluihin
- Edistynyt (sähköinen) allekirjoitus

- Älykortti- ja PKI-teknologiaan perustuva tekninen tietoturvallisuus
- Lainsäädäntö ja laatuvarmenne käytännöt ja vastuut suojaavat varmenteen haltijoita ja luottavia osapuolia – Selkeät pelisäännöt sähköisille henkilöllisyyksille

Suomen johtava viestintäpalvelujen tarjoaja

sonera