DOI:10.33179/BSV.99.SVI.11.CMC.13.1.3

Aleksej Jerman Blažič

Strokovni članek

ELEKTRONSKO VARNOSTNO OZNAČEVANJE

ELECTRONIC SECURITY LABELLING

Professional article

Povzetek Razvoj in širitev temeljne informacijske infrastrukture omogoča učinkovito izmenjavo in obdelavo elektronskih podatkov prek različnih organizacijskih ali varnostnih domen. Podatki v elektronski obliki so pri meddomenskem prehodu podvrženi drugačnim varnostnim načelom, saj je nadzor nad elektronsko vsebino bistveno zahtevnejši. Varnostna obravnava elektronskih podatkov skladno z načeli varovanja informacij, ki ima tudi ustrezno zakonsko podlago, je eden izmed aktualnejših tehnoloških in organizacijskih izzivov pri prehodu na elektronsko podporo upravljanja in odločanja, še posebno pri subjektih, kot so organizacije za nacionalno zaščito in obrambo. Za celovito varnostno obravnavo podatkov pri medsebojnem povezovanju različnih komunikacijsko-informacijskih sistemov je treba vključiti organizacijske vidike, na katere morajo odgovarjati ustrezni tehnološki pristopi. Med osnovne tehnološke elemente varnostne obravnave elektronskih podatkov štejemo tehnike elektronskega varnostnega označevanja, overjanja subjektov in nadzora dostopa, šifriranja podatkov in filtriranja prometa. Prispevek predstavlja pregled aktualnega tehnološkega razvoja in tehnološke standardizacije Nata na področju varnostne obravnave in varne izmenjave podatkov v meddomenskem okolju s posebnim poudarkom na tehnikah elektronskega varnostnega označevanja.

Ključne besede ***Varnostne domene, elektronsko varnostno označevanje, varnostna politika, nadzor dostopa, šifriranje.***

Abstract With the development and increase of basic information infrastructure, electronic data can be exchanged and processed through different organizational or security domains. Security aspects of electronic data are treated through a new perspective due to fundamental differences between the electronic and paper versions. Handling of electronic data in line with security measures, also defined by appropriate legislative principles, represents one of the most important technological and organizational challenges, especially for organizations such as national defence systems that are

dealing with sensitive and classified information on a daily basis. Contemporary technological approaches already support the use of techniques for security labelling, data protection and access control. In order to provide for integrated multi-domain solutions, organizational aspects need to be involved and supported with the design, development and implementation of key technology solutions. These are based on standardization processes which ensure inter-domain data exchange without affecting data security. The paper presents an overview of the latest developments in technology and standardization within NATO in the field of secure data interchange between domains, focusing on techniques of electronic confidentially labelling.

Key words ***Security domain, electronic security labelling, security policy, access control, encryption.***

Uvod

Prehod na elektronsko obliko upravljanja in odločanja postaja temeljna usmeritev organizacijskega razvoja na različnih področjih, vključno s poslovnim, upravnim in ne nazadnje tudi na področju izvajanja nacionalne zaščite in obrambe. Elektronska oblika prinaša številne prednosti in zagotavlja optimizacijo procesov upravljanja in odločanja, saj zagotavlja hiter, natančen in kakovosten informacijski pretok ter pospešeno, v določenih okoliščinah takojšnjo obdelavo podatkov. Z elektronsko obliko podprti procesi odločanja in upravljanja morajo pri tem ohranjati svoje ključne značilnosti, med katere vključujemo tudi varnostni kontekst in varnostno obravnavo podatkov.

Potrebe po varnostni obravnavi podatkov navadno identificiramo v organizacijskih okoljih, za katera je značilno ravnanje z informacijami, neposredno povezanimi z ukrepi za zagotavljanje nacionalne varnosti in zaščite ali v povezavi z vojaškimi operacijami, čeprav se z varnostno obravnavo podatkov pogosto srečamo tudi v civilnih okoljih, še posebno tistih, ki operirajo s podatki zasebnega ali finančnega značaja. Podlago za varnostno obravnavo podatkov v sistemih in organizacijah za zagotavljanje nacionalne zaščite in obrambe ter javno upravo na splošno sicer opredeljuje nacionalni pravni red, ki to področje ureja prek Zakona o tajnih podatkih (ZTP) skupaj s pripadajočimi podzakonskimi akti. ZTP opredeljuje skupna izhodišča enotnega sistema določanja, varovanja in dostopa do tajnih podatkov z delovnega področja državnih organov Republike Slovenije, ki se nanašajo na javno varnost, obrambo, zunanje zadeve ali obveščevalno in varnostno dejavnost države. Pomembno je hkrati omeniti, da varnostna obravnava ni omejena zgolj na državne organe, saj se z varnostno obravnavo informacij posredno ukvarjajo tudi drugi področni zakoni oziroma podzakonski akti. Zakon o varstvu osebnih podatkov (ZVOP) na primer določa pravila pri ravnanju s podatki, ki so zasebne narave. Zbiratelj oziroma upravitelj tovrstnih podatkov je zavezan k ustrezni varnostni obravnavi: zagotavljati mora ustrezen sistemsko organizacijski pristop pri označevanju in nadzoru dostopa do informacij zasebnega značaja.

Varnostna obravnava podatkov ima torej širok aplikativni pomen. Z varnostno obravnavo so povezani določeni organizacijski ukrepi kot tudi ustrezni tehnološki pristopi. Med organizacijske ukrepe vključujemo predvsem postopke, povezane z

dodeljevanjem in upravljanjem stopnje tajnosti podatkov ter izvajanjem nadzora dostopa do varnostno označenih podatkov. Z varnostnim označevanjem so povezani postopki identifikacije in odbiranja podatkov, določanje varnostne stopnje, nadzor nad spremembami varnostne stopnje itn., medtem ko so z vidika upravljanja pomembni predvsem postopki nadzora dostopa do varnostno označenih podatkov. Ti so lahko proaktivni (varno shranjevanje podatkov oziroma ločevanje informacijskih sistemov glede na stopnjo tajnosti) ali pasivni (preverjanje dostopnih pravic do podatkov znotraj istega sistema). Nadzor dostopa do tajnih podatkov je lahko določen na zakonodajni ravni, je na primer del pravil koalicijskega povezovanja oziroma del interne politike organizacije (poslovna skrivnost na primer).

Pri prehodu med različnimi organizacijskimi ali varnostnimi domenami pomenijo postopki varnostnega označevanja poseben organizacijsko-tehnološki izziv. Do meddomenskega prehajanja podatkov prihaja v številnih okoliščinah na ravni različnih organizacij ali znotraj organizacije, na nacionalni ravni ali na meddržavni ravni oziroma v okviru koalicijskih združenj. Prehod med različnimi organizacijskimi ali varnostnimi domenami ima lahko zelo velik vpliv na zagotavljanje zaupanja oziroma zaščite podatkov. Do ogrožanja varnosti podatkov lahko pride zaradi različnih vzrokov, kot je razhajanje oziroma neusklajenost organizacijskih varnostnih politik, neusklajenost postopkov varnostne obravnave ali neustrezna tehnološka podpora. Da bi presegli tovrstne razmejitve, je treba najprej uskladiti enakovredno varnostno obravnavo na organizacijski ravni, čemur sledi oblikovanje ustreznega tehnološkega pristopa in nato implementacija mehanizmov za varnostno obravnavo podatkov v meddomenskem prostoru.

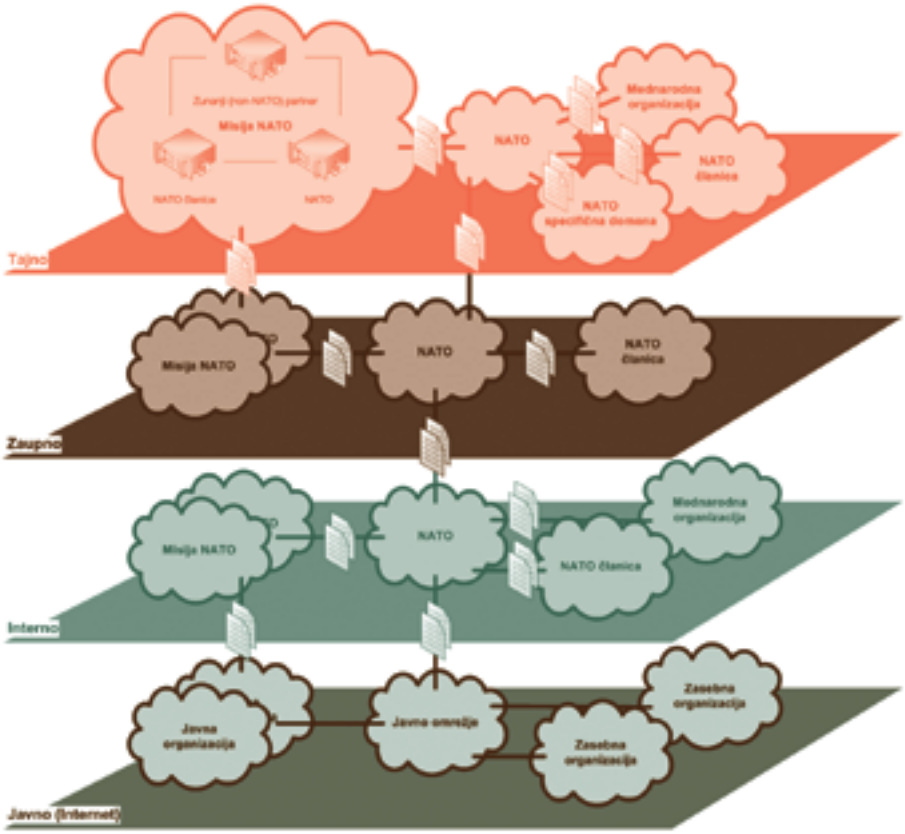
1 POVEZOVANJE IN ZAGOTAVLJANJE SKUPNIH ZMOGLJIVOSTI

Združevanje zmogljivosti na podlagi organizacijskega ter predvsem tehničnega povezovanja med organizacijami in znotraj posameznih organizacij ima številne pozitivne učinke pri optimizaciji procesov. Potrebe po tovrstnem povezovanju so zato prisotne v številnih procesih upravljanja in odločanja organizacij za zagotavljanje nacionalne zaščite in varnosti ter v mednarodnih koalicijah, kot je severnoatlantska zveza Nato. Strategija NNEC (NATO Network-Enabled Capabilites) predvideva zagotavljanje zmogljivosti na podlagi tehničnega povezovanja operativnih okolij od strateške ravni do vključno taktičnih ravni na podlagi medsebojnega povezovanja komunikacijsko-informacijske infrastrukture (NATO 2010-b). Pogoj za medsebojno povezovanje zmogljivosti je tehnično zagotavljanje varnostne obravnave in varne izmenjave podatkov, zato je varno meddomensko povezovanje tudi ena izmed osrednjih razvojnoraziskovalnih tematik koalicije Nato.

Z vprašanjem varnostne obravnave elektronskih podatkov se ukvarjajo različni tehnološki pristopi že od sedemdesetih letih naprej (ISO 1996a, NSA 1999, NIST 1994). Do danes je bilo zasnovanih več tehnoloških priporočil, ki omogočajo varnostno obravnavo podatkov in delujejo skladno z mehanizmi nadzora dostopa oziroma zaščite podatkov (ISO 1996b, ISO 2002, ITU 2000). Toda oblikovanje enotnega

tehnološkega pristopa za varnostno obravnavo podatkov je izredno zahtevno, v določenih okoliščinah celo tehnično neizvedljivo. Različne aktualne tehnike varnostnega označevanja podatkov je danes že mogoče aplicirati za sporočila in sporočilne sisteme, dokumente in dokumentne sisteme, podatke in podatkovne baze, pretočne vsebine in komunikacijske kanale itn.

Varnostno obravnavo podatkov je v sodobnih komunikacijsko-informacijskih sistemih treba zagotoviti celovito in oblikovati predvsem takšne rešitve, ki presegajo osnovno elektronsko varnostno označevanje. V nadaljevanju prispevka so predstavljeni rezultati aktivnosti agencije NC3A, pridobljeni prek delovnih skupin za meddomenske varnostne rešitve RTG-031 (Task Group on XML in Cross-Domain Security Solutions) in za varnost v povezanih omrežjih ET-061 (Task Group on Interconnected Networks and Security). Predstavljen je osnovni koncept varnostne obravnave podatkov in varnostnega elektronskega označevanja (Electronic Confidentiality Labeling). Namen razvoja standardiziranega pristopa varnostne obravnave elektronskih podatkov je definirati ustrezno sintakso za elektronske varnostne oznake in tehnične postopke, ki so povezani z označevanjem, upravljanjem oznak ter izvajanjem varnostne politike dostopa in uporabe podatkov v ciljnih sistemih na podlagi oznak.



Slika 1: Prehajanje različnih organizacijskih in varnostnih domen ima določen vpliv na varnostno obravnavo podatkov. Da bi omogočili varno izmenjavo informacij med domenami, je treba zagotoviti ustrezne organizacijske ukrepe in tehnološka sredstva za varnostno označevanje podatkov, varno izmenjavo med različnimi domenami in ustrezno obravnavo v ciljnih domenah.

2 ELEKTRONSKE VARNOSTNE OZNAKE

Problematiko elektronskega varnostnega označevanja obravnavajo različne metodologije in tehnike. Varnostno označevanje elektronske pošte, na primer, določa internetni standard RFC 2634 (Enhanced Security Services for S/MIME), ki specificira ustrezne varnostne parametre za klasificiranje varnostne stopnje sporočila (na primer elektronsko sporočilo, označeno kot zaupno ali tajno). Sintakso[1] varnostnega označevanja sporočil obravnavata tudi ameriški zvezni standard FIPS 188 (Standard Security Label for Information Transfer) in organizacija Nato (XML-Security Label Syntax and Processing). Z organizacijsko ravnjo varnostnega označevanja se ukvarjajo standardi ISO/IEC in priporočila ITU-T (Security Framework For Open Systems).

Celovita obravnava problematike varnostnega označevanja podatkov v kompleksnejših komunikacijsko-informacijskih sistemih (KIS), kot jih vzdržujejo organizacije za varnost in obrambo, zahteva vključevanje in povezovanje organizacijskih ukrepov s tehnološkimi sredstvi. Osnovo varnostne obravnave podatkov v sistemih KIS predstavljajo varnostne politike in izvrševanje varnostnih politik (nad varnostno obravnavanimi podatki) organizacijsko in tehnološko. Druga podporna sredstva za učinkovito varnostno obravnavo so v primeru elektronskih podatkov še sistemi za upravljanje procesov in podatkov, elektronske varnostne oznake, šifriranje, nadzor in upravljanje podatkovnega prometa ter druga sredstva za komunikacijo in informacijsko varnost.

V prispevku obravnavamo enega izmed najpomembnejših tehnoloških sredstev za varnostno obravnavo podatkov v sistemih KIS. Elektronske varnostne oznake so nov pristop pri medsebojnem povezovanju sistemov KIS, skladno s koncepti storitveno usmerjenih arhitektur (Service oriented Architectures, SoA). Elektronske varnostne oznake uvajajo naslednja tri načela:
- **načelo označevanja**, ki opredeljuje stopnjo tajnosti, način varnostnega označevanja in parametre označevanja podatkov;
- **načelo upravljanja**, ki opredeljuje življenjske cikle varnostnih oznak in način upravljanja oznak med življenjskim ciklom;
- **načelo izvrševanja varnostnih oznak**, ki obravnava izvrševanje varnostne politike skladno z vsebino varnostnih oznak.

Tehnološka sredstva za varnostno označevanje podatkov morajo strogo upoštevati vsa tri načela. Večina izmed sedanjih tehnoloških pristopov obravnava predvsem načelo označevanja, ki pa varnostne oznake postavlja v omejen kontekst uporabe.

V prispevku je predstavljena problematika varnostnega označevanja, kot ga obravnava Nato prek priporočil delovne skupine RTG-031 (NATO 2010-a). V delovni skupini je aktivno vključeno tudi slovensko Ministrstvo za obrambo prek

[1] *Pojem sintaska predstavlja nabor specifičnih oznak in njihov pomen v jeziku XML, uporabljene za potrebe varnostnega označevanja.*

svojega predstavnika s konkretnimi prispevki pri pripravi sintakse varnostnih oznak in procesnih navodil za upravljanje življenjskih ciklov in revizijskimi sledmi vsebinskih sprememb oznak.

Iz aktualnih priporočil delovne skupine RTG-031 so izvzeti vsi komplementarni sistemi, ki so sicer potrebni za celovito varnostno obravnavo podatkov pri prehodu med različnimi domenami, kot je na primer prehod za izmenjavo informacij (Information Exchange Gateway, IEG), prehod XML (XML Guard) ali ustrezni sistemi za šifriranje podatkov, čeprav elektronsko varnostno označevanje v formatu XML predvideva obstoj ustreznih podpornih tehnoloških sredstev. Vlogo podpornih tehnoloških sredstev in njihovo umeščanje v sisteme KIS obravnavajo druge delovne skupine Nata, kot je ET-061, ki je v času nastanka prispevka še v izvajanju.

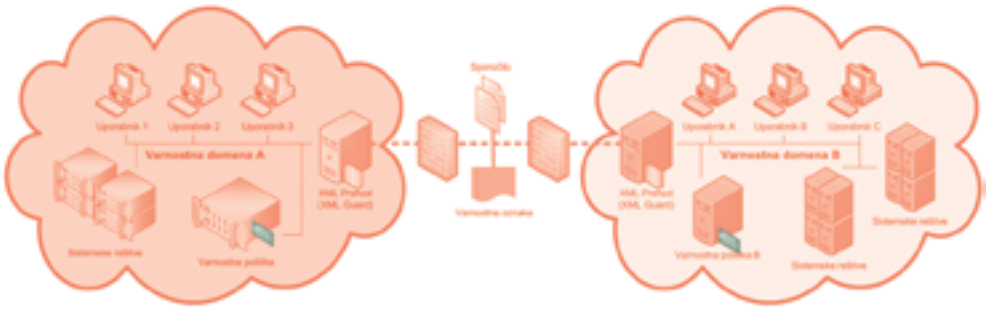
2.1 Označevanje

Varnostno označevanje obravnava različne oblike podatkov, med katere vključujemo sporočila, zapise v podatkovnih bazah, dokumente, ki so lahko strukturirani ali nestrukturirani, podatkovne toke oziroma podatkovne kanale idr. Vsebina oznake je lahko posebej prilagojena za določen proces upravljanja in določanja, medtem ko je generalna struktura vedno enaka. Elektronska oznaka skladno z zahtevami Nata vključuje najmanj (NATO 2010-a):

- informacijo o stopnjo tajnosti (Confidentiality Information);
- lastnika varnostne oznake oziroma identifikacijo subjekta, ki je definiral varnostno oznako (Originator);
- časovne parametre oznake (Creation Date);
- revizijsko sled sprememb varnostne oznake (Succession Handling).

Vsaka varnostna oznaka lahko vključuje še dodatne parametre, ki so namenjeni podpori pri obravnavi oznak in ravnanju z varnostno označenimi podatki v ciljnih sistemih. Med takšne parametre vključujemo na primer tip podatkov, na katere se oznaka nanaša, reference na varnostne politike, skladno s katerimi je bila varnostna oznaka pripravljena, kontekst, v katerem se varnostna oznaka obravnava, ipd.

Med dodatne parametre oznake uvrščamo tudi varnostne vsebine, ki povezujejo lastnika oziroma avtorja z oznako ter kažejo celovitost in avtentičnost oznake. Varnostne vsebine lahko dodatno kažejo tudi točen časovni obstoj oznake, torej verodostojen čas, kdaj je oznaka nastala oziroma kdaj je prišlo do sprememb v vsebini oznake. Med ustrezne tehnike varnostnih vsebin štejemo predvsem digitalne podpise in časovne žige (Eastlake 2002, W3C 2006).



Slika 2: Elektronsko varnostno označevanje temelji na dodajanju varnostnih oznak k sporočilom. Ciljna domena mora oznako ustrezno interpretirati in zagotoviti varnostno obravnavo prejetih sporočil.

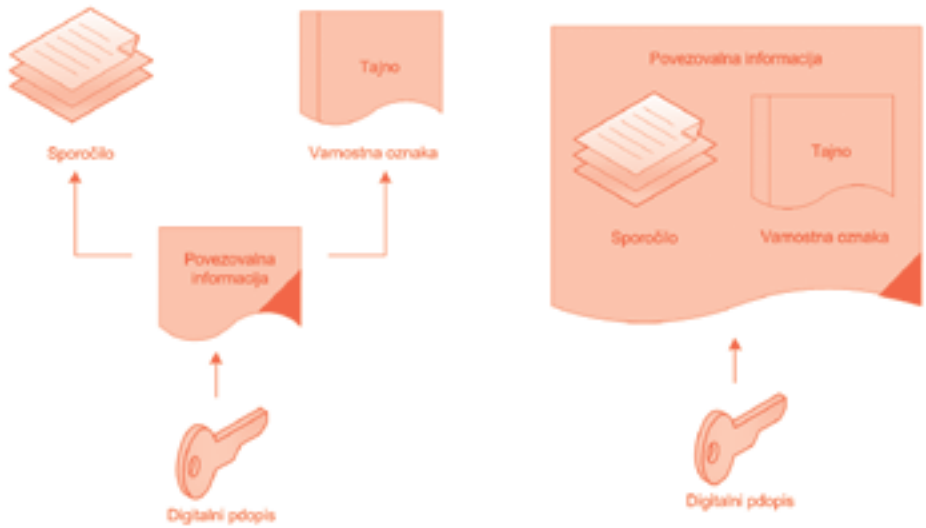
Referenca na varnostno politiko, na podlagi katere je oznaka nastala, je eden pomembnejših dodatnih parametrov (da to ni obvezen element, izhaja predvsem iz dejstva, da je mogoče elektronske oznake uporabljati tudi v okoljih, ki so zaprta in imajo enotno varnostno politiko, torej v okoliščinah, ko podatki prehajajo med različnimi organizacijskimi domenami). Pri izmenjavi dokumentov, ki so varnostno označeni, je namreč pomembno, da ciljni sistem zagotovi ustrezno interpretacijo varnostnega konteksta, v katerem je bil dokument oziroma podatek varnostno označen. Takšne primere lahko identificiramo pri meddržavni izmenjavi zaupnih informacij, pri čemer je treba najprej uskladiti razumevanje specifičnih stopenj zaupnosti, kot je na primer *tajno* (v okoliščinah, ko podatki prehajajo med različnimi varnostnimi domenami z različnimi varnostnimi politikami).

2.2 Upravljanje

Varnostne oznake so enako kot podatki, ki so varnostno označeni, podvržene različnim spremembam. Status sporočila ali dokumenta se lahko med življenjskim ciklom spremeni in preide iz ene stopnje v drugo, nižjo na primer. Tovrstne spremembe mora oznaka zajeti v revizijski sledi. Poleg tega mora sistem varnostnega označevanja vse spremembe propagirati skozi celotno infrastrukturo, torej najmanj v ciljne sisteme, kamor so bili podatki že posredovani.

Varnostne oznake opredeljujejo varnostni kontekst podatkov (sporočil, dokumentov), na katere se navezujejo, zato jih lahko obravnavamo tudi kot dodaten nabor opisnih podatkov. To pomeni, da so iz tehničnega vidika obravnavane kot impliciten del podatkov (so torej integralni del dokumenta) ali zunanji spremljajoči podatek in lahko potujejo neodvisno od dokumenta. V takšnih primerih, ko oznaka nastopa kot spremljajoč podatek, je treba poskrbeti za obveščanje o spremembah, ko do njih pride, in sicer v vseh sistemih, v katerih se podatki obravnavajo skupaj z varnostnimi oznakami. V primeru implicitnega vnosa oznak v dokument pa je treba poskrbeti za posodobitev dokumenta in zagotoviti objavo nove različice v vseh ciljnih sistemih.

Še posebno sta obravnava in obveščanje o spremembah občutljiva v primerih, ko varnostna klasifikacija podatkov prehaja iz nižje stopnje tajnosti v višjo stopnjo.



Slika 3: Varnostna oznaka je lahko vključena v sporočilo ali dodana kot samostojen zapis. Varnostne vsebine (digitalni podpis) zagotavljajo verodostojnost (vsebine) varnostnih oznak.

Nadzor sprememb (change management) mora biti torej integralni del sistemov za varnostno označevanje in mora zagotavljati ustrezno obvladovanje sprememb v širšem kontekstu od izvornega sistema (izvorne domene). To je najbolj občutljiv element varnostnega označevanja, ki mora upoštevati tudi spremembe, ki so posledica dejavnikov zunaj sistema varnostnega označevanja. Do sprememb lahko namreč pride tudi zaradi varnostnih politik, ki se med življenjskim ciklom oznake spreminjajo (oznaka vključuje tudi referenco na varnostno politiko). Za ustrezno uporabo mehanizmov elektronskega varnostnega označevanja morajo biti torej vsi komunikacijsko-informacijski sistemi (vse domene) med seboj usklajeni.

2.3 Izvrševanje varnostnih oznak

Varnostno označeni podatki lahko prehajajo med različnimi organizacijskimi ali varnostnimi domenami. Organizacijsko domeno razumemo kot okolje z enotnimi organizacijskimi ukrepi oziroma pravili, varnostna domena pa je sistem, ki je z vidika varnostne politike omejen, torej ima implementirano enotno varnostno politiko. Med prehodom varnostno označeni dokumenti zapuščajo izvorni sistem in pomembno je, da ciljni sistem:

– zna interpretirati vsebino varnostne oznake, ki se navezuje na določene podatke;
– zna identificirati ustrezno varnostno politiko, na katero se oznaka nanaša;
– izvrši ustrezne akcije skladno z varnostno oznako in varnostno politiko.

Vloga ciljnih sistemov ali domen je torej uskladiti vsebino varnostne oznake z lastno varnostno politiko. Če do uskladitve ne pride, mora ciljni sistem preprečiti razkritje podatkov (dokument, označen s stopnjo tajno, na primer ne sme vstopiti v sistem stopnje zaupno). Posebne okoliščine in s tem povezane tehnične težave lahko predstavljajo prehodni komunikacijsko-informacijski sistemi oziroma prehodne domene. Varnostno označeni podatki lahko potujejo skozi različne domene, ki niso usklajene in ne zagotavljajo ustreznega varnega okolja, s stopnjo tajnosti varnostno označenega podatka (sporočilo z oznako tajno, ki prehaja prek sistema s stopnjo zaupno). V takšnih primerih lahko pride do okoliščin, ko prehodni ali pa tudi ciljni sistemi ne morejo zagotoviti enakovredne varnostne obravnave, kot je to sicer določeno v varnostni oznaki, saj ne vključujejo ustreznih varnostnih sredstev. Pri medsebojni izmenjavi varnostno označenih podatkov je zato pred izmenjavo podatkov pomembno identificirati varnostne lastnosti ciljnega sistema. Temu so namenjeni varnostni prehodi (security guard), ki lahko preprečijo posredovanje dokumenta prek varnostno nezdružljivega sistema ali pa preprečujejo vnos podatkov v varnostno nezdružljiv sistem (Thümmel 2006). Vseh situacij, v katerih se bodo varnostno označeni podatki znašli, ni mogoče predvideti, zato je smotrno uporabiti ustrezne tehnike zaščite podatkov na podlagi šifriranja. Te preprečujejo razkrivanje podatkov v sistemih, v katerih to ni dovoljeno, oziroma v sistemih, za katere velja, da varnostne lastnosti niso enake ali usklajene z izhodiščnimi sistemi oziroma domenami.

3 SINTAKSA VARNOSTNIH OZNAK

Sintaksa varnostnih oznak, kot jo določa delovna skupina NATO RTG-031, je zasnovana na podlagi razširjenega označevalnega jezika in s formatom XML-povezanih tehnologij (NATO 2010-a, W3C 2004). Uporaba jezika XML ima številne prednosti predvsem z vidika združljivosti med različnimi sistemi KIS, storitveno orientirane arhitekture in povezovanja oziroma izkoriščanja drugih ustreznih tehnik in standardov. Sintaksa varnostne oznake v formatu XML je razdeljena na dva temeljna sklopa, in sicer:

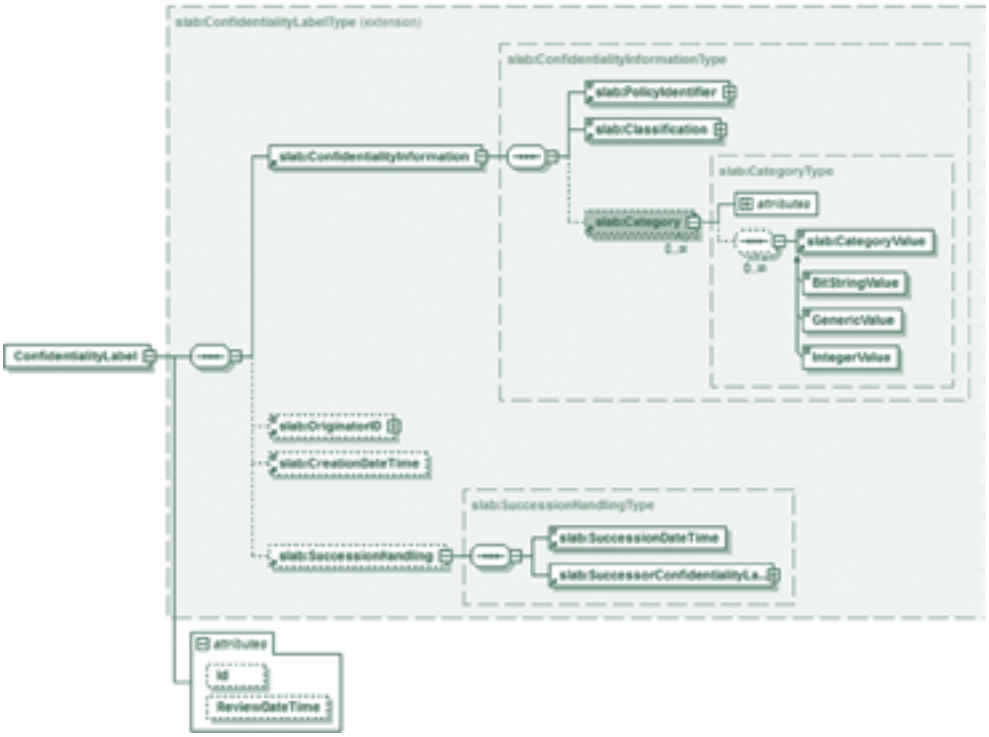
– **varnostna oznaka** (Confidentiality Label), ki združuje vse informacije v zvezi s stopnjo tajnosti podatkov in postopkov oziroma obravnavo označenih podatkov;
– **povezovalna informacija** (Trusted Binding), ki združuje informacije oziroma reference med varnostno oznako in varnostno označenimi podatki na zaupanja vreden način (z uporabo dodatnih varnostnih vsebin).

Vsebina oznake se lahko razlikuje glede na specifične vsebinske, organizacijske ali druge potrebe in je odvisna od varnostnega konteksta podatkov. Priporočilo varnostnega označevanja v formatu XML zato ne predpisuje univerzalne oblike, ki zadostuje vsem pogojem uporabe v sistemih KIS. Struktura varnostne oznake je dovolj prilagodljiva in jo je mogoče prilagajati za specifične potrebe, torej pripraviti različne profile glede na potrebe določenih procesov odločanja in upravljanja. Splošna struktura oznake vključuje najmanj:

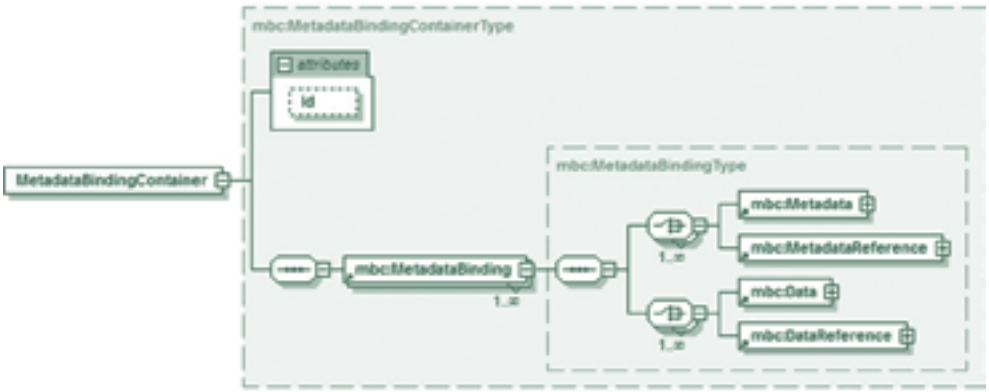
– klasifikacijo,
– (varnostno) politiko.

Dodatno lahko varnostna oznaka vsebuje še:
– kategorijo,
– izvor (avtorja),
– čas ustvarjanja,
– nadzor sprememb.

Eden izmed pomembnejših elementov oznake je referenca na podatke, ki so varnostno označeni. V določenih kontekstih mora biti tovrstna povezava nedvoumna in ji mora ciljni sistem zaupati. Tehnike sklicevanja na podatke so različne, med katerimi v storitveno orientiranih arhitekturah prevladuje predvsem standard uniformnega označevanja (Uniform Resource Identifier, URI). Tehnika temelji na uporabi sintakse internetnih naslovov, vendar pa pri uporabi takšne tehnike nastopijo resne omejitve s preverjanjem verodostojnosti reference. Če ta ni zaščitena z varnostnimi vsebinami ali drugimi mehanizmi, lahko pride do manipulacije oznak in s tem označenih podatkov (zamenjava podatkov na lokaciji, ki jo določa referenca na primer). Zato je mogoče prevzeti referenco na podlagi osnovne tehnike URI kot verodostojni podatek zgolj v primerih, kadar je varnostna oznaka ustvarjena znotraj izvornega sistema oziroma domene, ob prehodu med različnimi domenami pa je treba zagotoviti celovitost in avtentičnost reference.



Slika 4: Struktura elektronske varnostne oznake je sestavljena iz štirih podelementov, ki določajo stopnjo tajnosti in s tem povezane parametre, vključno z varnostno politiko, izvorom oziroma avtorja oznake, čas in revizijsko sled oznake. Opcijski atributi omogočajo vključevanje dodatnih informacij (predvidene spremembe npr.).



Slika 5: Povezovalna informacija zagotavlja verodostojno povezovanje oznake z (označenimi) podatki.

Varnostno označevanje na podlagi jezika XML uporablja za zaščito referenc tehnike digitalnega podpisovanja, ki zagotavljajo povezovanje oznake s podatki na nedvoumen in kriptografsko podprt način (Eastlake 2002, W3C 2006). Uporaba digitalnega podpisa ima dodatno prednost, in sicer omogoča vzpostavitev verodostojne relacije med lastnikom oznake in oznako ter demonstrirati integritete oznake, skupaj z varnostno označenimi podatki. Za dodatno zaščito varnostne oznake je lahko uporabljena še sintaksa evidenčnih podatkov (Evidence Record Syntax, ERS) (Brandner 2007), ki podaljšuje življenjsko dobo digitalnih podpisov in določa verodostojen časovni obstoj oznake (kdaj je bila oznaka ustvarjena oziroma kdaj je prišlo do sprememb).

Obravnava digitalnih podpisov (preverjanje) v vseh situacijah je seveda procesno potratno opravilo, zato je prav modularnost jezika XML prednost, ki jo izkoriščajo varnostne oznake. Ob prehodih med domenami lahko zagotovimo obravnavo oznake (preverjanje verodostojnosti in sklicevanje na podatke) ob vstopu v domeno s pomočjo varnostnih prehodov. Takšni sistemi preverijo veljavnost oznake in izločijo dodane varnostne vsebine z namenom, da je nadaljnje procesiranje varnostne oznake in varnostno označenih podatkov znotraj ciljne domene hitrejše in učinkovitejše.

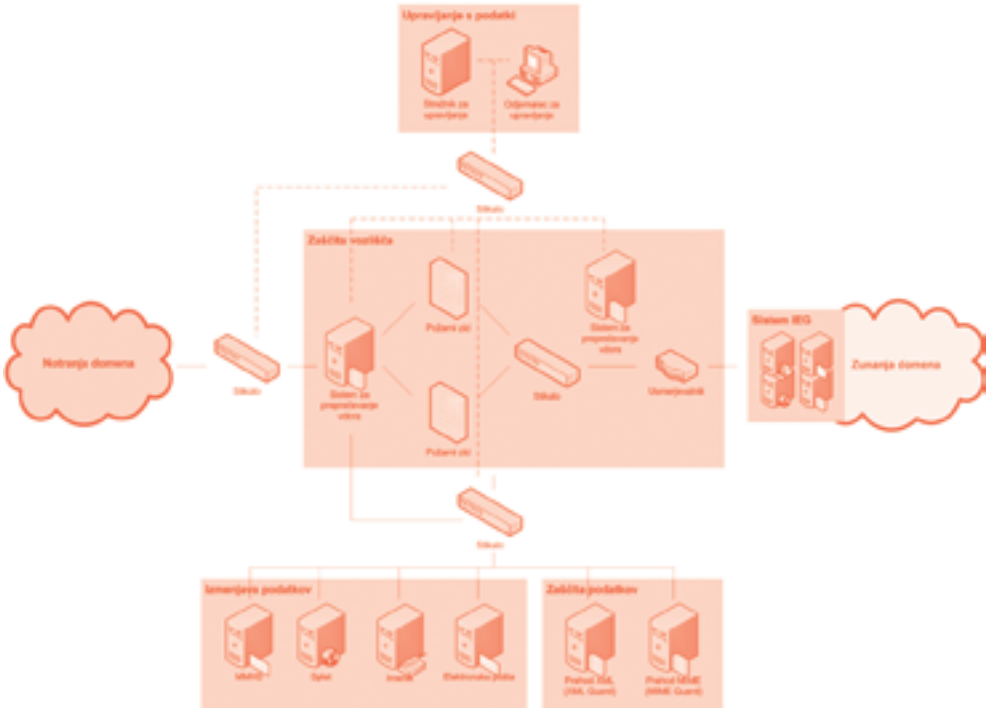
Sklep

Varnostno označevanje podatkov je postalo pomembno vprašanje z intenzivno informatizacijo v organizacijah za zagotavljanje nacionalne zaščite in obrambe ter na področju vojske. Komunikacijsko-informacijski sistemi so dosegli razvojno stopnjo, ki omogoča hitro in učinkovito medsebojno povezovanje informacijskih virov na podlagi konceptov storitveno orientiranih arhitektur. Strategija NNEC predvideva intenzivno podporo informacijskih sistemov na vseh ravneh odločanja in upravljanja. Da bi dosegli cilje strategije, je treba zagotoviti vse tiste tehnološke elemente, ki bodo zagotovili preprosto, hitro, učinkovito in predvsem varno medsebojno povezovanje ter podporo izmenjavi informacij med različnimi organizacijskimi ali varnostnimi domenami na varen in zaupanja vreden način.

Tehnična vprašanja, ki se pri tem odpirajo, so številna in ustrezen odgovor pri varni obravnavi podatkov v meddomenskem povezovanju ne bo eden. Ključno izhodišče za varno izmenjavo podatkov je razumevanje varnostnega konteksta, torej varnostnih implikacij in okoliščin, ki jih predstavlja izmenjava podatkov prek več različnih domen. Ustrezen tehnološki odgovor na takšne zahteve bo vseboval kombinacijo varnostnih mehanizmov oziroma tehnoloških sredstev, ki jih bo treba smiselno in usklajeno povezati v celoto. Varnostno označevanje v jeziku XML, kot ga določa delovna skupina Nato RTG-031, bo imelo bistveno vlogo pri opredelitvi, izmenjavi in razumevanju varnostnega konteksta podatkov, ki nastopajo v procesih upravljanja in odločanja. Uporaba tehnik XML je skladna s sodobnimi tehnološkimi koncepti (arhitekture SoA), splošno tehnološko strategijo razvoja razvejanih omrežij in njihovega medsebojnega povezovanja zato jo močno podpira tudi Nato.

Številne tehnološke osnove in varnostni gradniki za varno izmenjavo podatkov so že na voljo (šifriranje, varni prehodi, nadzori dostopa itn.). Prav tako so temeljni koncepti za medsebojno povezovanje obdelani in že dobro vpeljani v praksi na področjih KIS in drugod (storitveno orientirana arhitektura na podlagi tehnologij spletnih storitev na primer). Vzporedne aktivnosti za zagotavljanje dodatne tehnološke podpore hkrati potekajo na vsebinsko specifičnih področjih, kot so varni prehodi XML na primer (Thümmel 2006). Rezultati tovrstnih aktivnosti smiselno dopolnjujejo infrastrukturo in bodo v prihodnosti omogočili učinkovito medsebojno povezovanje komunikacijsko-informacijskih sistemov na varen način.

Slika 6 predstavlja primer povezovanja in združevanja različnih tehnoloških sredstev, na podlagi katerih lahko zagotovimo varno izmenjavo podatkov med različnimi (varnostnimi ali organizacijskimi) domenami in različnimi sistemi KIS. Sem spadajo sistem za varnostno označevanje, požarni zidovi, varnostna vozlišča, varnostni prehodi (IEG), sistemi za preprečevanje vdorov, sistemi za šifriranje podatkov, sistemi za upravljanje uporabnikov in pravic ter ne nazadnje aplikativni sistemi za podporo procesom upravljanja in določanja (sporočilni sistemi, sistemi za upravljanje delotokov, sistemi za upravljanje vsebin itn.).



Slika 6: Koncept varne izmenjave podatkov med različnimi sistemi KIS zahteva vključevanje več različnih tehnoloških sredstev. Med osnovna sredstva vključujemo sisteme za zaščito (požarni zid, preprečevanje vdorov), sisteme za varnostno označevanje in obravnavo označenih podatkov, sisteme za šifriranje ter sisteme za izvajanje varnostnih politik.

Slovenija aktivno sodeluje pri sooblikovanju tehnoloških izhodišč in pripravi temeljnih tehnoloških priporočil Nata, konkretno na področju elektronskega varnostnega označevanja (delovna skupina RTG-031) in na področju varnega povezovanja informacijskih sistemov (delovna skupina ET-061). Predstavniki MO RS sodelujejo pri razvoju sintakse varnostnih oznak in procesnih navodil za pripravo in obravnavo varnostnih oznak pri vključevanju in povezovanju varnostnih oznak z varnostnimi vsebinami ter pri metodologijah za vzpostavitev celovitih arhitektur za varno medsebojno povezovanje sistemov KIS. Nekatere članice Nata (Norveška, Združeno kraljestvo, Nizozemska in Kanada) dosegajo večje napredke in s konkretnimi implementacijami varnostnih oznak in varnostnega označevanja že podpirajo povezovanje različnih organizacijskih in varnostnih domen tako na nacionalni kot tudi na koalicijski ravni (Združeno kraljestvo, Norveška, Nizozemska in Kanada).

Literatura

1. *Brandner, R., Pordesch, U., Gondrom, T., 2007. Evidence Record Syntax (ERS), RFC4998. IETF (Internet Engineering Task Force).*
2. *Eastlake, D., Reagle, J., Solo, D., 2002. XML-Signature Syntax and Processing, RFC 3275, IETF (Internet Engineering Task Force).*
3. *ISO, 1996. Information Technology – Open Systems Interconnection – Security Frameworks for Open Systems: Overview, ISO 10181-1, ISO (International Organization for Standardization).*
4. *ISO, 1996. Information Technology – Open Systems Interconnection – Security Frameworks for Open Systems: Access Control Framework, ISO 10181-3, ISO (International Organization for Standardization).*
5. *ISO, 2002. Information Technology – Security Techniques – Security Information Objects for Access Control, ISO/IEC 15816, ITU-T X.841, ISO/ITU (International Organization for Standardization / International Telecommunication Union).*
6. *ITU, 2000. Security information objects for access control, ITU-T X.841, ISO/IEC 15816, ISO/ITU (International Organization for Standardization / International Telecommunication Union).*
7. *NSA, 1999. Common Criteria Labeled Security Protection Profile, NSA (National Security Agency)*
8. *NIST, 1994. Standard Security Label for Information Transfer, FIPS 1888, NIST (National Institute of Standards and Technology).*
9. *NATO, 2010-a. XML in Cross-domain Security Solutions, RTO Technical Report, RTG-031, NATO (North Atlantic Treaty Organization).*
10. *NATO, 2010-b, NATO Network Enabled Capabilities, NNEC Portal, https://transnet.act.nato.int/WISE/Informatio 10.9.2010. NATO (North Atlantic Treaty Organization).*
11. *Thümmel, A., Eckstein, K., 2006. Design and Implementation of a File Transfer and Web Services Guard Employing Crypto-graphically Secured XML Security Labels, Proceedings of the 7th IEEE Workshop on Information Assurance, U.S. Military Academy, West Point, NY, 21-23, IEEE (Institute of Electrical and Electronics Engineers).*
12. *W3C, 2004. Extensible markup language (XML) 1.0, W3C (World Wide Web Consortium).*
13. *W3C, 2006. XML Advanced Electronic Signatures (XAdES), W3C, (World Wide Web Consortium).*