



Projekt e-SLOG

Elektronsko poslovanje slovenskega gospodarstva

TEHNIČNO PRIPOROČILO ZA VARNO ELEKTRONSKO ARHIVIRANJE

v. 0.99
oktober 2003

STANJE DOKUMENTA

Namen dokumenta:	Elektronsko arhiviranje
Kratek naziv projekta:	e-SLOG – e-podpis
Vsebina:	<i>Glej "Vsebina"</i>
Status:	delovna
Verzija:	0.99
Datum verzije:	oktober 2003
Avtorji:	SETCCE
Naslovniki:	člani delovne skupine, ostali
Zgodovina verzij:	<i>Glej "Verzija"</i>

Verzija	Datum spremembe	Opombe
0.99	oktober 2003	

SETCCE

Elektronski arhiv

Tehnično priporočilo za varno elektronsko arhiviranje



Različica dokumenta: 0,99

Datum: 22.10.2003

Pripravil: SETCCE

KAZALO

1.	Uvod	3
2.	Elektronski arhiv	5
2.1.	Opredelitev in pomen arhiviranja	5
2.2.	Elektronski arhiv	6
2.3.	Zakonodaja	7
2.4.	Standardi in tehnološka priporočila.....	11
2.4.1	Standardi za elektronske arhive.....	11
2.4.2	Standardi za hranjenje vsebine.....	12
2.4.3	Standardi za zaščito elektronskih zapisov	12
2.4.4	Standardi za ohranjanje veljavnosti varnostnih atributov	13
3.	Tehnološka zasnova in gradniki.....	15
3.1.	Uvod	15
3.2.	Odprt arhivski informacijski sistem	16
3.2.1	Migracija	17
3.2.2	Emulacija.....	18
3.2.3	Enkapsulacija	19
3.3.	Protokol za arhiviranje digitalnih objektov	20
3.4.	Protokol za časovno žigosanje.....	21
3.5.	Validacija varnostnih atributov	21
3.6.	Razširjena sintaksa elektronskega podpisa	23
4.	Dodatek	27

1. UVOD

Elektronsko poslovanje predstavlja v najširšem pomenu preslikavo poslovnih procesov v elektronsko obliko na osnovi uporabe informacijskih tehnologij. Pisno obliko dokumentov, kot neposreden produkt številnih poslovnih in proizvodnih procesov, nadomeščajo zapisi v elektronski obliki. Pravila nad upravljanjem elektronskih zapisov se v osnovi ne razlikujejo bistveno od klasičnih in so urejene tudi s slovensko zakonodajo. Zakon o elektronskem poslovanju in elektronskem podpisu prepoznava elektronsko ustvarjene zapise in elektronske podpise kot formalno sredstvo poslovanja in v določenih primerih enači elektronski zapis in elektronski podpis s pisno obliko in lastnoročnim podpisom.

Kot evidentni ali dokazni material so poslovni subjekti zavezani k hranjenju poslovnih zapisov. Za pisane in elektronsko ustvarjene dokumente imajo pravila hranjenja poslovnih zapisov skupna izhodišča. Časovno obdobje hranjenja zapisov se med oblikami ne razlikuje. Zaradi same narave zapisov pa so pravila arhiviranja drugačna. Zahtevano obdobje hranjenja elektronskega zapisa lahko preseže dobo obstoja programske opreme za prikaz in urejanje ali preseže dobo veljavnosti digitalnega potrdila na osnovi katerega je bil ustvarjen pripadajoči elektronski podpis na dokumentu. Probleme arhiviranja elektronsko ustvarjenih zapisov rešujejo elektronski arhivi, katerih naloga je zagotoviti trajno hrambo poljubnega elektronskega zapisa in pripadajočih atributov, metapodatkov ali elektronskih podpisov.

Elektronski arhivi predstavljajo kompleksne sisteme za dolgoročno hranjenje elektronskih zapisov. Poleg ohranjanja berljivosti in veljavnosti elektronsko ustvarjenih zapisov rešujejo elektronski arhivi tudi probleme upravljanja z arhiviranimi zapisi. Priprava okolja za upravljanje z zapisi v elektronski obliki se sicer naslanja na že nekatere uveljavljene postopke shranjevanja podatkov v dokumentacijskih ali podatkovnih bazah. Namen priporočil za varno arhiviranje se nanaša predvsem in izključno na vpeljevanje enotnih procesov in tehnologij za revizijsko varno hranjenje elektronskih zapisov.

Številne aktivnosti na področju normativne ureditve arhiviranja so že v teku na nacionalnem in mednarodnem nivoju. V letu 2003 je pričakovana sprememba evropske Direktive 1999/93/EC, ki ureja področje elektronskega podpisa v Evropski uniji. Na področju arhiviranja elektronskih zapisov dopolnjuje direktivo poročilo EESSI z naslovom »Trusted Archival Services (TAS), Phase #3, Final report« iz leta 2000, ki se nanaša na metodologijo in način uporabe formatov elektronskega podpisa v arhivskih sistemih in metode za ohranjanje avtentičnosti, celovitosti in pravne veljavnosti elektronskih podpisov. Na področju upravljanja in zgradbe elektronskih arhivskih sistemov so na voljo različna tehnična priporočila, ki so jih sprejele številne države, vključno z Evropsko unijo. Priporočila se nanašajo predvsem na metode vnašanja zapisov v arhiv, upravljanje z zapisi, vzdrževanje zapisov in metode dostopa do zapisov. Ta tehnična priporočila eksplicitno ne vključujejo tehnik oziroma metod za zaščito zapisov in ohranjanje veljavnosti zapisov ter pripadajočih varnostnih atributov. Temu so namenjena posebna tehnološka priporočila in standardi, ki predstavljajo temeljne funkcije zaščite zapisov.

Namen priporočil za arhiviranje elektronskih dokumentov v okviru vpeljave elektronskih računov je definirati osnovno kombinacijo tehnik za revizijsko varno shranjevanje

elektronskih zapisov s pripadajočimi elektronskimi podpisi, za zagotavljanje berljivosti zapisov čez daljša časovna obdobja in za vzdrževanje veljavnosti varnostnih atributov (podpisov), čez kratkoročna in dolgoročna časovna obdobja.

2. ELEKTRONSKI ARHIV

2.1. Opredelitev in pomen arhiviranja

Arhiviranje je postopek prevzemanja, hranjenja, vzdrževanja, obdelave in uporabe dokumentarnega in arhivskega gradiva v zbirki dokumentarnega gradiva oziroma v arhivu organizacije ali posameznika. Arhivira se dokumentarno gradivo, ki je rešeno oziroma zaključeno in ni več predmet tekočega poslovanja oziroma obdelave. Dokumentarno gradivo arhiviramo zaradi različnih potreb in hranimo v arhivu organizacije ali ustanove, dokler ne potečejo roki hranjenja, ki jih narekujejo predpisi in potrebe poslovanja, ali dokler del dokumentarnega gradiva, ki ima značaj arhivskega gradiva (trajni pomen za zgodovino, znanost ali kulturo), ne odberemo ali izločimo pristojnemu javnemu ali zasebnemu arhivu.

Zapise na splošno ločimo na pisne, digitalne ter elektronske. Pisni dokumenti so tisti, ki jih uporabnik uporablja v njihovi fizični obliki in se kot takšni tudi hranijo. Digitalni dokumenti vsebujejo zapis v digitalni obliki, a so lahko predstavljeni tudi v ne-elektronski obliki medtem, ko so elektronski dokumenti ustvarjeni s pomočjo računalnika in jih lahko uporabljamo samo z njegovim posredovanjem.

Priporočila za elektronski arhiv se nanašajo predvsem na procedure za upravljanje z elektronskimi objekti, zaščito objektov in zagotavljanje berljivosti oziroma uporabe teh objektov čez daljša časovna obdobja. Delno se sicer na zagotavljanje nespremenljivosti elektronskih objektov in ohranjanje celovitosti vsebine nanaša tudi običajen elektronski arhiv, vendar kot varen elektronskih arhiv razumemo tisti arhiv, ki zagotavlja poleg privzetega ohranjanja celovitosti hranjenih elektronskih objektov tudi verodostojno beleženje aktivnosti nad arhivom, nadziranje in beleženje aktivnosti uporabnikov ter dolgotrajno hranjenje pripadajočih varnostnih atributov (elektronskih podpisov).

Elektronske dokumente ali digitalne objekte pogosto spremljajo številni atributi oziroma opisni elementi. Pripadajoče varnostne attribute najpogosteje predstavljajo različne oblike elektronskega podpisa. Elektronski podpis predstavlja eno izmed temeljnih funkcij varnega elektronskega poslovanja, ki ščiti elektronski zapis pred spremembami in enolično povezuje podpisnike z vsebino. Varen elektronski arhiv mora poleg avtentičnosti in celovitosti shranjenih podatkov oziroma nespremenljivost vsebine med hranjenjem zagotavljati še hranjenje pripadajočih varnostnih atributov. Potrebe po dokazovanju avtentičnosti in celovitosti izhajajo iz odgovornosti do elektronskega objekta, ki je lahko v času hranjenja podvržen nedovoljenim posegom spreminjanja vsebine in posledično nastalim poškodbam.

Varen elektronski arhiv zato vključuje osnovne funkcije za overjanje uporabnikov arhiva oziroma zapisov, zaščito integritete (celovitosti) zapisov, zaščito pred poškodbami zapisov (disaster recovery) in zaščito oziroma osveževanje varnostnih atributov, preverjanje veljavnosti elektronskih podpisov ter opcijsko validacijo ali preverjanje pravilnosti zapisov in vsebine zapisov.

Pred definiranjem splošnih tehnoloških priporočil je potrebno definirati zahteve glede časovnega obdobja v katerem bo hranjen elektronski zapis. Države postavljajo različne zahteve pri hranjenju dokumentov. V Avstriji je splošna meja 30 let, v Nemčiji 2 leti, 10 let ali 30 let odvisno od vrste elektronskih dokumentov, v Veliki Britaniji 6 let, 10 let ali 30 let itd. Glede na dolžino hranjenja so zapisi kategorizirani v tri skupine: kratkoživi, srednježivi in dolgoživi.

Slovenski zakonodajalec določa dobo hranjenja poslovno-upravnih dokumentov za 10 let. Način upravljanja in predvsem shranjevanje dokumentov v elektronski obliki za določeno časovno obdobje narekujejo tehnološki standardi in Zakoni o elektronskem poslovanju in elektronskem podpisu in/ali drugi podzakonski akti. Zakonodaja se na tehnologijo ne nanaša ampak zgolj določa pogoje, pod katerimi se elektronska oblika tretira enako kot pisna in pogoje, ki jih je potrebno izpolnjevati pri prejemanju in hranjenju elektronskih zapisov.

2.2. Elektronski arhiv

Elektronski arhiv se od tradicionalnega razlikuje v tem, da hrani dokumente v elektronski obliki. Ključni problem elektronskih dokumentov je zagotavljanje berljivosti čez daljša časovna obdobja. Problematika se nanaša na zastarelost aplikacij za obdelavo in predvsem prikaz elektronsko ustvarjenih dokumentov.

S tranzicijo na elektronske dokumente in s tem elektronske arhive se je spremenila tudi logika samega arhiviranja. Ta ne temelji več izključno na vzdrževanju in ohranjanju nosilcev in na njih zapisanih sporočil, ampak predvsem na vzpostavljanju, vzdrževanju in razumevanju kontekstov, v katerih so zapisi nastali ali bili uporabljeni.

Elektronske dokumente opredeljujejo posamezni procesni cikli: ustvarjanje, urejanje, opis in indeksiranje, razpošiljanje, prejemanje, podpisovanje, revidiranje, spreminjanje, hranjenje in uničevanje s strani ustvarjalcev in drugih lastnikov, distributerjev ter institucionalnih in individualnih uporabnikov. Ključen življenjski krog informacij se vrti v krogu ustvarjenja, pridobitev, katalogizacije/identifikacije, shranitve, hranjenja in dostopa.

Namen shranjevanja dokumentov v poslovnem ali upravnem okolju je vezano predvsem na procese evidentiranja oziroma dokazovanja obstoja določenih poslovno-upravnih procesov ali dogodkov. V primeru, da dokument vsebuje pravni akt (pogodba, račun...), mora stranka (stranke) po potrebi dokazovati pravno veljavnost vsebine zapisa. Vsebino elektronskega zapisa ščiti elektronski podpis.

Izvajanje posameznih procesov ali sklopov procesov nad dokumenti zagotavlja različna tehnološka oprema. Ključne funkcije, ki jih je potrebno zagotoviti nad arhiviranimi elektronskimi zapisi za potrebe hranjenja (kratkoročnega, srednjeročnega ali dolgoročnega) je berljivost oziroma prikaz vsebine dokumentov (preprečevanje tehnološke zastarelosti), zaščito celovitosti in zaščito oziroma ohranjanje veljavnosti pripadajočih (varnostnih) atributov.

Problem hranjenja elektronskih dokumentov in pripadajočih elektronskih podpisov je večdimenzionalen. Jedro problema se navezuje na zagotavljanje celovitosti oziroma preprečevanje nespremenljivosti čez različna časovna obdobja. Elektronski dokumenti zaradi nematerialne narave dopuščajo lažje brisanje sledi, ki sicer nastanejo pri spreminjanju vsebine in ker lahko s spreminjanjem vsebine škodujemo poslovnemu procesu, je potrebno v znotraj arhiva zagotoviti ustrezne mehanizme za preprečevanje poseganja v vsebino elektronskih zapisov.

Analogno pisni obliki, morajo biti elektronski in elektronsko podpisani dokumenti shranjeni v izvornem stanju. Zaradi tehničnih razlogov se shranjevanje elektronskih dokumentov razlikuje od shranjevanja dokumentov na papirju. Varen elektronski arhiv zato vključuje prezervacijske metode za hranjenje elektronskih dokumentov, vključno z zagotavljanjem berljivosti tudi, ko oprema za obdelavo in prikaz hranjenih zapisov ni več na voljo..

Elektronski podpis zaradi svoje narave povezuje podpisnika z vsebino na takšen način, da je mogoče zaznati vsako spremembo nad vsebino objekta. Elektronski podpis se zato smatra kot osnovno sredstvo varnega elektronskega arhiva. Uporaba elektronskega podpisa je sicer večplastna, saj poleg osnovnega namena povezovanja podpisnika z vsebino služi v primeru varnih elektronskih arhivov tudi in predvsem za preprečevanje spreminjanja vsebine s strani nepooblaščenih oseb. Varni arhivski sistemi zato kot temeljno funkcijo za zaščito elektronskih zapisov in pripadajočih atributov temeljijo na implementaciji različnih oblik elektronskih podpisov (elektronski podpis, časovni žig, itd.).

2.3. Zakonodaja

Poleg tehničnih vprašanj so na področju elektronskega arhiva izpostavljeni še organizacijski in pravni problemi hranjenja podatkov. Dokumenti v elektronski obliki so zaradi svoje narave izpostavljeni modifikacijskim posegom brez nadzora. Ključen problem elektronskih vsebin je zato osredotočen na ohranjanje avtentičnosti (verodostojnosti) in zagotavljanja integritete (celovitosti) podatkov.

Elektronski dokumenti dobijo dimenzijo kulturne in poslovne dediščine, ki jo je potrebno zaščititi na dolgi rok v povezavi z Zakonom o arhivih in arhivskemu gradivu – ZAGA (Ur. l. RS, št. 20/1997). Ta ureja odnose in pravilno poslovanje z arhivskim gradivom, zakonsko določa varstvo arhivskega gradiva in uporabo tega, podrobneje pa opisuje tudi pristojnosti in naloge posameznih arhivov.

Uporabo elektronskih medijev ter dokumentov in pravno formalno enakopravnost v primerjavi s papirnim dokumentom, v kolikor le ta omogoča preverjanje zgodovine oziroma nastanka dokumenta določa Zakon o elektronskem poslovanju in elektronskem podpisu – ZEPEP (Ur. List, št. 57). ZAGA in ZEPEP določata nekatera skupna izhodišča za vzpostavitev elektronskih arhivov¹. Na eni strani omogočata zavarovanje pomembnih

¹ ZAGA opredeljuje kot arhivski forma zgolj papir ali mikrofilm. Glede na ZEPEP imajo elektronski dokumenti pravno-formalno enako veljavnost kot običajni dokumenti in jih lahko smatramo kot izhodišče za elektronski arhiv, čeravno se pričakuje tudi zakonska ureditev elektronskih arhivov na osnovi direktiv EU.

dokumentov za njihovo vsestransko uporabo čez dolgo obdobje, na drugi strani pa določata pomembnim dokumentom tako vrednost, da jih lahko razglasimo za arhivsko gradivo.

Tak primer je na primer zakonsko določena oblika dokumenta, ki ga želimo hraniti. Oblike in kategorije arhivskega gradiva so v slovenski arhivski teoriji in praksi natančno opredeljene. Zakon (ZAGA) zahteva, da jih je v nadaljnjo hrambo v pristojni arhiv potrebno predati v izvirniku, s čemer je istočasno zagotovljena integriteta ter avtentičnost dokumenta. V domeni elektronskih dokumentov integriteto in avtentičnost zagotavlja digitalni podpis, opredeljen v ZEPEP. Ker ZAGA ne opredeljuje arhivsko gradivo v elektronski obliki in ker veljajo za elektronske dokumente drugačna tehnološka izhodišča in pravila (oblika izvirnika, veljavnost digitalnega podpisa, itd.), so v okviru priporočil podana tehnološka navodila za hranjenje elektronskih dokumentov na način, ki ga razumemo kot presek obeh zakonov.

Na področju tehnološke standardizacije je uveljavljenih nekaj rešitev oziroma tehnoloških priporočil, ki rešujejo problematiko elektronskega arhiviranja. Za ohranjanje elektronskih dokumentov skozi daljša časovna obdobja so pristojne naslednje vrste tehnoloških standardov:

- Standardi, ki služijo kot referenčni model za opis funkcionalnost in delovanja ter popis postopkov in konceptov elektronskih arhivov,
- Standardi, ki omogočajo ohranjanje elektronskih zapisov in njihovih predstavitev,
- Metapodatkovni standardi, ki omogočajo dostop do hranjenih vsebin, tako da opisujejo kontekst, strukturo, izvor ter anotacijo hranjenih vsebin
- Standardi za usklajeno delovanje.
- Standardi za ustvarjanje elektronskih podpisov, ohranjanje celovitosti in zaščito elektronskih zapisov
- Standardi za ohranjanje veljavnosti elektronskih podpisov čez poljubna časovna obdobja.

Različne države imajo različne zakonske in podzakonske zahteve glede vrste in časa hranjenja elektronskih podatkov ter glede varnostnih zahtev za shranjene elektronske podatke. Seznam nekaterih časovnih zahtev zakonov držav EU je podan v poročilu TAS. V Sloveniji o hranjenju elektronskih dokumentov govorijo predvsem člani ZEPEP 12 in 16 in 33. člen Uredbe o pogojih za elektronsko poslovanje in elektronsko podpisovanje.

Zakon o elektronskem poslovanju in elektronskem podpisu

12. člen

(1) Kadar zakon ali drug predpis določa, da se določeni dokumenti, zapisi ali podatki hranijo, se lahko hranijo tudi v elektronski obliki:

- če so podatki, vsebovani v elektronskem dokumentu ali zapisu, dosegljivi in primerni za kasnejšo uporabo in
- če so podatki shranjeni v obliki, v kateri so bili oblikovani, poslani ali prejeti, ali v kakšni drugi obliki, ki verodostojno predstavlja oblikovane, poslane ali prejete podatke in
- če je iz shranjenega elektronskega sporočila mogoče ugotoviti, od kod izvira, komu je bilo poslano ter čas in kraj njegovega pošiljanja ali prejema in

- če uporabljena tehnologija in postopki v zadostni meri onemogočajo spremembo ali izbris podatkov, ki ju ne bi bilo mogoče enostavno ugotoviti, oziroma obstaja zanesljivo jamstvo glede nespremenljivosti sporočila.

16. člen

Osebe, ki hranijo dokumente, ki so elektronsko podpisani z uporabo podatkov in sredstev za podpisovanje, morajo hraniti komplementarne podatke in sredstva za preverjanje elektronskega podpisa enako dolgo, kot se hranijo dokumenti.

Uredba o pogojih za elektronsko poslovanje in podpisovanje

33. člen

(1) Kdor hrani elektronsko podpisane podatke, mora najkasneje en mesec pred iztekom roka, ki ga je za veljavnost podatkov za elektronski podpis določil overitelj v javnem delu notranjih pravil, če tega roka ni, pa z dnem konca veljavnosti kvalificiranega potrdila, zagotoviti ponoven elektronski podpis teh podatkov s strani vseh oseb, ki so podatke elektronsko podpisale prvič, ali s strani notarja ali potrditev teh podatkov z varnim časovnim žigom overitelja.

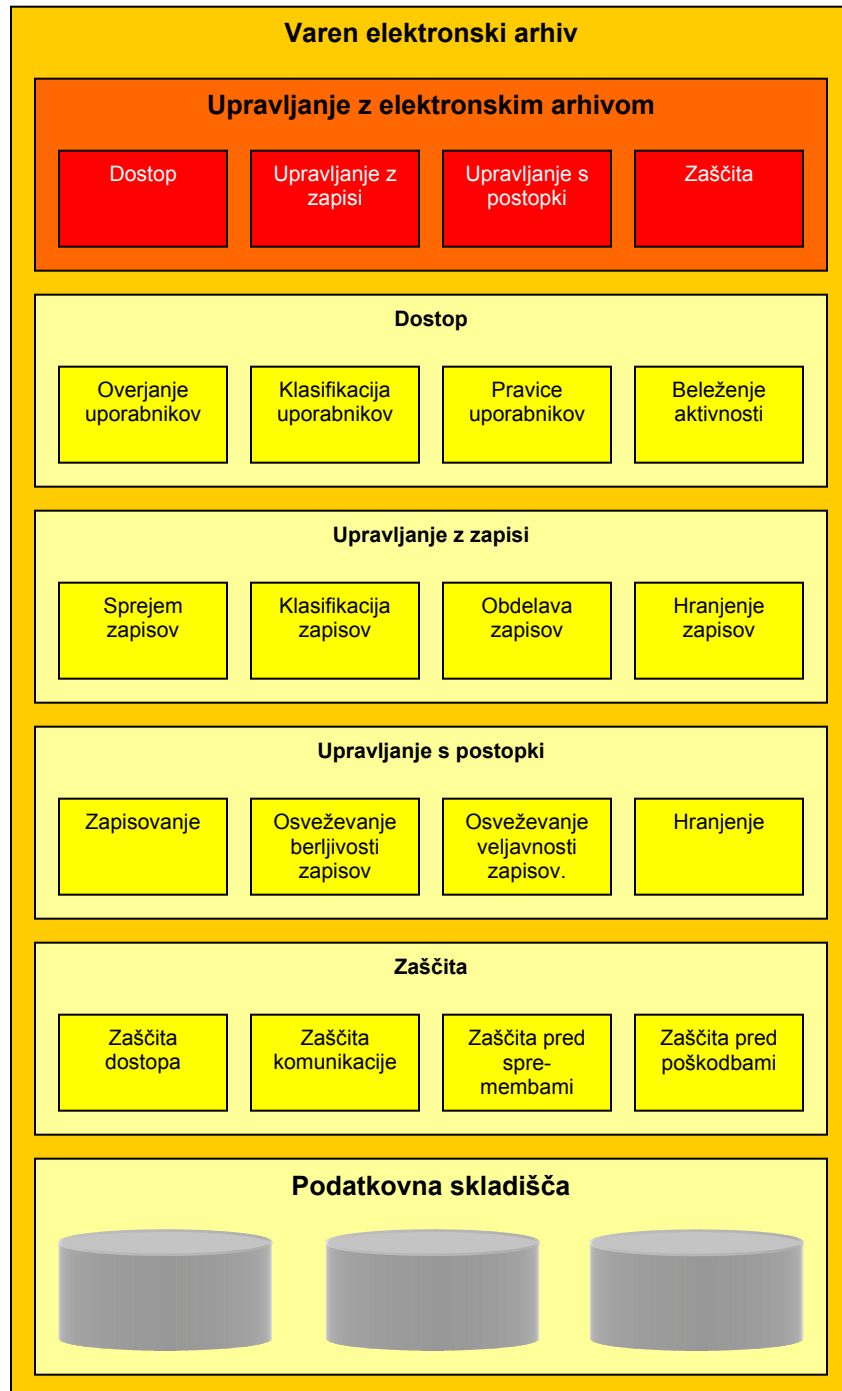
Uporabnik varnega elektronskega arhiva mora torej glede na zakonske predpise zagotoviti

- Poleg hranjenja elektronskih dokumentov hraniti še sredstva za branje oziroma prikaz vsebine
- Hranjenje dokumentov v isti obliki kot so bili elektronski dokumenti ustvarjeni in prejeti v arhiv
- Hraniti podatke o izvoru, kraju in času nastanka dokumenta
- Zagotoviti ohranjanje celovitosti oziroma preprečiti spreminjanje vsebine arhiviranih dokumentov
- Hranjenje vseh potrebnih komplementarnih podatkov in sredstev za preverjanje varnostnih atributov enako dolgo, kot se hranijo dokumenti
- Osveževanje digitalnih podpisov oziroma zagotoviti sredstvo za zaščito podpisov čez daljše časovno obdobje, tudi po tem, ko je veljavnost podpisa že pretekla.

Vloga varnega arhiva, ki omogoča poleg dokumentov hraniti tudi pripadajoče elektronske podpise je lahko dvojna. Objekti, shranjeni v arhiv, predstavljajo celotni dokument ali zgolj pripadajoči elektronski podpisi. V obeh primerih mora arhiv skrbeti za trajno obstojnost in veljavnost arhiviranih objektov (osveževanje veljavnosti digitalnih podpisov ali zagotavljanje celovitosti dokumentov). Shranjevanje zgolj elektronskih podpisov pomeni, da se morajo dokumenti hraniti na drugi lokaciji. Takšen koncept je primeren predvsem za arhive kot storitve, kjer je arhiviranje celotnega dokumenta pri ponudniku storitve nezaželeno. Kljub temu mora ponudnik storitve arhiviranja zagotoviti zaščito podatkov uporabnika (tistih informacij, ki jih lahko izluščimo iz varno shranjenega elektronskega podpisa).

Tehnična standardizacija na področju varnosti elektronskih arhivov se nanaša na različne funkcije, ki jih mora arhiv izpolnjevati. Te so:

- Način oziroma protokoli za varno posredovanje zahtevkov v lasten ali zunanje dostopen elektronski arhiv,
- Zaščita elektronskih zapisov pred spreminjanjem,
- Način in metode preverjanja statusa varnostnih atributov (elektronskih podpisov),
- Metode za zaščito in osveževanje varnostnih atributov (elektronskih podpisov).



Slika 1: Funkcionalna zgradba varnega arhiva.

2.4. Standardi in tehnološka priporočila

Priporočila in standardi, ki bi v celoti reševali problematiko arhiviranja elektronskih zapisov niso na voljo. Priporočila za varno arhiviranje se nanašajo na tehnološka ogrodja (framework) oziroma arhitekturo arhivov in na posamezne varnostne podatkovne ali logistične funkcije. Tehnološka priporočila za varno arhiviranje tako predstavljajo kombinacijo tehnoloških rešitev, ki kot zaključena celota zagotavljajo izvajanje vseh potrebnih funkcij za dolgoročno hranjenje in prezervacijo elektronskih zapisov. V nadaljevanju so predstavljena posamezna priporočila.

2.4.1 Standardi za elektronske arhive

Elektronski arhivi predstavljajo kompleksne tehnološke platforme za upravljanje in hranjenje elektronskih zapisov. Standardi na tem področju določajo predvsem koncepte oziroma metodološke in tehnološke zasnove elektronskih arhivov.

ISO 15489. Ker v širokem digitalnem okolju upravljanje digitalnih zbirk ne more biti odgovornost le ene centralne organizacije, je pomembno, da se v takem okolju sprejme koncepte, definicije ter postopke, ki veljajo splošno. Standard ISO 15489 omogoča organizacijam, da standardizirajo pojme in definicije, ki so povezane s področjem upravljanja z dokumenti, reguliranim okoljem, politiko in odgovornostmi, postopki in kontrolami na tem področju.

AS 4390. Standard razvit v na področju Avstralije je primer standarda ISO 15489, ki je sprejet v Severni Ameriki ter Evropi. Podobno kot vzorčni standard ISO predstavlja strategije in delovne napotke najboljše prakse arhiviranja. Nanaša se na vse vrste zapisov.

DoD 5015.2-STD. Soroden standard za specifikacijo pojmov in definicij je razvit za vojaške namene s strani ameriškega obrambnega ministrstva. Predlaga smernice implementacij in postopkov namenjene sistemom za upravljanje z dokumenti. V svoji zakonodajo ga vključuje vse več držav, ki razširjajo svoje zakone na tem področju.

OAIS. Splošno prepoznaven ISO standard, ki ga je definirala ameriška vesoljska agencija (NASA). Odprt arhivski informacijski sistem (Open Archival Information System, OAIS) natančno opisuje informacijske tokove ter zahteve, ki jih mora izpolnjevati sodoben arhivski sistem.

TAP. Protokol za varno arhiviranje² (Trusted Archive Protocol, TAP) je namenjen interakciji z varnim arhivom (Trusted Archive Authority, TAA). Protokol določa procedure za vstavljanje objektov v arhiv in prejemanje arhivskih dokumentov. Določa tudi metode za zaščito dokumentov čez daljša časovna obdobja, vključno z zaščito varnostnih atributov.

Tehnološke razvojne smernice na področju elektronskega arhiviranja se naslanjajo na priporočilo agencije NASA oziroma priporočilo organizacije ISO, ki postaja splošno uveljavljen standard. Za potrebe elektronskega poslovanja in obdelave elektronskih

² Internet draft: draft-ietf-pkix-tap-00.txt, IETF, Februar 2003.

dokumentov v poslovnih procesih je zato standard OAIS tudi metodološka, funkcionalna in tehnična osnova priporočila za varno arhiviranje.

2.4.2 Standardi za hranjenje vsebine

Standardi za elektronske arhive podaljšujejo procese zastarevanja dokumentov v semantičnem in fizičnem smislu. Dolgoročnost na osnovi tehnoloških priporočil je mogoče zagotovi le v primeru, če se ta ne spreminjajo oziroma če ti omogočajo kompatibilnost s predhodnimi različicami. Na področju dolgoročnega ohranjanje vsebine kot oblika dokumentov v digitalnem arhivu prevladujeta Portable Document Format (PDF) in eXtensible Markup Language (XML).

PDF. Je produkt podjetja Adobe, postal pa je »de facto« dokumentni standard. Uporablja image model jezika PostScript, ki preslika tekst in slike v natančne kopije originala. Ker uporabniki nimajo formalnega vpliva na izboljšave novih verzij, ta standard ne zagotavlja kompatibilnosti s prejšnjimi verzijami. Poleg tega format PDF ne izpolnjuje zahtev iskalnih možnosti digitalnih arhivov. Zaradi navedenih razlogov se format PDF, kot standard za ohranjanje vsebine kljub razširjeni uporabi ne priporoča.

XML. Razširjeni označevalni jezik (eXtensible Markup Language, XML) je mednarodno uveljavljen standard definiran pod okriljem organizacije World Wide Web Consortium (W3C) za sistemsko neodvisno interpretacijo podatkov. Informacijo oziroma podatek interpretirajo oznake (tag), katerih pomen je določen poljubno na nivoju aplikacije oziroma imenskih shem (namespace). Format XML izvira iz potreb po obvladovanju strukturiranih dokumentih in je zato običajno vezan na dokumentacijske sheme (DTD Schema, XML Schema), ki določajo strukturo dokumentov. Zaradi izredne fleksibilnosti in splošnega sprejemanja, format XML predstavlja tudi univerzalno sintaktično sredstvo v informacijskem okolju. Zaradi svojega izvirnega namena XML ne zagotavlja ohranjanje originalnega izgleda dokumentov, kar je nujno za zagotavljanje dokazne vrednosti digitalnih dokumentov. Temu so namenjene transformacijske sheme, ki spremljajo dokumente v zapisu XML. Ker se je format XML že uveljavil kot univerzalno sintaktično sredstvo in orodje za generiranje kompleksnih dokumentov ter zaradi vsesplošne podpore in uveljavljenih aplikacijskih standardov temelječih na formatu, se razširjen označevalni jezik priporoča kot sredstvo za pripravo dokumentov in njihovo arhiviranje v informacijskem sistemu.

2.4.3 Standardi za zaščito elektronskih zapisov

Zaščita arhivov in arhiviranih zapisov je osnova varnega arhiviranja. Različni standardi zagotavljajo zaščito podatkov na osnovi simetričnih in asimetričnih šifrirnih algoritmov. Kot temeljno sredstvo za zaščito zapisov je prepoznan elektronski podpis. Vloga elektronskega podpisa je različna, v osnovi pa povezuje podpisnika z vsebino in ščiti podatke pred nepooblaščenim spreminjanjem.

Za zagotavljanje celovitosti arhiviranih zapisov mora elektronski arhiv vsak posamezen zapis ali sveženj zapisov obdelati tako, da ustvari enoličen prstni odtis. V primeru spremembe zapisa, prstni odtis ni posledično zapis nista več veljavna. Prstni odtisi zapisov morajo biti

zaščiteni s kriptografskimi mehanizmi (šifriranjem). Kombinacijo prstnega odtisa in šifriranja predstavlja elektronski podpis.

Varni arhivi v osnovi niso namenjeni zaščiti vsebine zapisov pred vpogledom. Kljub temu je priporočljivo zaščititi komunikacijske poti z arhivom in predvsem zaščititi dostop uporabnikov do elektronskega arhiva. Zaščita dostopa temelji na močnem overjanju (strong authentication) uporabnikov. Subjekti, ki so predmet močnega overjanja se identificirajo na osnovi digitalnih potrdil ali enkratno uporabljenih vstopnih gesel (one-time password). V nadaljevanju so povzeti temeljni standardi za zaščito elektronskih zapisov in elektronskih arhivov.

ES. Elektronski podpis (Electronic Signature, ES) povezuje podpisnika s podpisanimi podatki in istočasno zagotavlja celovitost podpisanih podatkov. Elektronski podpisi so zasnovani na osnovi zgoščevalnih ter asimetričnih in simetričnih algoritmov. Osnova za podpisovanje so uporabniški zasebni in javni ključ. Uporabnika povezuje z javnim ključem digitalno potrdilo (Digital Certificate).

SSL. Sloj varnih vtičnic (Secure Sockets Layer, SSL) je varnostni protokol za zaščito komunikacije med subjekti. Temelji na asimetrični in simetrični kriptografiji, s čimer so vsi podatki med komunicirajočima strankama sprti šifrirani.

TS. Časovni žig (Time Stamp, TS) je različica elektronskega podpisa z vključenim časom ustvarjanja podpisa. Čas, ki je vključen v podpis mora biti povzet iz zanesljivega in točnega časovnega vira. Časovno žigosanje je funkcija, ki je glede na ZEPEP v domeni ponudnika overiteljskih storitev.

CRL. Preverjanje veljavnosti elektronskih podpisov vključuje tudi preverjanje veljavnosti relevantnih potrdil. Seznam preklicanih potrdil (Certificate Revocation List, CRL) vključuje vsa preklicana potrdila, ki jih je izdal overitelj. Če je potrdilo neveljavno (preklicano) so tudi vsi podpisi ustvarjeni s pomočjo potrdila neveljavni.

OCSP. Preverjanje veljavnosti potrdil temelji na trenutnem času in seznamu preklicanih potrdil. Protokol za spletno preverjanje potrdil (On-line Certificate Status Protocol, OCSP) omogoča aplikacijam in uporabnikom prek javnega omrežja ročno ali samodejno preveriti trenutni status digitalnega potrdila pri izdajatelju potrdila.

2.4.4 Standardi za ohranjanje veljavnosti varnostnih atributov

Elektronski podpisi oziroma šifriranje na splošno temelji na uporabi simetričnih in asimetričnih šifrirnih ključev. Dolžina uporabljenih ključev je odvisna od zahtevane stopnje zaščite. Trenutna praksa narekuje uporabo 1024 bitnih asimetričnih in 128 bitnih simetričnih ključev.

Zaradi tehnološkega razvoja dolžina uporabljenih ključev ne zagotavlja dolgoročno zaščito podatkov. Veljavnost digitalnih potrdil in pripadajočih ključev je zato časovno omejena. Ob preteku veljavnosti potrdila preteče veljavnost vseh na osnovi potrdila ustvarjenih podpisov. Za podaljševanje veljavnosti podpisov so glede na ZEPEP možni trije postopki. V domeni

elektronskih arhivov je postopek osveževanja veljavnosti vezan na časovno žigosanje. Tik pred iztekom veljavnosti podpisa (ali podpisov) se življenjska doba (veljavnega) podpisa podaljša z apliciranjem novega časovnega žiga.

DVCS. Standard za preverjanje veljavnosti varnostnih atributov³ (Data Validation and Certification Server, DVCS) določa postopke za ugotavljanje veljavnosti posedovanja podatkov in ugotavljanje veljavnosti elektronskih podpisov, ki so vključeni v dokument. Preverjanje veljavnosti se izvaja vedno pred vstopom zapisa v arhiv.

TSP. Protokol za časovni žig (TimeStamp Protocol, TSP) določa način časovnega žigosanja. Protokol je namenjen ohranjanju celovitosti elektronskih podatkov vključno z digitalnimi podpisi. Deluje na principu žetonov in ne razkriva vsebine dokumentov. Časovno žigosanje je temeljna funkcija varnih elektronskih arhivov.

ES-X. Razširjena sintaksa elektronskega podpisa⁴ (eXtended Electronic Signature, ES) specificira digitalni podpis. ES predvideva uporabo različnih podatkov za zagotavljanje celovitosti podatkov in ugotavljanje veljavnosti podpisov. Tri različice so relevantne za varne arhive: ES-T, ES-C in ES-X.

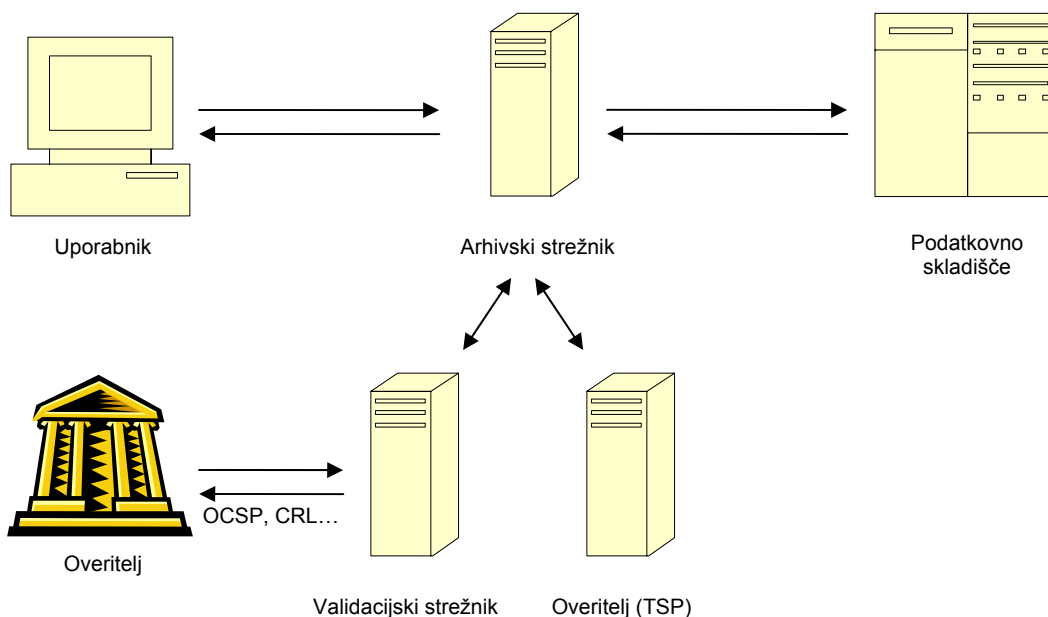
³ Data Validation and Certification Server Protocols, RFC 3029, Internet Society, 2001.

⁴ Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats, ETSI, Sempember 2002.

3. TEHNOLOŠKA ZASNOVA IN GRADNIKI

3.1. Uvod

Varen elektronski arhiv predstavlja skupek informacijskih tehnologij, ki so konfigurirane in povezane na način, da omogočajo varno hranjenje elektronskih zapisov ter pripadajočih atributov in podpisov. Struktura varnega arhiva vključuje predvsem mehanizme in protokole za interakcijo z arhivom, validacijske mehanizme, mehanizme za elektronsko podpisovanje in časovno žigosanje ter komunikacijske protokole za interakcijo med notranjimi in zunanji sklopi arhivskega sistema.

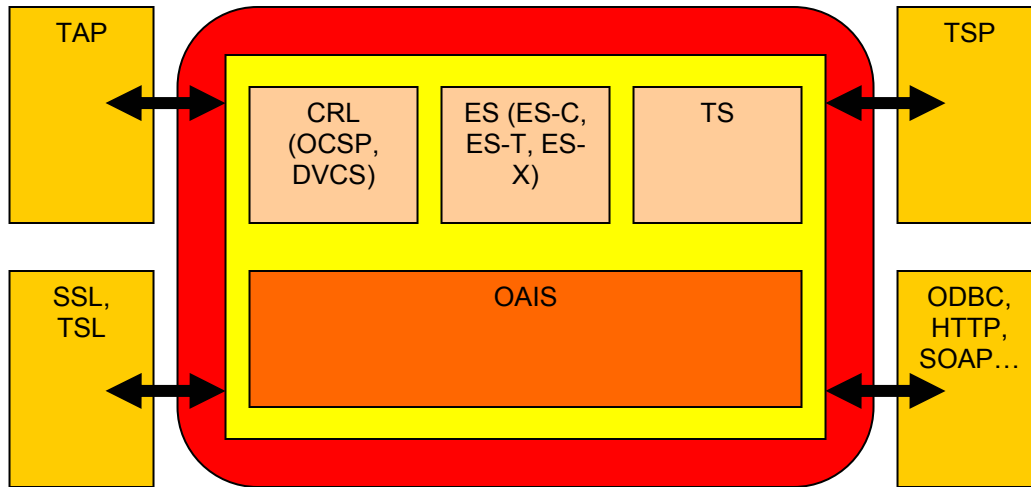


Slika 2: Infrastruktura sistema za varno arhiviranje.

Za hranjenje elektronskih dokumentov, ki jih spremljajo varnostni atributi (elektronski podpisi) je potrebno zagotoviti dodatne arhivske funkcije. Zaradi tehničnih omejitev elektronski podpisi po določenem času pretečejo. Varen arhiv zato poleg celovitost vsebin zagotavljanja hranjenje in osveževanje vseh pripadajočih varnostnih atributov.

V arhiv vnesene elektronsko podpisane dokumente je potrebno validirati in časovno žigosati. Časovni žig se lahko izvaja zgolj nad elektronskimi podpisi, v kolikor se ti že sami po sebi nanašajo na celoten digitalni objekt ali nad celotnimi elektronskimi zapisi. Poleg časovnega žigosanja je potrebno zagotoviti hranjenje vseh komplementarnih podatkov o pripadajočem elektronskem podpisu (digitalno potrdilo, verigo potrdil, itd.) za kasnejšo validacijo oziroma dokazovanje veljavnosti žigov. V nadaljevanju so podrobneje

predstavljeni posamezni sklopi. Izpuščeni so vsi mehanizmi, ki so predmet komplementarnih tehnoloških priporočil.



Slika 3: Tehnološki gradniki varnega elektronskega arhiva.

3.2. Odprt arhivski informacijski sistem

OAIS je tehnični priporočilo pripravljeno kot izhodišče standarda ISO. Predstavlja ogrodje funkcionalnega ter informacijskega koncepta, ki je primeren za razvoj elektronskega arhiva. Poseben poudarek na standardu je zagotavljanje dolgoročnega hranjenja elektronskih vsebin in se zato uveljavlja kot »de facto« standard na področju elektronskih arhivov.

Teoretični model odprtega informacijskega sistema za arhiviranje, ki ga je razvil Consultative Committee for Space Data System (CCSDS) agencije NASA, je bil razvit kot odgovor na standard ISO TC20/SC 13 z namenom, da bi ga nadaljnje obravnavali kot osnovo za standardizacijo na področju dolgoročnega arhiviranja. OAIS referenčni model omogoča širše razumevanje tega kaj je potrebno, da bi lahko ohranili in dostopali do informacij tudi na daljši rok. Služi kot osnova ali tehnični napotek za možne implementacije elektronskih arhivov izdelanih po predlaganem priporočilu.

Standard OAIS specificira elemente elektronskega arhiva in funkcije, ki se izvajajo nad arhivom. Temelj elektronskega arhiva so digitalni objekti, ki jih predstavljajo elektronski dokumenti in drugi elektronski zapisi ter postopki za upravljanje z hranjenimi objekti. Tri temeljne funkcije določajo delovanje arhiva: vnos, hranjenje in izvoz digitalnih objektov. Vse funkcije temeljijo na atributi v obliki ovojnic nad digitalnimi objekti.

V okviru standarda OAIS so določeni tudi postopki za ohranjanje berljivosti digitalnih objektov, medtem ko se samo priporočilo ne nanaša na varnostne attribute, ki so predmet dodatnih priporočil. Zaradi obsežnosti priporočila je podrobnejši opis podan v prilogi

(Reference Model for an Open Archival Information System – OAIS, CCSDS 650.0-B-1, BLUE BOOK, January 2002).

Ključna naloga fizičnih in elektronskih arhivov je ohranjanje verodostojnosti in berljivosti elektronskih zapisov. Pri ohranjanju berljivosti vsebin se pojavljata dva temeljna problema: neobstoynost digitalnih medijev, na katerem so shranjeni digitalni podatki ter hitrost tehnološkega razvoja, ki povzroči zastarelost platforme (strojne in programske opreme) in s tem dokumentov. V nasprotju z zapisi na tradicionalnih medijih (papir), za razumevanje katerih ni potrebna posebna programska oprema, zapisi na novejših medijih ne morejo ostati nedotaknjeni in berljivi čez daljše časovno obdobje.

Dolgoročno hranjenje digitalnih vsebin se nanaša na različne strategije, ki nastopajo posamezno ali v tehnološki kombinaciji. Poleg implementacijsko neprimernih papirnih kopij in tehnoloških muzejev so predmet priporočil sledeče strategije:

- Migracija
- Emulacija
- Enkapsulacija

Posamezni tehnološki pristopi se navezujejo na različne metode in potrebe arhiviranja. V okviru priporočil na področju elektronskega poslovanja prevladuje strategija enkapsulacije. Kljub temu se lahko na osnovi specifičnih potreb uporabniki odločijo za migracijo in sicer v primeru obdelave preprostih dokumentov (preprosta tekstovna oblika) oziroma emulacijo v primeru shranjevanja kompleksnih dokumentacijskih struktur.

Uporaba nekaterih izpeljank migracije ne omogoča ohranjanje veljavnosti elektronsko podpisanih dokumentov, zato kot takšna ni primerna za uporabo in je izvzeta iz tehnoloških priporočil za varno arhiviranje (omenjena je le migracija na zapisovalne medije). Glede na tehnične zahteve pri osveževanju veljavnosti elektronskih podpisov je najustreznejša strategija emulacije. V okviru tehnološkega priporočila so zato predstavljene le strategije oziroma deli strategij, ki so prepoznane kot najustreznejši tehnološki pristop pri prezervaciji digitalnih vsebin. Čeravno se model OAIS naslanja na strategijo migracije so preostale dve strategiji bili razviti v okviru odprtega arhivskega standarda.

3.2.1 Migracija

Migracija predstavlja proces periodičnega prenosa digitalnih gradiv med različnimi tehnološkimi konfiguracijami oziroma platformami (oziroma med različnimi generacijami računalniške tehnologije). Zapisovalni mediji namenjeni shranjevanju digitalnih vsebin se nahajajo v operativnem stanju največ nekaj let, preden postane verjetnost nepopravljivih izgub podatkov prevelika. Namen migracije je ohranjanje celovitosti digitalnih objektov in hkrati omogočiti, da so ti na voljo uporabnikom ob tranziciji na posodobljene ali nove tehnološke platforme.

Strategija migracije vključuje več prepoznavnih tehnik. Tehnološko najmanj zahtevna je tehnika osveževanja (Refreshment), na osnovi katere se izvede kopiranje vsebine v enaki obliki na nov medij. Tehnika osveževanja lahko premosti težave nestabilnosti medijev,

vendar ne opravlja problem tehnološke zastarelosti. Migracija na nova tehnološka okolja pogosto pomeni, da kopija ne bo popolnoma identična njeni originalni informaciji. Uspešna migracija mora namreč vsebovati informacije (metapodatke) o spremembah digitalnih objektov.

Najpreprostejša oblike migracije je kopiranje digitalne vsebine na stabilnejši ne-digitalni medij kot je na primer papir ali mikrofilm. V tej obliki informacije sicer zagotavljajo boljšo dolgoročno zanesljivost hranjenja, vendar ne predstavijo informacije v pravi obliki in ohromijo funkcionalnost ter izgled izvirnega digitalnega objekta in hkrati ne omogočajo hranjenje elektronsko podpisanih zapisov. Prenos na stabilnejši digitalni medij (npr. CD-R) pomeni kratko do srednjeročno rešitev hranjenja in omogočanja dostopa do hranjenih informacij. Migracija na ne-digitalne medije, se v okviru zahtev elektronskega računa in elektronskih dokumentov zaradi pomanjkljivosti ne izvaja.

Druga rešitev predstavlja uporaba programske opreme z podporo po vzratni kompatibilnosti. Kljub temu, da sodobne aplikacije omogočajo dekodiranje starih formatov v nove, strategija ni primerna za dolgoročno hranjenje ali za hranjenje kompleksnih digitalnih virov, ki so bili ustvarjeni na eni od specifičnih in na splošno uveljavljenih aplikacijah oziroma hranjenje elektronsko podpisanih objektov.

Tretji strateški pristop hranjenja digitalnih vsebin vključuje migracijo številnih formatov v nove (standardizirane). Prehod na novo standardiziran format predstavlja večjo stabilnost napram nestandardiziranim oblikam zapisa podatkov in zagotavlja možnost preoblikovanja v izvirni dokument vendar ne ohranja veljavnost pripadajočih elektronskih podpisov. Zaradi pomanjkljivosti pri ohranjanju izvirnih objektov se transformacija, kot oblika migracije ne uporablja.

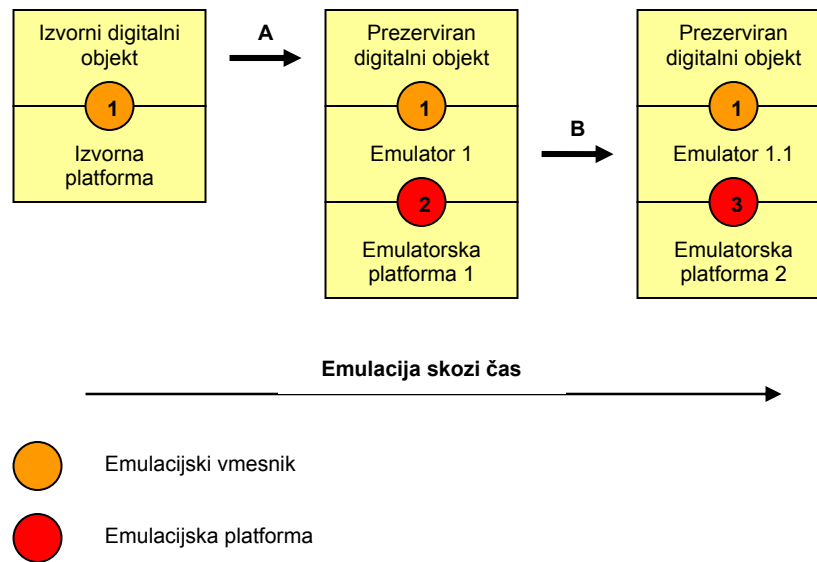
3.2.2 Emulacija

Princip emulacije deluje na osnovi programskih emulatorjev, ki poustvarjajo staro tehnično okolje na trenutni ali prihodnji tehnologiji oziroma platformi. Tehnološki pristop poustvarja delovanje izvirne računalniške in programske konfiguracije na trenutnem ali bodočem operacijskem sistemu in omogoča neokrnjeno uporabo oziroma prikaz digitalnih dokumentov iz preteklih časovnih obdobj.

Transformacija originalnega digitalnega objekta v prezerviran digitalni objekt, v emuliranem okolju omogoči prikaz lastnosti originalnega objekta. Takšen proces omogoča neoviran dostop do zapisov ne glede na to, da je prvotna platforma na kateri je izvirni dokument nastal že tehnološko zastarela. Proces transformacije je ponovljiv in zagotavlja sprotno posodobitev emulatorjev glede na novo strojno in programsko platformo. Med celotnim procesom osveževanja oziroma nadgradnje emuliranega okolja niz bitov digitalnega objekta ostaja nespremenjen.

Prednosti emulacije pred migracijo je, da izvirne informacije ne zastarijo in da je izvirni objekt ohranjen v izvornem formatu vključno z vsemi pripadajočimi atributi in elektronskimi podpisi. Namesto teh se spreminja emulacija tehnološkega okolja. Zaradi tega ta strategija omogoča celovito ohranitev funkcionalnosti ter izvirnega izgleda digitalnih informacij, ki bi

se drugače izgubili znotraj tehnološke zastarelosti. V primerjavi z drugimi prezervacijskimi tehnikami je emulacija primerna za dolgoročneje hranjenje vseh oblik elektronskih zapisov.



Slika 4: Proces shranjevanja digitalnih objektov na osnovi emulacije.

Implementacija emulacije se smatra za učinkovito, saj so podatki shranjeni skupaj z ustreznimi metapodatki, elektronskimi podpisi in programsko opremo. Dodatnih aktivnosti razen preprostega kopiranja na nove medije s tem emulacija ne zahteva. Emulacija omogoča tudi uporabo enotne rešitve (en emulator) za več podatkovnih objektov, ki za obdelavo in prikaz potrebujejo enako operativno okolje.

3.2.3 Enkapsulacija

Metoda enkapsulacije⁵ je znana sicer kot »migracija na zahtevo« (Migration on Request), saj gre za ohranjanje vsebine v izvorni obliki. Glede na zahtevo po digitalnem objektu iz arhiva, je samodejno izvršena migracija niza izvornih bitov. Ker je vsebina ločena od formata lahko zagotovimo avtentičnost objekta, ki je vedno shranjen v obliki izvornega zapisa.

Poleg digitalnega objekta strategija enkapsulacije zahteva hranjenje orodja za proces pretvorbe izvornih bitov v dokument, zato proces enkapsulacije obravnavamo tudi kot kombinacijo emulacije z migracijo. Orodje opisano v metapodatkih je lahko programska specifikacija ali emulator, ki oponaša originalno strojno ali programsko okolje.

⁵ Enkapsulacija je metoda v večjem delu razvita s strani projekta CEDARS (CURL Exemplars in Digital ArchiveS, Joint Information Systems Committee, UK), ki temelji na OAIS metodologiji. Projekt CEDARS temelji na dejstvu, da proces migracije datotek pomeni izgubo originalnih lastnosti digitalnega objekta in pripadajočih atributov.

Enkapsulacija je v kontekstu ohranjanja digitalnih vsebin tehnika, ki združuje skupaj digitalni objekt, ter vse potrebne informacije, ki so potrebne za dostop do tega objekta. S pomočjo vseh teh zajetih podatkov je metoda sposobna ustvariti originalno aplikacijo, preko katere je uporabnik prvotno dostopal do hranjene informacije, na novi platformi. Enkapsulacija je lahko dosežena z uporabo fizičnih ali logičnih struktur, označenih kot kontejnerji. Kontejnerji zagotavljajo povezavo med vsemi informacijami kot so digitalni objekt ter podporne informacije vključno z metapodatki.

Priporočen jezik za shranjevanje metapodatkov in navodil za prezerviranje digitalnih objektov je XML. Enkapsulacija tehnika izkorišča format zapisa XML kot ogrodje za kompleksno strukturo dokumentov sestavljenih iz posameznih dokumentov ali delov dokumentov. Princip enkapsulacije tudi preprečuje nepotrebno podvajanje podatkov za digitalne objekte istega formata.

3.3. Protokol za arhiviranje digitalnih objektov

Protokol za varno arhiviranje je namenjen povezovanju z varnim elektronskim arhivom, ki vključuje predvsem vnos objektov v arhiv in prevzemanje objektov iz arhiva na formalen način. Medtem ko model OAIS nekatere funkcionalnosti protokola TAP že vključuje, je protokol namenjen neodvisni zunanji interakciji z elektronskimi arhivi. Protokol TAP lahko predstavlja zunanjo funkcijo modela OAIS.

Elektronski arhiv prejema, vzdržuje in posreduje različne digitalne objekte, ki so predmet arhiviranja in ki lahko vključujejo varnostne attribute (elektronske podpise) ali ne. Zagotoviti mora vnos objektov, vnos varnostnih atributov, osveževanje varnostnih atributov in izbris oziroma odstranjevanje digitalnih objektov in varnostnih atributov.

Protokol TAP določa način vnosa, pregledovanja in izbrisa digitalnih objektov v elektronski arhiv. Vsi zahtevki so lahko overjeni ali ne, razen zahtevka za izbris, ki mora biti vedno overjen. Protokol TAP določa načine in metode za:

- Zahtevki za vnos v arhiv
- Odziv na zahtevo za vnos
- Format vnosa digitalnih objektov v arhiv
- Odziv na vnos objekta v arhiv
- Zahtevki za izbris iz arhiva
- Odziv na zahtevo za izbris
- Preverjanje varnostnih atributov

Protokol TAP deluje prek poljubnih komunikacijskih prenosnih protokolov (http, SSL, itd.). Dodatno določa še vse potrebne funkcije, ki se izvajajo nad samim arhivom (zbiranje informacij o veljavnosti varnostnih atributov, pridobivanje informacij o politiki TAA, itd.).

Protokol TAP je namenjen uporabi arhivskih storitev znotraj ali izven organizacije. Beleženje vseh aktivnosti vključno z overjanjem uporabnikov (zahtevkov) je priporočljivo za lažjo identifikacijo vseh izvedenih procesov. Za potrebe zaprtih sistemov se lahko implementira

tudi poljuben arhivski protokol, kjer je priporočljivo, da vključuje vse funkcije protokola TAP.

3.4. Protokol za časovno žigosanje

Časovni žig predstavlja različico elektronskega podpisa z vključenim časom ustvarjanja žiga. Čas je povzet iz zanesljivega in natančnega časovnega vira, da se lahko časovni žig tretira kot veljaven. Natančen časovni vir predstavljajo samostojne atomske ure ali atomske ure uporabljene za druge namene (GPS, telekomunikacijsko omrežje, itd.).

Zaradi tehničnih in formalnih zahtev je časovno žigosanje funkcija ponudnika overiteljskih storitev. Časovni žigosanje se izvaja prek posebnih, temu namenjenih protokolov. Protokola za časovno žigosanje (TSP) omogoča posredovanje zahtevkov za časovni žig prek javnega omrežja.

Časovno žigosanje izvajamo nad različnimi objekti:

- Elektronski zapis ali dokument in
- Elektronski podpisi.

Časovni žig dokazuje obstoj določenega objekta (zapisa ali podpisa) v določenem času in je zato temelj varnega arhiviranja. S časovnim žigom lahko dokazujemo čas ustvarjanja dokumenta, čas podpisa na dokumentu, čas preverjanja veljavnosti dokumenta ali podpisa, itd. S časovnim podpisom ohranimo tudi celovitost zapisa, s čimer dokažemo obstoj objekta v določenem času.

Časovni žig se v arhivskih sistemih uporablja predvsem za ohranjanje veljavnosti elektronskih podpisov. V kombinaciji z validacijskimi tehnikami zagotovimo obstoj in veljavnost podpisa v določenem času. Veljavnost podpisa je podaljšana s časovno veljavnostjo žiga.

Časovno žigosanje prek protokola TSP temelji na žetonih in zahtevkih. Za posamezen objekt, ki je predmet žigosanja, je pripravljen prstni odtis, ki ga podpiše oziroma žigosa ponudnik časovnega žigosanja. Prstni odtis je del zahtevka (žetona) za časovno žigosanje, ki ga kot žigosan odziv posreduje ponudnik časovnega žigosanja.

3.5. Validacija varnostnih atributov

Ena izmed ključnih funkcij arhiviranja elektronskih zapisov z vključenimi elektronskimi podpisi, je preverjanje veljavnosti atributov sprejetih v arhiv. Za validacijo varnostnih atributov je na voljo več tehnik. Preverjanje mora biti izvedeno ob neposrednem vnosu objekta v arhiv. Arhiv mora zagotoviti preverjanje:

- Veljavnost potrdila ali potrdil na osnovi katerega je bil ustvarjen posamezen digitalni podpis,

- Veljavnost potrdil v verigi,
- Veljavnost samega podpisa,
- Veljavnost časa preverjanja.

Preverjanje veljavnosti digitalnih podpisov temelji na seznamih preklicanih potrdila (CRL). Varni elektronski arhiv mora zagotoviti preverjanje veljavnosti potrdil lokalno ali oddaljeno. V primeru lokalnega preverjanja se vrši validacija na osnovi javno dostopnih seznamov preklicanih potrdil objavljenih s strani overiteljev. Validacija se vrši na osnovi dostopnih seznamov CRL in mehanizmov za preverjanje podpisov.

Druga (naprednejša) metoda validacije varnostnih atributov se izvaja na osnovi protokolov za preverjanje podatkov in potrdil (Data Validation and Certification Server Protocols, DVCS). Rezultat postopka DVCS so potrdila o validaciji podatkov (Data Validation Certificate, DVC), ki predstavljajo potrditev ali zavrnitev veljavnosti digitalnih podpisov in pripadajočih podatkov. Funkcijo DVCS izvaja zunanji ali notranji subjekt (izven ali znotraj organizacije, ki uporablja arhiv). V primeru notranjega izvajanja, mora uporabnik arhiva zagotoviti evaluacijo rešitve oziroma neoporečnost delovanja sistema DVCS.

Protokol DVCS ne nadomešča uporabo seznama CRL in protokola OCSP, ampak je namenjen predvsem zagotavljanju veljavnosti digitalnih potrdil in podpisov v času preverjanja s strani temu namenjenega subjekta (javno dostopnega ali znotraj organizacije). Na osnovi preverjanja pridobljeno potrdilo zagotovimo veljavnost digitalnega podpisa tudi po preteku veljavnosti potrdila na osnovi katerega je bil ustvarjen podpis.

DVCS na splošno zagotavlja štiri storitve:

- Potrjevanje posedovanja podatkov (Certification of Possession of Data, CPD).
- Potrjevanje zahteve o posedovanju podatkov (Certification of Claim of Possession of Data, CCPD)
- Validacija digitalno podpisanih dokumentov (Validation of Digitally Signed Document, VSD)
- Validacija javnih ključev (Validation of Public Key Certificates, VPKC).

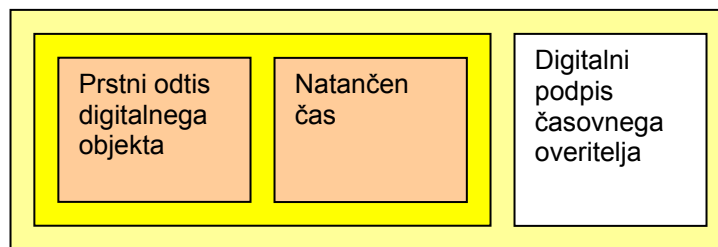
Za varen arhiv sta relevantni predvsem slednji dve funkciji, ki jih mora DVCS podpirati. Funkcija VSD preverja veljavnost vseh podpisov na osnovi informacije o statusih uporabljenih potrdil. Preveri tudi matematično veljavnost podpisov in verodostojnost podpisnikov prek verige uporabljenih potrdil. Za izvajanje uporablja CRL in OCSP. VPKC preveri veljavnost posameznih potrdil.

DVCS mora posredovati podpisan odziv na zahtevo za preverjanje veljavnosti varnostnih atributov. Potrdilo DVC je pripravljeno v obliki podpisanega sporočila. Prenos zahtevkov in odzivov DVCS lahko temelji na poljubnem protokolu: HTTP, HTTPS ali e-mail, itd.

3.6. Razširjena sintaksa elektronskega podpisa

Elektronski zapisi oziroma dokumenti so zaradi svoje elektronske narave podvrženi spremembam v življenjskem ciklu na takšen način, da teh sprememb brez ustrezne tehnologije ni mogoče zaznati. Ker je ena izmed temeljnih funkcij varnih arhivov ščititi vsebine pred spremembo, mora varen arhiv zagotoviti vse potrebne mehanizme, ki zagotavljajo celovitost objektov tudi čez daljša časovna obdobja.

Varen arhiv mora zato vsebovati programsko funkcijo elektronskega podpisovanja (na osnovi običajnega ali kvalificiranega potrdila) in sicer na takšen način, da je elektronsko podpisan vsak objekt, ki je vstavljen v arhiv, ne glede na to, ali objekt vsebuje še druge varnostne attribute (podpise). Varen arhiv mora zagotoviti tudi osveževanje arhivskih digitalnih podpisov in sicer pred iztekom veljavnosti potrdila, na osnovi katerega je bil ustvarjen arhivski podpis. Za ustvarjanje arhivskega podpisa se uporablja časovni žig (Electronci Signature TimeStamp, ES-T), lasten ali izdan s strani ponudnika storitve časovnega žigosanja (slika 3).



Slika 5: Časovni žig digitalnega objekta.

Elektronske zapise, ki so predmet arhiviranja, pogosto spremljajo elektronski podpisi. Zaradi tehničnih omejitev je veljavnost podpisov časovno omejena, medtem ko lahko prenehajo veljati tudi zaradi drugih razlogov (preklic potrdila, prešibek algoritem, itd.). Upravljanje z elektronskimi podpisi je dodatna zahteva, ki jo mora varen elektronski arhiv izpolnjevati.

Digitalna potrdila na osnovi katerih apliciramo varnostne attribute imajo omejen čas veljavnost, ker se smatra:

- Da s časom varnostni algoritmi postanejo prešibki
- Da uporabljena dolžina ključev ne zadostuje

Poleg naštetih razlogov obstajajo še drugi (subjektivni) razlogi, kot je prenehanje delovanja overitelja, prenehanje vzdrževanja seznama preklicanih, itd. Zaradi omenjenih tehničnih dejstev je potrebno varnostne attribute pred iztekom veljavnosti osvežiti.

Osveževanje varnostnih atributov je odvisno od potreb po hranjenju elektronskih dokumentov. Arhiviranje elektronsko podpisanih zapisov ločimo na:

- Kratkoročno

- Srednjeročno
- Dolgoročno

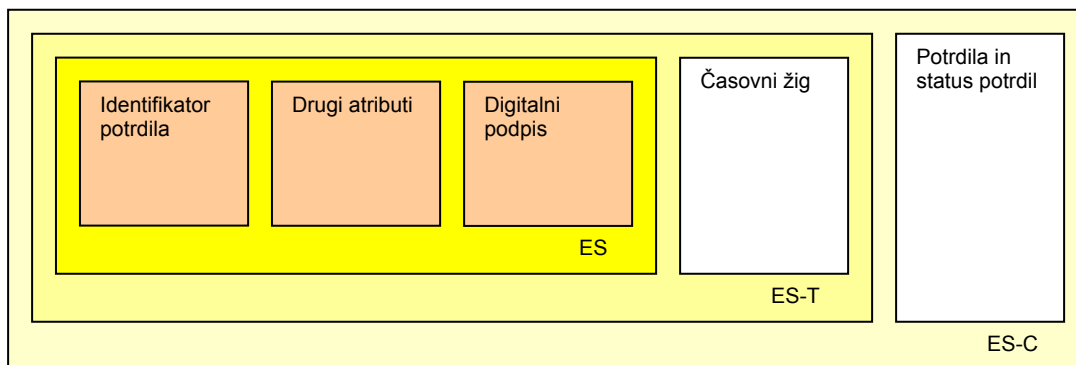
Kratkoročno arhiviranje

Kratkoročno arhiviranje se smatra za obdobje neposredno po ustvarjenem digitalnem objektu in pripadajočem elektronskem podpisu. V takšnem primeru je predviden obstoj vseh elementov za preverjanje veljavnosti digitalnih podpisov:

- Vsa potrdila v verigi potrdil na osnovi katere je bil ustvarjen elektronski podpis
- Status potrdil ob času ustvarjanja elektronskega podpisa (na osnovi seznama preklicanih potrdil)

Za potrebe kratkoročnega arhiviranja je ob prejemu objekta z elektronskim podpisom potrebno preveriti veljavnost varnostnih atributov. V kolikor so vasi atributi veljavni je potrebno ustvariti časovni žig (ES-T) čez varnostne attribute (Slika 3). S časovnim žigom zagotovimo nespremenljivost varnostnih atributov in potrdimo veljavnost elektronskega podpisa ob času ustvarjanja žiga.

Časovni žig lahko opcijsko spremljajo tudi podatki o statusu potrdila, vključno s samim potrdilom na osnovi katerega je bil izdelan elektronski podpis (Electronic Signature with Complete information, ES-C). Shranjevanje potrdil in statusa je namenjeno kasnejšemu preverjanju veljavnosti podpisa. Priporočljivo je, da je čas med ustvarjanjem digitalnega podpisa in časovnega žiga čim krajši.



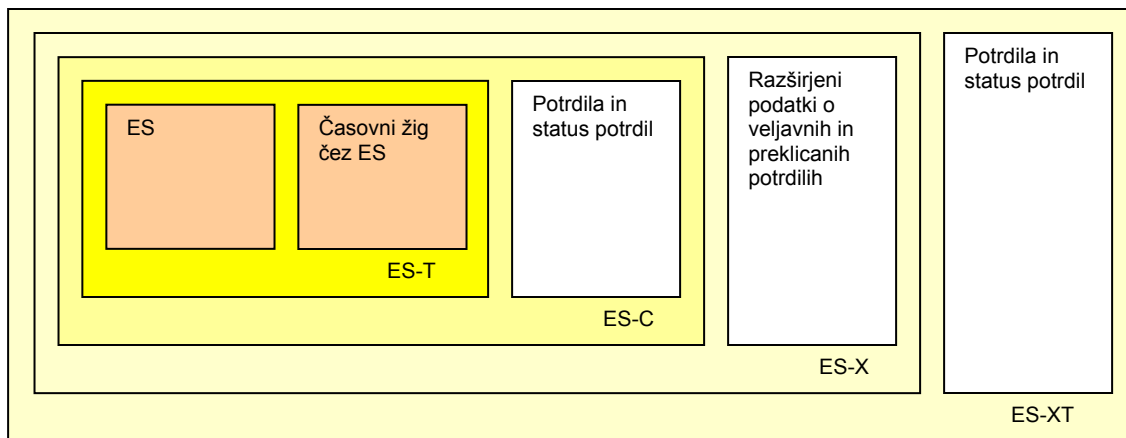
Slika 6: Kratkoročno arhiviranje digitalno podpisanih objektov na osnovi časovnega žiga.

Srednjeročno arhiviranje

Za srednjeročno varno arhiviranje se smatra tisto časovno obdobje, ko podatki za preverjanje veljavnosti ustvarjenih varnostnih atributov niso več na voljo oziroma so pomanjkljivi. To pomeni, da je veljavnost potrdila ali potrdil v verigi pretekla, seznam preklicanih potrdil ni več dostopen, itd.

Da bi zagotovili postopek validacije varnostnih atributov, je potrebno ob vlaganju digitalnega objekta v arhiv zagotoviti podatke v času prvotnega preverjanja digitalnega podpisa objekta veljavnost potrdila in celotne verige potrdil vključno z odzivi s seznama preklicanih potrdil (Certificate Revocation List, CRL) ali protokola za preverjanje veljavnosti potrdil (On-line Certificate Status Protocol, OCSP), ki dokazujejo veljavnost posameznih potrdil ob času nastanka podpisa. Časovni žig mora biti apliciran čez celotno verigo potrdil in odziv na poizvedbo CRL ali OCSP.

Srednjeročno hranjenje digitalno podpisanih objektov temelji na razširjenih podatkih o digitalnem podpisu (ES with extended validation data, ES-X) in časovnemu žigu razširjenih podatkov (ES-X with Timestamp, ES-XT). Pod razširjene podatke spadajo vsi podatki v zvezi z verigo potrdil, odzivom na CRL in OCSP (Slika 5).

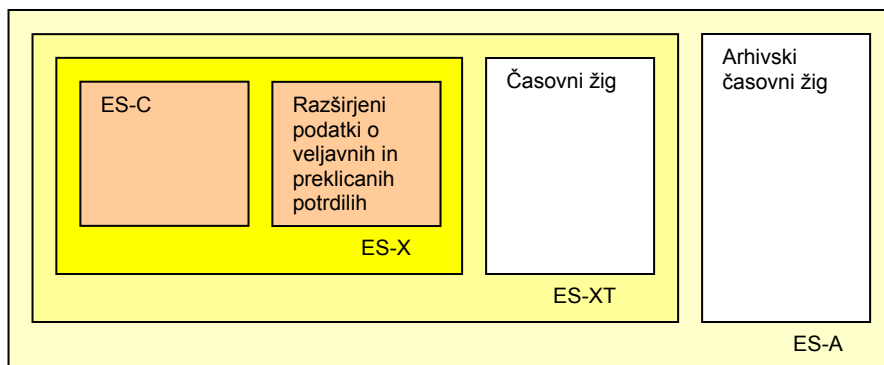


Slika 7: Srednjeročno arhiviranje digitalno podpisanih objektov na osnovi razširjenih podatkov o veljavnosti varnostnih atributov in časovnega žiga.

Dolgoročno arhiviranje

Dolgoročno arhiviranje elektronskih dokumentov s podpisom se smatra za tisti čas, ko kriptografski mehanizmi s katerimi je bil ustvarjen podpis na objektu niso več varni. Takšen način arhiviranja je namenjen nedefiniranemu časovnemu obdobju. Preden postanejo v času podpisa uporabljeni algoritmi in ključi ter drugi ustvarjeni kriptografski podatki prešibki, ali poteče veljavnost ustvarjenih časovnih žigov je potrebno varnostne attribute osvežiti oziroma ponovno časovno žigosati. V kolikor so razlog za pretek veljavnosti izvornih varnostnih atributov prešibki algoritmi, mora nov časovni žig temeljiti na močnejših algoritmi.

Dolgoročno arhiviranje elektronsko podpisanih dokumentov temelji na časovno žigosanih razširjenih elektronskih podpisih s dodatnimi podatki in dodatnim časovnim žigom (ES Archival Validation Data, ES-A). Ponovno žigosanje se izvaja vedno, ko postane obstoječi podpis ES-A prešibek. Objekt lahko tako nosi tudi po več podpisov ES-A (Slika 6).



Slika 8: Dolgoročno arhiviranje digitalno podpisanih objektov na arhivskega časovnega žiga.

4. DODATEK