

KONFERENCIJA EU PROJEKTA



Capacity building of Croatian Accreditation Agency for development of accreditation scheme to support **Cybersecurity Act**

(Action No. 2020-HR-IA-0201)

Zagreb, 26. veljače 2024.



Sufinancirano instrumentom Europske
unije za povezivanje Europe



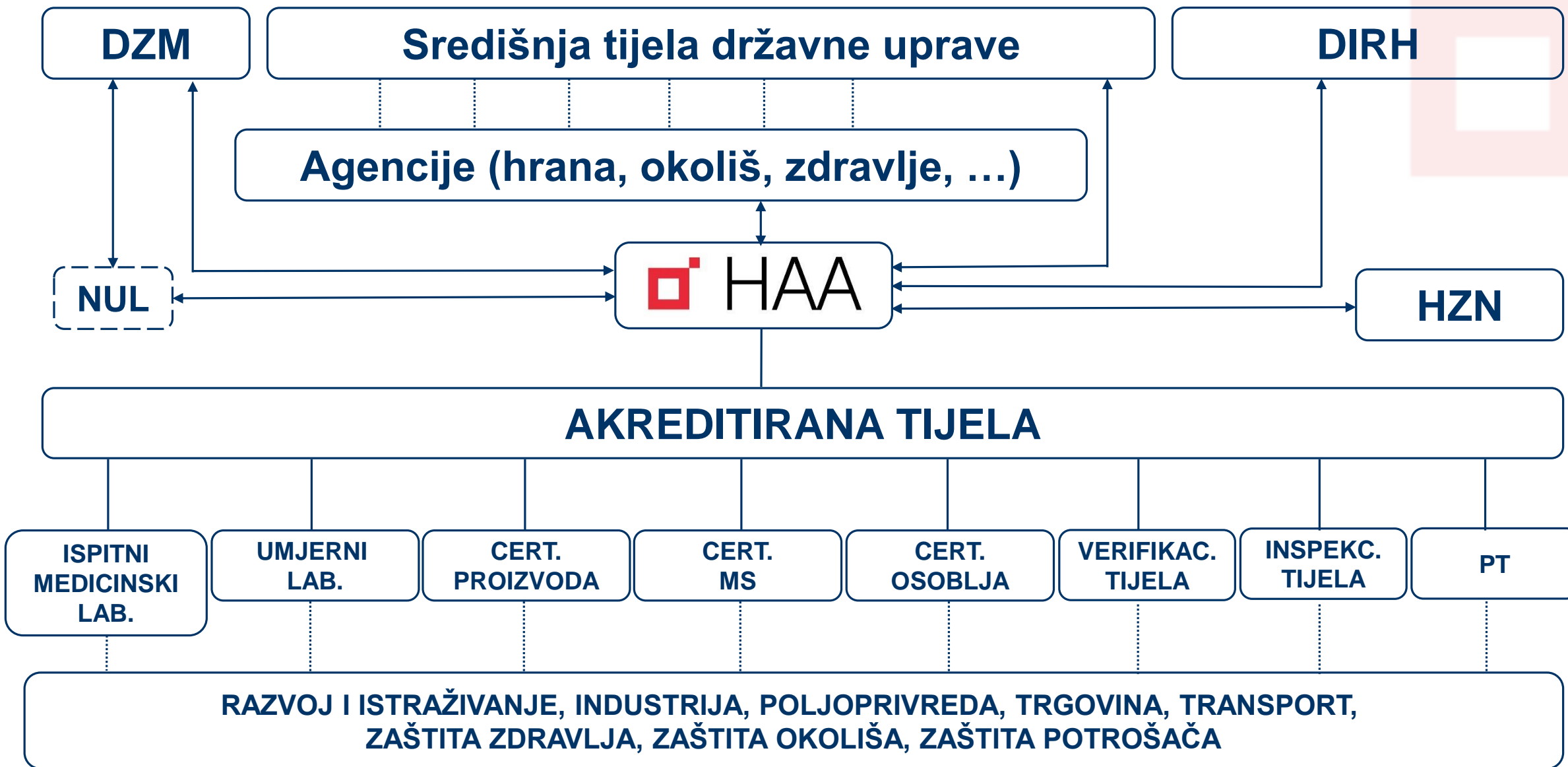
Sufinancira
Europska unija

Hrvatska akreditacijska agencija

- ❑ HAA je neovisna i neprofitna javna ustanova koja obavlja poslove nacionalne službe za akreditaciju u Republici Hrvatskoj prema Uredbi (EZ) br. 765/2008 o akreditaciji i nadzoru nad tržištem te zadovoljava sve zahtjeve norme za akreditacijska tijela HRN EN ISO/IEC 17011

AKREDITACIJA = POVJERENJE
u kompetentnost, osposobljenost, odnosno rezultate rada TOS-a

- ❑ akreditacija u Hrvatskoj – dio europskog akreditacijskog sustava
- ❑ sustav akreditacije u Republici Hrvatskoj međunarodno je priznat od 2010. godine:
 - ❑ Multilateralni sporazum o priznavanju akreditacije s Europskom organizacijom za akreditaciju (**EA MLA**)
 - ❑ Sporazum o uzajamnom priznavanju akreditacije s Međunarodnom organizacijom za akreditaciju laboratorija (**ILAC MRA**)
- ❑ akreditirana tijela - ravnopravna konkurencija na međunarodnom tržištu roba i usluga



Tijela nadležna za ovlašćivanje



REPUBLIKA HRVATSKA
Ministarstvo mora, prometa
i infrastrukture

- ❑ elektromagnetska kompatibilnost (EMC)
- ❑ radiofrekvencijska i telekomunikacijska oprema / radijska oprema (RTT)
- ❑ interoperabilnost željezničkih sustava
- ❑ tehnička ispravnost vozila
- ❑ žičare, vučnice, uspinjača

Primjeri propisa
Direktiva 2013/53/EU o rekreacijskim plovilima i osobnim plovilima na vodomlazni pogon



REPUBLIKA HRVATSKA
Ministarstvo gospodarstva
i održivog razvoja

- ❑ industrijski proizvodi: oprema pod tlakom, strojevi, dizala, električni uređaji, plinski aparati, osobna zaštitna oprema
- ❑ zaštita okoliša: kvaliteta zraka i emisije onečišćujućih tvari u zrak, tlo; GHG; EMAS; vode; tekuća naftna goriva; gospodarenje otpadom; vodonepropusnost građevina za odvodnju, površinske, podzemne i otpadne vode

Primjeri propisa
Direktiva PED 2014/68/EU o tlačnoj opremi
Direktiva 2014/33 o sigurnosti dizala



REPUBLIKA HRVATSKA
Ministarstvo
unutarnjih poslova

- ❑ oprema i uređaji za rad u eksplozivnoj atmosferi (ATEX)
- ❑ eksplozivi za civilnu uporabu
- ❑ pirotehnička sredstva
- ❑ vatrogasni aparati
- ❑ forenzika
- ❑ zaštita od ionizirajućeg zračenja
- ❑ strojevi i oprema za razminiranje

Primjeri propisa
Direktiva ATEX 2014/34/EU o uporabi opreme za rad u potencijalno u eksplozivnim atmosferama



REPUBLIKA HRVATSKA
Ministarstvo prostornoga uređenja,
građiteljstva i državne imovine

- ❑ građevni proizvodi
- ❑ strojarske instalacije
- ❑ oprema i postrojenja u građevinama



REPUBLIKA HRVATSKA
Ministarstvo rada, mirovinskoga sustava, obitelji i socijalne politike

- ❑ osobna zaštitna oprema

Tijela nadležna za ovlašćivanje



REPUBLIKA HRVATSKA
Ministarstvo
poljoprivrede

- ❑ službena kontrola hrane
- ❑ proizvodi iz ekološke proizvodnje
- ❑ proizvodi s oznakama zemljopisnog podrijetla i izvornosti
- ❑ vino i maslinovo ulje



REPUBLIKA HRVATSKA
Državni inspektorat

- ❑ veterinarski pregledi i kontrole (delegirana tijela)



REPUBLIKA HRVATSKA
Ministarstvo
zdravstva

- ❑ voda za ljudsku potrošnju
- ❑ bazenska voda
- ❑ otpadne vode
- ❑ predmeti opće uporabe
- ❑ buka
- ❑ zaštita od neionizirajućeg zračenja
- ❑ medicinski proizvodi
- ❑ igračke
- ❑ GMO
- ❑ medicinski laboratoriji



REPUBLIKA HRVATSKA
Državni zavod za mjeriteljstvo

- ❑ vodomjeri
- ❑ plinomjeri
- ❑ brojila električne energije
- ❑ tlakomjeri za gume
- ❑ agregati za istakanje goriva
- ❑ vage i utezi
- ❑ mjerila uzemljenja i izolacijskog otpora električnih instalacija
- ❑ taksimetri



REPUBLIKA HRVATSKA
Ministarstvo
financija

- ❑ automati i stolovi za igre na sreću
- ❑ automati za zabavne igre



REPUBLIKA HRVATSKA
Zavod za sigurnost informacijskih sustava

- ❑ IT sigurnosni proizvodi i sustavi

Capacity building of Croatian Accreditation Agency

for development of accreditation scheme to support
Cybersecurity Act (2020-HR-IA-0201)



▣ HaDEA i HAA

- ▣ ugovor o dodjeli bespovratnih sredstava br. INEA/CEF/ICT/A2020/2396357

▣ Glavni cilj

- ▣ proširenje akreditacijskih aktivnosti na novu akreditacijsku shemu za kibernetičku sigurnosnu certifikaciju u sklopu postojećih akreditacijskih shema:
 - ▣ HRN EN ISO/IEC 17025 - akreditacija ispitnih laboratorija
 - ▣ HRN EN ISO/IEC 17065 - akreditacija certifikacijskih tijela (certifikacija proizvoda, usluga i procesa)



Capacity building of Croatian Accreditation Agency

for development of accreditation scheme to support
Cybersecurity Act (2020-HR-IA-0201)



- ❑ ispunjavanje uvjeta u:
 - ❑ Uredbi (EU) 2019/881 (Akt o kibersigurnosti)
 - ❑ Zakonu o provedbi kibernetičke sigurnosne certifikacije (NN br. 63/22)
- ❑ ukupni prihvatljivi troškovi: **758.737,36 €**
- ❑ maksimalni doprinos bespovratnih sredstava: **569.053,02 € (75%)**
- ❑ provedba projekta: od **1. listopada 2021.** do **30. rujna 2024.** godine

Capacity building of Croatian Accreditation Agency

for development of accreditation scheme to support
Cybersecurity Act (2020-HR-IA-0201)



AKTIVNOST 1

- Izgradnja i unapređenje internih kapaciteta i sposobnosti HAA

ZADATAK 1.1

- Izobrazba za osoblje HAA, vodeće ocjenitelje i eksperte (NAH)

ZADATAK 1.2

- Tehnička pomoć HAA iz države članice EU (RvA)

ZADATAK 1.3

- Studijska posjeta NAT-u iz države članice EU (RvA)

ZADATAK 1.4

- Nabava i integracija odgovarajuće IT infrastrukture

AKTIVNOST 2

- Razvoj učinkovitog postupka akreditacije za kibernetičku sigurnosnu certifikaciju
- Izrađena dokumentacija implementirana u sustav upravljanja HAA

AKTIVNOST 3

- Upravljanje projektom, aktivnosti komunikacije i diseminacije

Razvoj akreditacijske sheme

AKTIVNOST 1

- **Izgradnja i unapređenje internih kapaciteta i sposobnosti HAA**

ZADATAK 1.1

- **Izobrazba za osoblje HAA, vodeće ocjenitelje i eksperte**
- provedeno u suradnji s NAH-om
- 4.-8.7.2022.
- 17 sudionika

ZADATAK 1.2

- **Tehnička pomoć HAA iz države članice EU**
- provedeno u suradnji s RvA-om
- 31.1.2024. - 1. dio radionice; 16 sudionika
- 22.2.2024. - 2. dio radionice; 19 sudionika
- 01/2023 - 02/2024 – RvA – HAA online komunikacija, razmjena znanja i iskustava te pomoć u razvoju HAA dokumentacije

ZADATAK 1.3

- **Studijska posjeta NAT-u iz države članice EU**
- provedeno u suradnji s RvA-om
- 21.–23.3.2023.; 5 sudionika
- razmjena iskustava i sudjelovanje u ocjenama TOS-eva prema 17065 i 17025 u području kibernetičke sigurnosti

Razvoj akreditacijske sheme



AKTIVNOST 2

- Razvoj učinkovitog postupka akreditacije za kibernetičku sigurnosnu certifikaciju

04/2023 – 02/2024

- **Izrađena dokumentacija implementirana u sustav upravljanja HAA:**
 - HAA-Up-1/1 Akreditacija ispitnih laboratorija u području kibernetičke sigurnosne certifikacije
 - HAA-Up-1/2 Akreditacija certifikacijskih tijela za shemu kibernetičke sigurnosne certifikacije
 - 23.2.2024. interna izobrazba osoblja HAA

Akreditacija u području kibernetičke sigurnosne certifikacije

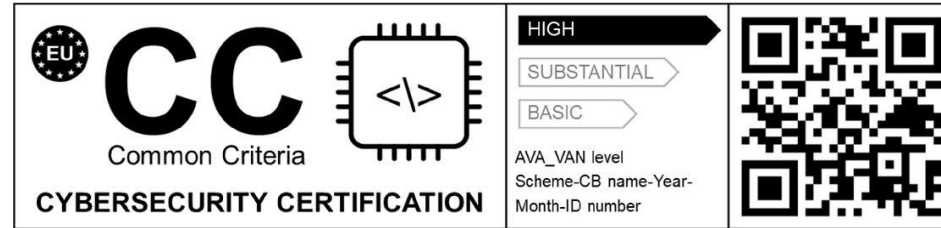


Kibernetska sigurnost



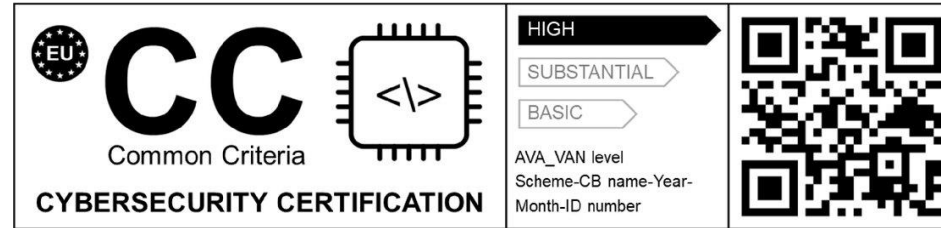
- ▣ Uredba (EU) 2019/881 (Akt o kibersigurnosti)
- ▣ aktivnosti koje su nužne za zaštitu od kiberprijetnji mrežnih i informacijskih sustava, korisnika tih sustava i drugih osoba na koje one utječu
- ▣ okvir za uspostavu europskih programa kibernetičke sigurnosne certifikacije za potrebe osiguranja prikladne razine kibernetičke sigurnosti
- ▣ ENISA - the European Union Agency for Cybersecurity
 - ▣ osnovana 2004. godine
 - ▣ opseg aktivnosti opisan Aktom o kibersigurnosti
 - ▣ podupire i promiče razvoj i provedbu politike Unije o kibernetičkoj sigurnosnoj certifikaciji IKT proizvoda, IKT usluga i IKT procesa

EUCC shema



- ❑ Provedbena Uredba Komisije (EU) 2024/482 o utvrđivanju pravila za primjenu Uredbe (EU) 2019/881 Europskog parlamenta i Vijeća u pogledu donošenja **europskog programa kibernetičke sigurnosne certifikacije na temelju zajedničkih kriterija (EUCC)**
- ❑ vezana za CC, CEM dokumente
- ❑ opisuje postupak kibernetičke sigurnosne certifikacije IKT proizvoda
 - ❑ provodi se s obzirom na potrebnu sigurnost
- ❑ opisani osnovi kriteriji za kibernetičku sigurnosnu certifikaciju IKT proizvoda

EUCC shema



- ❑ postupak certifikacije se temelji na radu dvije vrste tijela za ocjenjivanje sukladnosti (TOS)
 - ❑ ITSEF – *Information Technology Security Evaluation Facility*
 - ❑ ispitni laboratorij akreditiran prema normi HRN EN ISO/IEC 17025
 - ❑ CB – *Certification Body*
 - ❑ certifikacijsko tijelo za certifikaciju proizvoda akreditiran prema normi HRN EN ISO/IEC 17065
- ❑ EUCC – temeljni dokument za akreditaciju u području kibernetičke sigurnosti
 - ❑ na njega se vežu ostali dokumenti koji detaljno definiraju kriterije za akreditaciju

Vezani dokumenti



- ▣ EUCC shema temelji se na:
 - ▣ CC - *Common Criteria* - zajednički kriteriji za vrednovanje sigurnosti informacijske tehnologije kako su utvrđeni u normama niza ISO/IEC 15408
 - ▣ CEM - *Common Evaluation Methodology* - zajednička metodologija za vrednovanja sigurnosti informacijske tehnologije kako je utvrđena u normi ISO/IEC 18045
 - ▣ <https://commoncriteriaportal.org/cc/index.cfm>
 - ▣ *State-of-the-art* dokumenti – navedeni u Prilogu I. Provedbene Uredbe Komisije (EU) 2024/482
 - ▣ <https://certification.enisa.europa.eu/>

Postupak EUCC certifikacije



- ▣ Kriteriji za EUCC certifikat
 - ▣ CC/CEM dokumenti
 - ▣ razina rizika vezana za namjeravanu uporabu proizvoda (osnovna, znatna ili visoka)
 - ▣ *State-of-the-art* dokumenti
 - ▣ **certificirani** zaštitni profili

Postupak EUCC certifikacije



- ▣ postupak certifikacije
 - ▣ sve bitne informacije ITSEF-u i CT-u
 - ▣ ITSEF provodi evaluaciju temeljem postavljenih kriterija
 - ▣ sva ispitivanja i evaluacije
 - ▣ tehničko izvješće o evaluaciji
 - ▣ CT
 - ▣ pregled rezultata evaluacije
 - ▣ potvrda o prikladnosti tehničkih izvješća
 - ▣ Izvješće o certifikaciji - Prilog V.
 - ▣ EUCC certifikat - Prilog VII.
 - ▣ certifikat i izvješće o certifikaciji dostavljaju se NCCA-u radi objave
 - ▣ certifikacija zaštitnih profila sličan postupak
 - ▣ ITSEF evaluira je li profil zaštite potpun, dosljedan, tehnički prihvatljiv i djelotvoran za predviđenu uporabu i sigurnosne ciljeve

EUCC certifikat

- ❑ trajanje određuje CT
 - ❑ maksimalno pet godina
- ❑ moguća revizija
 - ❑ na temelju nositelja ili CT-a
 - ❑ opisano u Prilogu IV.
 - ❑ CT po potrebi uključuje ITSEF
- ❑ suspenzija certifikata
 - ❑ dok se ne poduzmu prikladne korektivne mjere
- ❑ povlačenje certifikata
 - ❑ kao rezultat revizije
 - ❑ moguće odmah izdavanje novog s istim opsegom ili s drugim opsegom
 - ❑ o svakom povlačenju obavijestiti NCCA

Akreditacija u području kibernetičke sigurnosti

- ❑ akreditacijska shema za ispitne laboratorije i certifikacijska tijela za proizvode u području kibernetičke sigurnosne certifikacije
- ❑ temeljena na EUCC shemi, ali vrijedi za sve sheme temeljene na *Common Criteria*
- ❑ razvijena dva dokumenta:
 - ❑ HAA-Up-1/1 Akreditacija ispitnih laboratorija u području kibernetičke sigurnosne certifikacije
 - ❑ HAA-Up-1/2 Akreditacija certifikacijskih tijela za shemu kibernetičke sigurnosne certifikacije
- ❑ HAA ima obvezu obavijestiti ZSIS o svakoj prijavi i dodijeljenoj akreditaciji
- ❑ u slučaju ako postoji poseban ili dodatan zahtjev u EUCC shemi, akreditirano tijelo ima obvezu ishodačenja dodatne autorizacije od NCCA

Akreditacija ITSEF-a

- ❑ HAA-Up-1/1 Akreditacija ispitnih laboratorija u području kibernetičke sigurnosne certifikacije
- ❑ osnovni kriteriji:
 - ❑ HRN EN ISO/IEC 17025
- ❑ dodatni kriteriji:
 - ❑ ISO/IEC TS 23532-1 *Information security, cybersecurity and privacy protection - Requirements for the competence of IT security testing and evaluation laboratories - Part 1: Evaluation for ISO/IEC 15408*
 - ❑ Provedbena Uredba Komisije (EU) 2024/482 o utvrđivanju pravila za primjenu Uredbe (EU) 2019/881 Europskog parlamenta i Vijeća u pogledu donošenja europskog programa kibernetičko sigurnosne certifikacije na temelju zajedničkih kriterija (EUCC)
 - ❑ *State-of-the-art* dokumenti za akreditaciju ITSEF-a za EUCC shemu
 - ❑ Akt o kibersigurnosti - Uredba (EU) 2019/881
 - ❑ CC/CEM dokumenti

Akreditacija ITSEF-a



▣ dodatni elementi:

- ▣ minimalna osposobljenost za vrednovatelje prema ISO/IEC 15408 - prema zahtjevima ISO/IEC 19896-1 i ISO/IEC 19896-3
- ▣ zahtjevi za prostorije i okolišne uvjete mogu biti primjenjivi
- ▣ mjerna sljedivost - na ITSEF-u je odgovornost da dokaže opravdanost politike osiguranja mjerne sljedivosti
- ▣ uzorkovanje se može pojaviti, na primjer uzorkovanje proizvoda koji se testiraju, ali ne nužno u području rada ITSEF-a
- ▣ procjena mjerne nesigurnosti općenito nije primjenjiva
- ▣ osiguranje valjanosti rezultata - HAA-Pr-2/6
 - ▣ vanjska kontrola kvalitete – ispitivanja sposobnosti pomoću međulaboratorijskih usporedbi
 - ▣ unutarnje kontrole kvalitete – unutar laboratorijske usporedbe, međuprovjere opreme, ponovna testiranja

Akreditacija CT-a

- ❑ HAA-Up-1/2 Akreditacija certifikacijskih tijela za shemu kibernetičke sigurnosne certifikacije
- ❑ osnovni kriteriji:
 - ❑ HRN EN ISO/IEC 17065
- ❑ dodatni kriteriji:
 - ❑ Provedbena Uredba Komisije (EU) 2024/482 o utvrđivanju pravila za primjenu Uredbe (EU) 2019/881 Europskog parlamenta i Vijeća u pogledu donošenja europskog programa kibernetičko sigurnosne certifikacije na temelju zajedničkih kriterija (EUCC)
 - ❑ EUCC *state-of-the-art* dokumenti za akreditaciju CT-a
 - ❑ Akt o kibersigurnosti - Uredba (EU) 2019/881
 - ❑ CC/CEM dokumenti
- ❑ certifikacijska shema
 - ❑ temeljena na propisima (poput EUCC sheme), privatnim/komercijalnim zahtjevima ili je mogu razviti vlasnici sheme u skladu sa specifičnim zahtjevima

Postupak akreditacije



- ❑ HAA-Pr-2/1 Pravila za akreditaciju TOS
- ❑ pretprijavne aktivnosti
 - ❑ e-upit <https://akreditacija.hr/eupit/>
 - ❑ informativni sastanak
- ❑ prijava za akreditaciju
 - ❑ dostava prijavnih dokumenata
 - ❑ obrazac Prijave za akreditaciju
 - ❑ obrazac Dodatka AS x
 - ❑ registracija djelatnosti kod nadležnog Trgovačkog suda
 - ❑ statut tvrtke ili drugi odgovarajući dokument
 - ❑ korelacijska tablica
 - ❑ dokumentacija sustava upravljanja
 - ❑ izvještaj unutarnje neovisne ocjene, izvještaj upravine ocjene

Postupak akreditacije



- ▣ prijedlog ocjeniteljske skupine i ugovor s troškovnikom
 - ▣ sastav ocjenitelja
 - ▣ vodeći ocjenitelj
 - ▣ stručni ocjenitelji/eksperti
- ▣ ocjenjivačke aktivnosti
 - ▣ ocjena dokumentacije
 - ▣ ocjena na licu mjesta
 - ▣ witness auditi
 - ▣ pisanje izvještaja
 - ▣ upravljanje nalazima s ocjene

Postupak akreditacije - ocjena



▣ ocjena dokumentacije

- ▣ početne i ponovne akreditacije
- ▣ zaključak o prikladnosti dokumentacije i spremnosti za ocjenu na licu mjesta

▣ ocjena na licu mjesta

- ▣ jasno definirani kriteriji akreditacije
- ▣ plan ocjene
- ▣ uvodni sastanak
- ▣ provedba ocjene
- ▣ nalazi na ocjeni
- ▣ završni sastanak

Postupak akreditacije - ocjena



- ▣ izvještaji s ocjene
 - ▣ izvještaji ocjenitelja/eksperata
 - ▣ završni izvještaj vodećeg ocjenitelja
- ▣ upravljanje nalazima
 - ▣ popis nalaza sa ocjene
 - ▣ analiza uzroka, opsega i prijedlog ispravaka i popravni radnji
 - ▣ konačni popis nalaza s prijedlogom o akreditaciji

Postupak akreditacije



- ❑ donošenje odluke o akreditaciji
 - ❑ konačno definiranje područja akreditacije
 - ❑ svi nalazi moraju biti riješeni
 - ❑ sve obveze moraju biti podmirene

- ❑ akreditirano tijelo
 - ❑ područje akreditacije nalazi se u Registru akreditacija <https://akreditacija.hr/registar/>
 - ❑ akreditacija vrijedi 5 godina
 - ❑ unutar razdoblja važenja akreditacije provode se redovni nadzori

- ❑ suženje, suspenzija i povlačenje akreditacije
- ❑ pritužbe i žalbe

Područje akreditacije

Vrednovanje IKT kibernetičke sigurnosti

Br. No.	Materijali/Proizvodi <i>Materials/Products</i>	Vrsta ispitivanja/Svojstvo <i>Type of test/Property</i> Raspon/Range	Metoda ispitivanja/ <i>Test method</i>
1.	IT proizvodi i sustavi (specifični proizvodi i sustavi bi trebali biti navedeni ako je primjenjivo)	Vrednovanje IKT kibernetičke sigurnosti (tip testa može biti naveden) (raspon može biti naveden, npr. do EAL 3 pojačan s ALC_FLR.1.)	ISO/IEC 15408-1 ISO/IEC 15408-2 ISO/IEC 15408-3 ISO/IEC 15408-4 ISO/IEC 15408-5 Common Criteria for Information Technology Security Evaluation (CC) ISO/IEC 18045 Common Criteria Evaluation Methodology for Information Technology Security Evaluation (CEM)

IKT kibernetička sigurnosna certifikacija

Br. No.	Materijal/Proizvod <i>Material/Product</i>	Postupak ocjenjivanja sukladnosti/ <i>Conformity assessment procedure</i>	Norma/Normativni dokument <i>Standard/Normative document</i>
1.	IT sigurnosni proizvodi i sustavi	Europska CC shema (EUCC): IKT kibernetička sigurnosna certifikacija	ISO/IEC 15408-1 ISO/IEC 15408-2 ISO/IEC 15408-3 ISO/IEC 15408-4 ISO/IEC 15408-5 Common Criteria for Information Technology Security Evaluation (CC) ISO/IEC 18045 Common Criteria Evaluation Methodology for Information Technology Security Evaluation (CEM)

Područje akreditacije – primjer RvA



Security Law

This annex is valid from: **21-09-2023** to **01-09-2027**

Replaces annex dated: **17-11-2021**

No.	Material or product	Type of activity ¹	Internal reference number	Location
2	IT products and systems	Evaluation of IT-security products	- Common Criteria v3.1 - NEN-ISO/IEC 15408-1, -2, -3 - Common Evaluation Methodology v3.1 -NEN-ISO/IEC 18045 For EAL1-EAL7, ALC_FLR.3, ASE TSS.2	DE

Područje akreditacije – primjer RvA




Product ¹ / Product Group	Certification Scheme ²	Standard / normative document ³
IoT-Products and - Platforms	Security Evaluation Standard for IoT Platforms (SESIP) <ul style="list-style-type: none"> - Type examination (testing) - Site audit (audits) 	Global Platform Security Evaluation Standard for IoT Platforms (SESIP) TrustCB scheme procedures for SESIP ISO/IEC 15408-1:2009, -2:2008, -3:2008, Common Criteria for Information Technology Security Evaluation (CC) v3.1, rev 5, and ISO/IEC 18045:2008, Common Criteria Evaluation Methodology for Information Security Evaluation (CEM) v3.1, rev 5 ISO/IEC 15408-1, -2, -3, -4, -5, and ISO/IEC 18045
IT Security Products and Systems	Netherlands Scheme for Certification in the area of IT security (NSCIB) <ul style="list-style-type: none"> - Type certification (testing) - Site audit (audit) 	ISO/IEC 15408-1:2009, -2:2008, -3:2008, Common Criteria for Information Technology Security Evaluation (CC) v3.1, rev 5, and ISO/IEC 18045:2008, Common Criteria Evaluation Methodology for Information Security Evaluation (CEM) v3.1, rev 5 ISO/IEC 15408-1, -2, -3, -4, -5, and ISO/IEC 18045



Hrvatska akreditacijska agencija

Ulica grada Vukovara 78

HR-10000 ZAGREB

 **+385 1 610 63 22**

 **akreditacija@akreditacija.hr**

 **hrvatska-akreditacijska-agencija**

<http://www.akreditacija.hr>



**Sufinancirano instrumentom Europske
unije za povezivanje Europe**



**Sufinancira
Europska unija**

Sadržaj ove publikacije isključiva je odgovornost Hrvatske akreditacijske agencije i ne odražava nužno mišljenje Europske unije.



HAA

Hrvatska akreditacijska agencija
Croatian Accreditation Agency