GOSPODARSKA ZBORNICA SLOVENIJE

crea d.o.o.

Projekt e-SLOG

Elektronsko poslovanje slovenskega gospodarstva

APLIKACIJA ZA VARNO ELEKTRONSKO PODPISOVANJE IN PREVERJANJE PODPISA

priporočila

v. 1.0
junij 2004

STANJE DOKUMENTA

Namen dokumenta:	Dokument vsebuje priporočila, ki opisujejo lastnosti aplikacije za izdelavo in preverjanje elektronskega podpisa in postopek integracije elektronskega podpisa v aplikacije.
Kratek naziv projekta:	e-SLOG – e-podpis
Vsebina:	*Glej "Vsebina"*
Status:	Veljavna različica
Verzija:	1.0
Datum verzije:	10.6.2004
Avtorji:	CREA d.o.o.
Naslovniki:	Dušan Zupančič (GZS), dusan.zupancic@gzs.si Ariana Grobelnik (GZS), ariana.grobelnik@gzs.si Samo Grčman (GZS), samo.grcman@gzs.si Dr. Aleš Dobnikar (CVI), ales.dobnikar@gov.si Dr. Alenka Žužek (CVI), alenka.zuzek@gov.si Matej Trampuš (CREA), matej.trampus@crea.si Igor Lesjak (CREA), igor.lesjak@crea.si Roman Puhek (CREA), roman.puhek@crea.si Rudi Ponikvar (Hermes Plus), rudi.ponikvar@hermes-plus.si Tine Prislan (Hermes Plus), tine.prislan@hermes-plus.si Aljoša Blažič (SETCCE), aljosa@setcce.org Gašper Lavrenčič (SETCCE), gasper@setcce.org Dr. Tomaž Klobučar (SETCCE), tomaz@setcce.org Boštjan Berčič (Institut za pravno informatiko), bostjan.bercic@ipri-zavod.si
Zgodovina verzij:	*Glej "Verzija"*

Verzija	**Datum spremembe**	**Opombe**
0.9 delovna	10.6.2003	Osnutek
0.9f delovna	29.6.2003	Usklajeno z smernicami drugega sestanka delovne skupine (praktična naravnanost, kontrolni seznam)
0.9g delovna	1.10.2003	Upoštevane pripombe na dokumentacijo, posredovane 23.7.2003 (praktična naravnanost, kontrolni seznam)
0.9h delovna	1.5.2004	Odstranjeni komentarji, seznami TODO.
1.0	10.6.2004	Usklajeno s predlogo e-SLOG

VSEBINA

1. PRIPOROČILA PO PODROČJIH

1.1. Uvod

Elektronski podpis je eden temeljnih varnostnih mehanizmov, ki ščiti podatke v elektronski obliki. Podatkom zagotavlja celovitost, nezatajivost njihovega izvora in avtentičnost podpisnika. V poslovnih aplikacijah se najpogosteje uporablja za zanesljivo in varno izmenjevanje elektronskih dokumentov.

Elektronski podpis izvedemo s *sredstvom za varno elektronsko podpisovanje*, ki ga sestavljata *aplikacija, ki podpisuje* in *naprava za ustvarjanje podpisa*. Preverjanje elektronskega podpisa izvedemo s *sredstvom za preverjanje elektronskega podpisa*. Sredstvi praviloma ne obstajata kot samostojni namenski aplikaciji, ampak sta običajno funkcionalni del določene poslovne aplikacije. Zato je pomembna tudi varna integracija *sredstva za varno elektronsko podpisovanje* s poslovno aplikacijo.

1.1.1 Področje, namen in organizacija poglavja

V poglavju **navajamo**:

- priporočila, ki opisujejo lastnosti sredstva za varno elektronsko podpisovanje in
- sredstva za preverjanje elektronskega podpisa,
- priporočila za integracijo elektronskega podpisa v poslovne procese podjetij ter
- priporočila glede kriterijev vrednotenja aplikacije.

Ciljna publika poglavja so

- predvsem slovenska podjetja, ki želijo v svoje poslovne procese integrirati elektronski podpis, deloma pa tudi
- ponudniki programske opreme, ki vključuje elektronski podpis.

Namen poglavja je navesti praktična priporočila na podlagi mednarodnih standardov in priporočil, ki bodo ciljni publiki olajšala razumevanje zahtev in vrednotenje rešitev za varno elektronsko podpisovanje.

Poglavje je organizirano na naslednji način:

- v nadaljevanju uvodnega dela navajamo priporočila in standarde, ki se nanašajo na izvedbo elektronskega podpisa;
- v poglavju X.2 podajamo pravno analizo izvedbe elektronskega podpisovanja;
- v poglavju X.3 so zahteve za izdelavo aplikacij za elektronsko podpisovanje povzete v okviru praktičnega kontrolnega seznama;
- terminološki slovar pojasnjuje pojme, ki se v poglavju uporabljajo;
- v prilogi podrobneje opisujemo zahteve, ki se nanašajo na izdelavo in preverjanje elektronskega podpisa; priloga dejansko povzema vsebino ustreznih standardov in priporočil ter definira terminologijo; dodatno navajamo tudi okvirne smernice za politiko e-podpisa.

1.1.2 Standardi in priporočila

V Sloveniji ureja področje elektronskega podpisa Zakon o elektronskem poslovanju in elektronskem podpisu (Ur.l. RS, št. 57/2000, 30/2001), s pripadajočo Uredbo o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Ur.l. RS, št. 77/2000, 2/2001).

V Evropski uniji je evropska komisija pooblastila organizacijo CEN (fr. Comite European de Normalisation) za pripravo evropskih standardov s področij informatike, ki ne sodijo v področji elektrotehnike in telekomunikacij. CEN je ustanovila posebno delovno telo, t.i. sistem standardizacije informacijske družbe (angl. Information Society Standardization System oz. CEN/ISSS), prek katerega se odvijajo delavnice, ki so odprtega tipa. Rezultati teh delavnic so objavljeni pod oznako CWA (angl. CEN Workshop Agreements).

Delavnica CEN/ISSS E-SIGN je odgovorna za del EESSI delovnega programa, ki se nanaša na kvalitativne in funkcijske

standarde za *sredstva za elektronsko podpisovanje* in *sredstva za preverjanje elektronskega podpisa* ter tudi za kvalitativne in funkcijske standarde za *overitelje* digitalnih potrdil.

Pod okriljem CEN/ISSS so bili s področja, ki ga pokriva ta dokument doslej pripravljeni naslednji dokumenti:
[CWA], [ETSI]:

- O *aplikaciji, ki podpisuje* in *aplikaciji, ki preverja* podpis:
  - CWA 14170 Security Requirements for Signature Creation Systems,
  - CWA 14171 Procedures for Electronic Signature Verification,
  - CWA 14172-4 EESSI Conformity Assessment Guidance – Part: 4: Signature Creation Application and Procedures for Electronic Signature Verification,
- O *napravi za ustvarjanje podpisa*:
  - CWA 14169 Secure Signature-Creation Devices, version 'EAL 4+',
  - CWA14172-5 EESSI Conformity Assessment Guidance – Part: 5: Secure signature creation devices,
- O *politiki e-podpisa*:
  - ETSI TR 102 041 V1.1.1 (2002-02) Signature Policy Report

Pričujoči dokument gradi na naštetih dokumentih. Od teh dokumentov se razlikuje v naslednjih točkah:
- se naslanja tudi na lokalno zakonodajo ([ZEPEP], [Uredba]),
- je bolj praktično naravnan (iz uporabniškega in razvojnega vidika),
- podaja konsistenten in celovit pogled (CWAji mestoma uporabljajo različno terminologijo in način podajanja problematike).

1.2. Pravna analiza

1.3. Kontrolni seznam

Elektronski podpis izvedemo s *sredstvom za varno elektronsko podpisovanje*, ki ga sestavljata *aplikacija, ki podpisuje*, in *naprava za ustvarjanje podpisa*. *Aplikacija, ki podpisuje* je najpogosteje programska oprema, s pomočjo katere podpisnik ustvarja elektronsko podpisane poslovne dokumente. Uporabniku prikaže vsebino dokumenta, mu omogoči izbor ustreznega digitalnega potrdila za podpisovanje, varen elektronski podpis pa dejansko izvede s pomočjo *naprave za ustvarjanje podpisa*. *Naprava za ustvarjanje podpisa* je poleg dejanske izvedbe elektronskega podpisa, zadolžena tudi za varno hranjenje *podatkov za elektronsko podpisovanje*. *Podatke za elektronsko podpisovanje* najpogosteje predstavlja digitalno potrdilo s pripadajočim zasebnim ključem, tipični primer *naprave* pa je ali pametna kartica. Manj varne izvedbe *naprave* lahko predstavlja tudi sklop programskih knjižnic, ki *podatke za elektronski podpisovanje* shranjujejo kar na zaščitenem delu trdega diska. **Preverjanje elektronskega podpisa** izvedemo s *sredstvom za preverjanje elektronskega podpisa*, ki je navadno del iste aplikacije. Vsi pojmi, ki se nanašajo na varno izvedbo in preverjanje elektronskega podpisa so podrobno obrazloženi v prilogi.

Sredstvi za podpisovanje in preverjanje praviloma ne obstajata kot samostojni namenski aplikaciji, ampak sta običajno funkcionalni del določene poslovne aplikacije. V poslovni aplikaciji tipično nastajajo poslovni dokumenti, ki so kasneje dejansko predmet elektronskega podpisa. Ker je uporabnik navajen dela z osnovno aplikacijo, je za dobro izdelani *sredstvi* najbolje, da sta v poslovno aplikacijo čim bolj nevidno integrirani. **Varna integracija** *sredstva za varno elektronsko podpisovanje* s poslovno aplikacijo je še posebej pomembna.

Aplikacije, ki ustvarjajo in preverjajo elektronski podpis, morajo vsebovati kopico **predpisanih funkcionalnosti** in izpolnjevati številne **zahteve glede izvedbe podpisovanja**. Praktična priporočila glede izvedbe varnega elektronskega podpisovanja podajamo v obliki kontrolnega seznama. V seznamu so predstavljene zahteve ki se nanašajo na ustvarjanje varnega elektronskega podpisa, njegovo preverjanje, uporabo časovnega žiga, namestitev aplikacij in na okolje, v katerem se podpisovanje izvaja. Priporočljivo je, da aplikacije zadoščajo vsem zahtevam iz seznama.

Kontrolni seznami v nadaljevanju so opredeljeni po tipičnih scenarijih uporabe elektronskega podpisa v poslovnem okolju.

1.3.1 Ustvarjanje podpisa – scenarij C2C ali C2B.

Kontrolni seznam v nadaljevanju podaja opis funkcionalnosti, ki se nanašajo na primer, ko uporabnik neposredno uporablja *aplikacijo za varno elektronsko podpisovanje*. Tipično gre za scenarije C2C ali C2B, kjer (pogosto na novo razvito) aplikacijo uporabljajo fizične osebe, samostojni podjetniki ali manjša podjetja, ki nimajo lastnega zalednega informacijskega sistema.

Primeri uporabe:
- integracija varnega elektronskega podpisa v spletno aplikacijo,
- namenska komponenta, ki se tesno pointegrira v zalednega aplikacijo (pametni odjemalec) ali spletno aplikacijo (npr. Javanski applet, komponenta ActiveX).

☐ **(K1) Pred podpisom si podpisnik lahko ogleda vsebino** *dokumenta za podpis* **v njemu razumljivi obliki.**

Podpisnik mora pred vsakim podpisom in ob vsakem preverjanju podpisa videti vsebino, ki je predmet elektronskega podpisa. Predstavitev podatkov mora biti narejena v njemu razumljivi obliki.

☐ **(K2) Če je dokument sestavljen na način, ki ločuje podatke od njihove predstavitve, mora elektronski podpis varovati oboje: tako podatke kot njihovo predstavitev.**

Pogosto so elektronski dokumenti sestavljeni tako, da so podatki ločeni od njihove predstavitve (načelo ločevanja podatkov in oblike). Ker oblika bistveno prispeva k razumljivosti, pogosto pa lahko tudi spremni sam pomen, mora elektronski podpis varovati tako podatke kot njihovo predstavitev.

☐ **(K3) Uporabnik sam določi, kateri** *podatek za elektronsko podpisovanje* **se uporabi za izvedbo varnega elektronskega podpisa.**

Digitalno potrdilo je v trenutnih izvedbah elektronskega podpisovanja praktično edini primer *podatkov za elektronsko podpisovanje*. Podpisnik mora ob podpisu imeti možnost izbora digitalnega potrdila. To lahko naredi pred vsakim podpisom, lahko pa npr. potrdilo izbere v nastavitvah, ki veljajo za vse nadaljnje podpisovanje, aplikacija pa ga o izbranem potrdilu le obvesti.

☐ *(***K4***) Aplikacija, ki podpisuje* **mora biti povezano s poslovno aplikacijo na način, ki preprečuje uporabo sredstva iz druge, zlonamerne aplikacije iz okolja.**

Sredstvo za varno elektronsko podpisovanje ali njegov del (npr. zgolj izvedba elektronskega podpisa) običajno izvedemo v obliki programske sestavine (komponente), ki jo nato vključujemo v različne poslovne aplikacije. Programska sestavina mora omogočati varno integracijo v poslovno aplikacijo, ki temelji na vzpostavitvi zaupanja z aplikacijo. Na ta način preprečimo, da bi zlonamerna aplikacija (npr. trojanski konj) pridobila dostop do komponente, s tem pa do podatkov za elektronsko podpisovanje in brez vpliva uporabnika izvedla elektronski podpis.

Varovanje je še posebej pomembno v primeru, ko npr. prikaz podpisnih podatkov ni del programske sestavine, ampak je izveden v poslovni aplikaciji, npr. v že obstoječih prikazih poslovnih dokumentov. V tem primeru bi zlonamerna aplikacija lahko npr. uporabniku prikazala en poslovni dokument, s pomočjo slabo zasnovane komponente pa dejansko izvedla elektronski podpis drugega dokumenta.

☐ **(K5)** *Aplikacija, ki podpisuje***, mora vsebovati razumljiv uporabniški vmesnik.**

Izvedba *aplikacije, ki podpisuje*, mora uporabljati kar se da preprost in najširšemu krogu uporabnikov razumljiv (intuitiven) uporabniški vmesnik. Npr. uporabniku, ki razume le slovenski jezik, *aplikacija* ne sme prikazovati

besedila v angleškem jeziku.

☐ **(K6) Če bo podpisan le del dokumenta, mora biti jasno razvidno, kateri del.**

Uporabnika mora aplikacija jasno opozoriti, kadar niso vsi podatki, ki jih uporabnik, vidi, predmet elektronskega podpisa. *Aplikacija, ki podpisuje* mora jasno prikazati, kateri del podatkov je predmet elektronskega podpisa. Primer takšnega podpisa je npr. račun, katerega posamezne postavke podpisujejo ločeni podpisniki, ali pogodba dveh izvajalcev, pri kateri je posamezni izvajalec odgovoren le za njen del.

☐ **(K7)** *Naprava za ustvarjanje podpisa* **preveri istovetnost** *podpisnika.*

Dostop do podatkov za ustvarjanje podpisa (privatnih ključev ipd.), ki jih hrani naprava za ustvarjanje podpisa mora biti dovoljen samo imetniku teh podatkov – podpisniku. Naprava mora ob vsaki uporabi teh podatkov preveriti njegovo istovetnost. Če se kot *naprava za ustvarjanje podpisa* uporablja npr. pametna kartica, ta ponavadi preveri podpisnikovo istovetnost z vnosom osebne identifikacijske številke (PIN).

☐ **(K8) Uporabnik ima možnost lokalnega hranjenja in pregledovanja** *dokumenta za podpis* **in** *rezultata podpisa***.**

Aplikacija, ki podpisuje, mora uporabniku (tj. tako podpisniku kot uporabniku, ki podpis preverja) omogočati lokalno hranjenje vseh *dokumentov za podpis*, tj. ki jih podpisuje, in dokumentov, katerih podpis preverja. Lokalna kopija podatkov uporabniku omogoča pregledovanje *dokumenta* tudi, ko ni povezan z *elektronskim arhivom*.

☐ **(K9) Uporabnik ima dostop do** *politike e-podpisa***.**

Politika e-podpisa vsebuje določila o podpisovanju in preverjanju podpisa. Uporabnik (tj. tako podpisnik kot uporabnik, ki podpis preverja) mora imeti dostop do nje. Obstajati mora tudi način, na katerega lahko uporabnik ugotovi, da je politika avtentična. Nekaj najbolj pogostih oblik objave politike:

- politika je objavljena na strežniku, do katerega je možen dostop preko protokola SSL;
- besedilo politike je vgrajeno v aplikacijo, ki ji uporabnik zaupa in katere izvor pozna;
- »tradicionalna« različica politike je natisnjena na papirju in potrjena z žigom ali navadnim podpisom;

☐ **(K10) Pred podpisom mora biti podpisnik seznanjen z vrednostjo** *podpisnih atributov***.**

Podpisni atributi so skupaj z *dokumentom za podpis* vključeni v elektronski podpis, katerega dodatno opredeljujejo. Njihov nabor in pomen je podrobno opredeljen v *politiki e-podpisa.* Primeri podpisnih atributov so npr. sklic na podpisnikovo digitalno potrdilo, namen elektronskega podpisa ipd. Uporabnik mora biti pred podpisom seznanjen z vrednostjo vseh podpisnih atributov, ki so vključeni v elektronski podpis. Najpomembnejše atrubute, npr. podpisno digitalno potrdilo, je najprimerneje prikazati v uporabniškem vmesniku aplikacije.

☐ **(K11)** *Sredstvo za ustvarjanje varnega elektronskega podpisa* **podpira delo z** *napravo za ustvarjanje podpisa***, ki za hranjenje** *podatkov za podpisovanje* **uporablja namensko strojno opremo.**

Varno hranjenje *podatkov za elektronsko podpisovanje* je naloga podpisnika[1]. Danes lahko dovolj visoko stopnjo varnosti teh podatkov dosežemo le z uporabo namenske strojne opreme – npr. pametnih kartic. Uporaba manj varne izvedbe *naprave za ustvarjanje podpisa*, npr. sklopa programskih knjižnic, ki *podatke za elektronsko podpisovanje* shranjujejo kar na zaščitenem delu trdega diska splošno-namenskega računalnika, ni priporočljivo.

☐ **(K12)** *Sredstvo za ustvarjanje varnega elektronskega podpisa* **ne uporablja** *podatkov za elektronsko podpisovanje* **brez vednosti imetnika teh podatkov.**

[1] ZEPEP, 22. člen.

Vsaka uporaba *podatkov za elektronsko podpisovanje* brez vednosti podpisnika je prepovedana. Uporabnik mora biti torej seznanjen z vsako uporabo podatkov za elektronsko podpisovanje. Uporabniški vmesnik aplikacije mora uporabnika jasno obvestiti o uporabi *podatkov*. To najlažje zagotovimo s poenotenim uporabniškim vmesnikom pred vsako izvedbo podpisovanja v aplikaciji, npr. z nekaj jasnimi stavki o nameri in gumbom »Podpiši«.

☐ **(K13) Za vzpostavitev enakovrednosti elektronskega podpisa z lastnoročnim mora podpisnik uporabiti kvalificirano digitalno potrdilo.**

Če želimo doseči pravno veljavnost elektronsko podpisanih podatkov, mora podpisnik pri podpisovanju uporabiti kvalificirano digitalno potrdilo. Zahteve za izdajanje kvalificiranih digitalnih potrdil navaja [ZEPEP]. Primera overiteljev, ki v Sloveniji izdajajo kvalificirana digitalna potrdila, sta SIGEN-CA ali Pošta®ca.

☐ **(K14) Format** *dokumenta za podpis* **je dokumentiran. Dokumentacija je dostopna na zahtevo.**

Oblika *dokumenta za podpis* naj bo dokumentirana. To omogoča uporabo in prikaz dokumenta tudi tretjim aplikacijam. Priporočljivo (ne pa tudi nujno) je, da je format standardiziran. Standardiziran format, npr. XML za vsebino podatkov in XSLT za prikaz podatkov, omogoča uporabo standardnih prikazovalnikov, npr. spletnega brskalnika.

☐ **(K15) Format** *rezultata podpisa* **temelji na standardih in je dokumentiran. Dokumentacija je dostopna na zahtevo.**

Format *rezultata podpisa* mora biti dokumentirana in standardizirana, kar omogoča posredovanje *rezultata podpisa* in preverjanje podpisa tudi tretjim osebam. Najbolj razširjena standardna formata *rezultata podpisa* sta standard podjetja RSA PKCS#7 [PKCS#7] in standard organizacije W3C XML-Signature [XML-DSIG].

☐ **(K16)** *Sredstvo za ustvarjanje varnega elektronskega podpisa* **ne spreminja podatkov, ki jih podpisuje.**

Sredstvo za ustvarjanje elektronskega podpisa ne sme spremeniti podatkov, ki jih podpisuje. To podpisniku zagotavlja, da bodo dejansko podpisani tisti podatki, ki mu jih je prikazala aplikacija.

☐ **(K17) Če bi lahko** *dokument za podpis* **vseboval skrite podatke, npr. skrito besedilo, makroje ali aktivne vsebine, mora** *sredstvo za ustvarjanje varnega elektronskega podpisa* **o tem opozoriti podpisnika.**

Skriti podatki, tj. skrito besedilo, makroji, skripte ali druge aktivne vsebine lahko spremenijo pomen ali prikaz poslovnega dokumenta. Primer aktivne vsebine je skripta, ki v odvisnosti od časa ali datuma prikaže na ekranu drugačno vsebino dokumenta. To pomeni, da v času preverjanja podpisa vidimo drugačno predstavitev dokumenta kot v trenutku podpisa, kar je v nasprotju z osnovnim namenom elektronskega podpisa.

☐ **(K18) Če je podpisnik daljše obdobje neaktiven, se postopek podpisa prekine.**

Podpisnik lahko v času izvedbe elektronskega podpisa postopek pozabi prekiniti in zapusti svoj osebni računalnik. Če je naprava za podpisovanje že preverila njegovo istovetnost, bi napadalec lahko izkoristi začasno odsotnost podpisnika in izvedel postopek elektronskega podpisovanja do konca. Po prekinitvi se postopek ne sme nadaljevati, ampak se mora začeti od začetka.

☐ **(K19)** *Sredstvo za ustvarjanje varnega elektronskega podpisa* **deluje skladno s** *politiko e-podpisa.*

Natančna pravila, po katerih je potrebno izvesti elektronski podpis, je potrebno opredeliti tudi v *politiki e-podpisa*. To z drugimi besedami pomeni, da je potrebno vse zahteve za izvedbo varnega elektronskega podpisa, ki jih navajamo v tem poglavju, navesti v *politiki e.podpisa*. *Sredstvo za ustvarjanje varnega elektronskega podpisa* mora biti

skladno z določili te politike.

☐ **(K20) Podpisnik mora podpisan elektronski dokument shraniti v elektronski arhiv.**

Rezultat podpisa, običajno želimo varno shraniti. Elektronski arhiv zagotavlja varno shranjevanje in dosegljivost elektronskega dokumenta. Doba arhiviranja je odvisna od vrste dokumenta. Zahteve za elektronski arhiv so opredeljene v [ESlogArhiv].

1.3.2 Ustvarjanje podpisa – scenarij B2C ali B2B za interaktivne obdelave.

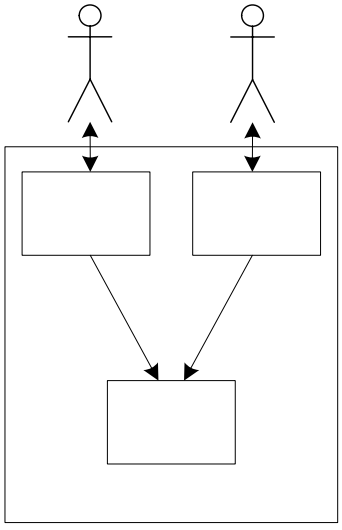
Kontrolni seznam v nadaljevanju podaja opis funkcionalnosti, ki se nanašajo na primer, kjer končni uporabniki (podpisniki) nimajo neposrednega stika z *napravo za ustvarjanje podpisa*, ampak z njo sodelujejo posredno, preko obstoječe zaledne aplikacije. Elektronsko podpisane dokumente ustvarjajo torej s pomočjo obstoječe aplikacije, ki pa sama nima sposobnosti elektronskega podpisovanja ali pa vgraditev tovrstne komponente predstavlja prezahteven poseg vanjo. Tipično gre za poslovne uporabnike v večjih podjetjih, kjer že imajo vzpostavljen lasten zaledni informacijski sistem z množico vnosnih ali preglednih obrazcev, ki predstavljajo vmesnik za elektronske dokumente. Zaledje običajno sestavlja (modularna) enotna poslovna aplikacija (npr. sistem ERP) ali pa množica različnih poslovnih aplikacij.

Opomba: podjetje lahko v posameznih primerih integrira elektronsko podpisovanje tudi neposredno v zaledno aplikacijo. V tem primeru gledamo na ustvarjanje podpisa enako kot pri scenariju C2X v točki 1.3.1.

V primeru B2C ali B2B (B2X) je *aplikacija, ki podpisuje*, kot na porazdeljeni sistem, ki ga sestavljajo

- zaledne aplikacije (Z1, Z2, ..., Zn) in
- *komponenta za elektronsko podpisovanje* (K).

Slika 1 prikazuje zgradbo opisanega porazdeljenega sistema. Večji del *funkcionalnosti, povezane z elektronskim podpisom*, ostaja v komponenti za elektronsko podpisovanje, del pa se seli v zaledni sistem. Povedano drugače – zahtevana funkcionalnost *aplikacije, ki podpisuje*, je sedaj porazdeljena med aplikacije zalednega sistema Z in *komponento za elektronsko podpisovanje* K. Tipično zaledne aplikacije v svojih obrazcih že vsebujejo prikaz vseh elektronskih dokumentov. Zato pri najbolj naravni delitvi funkcionalnosti zaledne aplikacije običajno izvedejo prikazovalnik *dokumenta za podpis* in poskrbijo za interakcijo z uporabnikom, komponenta pa neposredno komunicira z *napravo za ustvarjanje podpisa* in poskrbi za ostale funkcionalnosti.



Slika 1 – šibka povezanost med zaledjem in komponento za elektronsko podpisovanje

Povezava med sestavnimi deli je šibka - integracija je npr. izvedena na nivoju podatkovnega vira (npr. z izvozom

dokumentov iz podatkovne baze).

☐ **Točke iz kontrolnega seznama, ki se prenesejo na zaledne aplikacije so: (K1)**, **(K5)**, **(K6)**, **(K9)**, **(K10) in (K12)**.

Ker zaledne aplikacije v obstoječih obrazcih običajno že vsebujejo prikazovalnik *dokumenta za podpis* in poskrbijo za interakcijo z uporabnikom, morajo poskrbeti za vse funkcionalnosti, ki se na prikazovalnik nanašajo.

☐ **Točke iz kontrolnega seznama, ki ostanejo nespremenjene: (K4)**, **(K11)**, **(K13)**, **(K14)**, **(K15)**, **(K16), (K19) in (K20)**.

Točka (K4) se vsebinsko dopolnjuje s točkama (K20) in (K21). Pri ostalih gre za splošna načela, ki veljajo tudi za scenarij B2X.

☐ **Točke iz kontrolnega seznama, ki so v opisanem scenariju nepotrebne: (K7), (K8), (K17), (K18)**.

V scenariju B2X se opisane točke rešujejo z drugačnimi mehanizmi.

Spremenjene točke iz kontrolnega seznama:

☐ **(K2) → (K2') Podpis predstavitve je opcijski.**

Ker je prikaz podatkov izveden v zaledni aplikaciji, oblika prikaza pa je tipično nestandardna (npr. zaslonska slika v programu DOS), je vključevanje predstavitve v tem primeru nesmiselno. Za pravilno predstavitev dokumenta uporabniku (podpisniku) poskrbimo s pravilno integracijo dokumenta v zaledni sistem. Pri scenariju B2B takšna izvedba zadošča.

Če je prejemnik elektronskega sporočila končni uporabnik (scenarij B2C), ki bo dokument želel videti v človeku razumljivi obliki, je priporočljivo, da sporočilu dodamo tudi (referenco na) predstavitev, s katero bo dokument pogledal prejemnik. V tem primeru mora elektronski podpis varovati tudi predstavitev. Predstavitev mora biti vsebinsko enakovredna tisti v zaledni aplikaciji.

☐ **(K3) → (K3') Lahko se uporablja skupno digitalno potrdilo.**

Pri scenarijih B2X se najbolj pogosto uporabi eno digitalno potrdilo za podpis vseh dokumentov, ki se nanašajo na podjetje ali posamezni oddelek. Takrat je najbolje uporabiti digitalno potrdilo, ki se glasi na uveljavljeno splošno ime podjetja, npr. »Računovodstvo podjetja X«. V tem primeru je uporabnika potrebno o uporabljenem potrdilu zgolj obvestiti.

Nove točke kontrolnega seznama:

☐ **(K21) Zaledna aplikacija in** *komponenta za elektronsko podpisovanje* **morata komunicirati preko** *zaupanja vredne povezave.*

Ker govorimo o porazdeljenem sistemu, je varna in nadzorovana integracija *komponente za elektronsko podpisovanje* z zalednimi aplikacijami temeljnega pomena. Katerakoli zaledna aplikacija lahko uporablja *komponento* le z vzpostavitvijo zaupanja vredne povezave. Ker gre za nadzorovano zaledno okolje, lahko tovrstno povezavo zagotovimo z različnimi kombinacijami fizičnega varovanja, omejevanja na omrežnem nivoju (npr. omejevanje povezljivosti po številkah IP, uporaba požarne pregrade, povezave VPN ipd.) ali s preverjanjem istovetnosti na aplikacijskem nivoju (npr. z uporabo protokola SSL, kjer obe aplikaciji preverita istovetnost druge strani).

☐ **(K22) Povezava med zalednimi aplikacijami in *komponento za elektronsko podpisovanje* mora biti dokumentirana.**

Povezava med bistvenimi komponentami porazdeljenega sistema mora biti dokumentirana. Jasno morajo biti opredeljeni elementi vzpostavljanja zaupanja vredne povezave. Opisana mora biti delitev *funkcionalnosti, povezane z elektronskim podpisom*, med porazdeljenimi elementi sistema. Opredeljeno naj bo, kako se uporabniška interakcija z zaledno aplikacijo preslika v zahteve za elektronsko podpisovanje.

☐ **(K23) Integracija elektronskega dokumenta z zaledno aplikacijo mora biti dokumentirana.**

Integracija elektronskega dokumenta v zaledni sistem poskrbi za pravilno predstavitev dokumenta uporabniku (podpisniku), ki ne sme spreminjati pomena elektronskega dokumenta. V primeru podpisovanja gre za pravilen izvoz dokumenta iz zaledja. Pomen dokumenta za podpis, ki je predstavljen podpisniku, ni opredeljen s predstavitvijo (kot pri scenariju C2X), ampak je opredeljen z integracijo. Integracija mora biti dokumentirana.

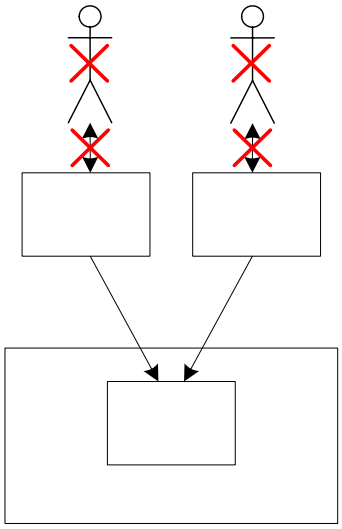
1.3.3 Ustvarjanje podpisa – scenarij B2C ali B2B za samodejne obdelave.

Kontrolni seznam v nadaljevanju podaja opis funkcionalnosti, ki se nanašajo na poseben primer sistema B2X, kjer izdelave elektronskega dokumenta ne prožijo uporabniki, ampak dokument nastane kot rezultat samodejne obdelave v zalednem informacijskem sistemu. Gre za predvideni odziv[2] zaledne aplikacije, ki se lahko samodejno sproži ob določenem času ali pa gre za samodejen odziv na prejeto sporočilo iz okolja (npr. prejem zahteve za poročilo o stanju zalog). Pogosto zaledna poslovna aplikacija sama nima sposobnosti elektronskega podpisovanja.

V tem primeru gledamo na *aplikacijo, ki podpisuje*, kot na porazdeljeni sistem, ki ga sestavljajo

- zaledne aplikacije (Z1, Z2, ..., Zn) in
- *komponenta za elektronsko podpisovanje* (K), ki neposredno komunicira z *napravo za ustvarjanje podpisa*,
- uporabniki pa niso udeleženi pri izdelavi elektronskega podpisa.

Zaledni sistem lahko v tem primeru pustimo praktično nespremenjen, tako da ne izvaja *funkcionalnosti, povezane z elektronskim podpisom*, te *funkcionalnosti* (sicer okrnjena) lahko v celoti prepusti komponenti za elektronsko podpisovanje. Spodnja slika prikazuje zgradbo opisanega porazdeljenega sistema.



Slika 2 – samodejni odziv zaledja in aplikacije za elektronsko podpisovanje

[2] . Samodejni odziv informacijskega sistema je opredeljen v 5. členu [ZEPEP]

Poslovne odločitve ob samodejnem odzivu ne sprejme človek - izdelava poslovnega dokumenta je rezultat nadzorovanega, sprogramiranega informacijskega sistema, zato so tudi zahtevane funkcionalnosti *sredstva za varno elektronsko podpisovanje* drugačne. Posebnost opisanega scenarija v primerjavi z interaktivnim scenarijem so opisane v nadaljevanju.

☐ **Točke iz kontrolnega seznama, ki ostanejo nespremenjene: (K2'), (K3'), (K4)**, **(K11)**, **(K13)**, **(K14)**, **(K15)**, **(K16), (K19), (K20), (K21), (K22) in (K23)**.

Točka (K4) se vsebinsko dopolnjuje s točkama (K20) in (K21). Pri ostalih gre za splošna načela, ki veljajo tudi za scenarij »samodejno proženega« B2X.

☐ **Točke iz kontrolnega seznama, ki so v opisanem scenariju nepotrebne: (K1)**, **(K5)**, **(K6)**, **(K7), (K8), (K9)**, **(K10), (K12), (K17) in (K18)**.

Ker poslovne odločitve in izdelave ustreznega dokumenta ne sprejme človek, so nepotrebne predvsem funkcionalnosti varnega pregledovalnika.

1.3.4 Preverjanje podpisa – scenarij B2C in C2C

Kontrolni seznam v nadaljevanju podaja opis funkcionalnosti, ki se nanašajo na primer, ko uporabnik (prejemnik elektronskega dokumenta) neposredno uporablja *aplikacijo za preverjanje elektronskega podpisa*. Tipično gre za scenarije C2C ali B2C (X2C), kjer *aplikacijo* uporabljajo fizične osebe, samostojni podjetniki ali manjša podjetja, ki nimajo lastnega zalednega informacijskega sistema.

Primeri:
- integracija varnega preverjanja elektronskega podpisa v spletno aplikacijo,
- namenska komponenta, tesno povezana z zaledno aplikacijo (pametnim odjemalcem) ali spletno aplikacijo (npr. Javanski »applet«, komponenta ActiveX).

☐ **(K24) Uporabnik si v trenutku preverjanja podpisa lahko ogleda** *dokument za podpis, status podpisa*, *podpisne* **in** *ostale atribute* **ter** *overitveno pot.*

V času preverjanja podpisa mora biti dokument prikazan na takšen način, da ima isti pomen kot takrat, ko je bil prikazan podpisniku. Pomen dokumenta se od trenutka podpisovanja ne sme spremeniti. Če dokument vsebuje več podpisov, mora biti razviden skupen status veljavnosti, na zahtevo pa tudi statusi posameznih podpisov. Če podpis ni veljaven, mora biti to jasno prikazano, navesti pa je potrebno tudi razlog. Uporabnik si lahko ogleda, s katerim digitalnim potrdilom je bilo sporočilo podpisano, kakšna je njegova overitvena pot in preveri veljavnost vseh potrdil na overitveni poti.

☐ **(K25) Če je podpisan le del** *dokumenta*, **je jasno razvidno, kateri del je podpisan.**

Nekatere rešitve za elektronsko podpisovanje omogočajo podpisovanje delov dokumentov. Uporabnik mora imeti jasno informacijo o tem, kateri deli so podpisani.

☐ **(K26) Če je** *dokument* **podpisalo več podpisnikov, je to jasno razvidno. Razvidno je tudi, kdo je podpisal kateri del** *dokumenta*.

Nekatere rešitve za elektronsko podpisovanje omogočajo, da en dokument podpiše več podpisnikov. Uporabnik mora imeti jasno informacijo o tem, kateri deli so podpisani, kdo jih je podpisal in kako (če sploh so) so podpisi gnezdeni.

☐ **(K27)** *Sredstvo za preverjanje elektronskega podpisa* **opozori uporabnika, kadar ne more pridobiti vseh**

ustreznih *podatkov za overjanje podpisa***.**

Tipičen primer *podatkov za overjanje podpisa* je seznam preklicanih digitalnih potrdil, ki so objavljena na overiteljskem strežniku. Praviloma seznam je dostopen preko omrežja. Pri preverjanju podpisa se lahko zgodi, da dostop do teh podatkov ni možen (npr. uporabnik nima dostopa do omrežja, strežnik, ki ponuja podatke ne deluje ipd). V takšnem primeru mora *sredstvo za preverjanje elektronskega podpisa* jasno opozoriti uporabnika, da teh podatkov ni bilo moč pridobiti, status elektronskega podpisa pa je v tem primeru neznan.

☐ **(K28) Če rezultat podpisa ob podpisu ni bil časovno žigosan, se mora ob vstopu v prejemnikov informacijski sistem izvesti tudi časovni žig**.

Če prejemnik sprejme poslovno odločitev na podlagi v elektronsko podpisanem dokumentu opredeljene zaveze podpisnika, je izpostavljen tveganju v primeru naknadnega preklica podpisnikovega digitalnega potrdila. S tem postane podpis neveljaven, poslovni dogovor pa za podpisnika nezavezujoč. S časovnim žigom se prejemnik zavaruje - podpisniku onemogoči naknadno nezmožnost zanikanja. Žigosani morajo biti tako *rezultat podpisa* kot tudi *podatki za preverjanje elektronskega podpisa*.

Če je bil časovni žig izveden že ob podpisu, ta korak ni potreben.

☐ **(K29) Uporabnik ima dostop do** *politike e-podpisa***.**

Politika e-podpisa vsebuje določila o podpisovanju in preverjanju podpisa. Podobno, kot to velja pri podpisovanju, mora tudi uporabnik, ki podpis preverja, imeti dostop do *politike*. Obstajati mora tudi način, na katerega lahko uporabnik ugotovi, da je politika avtentična. Nekaj najbolj pogostih oblik objave politike:

- politika je objavljena na strežniku, do katerega je možen dostop preko protokola SSL;
- besedilo politike je vgrajeno v aplikacijo, ki ji uporabnik zaupa in katere izvor pozna;
- »tradicionalna« različica politike je natisnjena na papirju in potrjena z žigom ali navadnim podpisom;

☐ **(K30)** *Sredstvo za preverjanje elektronskega podpisa* **deluje skladno s** *politiko e-podpisa.*

Natančna pravila, po katerih je potrebno preveriti elektronski podpis so podana v *politiki e.podpisa*. *Sredstvo za preverjanje elektronskega podpisa* mora biti skladna z določili te politike.

☐ **(K31)** *Sredstvo za preverjanje elektronskega podpisa* **opozori uporabnika, če zazna, da podpis ni skladen s** *politiko e-podpisa***.**

V nekaterih primerih lahko *sredstvo za preverjanje elektronskega podpisa* ugotovi, da podpis ni skladen s politiko *e-podpisa*. Sredstvo lahko npr. ugotovi, da določeni *podpisnimi atributi* (npr. sklic na *politiko e-podpisa*) manjkajo, zazna neznan ali nedovoljen format dokumenta, ugotovi lahko, da se je za izvedbo elektronskega podpisa uporabilo digitalno potrdilo, izdano s strani overitelja, ki ni priznan v okviru politike ali ki ne izdaja kvalificiranih potrdil ipd.

Seveda nekaterih kršitev *politike e-podpisa sredstvo za preverjanje elektronskega podpisa* zaradi njihove narave ne more odkriti. *Sredstvo* npr. ne more preveriti, ali so izpolnjene zahteve, ki se nanašajo na okolje, v katerem deluje *aplikacija, ki podpisuje*.

☐ **(K32) Prejemnik mora podpisan elektronski dokument, ki je predmet preverjanja, shraniti v elektronski arhiv**.

Prejeti elektronski dokument, s podpisom katerega se pošiljatelj zaveže za njegovo vsebino, želimo kot prejemnik varno shraniti. Elektronski arhiv zagotavlja varno hranjenje in dosegljivost elektronskega dokumenta. Arhivirati je potrebno vse podatke, ki vstopajo v preverjanje elektronskega podpisa (*rezultat podpisa*, *dokument za podpis*, *podatke za preverjanje elektronskega podpisa* in *podatke za vrednotenje podpisa*), ponavadi jih je večina že

vključenih v dokument. Doba arhiviranja je odvisna od vrste dokumenta. Zahteve za elektronski arhiv so opredeljene v [ESlogArhiv].

1.3.5 Preverjanje podpisa – scenarij B2B in C2B

Kontrolni seznam v nadaljevanju podaja opis funkcionalnosti, ki se nanašajo na primer, kjer končni uporabniki nimajo neposrednega stika z *aplikacijo za preverjanje elektronskega podpisa*, ampak z njo sodelujejo posredno, preko obstoječe zaledne aplikacije. Vmesnik do elektronskih dokumentov še vedno predstavlja množica obstoječih obrazcev v zalednem sistemu, ki pa sam nima sposobnosti preverjanja elektronskega podpisa ali pa vgraditev tovrstne funkcionalnosti predstavlja prezahteven poseg vanj. Tipično gre za poslovne uporabnike v večjih podjetjih, kjer že imajo vzpostavljen lasten zaledni informacijski sistem - (modularno) poslovno aplikacijo (npr. sistem ERP) ali množico različnih poslovnih aplikacij.

Opomba: podjetje lahko v posameznih primerih integrira preverjanje elektronskega podpisa tudi neposredno v zaledno aplikacijo. V tem primeru gledamo na preverjanje podpisa enako kot pri scenariju X2C v točki 1.3.4.

V primeru X2B sestavljata *aplikacija za preverjanje elektronskega podpisa* in zaledni sistem povezan porazdeljeni sistem, ki

- zagotavlja varno preverjanje elektronskega podpisa,
- uporabnikom pa še vedno omogoča delo z dokumenti v obstoječem zalednem informacijskem sistemu.

Povezava med sestavnimi deli je šibka - integracija je npr. izvedena na nivoju podatkovnega vira (npr. z izvozom dokumentov iz podatkovne baze).

Nove točke kontrolnega seznama, ki se nanašajo predvsem na integracijo:

☐ **(K33) Zaledna aplikacija in** *aplikacija za preverjanje elektronskega podpisovanja* **morata komunicirati preko** *zaupanja vredne povezave.*

Ker govorimo o porazdeljenem sistemu, je varna in nadzorovana integracija *aplikacije za preverjanje elektronskega podpisa* z zalednimi aplikacijami temeljnega pomena. Katerakoli zaledna aplikacija lahko uporablja *rezultate preverjanja* le z vzpostavitvijo zaupanja vredne povezave. Tovrstno povezavo lahko zagotovimo z različnimi kombinacijami fizičnega varovanja, omejevanja na omrežnem nivoju (npr. omejevanje povezljivosti po številkah IP, uporaba požarne pregrade, povezave VPN ipd.) ali s preverjanjem istovetnosti na aplikacijskem nivoju (npr. z uporabo protokola SSL, kjer obe aplikaciji preverita istovetnost druge strani).

☐ **(K34) Vsi elektronsko podpisani dokumenti vstopajo v informacijski sistem le preko** *aplikacije za preverjanje elektronskega podpisa***. Rezultat preverjanja so** *dokument za podpis, status podpisa***,** *podpisni* **in** *ostali atribute* **ter** *overitvena pot***. Če so bili podpisani le deli dokumenta, je tudi ta informacija del rezultata preverjanja. Rezultat se posreduje v zaledno aplikacijo.**

Preverjanje elektronskega podpisa mora biti eden od prvih korakov po vstopu dokumenta v informacijski sistem prejemnika. Rezultat preverjanja (dokument za podpis, status podpisa, podpisni in ostali atributi, overitvena pot), je predmet integracije v zaledni informacijski sistem.

☐ **(K35). Zaledna aplikacija ne spreminja podpisanega dokumenta po tem, ko ga je prevzela od** *aplikacije za preverjanje elektronskega podpisa***.**

Ker zaledna aplikacija uporablja izvorni elektronski dokument, ki ni več zaščiten z elektronskim podpisom, mora lastnost nespremenljivosti zagotoviti z drugimi mehanizmi, ki naj bodo določeni že v arhitekturi in zasnovi porazdeljenega sistema.

☐ **(K36)** *Aplikacija za preverjanje elektronskega podpisa* **zadrži nadaljnji prenos dokumenta v zaledni informacijski sistem, kadar ne more pridobiti vseh ustreznih** *podatkov za overjanje podpisa***.**

Tipičen primer *podatkov za overjanje podpisa* je seznam preklicanih digitalnih potrdil, ki so objavljena na overiteljskem strežniku. Praviloma je seznam dostopen preko omrežja. Pri preverjanju podpisa se lahko zgodi, da dostop do teh podatkov ni možen (npr. uporabnik nima dostopa do omrežja, strežnik, ki ponuja podatke ne deluje ipd). V takšnem primeru mora *aplikacija za preverjanje elektronskega podpisa* onemogočiti prenos nepreverjenega dokumenta v zaledje. Zaledni aplikaciji morajo biti na voljo podatki o tem, da teh podatkov ni bilo moč pridobiti, status elektronskega podpisa pa je v tem primeru neznan.

☐ **Točke, ki se smiselno prenesejo na zaledno aplikacijo: (K24), (K25), (K26)**.

Podatke, ki so rezultat preverjanja elektronskega podpisa, mora zaledna aplikacija prikazati uporabniku. Tovrstna nadgradnja pomeni preprostejši poseg v zaledno aplikacijo od neposredne integracije elektronskih dokumentov. Z varno integracijo porazdeljenega sistema pa dosežemo praktično enakovreden nivo računalniške varnosti.

☐ **Točke iz kontrolnega seznama, ki ostanejo nespremenjene: (K28), (K29), (K30), (K32)**

Gre za splošna načela, ki veljajo tudi za scenarij X2B.

1.3.6 Namestitev

☐ **(K37) Postopek za namestitev in konfiguracijo** *sredstva za varno elektronsko podpisovanje* **in** *preverjanje podpisa* **mora biti varen.**

Aplikacija se mora namestiti iz varnega medija npr. CD plošče, katere avtentičnost in integriteto lahko uporabnik enostavno potrdi na podlagi vtisnjenega holograma. Če se aplikacija ali njen del prenese iz Interneta, mora biti elektronsko podpisan(a). Pred namestitvijo aplikacije mora biti podpis preverjen, rezultati preverjanja podpisa (*status podpisa*, *overitvena pot*,...) pa prikazani uporabniku.

☐ **(K38) Uporabnik je obveščen o vseh varnostnih posodobitvah, ki se nanašajo na** *sredstvo za varno elektronsko podpisovanje* **in** *preverjanje podpisa***.**

Priporočljivo je, da sta preverjanje izdajanja varnostnih posodobitev in njihova namestitev vgrajena v samo aplikacijo. Drug primer obveščanja uporabnikov je obveščanje po elektronski pošti. Postopek namestitve posodobitev naj bo kar se da enostaven.

1.3.7 Okolje

☐ **(K39) Uporabnik ima ustrezna navodila o tem, kako varovati** *sredstvo za varno elektronsko podpisovanje* **in** *preverjanje podpisa,* **ter opis okolja, v katerem to sredstvo deluje . Navodila morajo biti izvedljiva.**

Uporabnika moramo podučiti o varnem ravnanju s *sredstvom za varno elektronsko podpisovanje*. Varovanje ponavadi vključuje omejevanje dostopa do računalnika, uporabo požarnega zidu, uporabo protivirusnih programov ipd.

1.3.8 Scenarij elektronskega poslovanja s posrednikom – B2X in X2B

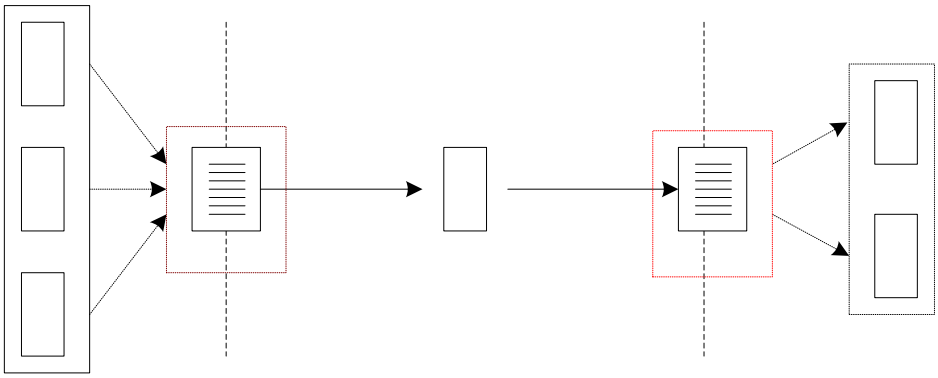
Elektronsko poslovanje je za vsako podjetje velik zalogaj tako iz vsebinskega kot tehničnega vidika. Vsebinsko poznavanje problematike zahteva specifična znanja, poznavanje zakonodaje, ki se še vedno spreminja in dopolnjuje, za vzpostavitev sistema pa je potrebna namenska strojna in programska oprema. Iz teh razlogov je za veliko podjetij smotrneje, da v svet elektronskega poslovanja vstopijo preko posrednikov.

Strogo tehnično gledano je glavna naloga posrednika, da podjetjem, ki si želijo neposredno izmenjati vsebinsko enakovredna sporočila, pomaga premostiti razlike v

- komunikacijskih protokolih in
- oblikah izmenjanih sporočil

Elektronski podpis in premoščanje razlike v obliki sporočila

Tipični primer izmenjave B2B dveh podjetij s pomočjo posrednika opisuje slika 3. Podjetje 1 iz zaledne aplikacije na dogovorjen način izvozi elektronska sporočila v obliki, na katero so integrirane njegove zaledne aplikacije (npr. enostavni račun v obliki e-SLOG XML). Ker je oblika sporočil, ki jih pričakuje podjetje 2 drugačna (npr. račun v obliki sporočila e-SLOG EDIFACT), posrednik izvede preoblikovanje sporočila iz oblike XML v EDIFACT. Težava opisanega scenarija je v tem, da posrednik ne sme spremeniti elektronsko podpisanega sporočila podjetja 1, saj bi podpis s tem postal neveljaven.



Slika 3 – scenarij izmenjave s posrednikom

Opisano težavo najlažje rešimo tako, da posrednik preveri elektronski podpis na prejetem sporočilu. *Dokument za podpis1* (Podjetja 1) preoblikuje v vsebinsko enakovreden *dokument za podpis 2* (Podjetja 2), ki ga podpiše s svojimi *podatki za elektronsko podpisovanje*. Sporočilo posreduje podjetju 2.

Opisano velja tudi za scenarij z več posredniki.

Kontrolni seznam, ki opisuje zahteve glede preverjanja podpisa, preoblikovanja in podpisovanja posrednika:

IS1

☐ **(K40) Posrednik mora preveriti elektronski podpis na prejetem dokumentu podjetja pošiljatelja v skladu s priporočili za scenarij X2B.**

Z arhivsko kopijo podpisanega dokumenta, bo posrednik podjetju dokazal zahtevo za posredovanje sporočila.

Z1

☐ **(K41) Nobena preslikava, ki jo posrednik izvaja, ne sme spremeniti vsebine sporočila.**

Preslikave, ki jih posrednik izvaja, lahko spremenijo le obliko sporočila. Vsebina sporočila mora ostati nespremenjena.

☐ **(K42) Posrednik mora imeti dokumentirano vsako preslikavo, ki jo bo izvajal.**

Z2

P

XML

Z3

V dokumentaciji preslikave se lahko vedno preveri njena vsebinska ustreznost. Dokumentacija se uporabi tudi ob preverjanju pravilnosti preoblikovanja.

☐ **(K43) Posrednik mora elektronsko podpisati sporočilo, ki ga bo posredoval podjetju prejemniku v skladu s priporočili za scenarij X2B.**

Z arhivsko kopijo prejetega in poslanega dokumenta, bo posrednik lahko vedno dokazal pravilnost preslikave.

Delitev odgovornosti (opredeljena v politiki vsakega od podpisnikov) med udeleženci pri scenariju s posrednikom je naslednja.

- Podjetje 1 pripravi elektronsko podpisano sporočilo v skladu s priporočili za scenarij B2X. Oblika dokumenta je dokumentirana (K14), v dokumentaciji pa je sporočilo vsebinsko opredeljeno (npr. pomen posameznih elementov datoteke XML). **Podjetje je odgovorno za vsebino sporočila, ki ga odda posredniku**, kar zagotovi s svojim elektronskim podpisom.
- Posrednik preveri elektronski podpis na prejetem sporočilu podjetja 1 v skladu s priporočili X2B. V primeru, da je podpis veljaven ima veljavno zahtevo podjetja 1 za posredovanje sporočila. Preoblikovanje iz oblike podpisnika v obliko prejemnika mora biti dokumentirano. Iz dokumentacije je razvidno, ali je preslikava vsebinsko korektna. **Posrednik je odgovoren za vsebinsko pravilnost preslikave**, kar zagotovi s svojim elektronskim podpisom rezultata preslikave. Pravilnost preslikave dokazuje na podlagi arhivske kopije prejetega in oddanega sporočila.
- Podjetje 2 preveri elektronski podpis na posrednikovem sporočilu v skladu s priporočili X2B. Oblika dokumenta ki ga pričakuje, je dokumentirana, v dokumentaciji pa je sporočilo vsebinsko opredeljeno.

1.3.9 Izjava o skladnosti

☐ **(K44) Izjava o skladnosti s pričujočimi priporočili poda proizvajalec** *sredstva za varno elektronsko podpisovanje* **in** *preverjanje podpisa***.**

Zaradi kompleksnosti procesa, ki je potreben za izdelavo *sredstva za varno elektronsko podpisovanje* in *preverjanje podpisa*, in zaradi širokega nabora možnosti za izvedbo tovrstnih aplikacij, za skladnost *sredstev* jamči proizvajalec sam.

Skladnost s temi priporočili lahko proizvajalec ugotovi na podlagi presoje, ki jo izvede sam, ali pa se za presojo obrne na tretjo stranko, ki je specializirana za tovrstne presoje. V obeh primerih lahko le sam poda izjavo o skladnosti s priporočili in s tem prevzame tudi morebitne obveznosti.

1.4. Terminološki slovar

časovni žig - časovni žig je elektronsko podpisano potrdilo overitelja, ki nedvoumno poveže vsebino elektronskega dokumenta s časom, v katerem je dokument obstajal, s čimer ponuja dokaz, da je elektronski dokument nastal pred navedenim časom.

podatki za elektronsko podpisovanje - podatki za elektronsko podpisovanje so edinstveni podatki, kot so šifre ali zasebni šifrirni ključi, ki jih podpisnik uporablja za oblikovanje elektronskega podpisa (ZEPEP, 2.člen)

podatki za preverjanje elektronskega podpisa - edinstveni podatki, kot so šifre ali javni šifrirni ključi, ki se uporabljajo za preverjanje elektronskega podpisa (ZEPEP, 2.člen)

politika e-podpisa – zbirka pravil za ustvarjanje in preverjanje elektronskega podpisa. Določa tudi pogoje, pod katerimi je elektronski podpis veljaven.

overitelj - fizična ali pravna oseba, ki izdaja potrdila ali opravlja druge storitve v zvezi z overjanjem ali elektronskimi

podpisi (ZEPEP, 2. člen)

sredstvo za preverjanje elektronskega podpisa - nastavljena programska ali strojna oprema, ki se uporablja za preverjanje elektronskega podpisa (ZEPEP, 2. člen)

sredstvo za varno elektronsko podpisovanje - nastavljena programska ali strojna oprema, ki jo podpisnik uporablja za oblikovanje varnega elektronskega podpisa (ZEPEP, 2. člen)

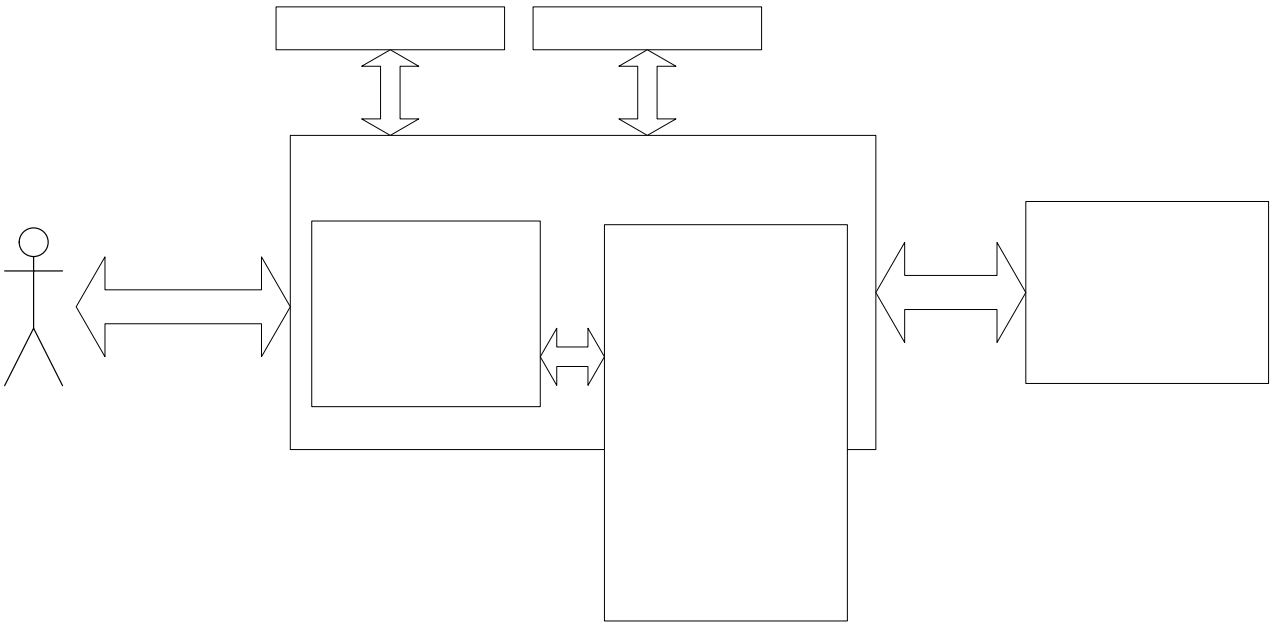
zaupanja vredna povezava – (trusted path)

1.5. Priloge

1.5.1 Izdelava in preverjanje elektronskega podpisa

1.5.1.1 Izdelava elektronskega podpisa

Slika 4 prikazuje komponente, ki nastopajo v procesu izdelave elektronskega podpisa in opredeljuje relacije med njimi. Povezave med komponentami morajo biti izvedene v obliki *zaupanja vredne povezave.*



Slika 4 – Komponente, ki nastopajo pri izdelavi elektronskega podpisa

Sredstvo za varno elektronsko podpisovanje je nastavljena programska ali strojna oprema, ki jo podpisnik uporablja za oblikovanje varnega elektronskega podpisa.

Sestavljajo ga
- *aplikacija, ki podpisuje*,
- *naprava za ustvarjanje podpisa*.

Aplikacija, ki podpisuje[3] je aplikacija, ki vodi podpisnika skozi proces izdelave varnega elektronskega podpisa. Za dejansko izvedbo podpisa uporablja *napravo za ustvarjanje podpisa.*

[3] Za razliko od tega dokumenta uporablja CWA 14170 ožji pogled. Tam je namreč uporabljen termin »Aplikacija za ustvarjanje elektronskega podpisa« (Signature Creation Application). Takšna aplikacija naj bi vsebovala predvsem funkcionalnost, ki je namenjena podpisovanju. Ostale funkcionalnosti aplikacije niso izrecno izpostavljene.

Aplikacije so v osnovi namenjene podpori poslovnim procesom in implementirajo določena poslovna pravila. Elektronski podpis je ponavadi le ena izmed infrastrukturnih funkcij tipične namenske aplikacije, ki jo uporablja podpisnik. Aplikacija lahko npr. uporabniku omogoča analizo podatkov in na podlagi analize pripravo ponudbe, ki jo lahko uporabnik digitalno podpiše. Drug primer je npr. program za branje in pošiljanje elektronske pošte, ki omogoča tudi elektronsko podpisovanje sporočil. Namen uporabe elektronskega podpisa je običajno prenos pravne veljavnosti papirnih dokumentov v elektronsko obliko, lahko pa ga uporabljamo zgolj kot dodaten varnostni element (povišanje nivoja varnosti). V zadnjem času je moč opaziti trend razvoja celovitih poslovnih aplikacij, ki integrirajo različno poslovno in infrastruktuno funkcionalnost (npr. elektronsko bančništvo kot del celovite računovodske aplikacije). Celovite aplikacije so tudi preprostejše za uporabo. Zato lahko upravičeno pričakujemo, da bodo v prihodnosti namenske aplikacije za elektronsko podpisovanje redke, funkcija elektronskega podpisa pa bo integrirana v same aplikacije. Varen način integracije funkcionalnosti za elektronsko podpisovanje je bistveni element varnosti *aplikacije, ki podpisuje*.

Aplikacija, ki podpisuje vsebuje torej funkcionalnost, ki je vezana na elektronski podpis in ostalo funkcionalnost. Funkcionalnost, ki je vezana na elektronski podpis, je naslednja:

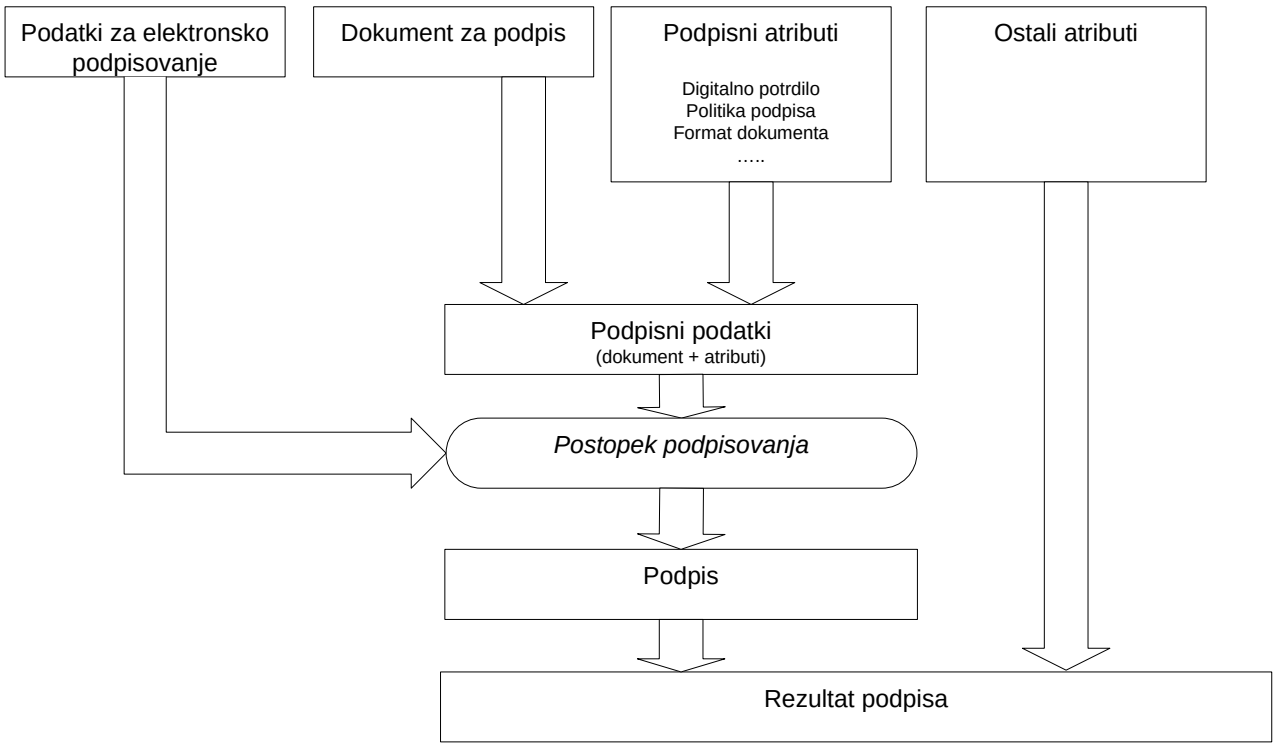
- priprava *dokumenta za podpis*,
- dostop do podatkov in storitev, ki jih ponuja *overitelj* digitalnih potrdil in dostop do *politike e-podpisa* (glej poglavje 1.5.1.3),
- avtentikacija podpisnika za namen dostopa do *podatkov za elektronsko podpisovanje,*
- komunikacija z *napravo za ustvarjanje podpisa*..

Naprava za ustvarjanje podpisa je zadolžena za dejansko izvedbo *varnega elektronskega podpisa* in varno hranjenje *podatkov za elektronsko podpisovanje* – t.j. edinstvenih podatkov, ki jih podpisnik uporablja za oblikovanje elektronskega podpisa.

Sredstvo za varno elektronsko podpisovanje praviloma deluje v nekem **okolju**. *Aplikacija, ki podpisuje*, tako lahko npr. uporablja storitve operacijskega sistema kot so prikaz uporabniškega vmesnika, dostop do zunanjih naprav (npr. trdih diskov) in omrežja. V okviru operacijskega sistema se ponavadi izvajajo tudi druge aplikacije. *Sredstvo za varno elektronsko podpisovanje* mora biti zaščiteno pred zlonamernimi aktivnostmi iz *okolja* (npr. trojanskimi konji, virusi,...), ki bi lahko varnostno ogrožale izvedbo elektronskega podpisa.

1.5.1.2 Postopek podpisovanja

Slika 5 prikazuje podatke, ki nastopajo pri izvedbi elektronskega podpisa. Natančen format podpisa presega okvir tega dokumenta. Opredeljen je v ločenem dokumentu [ESlogFormat].



Slika 5 – podatki, ki nastopajo pri izdelavi elektronskega podpisa

Postopek podpisovanja in parametri, ki v njem nastopajo je opredeljen v *politiki e-podpisa.*

Dokument za podpis je dokument, ki ga je podpisnik izbral ali sestavil v okviru *aplikacije, ki podpisuje*. Oblika (format) dokumenta je lahko različna. Dokument je lahko npr. v formatu, ki ga lahko neposredno prikažemo uporabniku (npr. slika). Žal takšni formati niso vedno primerni za nadaljnjo računalniško obdelavo podatkov. Zato je *dokument za podpis* ponavadi v obliki, ki je prijaznejša računalnikom – npr. v formatu EDI ali XML. Preden lahko takšen dokument prikažemo uporabniku, ga moramo preoblikovati (transformirati) v obliko, ki je primerna za prikaz. Transformacija mora ohraniti pomen dokumenta. Če je npr. dokument v obliki XML lahko za transformacijo uporabimo predlogo XSLT, ki iz XML dokumenta izdela stran HTML. Stran HTML pa je standardna oblika za prikaz v spletnem brskalniku. Priporočljivo je, da takšno transformacijo podpišemo skupaj z dokumentom. Ob preverjanju podpisa lahko tako preverimo tudi, ali uporabljamo pravilno transformacijo za prikaz dokumenta. Sam format dokumenta je praviloma podan kot eden izmed *podpisnih atributov*.

Dokument za podpis ne sme vsebovati skritih podatkov, npr. skritega besedila, makrojev ali aktivnih vsebin. Takšni podatki predstavljajo varnostno grožnjo, saj so odvisni od nepodpisane vsebine in se jih ponavadi podpisnik ali oseba, ki preverja podpis, ne zavedata.

Različne naprave lahko zaradi svojih omejitev (ločljivosti, števila barv, razsežnosti zaslona,...) prikažejo dokumente na različne načine. Če je izgled dokumenta bistven za njegov pomen (npr. pri dokumentu, ki predstavlja načrt za celostno grafično podobo podjetja), morajo biti uporabljene naprave in formati, ki zagotavljajo verodostojno predstavitev dokumenta. Tovrstne omejitve morajo biti podane v *politiki e-podpisa.*

Podpisni atributi vsebujejo dodatne podatke, ki se nanašajo na elektronski podpis. Podpisni atributi so tako kot sam *dokument za podpis* vključeni v podpis. Njihov nabor je podan v *politiki e-podpisa..* Primeri podpisnih atributov:

- sklic na digitalno potrdilo, ki se nanaša na podpisnikove *podatke za elektronsko podpisovanje*
- sklic na *politiko e-podpisa,*
- format *dokumenta za podpis,*
- namen podpisa (npr. strinjanje z dokumentom, dokaz prejema dokumenta, ipd.),
- dodatni atributi, ki jih določa *politika e-podpisa.*

Dokument za podpis in *podpisni atributi* skupaj tvorijo **podpisne podatke**[4]**.**

Ostali atributi vsebujejo dodatne podatke, ki se nanašajo na elektronski podpis, niso pa vključeni v sam podpis. Npr: različica aplikacije, s katero je narejen podpis. Njihov nabor je podan v *politiki e-podpisa..*

Podpisovanje se izvede po naslednjem postopku:

1. Podpisnik preko *aplikacije, ki podpisuje* ustvari ali izbere *dokument za podpis*
2. Če ima podpisnik več naborov *podatkov za podpis* (npr. več elektronskih potrdil) izbere, katere bo uporabil. Ta korak se lahko izvede tudi v okviru avtentikacije uporabnika aplikaciji (npr. če spletna aplikacija ob začetku dela uporabnika avtenticira na podlagi njegovega digitalnega potrdila in pripadajočih ključev).
3. *Aplikacija, ki podpisuje* na podlagi *politike e-podpisa* določi nabor in vrednosti za *podpisne atribute.*
4. Podpisnik ima možnost, da si pred nadaljevanjem ogleda *dokument za podpis* in *podpisne atribute* in da, če to želi, postopek podpisovanje prekine.
5. *Aplikacija, ki podpisuje* na podlagi *dokumenta za podpis* in *podpisnih atributov* določi *podpisne podatke*.
6. Preden lahko podpisnik dostopa do *podatkov za elektronsko podpisovanje,* se mora predstaviti *napravi za kreiranje podpisa* tako da npr. vnese PIN ali poda svoje biometrične podatke. Če naprava za kreiranje podpisa nima svojega uporabniškega vmesnika (npr. če ne uporabljamo čitalca pametnih kartic, ki ima integrirano tipkovnico za vnos PINa), se lahko uporabi uporabniški vmesnik *aplikacije, ki podpisuje.*
7. *Aplikacija, ki podpisuje* posreduje *podpisne podatke* ali njihov izvleček *napravi za ustvarjanje podpisa.*
8. *Naprava za ustvarjanje podpisa* na podlagi *podpisnih podatkov* in *podatkov za ustvarjanje podpisa* ustvari podpis in ga posreduje *aplikaciji, ki podpisuje*.
9. *Aplikacija, ki podpisuje* podpisu doda *ostale atribute* ter morebitne druge podatke (npr. *dokument za podpis*) in oblikuje *rezultat podpisa* v določenem formatu (npr. [XML-DSIG] ali [PKCS#7]). Opis formata *rezultata podpisa* presega okvir tega dokumenta.

Priporočljivo je, da se *rezultatu podpisa* doda tudi *časovni žig*. S pomočjo časovnega žiga lahko kasneje dokažemo, da je bil podpis izveden pred časom žigosanja in da je takrat obstajal tudi *dokument za podpis.*

V nekaterih primerih z *aplikacijo, ki podpisuje* podpisnik ne komunicira direktno, ampak posredno - preko nekega drugega informacijskega sistema. Takšen je npr. naslednji primer:

> Primer: Uporabnik uporablja interni informacijski sistem podjetja, v okviru tega tudi pripravlja različne dokumente. Preden se takšen dokument pošlje naslovniku v drugem podjetju, se pretvori v obliko, ki je primerna za izmenjavo podatkov med podjetji (npr. dokument XML). Pretvorjen dokument se posreduje *aplikaciji, ki podpisuje.* Ta dokumentu doda elektronski podpis in ga posreduje naslovniku.

Če se kateri izmed zgornjih korakov prenese na informacijski sistem, mora biti med *aplikacijo, ki podpisuje* in tem informacijskim sistemov vzpostavljena *zaupanja vredna povezava,* preko katere si lahko *aplikacija, ki podpisuje* in informacijski sistem na varen način izmenjata podatke. Ponavadi informacijski sistem prevzame eno ali več od naslednjih funkcij: priprava in ogled dokumenta, avtentikacija podpisnika, določitev vrednosti nekaterih *podpisnih atributov* ipd.

Ne glede na to, ali podpisnik komunicira z *aplikacijo, ki podpisuje* posredno ali neposredno, pa mora biti podpisnik seznanjen s *politiko e-podpisa*, ki jasno opredeljuje, kaj, kdaj in kako se podpisuje.

1.5.1.3 Politika e-podpisa

Politika e-podpisa je zbirka pravil za ustvarjanje in preverjanje elektronskega podpisa. Določa tudi pogoje, pod katerimi je elektronski podpis veljaven. Opredeljuje medsebojna razmerja, odgovornosti, pravna razmerja in tehnične pogoje vseh vključenih v storitev (podpisnika, *overitelja*, tistega, ki preverja podpis).

[4] *Podpisni podatki* niso isto kot *podatki za elektronsko podpisovanje*. Prvi predstavljajo podatke, ki bodo (ali so bili) podpisani, drugi pa edinstvene podatke, ki pripadajo podpisniku in jih le-ta uporablja pri oblikovanju podpisa kateregakoli dokumenta.

Priporočljivo je, da je sklic na *politiko e-podpisa* vključen v podpis kot eden izmed *podpisnih atributov (*glej poglavje 1.5.1.2). V nasprotnem primeru mora biti uporabljena *politika e-podpisa* podana na kakšen drug način (npr. v samem *dokumentu za podpis,* ali v ločeni pogodbi v primeru zaprtih sistemov).

Za spoštovanje *politike e-podpisa* so odgovorni vsi, na katere se ta varnostna politika nanaša. Upoštevanje tehničnih določil, ki jih postavlja *politika e-podpisa* je mogoče do neke mere vgraditi tudi v programsko opremo (npr. kot del *sredstva za varno elektronsko podpisovanje* ali *sredstva za preverjanje podpisa*). Za upoštevanje drugih določil (npr. uporabo požarnih zidov in protivirusnih programov) so odgovorni uporabniki.

Politika e-podpisa mora obstajati v obliki, ki je razumljiva uporabnikom. *Politika e-podpisa* lahko obstaja tudi v računalniški obliki (npr. v formatu XML[5]), če tehnične zahteve, ki jih določa niso fiksno vgrajene v aplikacije, na katere se nanaša.

Politika e-podpisa mora vsebovati:

- splošne podatki:
  - ime izdajatelja politike,
  - enolično oznako politike,
  - datum izdaje politike,
  - področje uporabe politike,
  - podatki o priznanih *overiteljih* digitalnih potrdil,
- podatke, ki se nanašajo na ustvarjanje digitalnega podpisa:
  - seznam obveznih *podpisnih atributov* in *ostalih atributov,*
  - tehnične zahteve glede uporabljenih algoritmov za digitalni podpis in parametrov teh algoritmov (nabor dovoljenih algoritmov, dolžine ključev ipd.),
  - zahteve, ki se nanašajo na uporabo *časovnega žiga* (podrobnosti so opisane v nadaljevanju),
  - tehnične zahteve glede formata *rezultata podpisa* (npr. [XML-DSIG], [PKCS#7],...),
  - zahteve, ki se nanašajo na *sredstvo za varno elektronsko podpisovanje* in okolje, v katerem to sredstvo deluje,
- podatke, ki se nanašajo na preverjanje podpisa:
  - pravila za gradnjo *overitvene poti* (certification path)[6],
  - pravila za preverjanje veljavnosti digitalnih potrdil v *overitveni poti* (npr. ugotavljanje statusa veljavnosti digitalnega potrdila s pomočjo CRL in OCSP),
  - zahteve, ki se nanašajo na uporabo *časovnega žiga,*
  - zahteve, ki se nanašajo na *aplikacijo, ki preverja podpis* in okolje, v katerem ta aplikacija deluje.

Politika e-podpisa mora biti skladna z določili tistih *overiteljev* digitalnih potrdil, katerih digitalna potrdila se uporabljajo v okviru te *politike e.podpisa.*

Pri zahtevah, ki se nanašajo na uporabo *časovnega žiga* oziroma *časovne oznake* (glej poglavje 26 sta praviloma opredeljena dva največja dovoljena časovna razmika:

- največji dovoljeni časovni razmik med časom, podpisa dokumenta (kot ga podaja podpisnik) in časom časovnega žigosanja,
- največja dolžina **prehodnega obdobja** – t.j. obdobja, po časovnem žigosanju znotraj katerega je podpis še neveljaven.

Politika e-podpisa lahko vsebuje tudi druga določila kot so npr: časovno obdobje, znotraj katerega je dovoljeno podpisovati in znotraj katerega so podpisi veljavni, katere podatke, ki so potrebni za preverjanje podpisa, mora priskrbeti podpisnik, katere pa tisti, ki preverja podpis ipd.

Natančna priporočila za izdelavo *politike e-podpisa* presegajo okvir tega dokumenta. Zapisana so v dokumentu [ESlogPolitika].

---

[5] Primer XML formata za *politiko e-podpisa* je podan v ETSI TR 102 038 V1.1.1 (2002-04) TC Security - Electronic Signatures and Infrastructures (ESI); XML format for signature policies.

[6] Glej npr. RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, poglavje 6 (str 52).

1.5.2 Preverjanje elektronskega podpisa

Sredstvo za preverjanje elektronskega podpisa je nastavljena programska ali strojna oprema, ki se uporablja za preverjanje elektronskega podpisa.

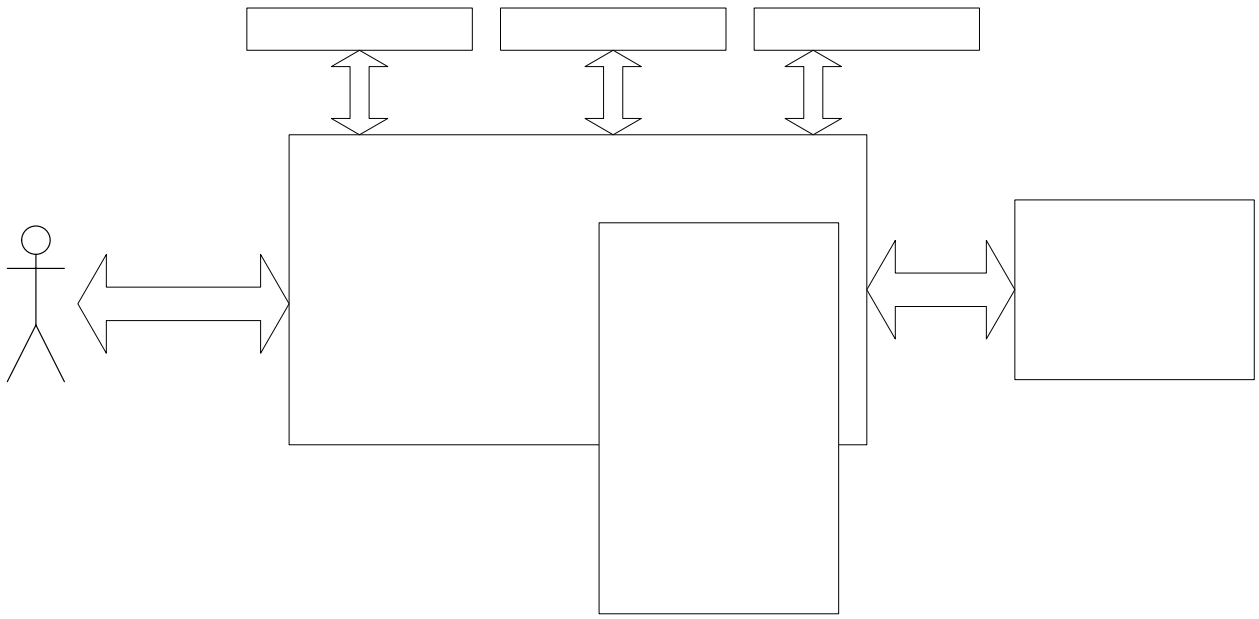
Aplikacija, ki preverja podpis, poleg funkcionalnosti, ki je namenjena preverjanju elektronskega podpisa opravlja tudi druge funkcije (npr. obdelava sprejetih dokumentov). Podobno kot pri izdelavi elektronskega podpisa (glej stran 19) lahko tudi pri preverjanju pričakujemo, da bo funkcija preverjanja elektronskega podpisa integrirana v aplikacije in da bodo namenske aplikacije za preverjanje podpisa redke.

Če oseba ali sistem, pri sebi nima celotnega dokumenta, nad katerim želi preveriti elektronski podpis, lahko manjkajoče dele pridobi iz zunanjih **virov dokumentov.**

Na postopek preverjanja elektronskega podpisa vplivata tudi *politika e-podpisa* in dodatni podatki, ki jih ponuja *overitelj* digitalnih potrdil (npr. podatki o preklicanih digitalnih potrdilih).

Tako kot *sredstvo za varno elektronsko podpisovanje* tudi *sredstvo za preverjanje podpisa* praviloma deluje v nekem **okolju**. Potrebno je preprečiti, da bi negativni vplivi iz okolja spremenili rezultat preverjanja podpisa.

Slika 6 prikazuje komponente, ki sodelujejo v postopku preverjanja elektronskega podpisa. Vse povezave med komponentami, razen povezave do virov dokumentov[7], morajo biti izveden v obliki *zaupanja vredne povezave.*



Slika 6 – komponente, ki nastopajo pri preverjanju elektronskega podpisa

1.5.2.1 Postopek preverjanja elektronskega podpisa

Naloga postopka je, da ugotovimo, *veljavnost podpisa* – t.j ali je bil podpis veljaven v času, ko je nastal. Slika 7 prikazuje podatke, ki nastopajo v postopku preverjanje elektronskega podpisa.

Rezultat podpisa je rezultat postopka podpisovanja (glej poglavje 1.5.1.2).

[7] Če do virov dokumentov ne obstaja *zaupanja vredna povezava*, lahko napadalec podtakne drug ali spremenjen dokument. Takšno spremembo pa bomo v postopku preverjanja podpisa seveda odkrili.

Overitelj Politika e

Podatki za preverjanje elektronskega podpisa so edinstveni podatki, kot so šifre ali javni šifrirni ključi, ki se uporabljajo za preverjanje elektronskega podpisa.

Podatki za vrednotenje podpisa so ostali podatki, s pomočjo katerih določimo *status podpisa*. Vključujejo lahko dodatna digitalna potrdila, podatke o preklicu digitalnih potrdil, *časovne žige* in podobo. Ti podatki so lahko delno vključeni v *rezultat podpisa*.

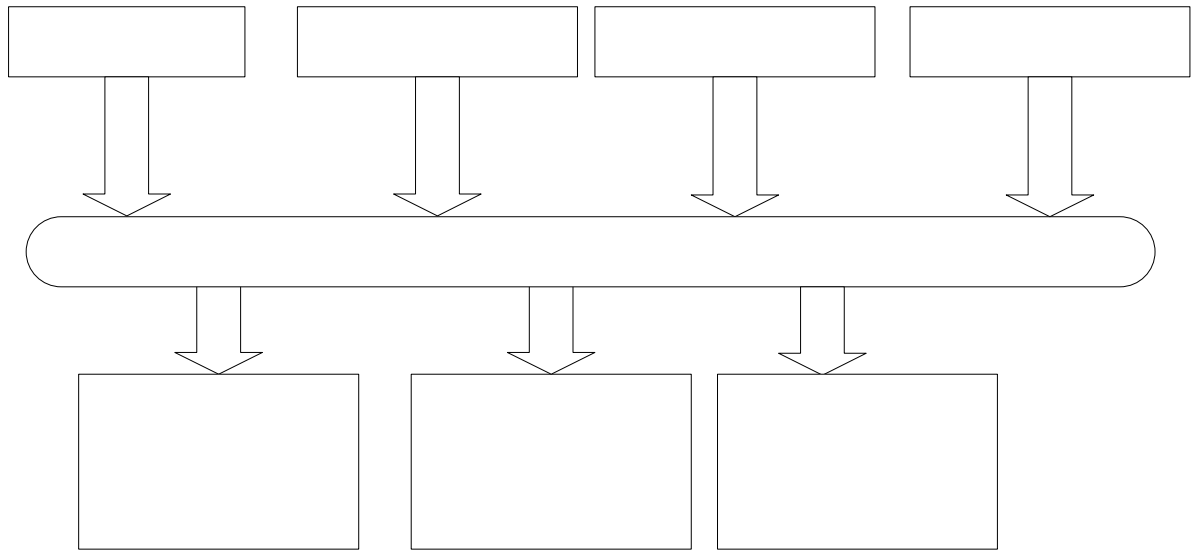
Dokument za podpis je dokument, ki ga je podpisal podpisnik (glej poglavje 1.5.1.2) . V nekaterih primerih je vsebovan kar v *rezultatu podpisa*. V tem primeru postopek preverjanja iz *rezultata podpisa* izlušči *dokument za podpis*, da ga lahko uporabimo v nadaljnjih procesih (npr. za tiskanje, ogled, ipd.)

V nekaterih primerih je *dokument za podpis* sestavljen iz množice poddukumentov, ki so lahko dosegljivi preko različnih *virov dokumentov.* Tako npr. standard [XML-DSIG] omogoča skupnen podpis množice poddokumentov (slik, besedila ipd.), ki se nahajajo na različnih mestih, na katere se sklicujemo preko URI (Uniform Resource Identifier). Primer *vira dokumentov* je tudi varen elektronski arhiv. Preden lahko preverimo podpis, moramo od *virov dokumentov* pridobiti vse potrebne podatke.

Postopek preverjanja iz *rezultata* podpisa izlušči tudi *podpisne atribute*, ki jih je podpisnik podpisal skupaj z dokumentom in *ostale atribute*, ki niso bili podpisani (glej poglavje 1.5.1.2)

Status podpisa pove, ali je podpis veljaven ali ne. Možne so naslednje vrednosti:

- veljaven – podpis je veljaven in v skladu z *politiko e-podpisa,*
- neveljaven – podpis ni v skladu s *politiko e-podpisa* (npr. format podatkov je napačen, podatki so bili spremenjeni, elektronsko potrdilo je neveljavno,...)
- neznan – na voljo je premalo informacij, da bi lahko podpis razglasili za veljavnega ali neveljavnega. Razlogi za to so lahko različni (npr. napaka pri dostopu do statusa digitalnih potrdil).



Slika 7 – podatki, ki nastopajo pri preverjanju elektronskega podpisa

Tako kot postopek izdelave elektronskega podpisa je tudi postopek preverjanja elektronskega podpisa skupaj z njegovimi parametri podrobno definiran v *politiki e-podpisa.*

Pri preverjanju elektronskega podpisa ugotavljamo, ali je bil podpis veljaven v času, ko je podpis nastal. V praksi je potrebno digitalno podpisane dokumente hraniti dolgo časa. V tem času lahko digitalno potrdilo, s pomočjo katerega je bil izveden elektronski postane neveljavno. Razlogi za to so lahko različni:

- digitalna potrdila imajo omejen rok trajanja (ponavadi nekaj let),

- podpisnik je preklical digitalno potrdilo, ker se je do njegovih *podatkov za elektronsko podpisovanje* dokopala tretja oseba,
- zlonamerni podpisnik je preklical digitalno potrdilo, da bi lahko zanikal podpis dokumentov, katerih čas podpis ni točno določen
- ...

Zaradi naštetih razlogov moramo imeti zanesljivo informacijo o tem, kdaj je bil dokument podpisan. To lahko zagotovimo s pomočjo *časovnega žigosanja*. Če žigosanja ni opravil že podpisnik, je priporočljivo, da to izvede tisti, ki preverja podpis. Časovni žig nad *rezultatom podpisa* je del *podatkov za vrednotenje podpisa.*

V postopku preverjanja podpisa pa nastopajo tudi drugi *podatki za vrednotenje podpisa* – npr. status preklica potrdil. Če hočemo v prihodnosti dokazati, da je bil podpis v času nastanka veljaven, moramo *časovno žigosati* tudi *podatke za vrednotenje podpisa* in jih skupaj z ostalimi podatki shraniti v elektronski arhiv. Natančen opis elektronskega arhiva presega obseg tega dokumenta. Nahaja se v ločenem dokumentu [ESlogArhiv].

Postopek preverjanja podpisa je natančno opredeljen s politi *e-podpisa*, v grobem pa ga sestavljajo naslednji koraki:

1. Tisti, ki preverja podpis izbere *dokument* (*dokument za podpis*[8]), na katerem želi preveriti elektronski podpis.
2. *Aplikacija, ki preverja podpis* zbere vse manjkajoče podatke, ki niso na voljo:
    a. Če *rezultat podpisa* ni na voljo ga *aplikacija, ki preverja podpis* prenese iz ustreznega vira. Praviloma je *rezultat podpisa* na voljo že pred začetkom postopka.
    b. Če *dokument* deloma ali v celotni ni voljo, prenese *aplikacija, ki preverja podpis* manjkajoče podatke iz ustreznih *virov dokumentov*.
    c. Če *podatki za preverjanje podpisa* niso na voljo, jih *aplikacija ki preverja podpis* prenese iz ustreznih virov. Priporočljivo je, da so ti podatki vključeni v *rezultat podpisa.*
    d. Če *podatki za vrednotenje podpisa* niso na voljo, jih *aplikacija, ki preverja podpis* prenese iz ustreznih virov (seznam preklicanih digitalnih potrdil lahko npr. prenese od *overitelja*). Velikokrat na začetku postopka celoten nabor *podatkov za vrednotenje podpisa* ni znan, zato se ta korak med samim preverjanjem lahko večkrat ponovi.
3. Če *aplikacija, ki preverja podpisa* ne pozna *politike e-podpisa* (ta je praviloma opredeljena z enim izmed *podpisanih atributov)*, mora uporabnika o tem obvestiti.
4. *Aplikacija, ki preverja podpisa* na podlagi *rezultata podpisa, dokumenta* in *podatkov za preverjanje elektronskega podpisa* preveri podpis. V tem koraku ponavadi ugotovimo le, ali je bil *dokument* po podpisu spremenjen. Če je bil, podpis razglasimo za neveljaven in postopek prekinemo.
5. *Aplikacija, ki preverja podpis* na podlagi *podatkov za vrednotenje podpisa* podpis *ovrednoti*. V tem koraku ugotovimo, ali je podpis dejansko veljaven, in kdo ga je izvedel. Postopek *ovrednotenja* je podrobneje opisan v nadaljevanju.
6. Če je neposredni uporabnik *aplikacije, ki preverja podpis* človek, mu aplikacija na njegovo željo prikaže vse podatke, zbrane v postopku:
    a. *dokument* - pri tem mora uporabiti prikazovalnik, ki je sposoben prikazati ustrezen *format dokumenta*. Format je ponavadi opredeljen v enem od *atributov za podpis.* Dokument mora biti prikazan na takšen način, da
        i. ima isti pomen kot takrat, ko je bil prikazan pri podpisniku,
        ii. lahko uporabnik zanesljivo ugotovi, kateri podatki so bili podpisani,
    b. *status podpisa* skupaj z morebitnimi dodatnimi informacijami, na podlagi katerih se uporabnik lahko odloči, kako ukrepati (npr. zakaj je podpis neveljaven),
    c. *vrednosti podpisnih atributov*, ki jih je podpisnik bili podpisal skupaj z *dokumentom*,
    d. vrednosti *ostalih atributov*, ki niso bili podpisani,
    e. rezultate preverjanja morebitnih časovnih žigov.
    f. na zahtevo še *politiko e-podpisa*, ki je bila uporabljena za ustvarjanje in preverjanje podpisa.

    Našteti podatki morajo biti prikazani na uporabniku razumljiv način in skupaj (npr. v istem delu

[8] *Dokument za podpis* je dokument, ki ga je podpisal podpisnik. V pričujočem scenariju ga uporabljamo za preverjanje podpisa in ne za podpisovanje. Zaradi jasnosti bomo v naslednjih korakih zanj uporabljali kar krajši izraz – »dokument«.

zaslona/pogovornem oknu) tako da uporabnik razume, da so vsi del postopka preverjanja podpisa.

7. Če neposredni uporabnik aplikacija, ki preverja podpis ni človek, ampak nek drug informacijski sistem, je potrebno temu informacijskemu sistemu podatke, naštete v prejšnji točki dostaviti po *zaupanja vredni povezavi* na varen način.

V postopku *vrednotenja* podpisa (korak 5) ovrednotimo podpis na podlagi določil *politike e-podpisa* in *podatkov za vrednotenje*. Pri tem poizkušamo zgraditi veljavno *overitveno pot* (ang. certification path/chain) med podpisnikovim digitalnim potrdilom in digitalnim potrdilom enega izmed zaupanja vrednih *overiteljem digitalnih potrdil*. Kateri so ti overitelji določa politika e-podpisa. Na začetku overitvene poti se nahaja digitalno potrdilo zaupanja vrednega ovetielja, na koncu pa digitalno potrdilo podpisnika. Vsak element v tej poti jamči za identiteto naslednjega elementa. Politika *e-podpisa* lahko podaja še dodatne omejitve glede pravil gradnje overitvene poti (npr. omejitve povezane z dolžino poti, poimenovanji naslednjih elementov, pravila za preslikavo politik ipd). *Overitvena pot* je veljavna le, če je veljavno vsako izmed potrdil na tej poti. Pri veljavnosti posameznih potrdil preverjamo vsaj:

- časovno veljavnost potrdila,
- ali je bilo potrdilo preklicano – to informacijo ponavadi pridobimo od *overitelja potrdil.* Naslov za preverjanje statusa preklica je lahko zapisan v samem potrdilu.
- veljavnost odnosov med tem potrdilom in predhodnim potrdilom (ali je podpis na tem potrdilu, ki ga je izvedel neposredni predhodnik v *overitveni poti* veljaven, ali je časovna veljavnost pravilno gnezdena,...)

Natančnejši opis postopka vrednotenja *overitvene poti* za digitalna potrdila, ki so v format X.509 se nahaja v šestem poglavju dokumenta [RFC2459]. Opis grajenja in vrednotenja *overitvene poti* v operacijskem sistemu Windows opisuje Dokument [WinCert].

Če je v *politiki e-podpisa* določeno *prehodno obdobje* (glej poglavje 1.5.2.2) moramo biti pazljivi: kadar preverjamo elektronski podpis znotraj tega obdobja, lahko ugotovimo, le, ali je podpis neveljaven (ker je bil npr. dokument spremenjen), ne moremo pa z gotovostjo zatrditi, da je podpis veljaven. Znotraj tega obdobja ima namreč podpisnik možnost, da prekliče svoje digitalno potrdilo in s tem razveljavi svoj podpis. Če *prehodnega obdobja* ni, npr. tvegamo, da razglasimo podpis za veljaven, preden podpisnik ugotovi, in prijavi morebitno krajo njegovih *podatkov za elektronsko podpisovanje.*

1.5.2.2 Čas podpisa

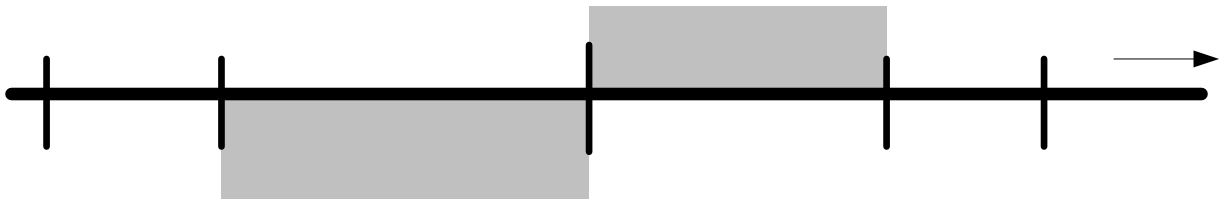
Ker pri preverjanju podpisa želimo ugotoviti, ali je bil podpis veljaven v času, ko je nastal, pa tudi zaradi drugih razlogov je pomembno, da imamo podatek o tem, kdaj je informacijo o tem, kdaj je nek dokument nastal oziroma, kdaj je bil elektronsko podpisan. Ta podatek lahko zagotovimo na naslednja načina:

- s shranjevanjem elektronskega podpisa in časovne oznake v varno revizijsko sled ali
- z uporabo *časovnega žiga*.

Priporočljiva je uporaba *časovnega žiga*. *Časovni žig* je posebna vrsta elektronskega podpisa, ki ga izvede overitelj tako, da trenutni čas skupaj z *rezultatom podpisa* nekega dokumenta. S tem potrdi, da je podpisan dokument obstajal v času žigosanja.

Slika 8 prikazuje dogodke povezane z dokumentov in njegovim elektronskim podpisom:

- T_n dokument je ustvarjen,
- T_{po} podpisnik podpiše dokument,
- $T_{čž}$ podpisan dokument je *časovno žigosan* ali *časovno označen*, začne teči prehodno obdobje, znotraj katerega podpis še ni veljaven,
- T_{kpo} – konec prehodnega obdobja, podpis je zdaj veljaven
- T_{pr} – preverjanje podpisa.



Slika 8 – ključni dogodki, ki nastopajo pri elektronskem podpisovanju

Prehodno obdobje začne teči v trenutku *časovnega žigosanja/označevanja*. Potrebuje se lahko ker:

- v primeru kraje *podatkov za elektronsko podpisovanje* podpisnik vedno potrebuje nekaj časa, da to odkrije in sporoči *overitelju* digitalnih potrdil,
- overitelj digitalnih potrdil ponavadi objavlja informacijo o preklicanih digitalnih potrdilih na vnaprej določene časovne intervale. Ko je neko digitalno potrdilo preklicano, se ni nemudoma vidno v seznamu preklicanih potrdil.

Uporabo *prehodnega obdobja* in njegovo dolžino, ter največji dovoljeni razmik med podpisom dokumenta in njegovim časovnim žigosanjem/označevanjem opredeljuje *politika e-podpisa*.

Kaj pa če čas podpisa ni znan? V tem primeru pri preverjanju namesto neznanega časa podpisa uporabimo čas preverjanja podpisa. Pri tem uporabimo trenutno veljavne podatki za overjanje podpisa. S tem tvegamo, da podpis kljub bil veljaven v dejanskem, a neznanem času podpisa ob preverjanju razglasimo za neveljaven (ker je podpisnik potrdilo, s katerim je podpisa, kasneje preklical). Ne tvegamo, pa tega da bi podpis opravljen z neveljavnim potrdilom razglasili za veljavnega, saj overitelji praviloma ne dovoljujejo »odpreklica« potrdila - ko je enkrat elektronsko potrdilo preklicano, ne bo nikoli več veljavno.

1.6. Izjava o skladnosti s temi priporočili

Pričujoči dokument podaja priporočila, ki naj se jih držijo aplikacije, ki ustvarjajo ali preverjajo elektronski podpis. Dokument ne podaja strogo formaliziranih opisov lastnosti teh aplikacij oziroma procesa izdelave takšnih aplikacij, ki bi lahko bili podlaga za formalno presojo. Zaradi kompleksnosti procesa, ki je potreben za izdelavo takšnih aplikacij in zaradi širokega nabora možnosti za izvedbo tovrstnih aplikacij je zato najbolj smiselno, da za skladnost jamči proizvajalec teh aplikacij.

Skladnost s temi priporočili lahko proizvajalec ugotovi na podlagi presoje, ki jo izvede sam, ali pa se za presojo obrne na tretjo stranko, ki je specializirana za takšne presoje. Ne glede na to, na kakšen način je proizvajalec ugotavljal skladnost, pa lahko le on poda izjavo o skladnosti s temi priporočili in s tem prevzame tudi morebitne obveznosti.

Podoben način zagotavljanja skladnosti je uveljavljen tudi v EU (CWA 14172-4).

1.7. Dodatni viri

[RFC2459]: RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile, http://www.ietf.org/rfc/rfc2459.txt

[WinCert] Brina Komar, Troubleshooting Certificate Status and Revocation, Microsoft Corporation, 2001, http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/pubkey/tshtcrl.asp

[XML-DSIG] XML-Signature Syntax and Processing, W3C 2002, http://www.w3.org/TR/xmldsig-core/

[PKCS#7] PKCS #7 - Cryptographic Message Syntax Standard, RSA Laboratories,

http://www.rsasecurity.com/rsalabs/pkcs/pkcs-7/

[CWA] CEN Workkshop agreement – Electronic Signatures - http://www.cenorm.be/isss/CWAs/cwalist.htm#Electronic%20Signatures

- CWA 14170 Security Requirements for Signature Creation Systems,
- CWA 14171 Procedures for Electronic Signature Verification,
- CWA 14172-4 EESSI Conformity Assessment Guidance – Part: 4: Signature Creation Application and Procedures for Electronic Signature Verification,
- CWA 14169 Secure Signature-Creation Devices, version 'EAL 4+',
- CWA 14168 Secure Signature-Creation Devices, version 'EAL 4',
- CWA14172-5 EESSI Conformity Assessment Guidance – Part: 5: Secure signature creation devices,

[ETSI] ETSI - Electronic Signatures and Infrastructures http://portal.etsi.org/esi/el-sign.asp

- ETSI TR 102 041 V1.1.1 (2002-02) Signature Policy Report

[ZEPEP] Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP) http://objave.uradni-list.si/bazeul/URED/2000/057/B/522615430.htm

[Uredba] Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje http://www.gov.si/cvi/slo/ep/Uredba.htm

[EslogFormat] Tehnično priporočilo za varno elektronsko arhiviranje, projekt e-SLOG, GZS, Ljubljana, 2004.

[ESlogPolitika] Priporočila za izdelavo politike elektronskega podpisa, projekt e-SLOG, GZS, Ljubljana, 2004.

[ESlogArhiv] Priporočila za format dokumenta za varen elektronski podpis, projekt e-SLOG, GZS, Ljubljana, 2004.

Opomba: internetne povezave na dokumente so podane kot pomoč in so lahko zaradi svoje narave v času branja tega dokumenta že neveljavne.