Organizační pokyny

- webinář probíhá od **13:00 do cca 14:30**
- kamery účastníků defaultně **vypnuty**
- webinář bude **nahráván** a záznam bude sdílen na YouTube NÚKIB / webu NKC
- **dotazy** je možné psát v průběhu webináře do chatu
- **prezentace** bude registrovaným zaslána

WEBINÁŘ NKC – AKTUÁLNÍ VÝZVY V EU PROGRAMECH V OBLASTI KYBERNETICKÉ BEZPEČNOSTI

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

Webinář je organizován ve spolupráci s **Technologickým centrem Praha** a **CzechInvest.**

Činnost NKC je podpořena z programu Digitální Evropa v rámci projektu **National Coordination Centre in the Czech Republic** (zkr. NCC-CZ, č. 101127941).

NCC-CZ
CZECHIA CYBERSECURITY
COORDINATION CENTRE

ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

Spolufinancováno
Evropskou unií

Harmonogram webináře

- **13:00–13:05** Úvod a přivítání účastníků (NKC)
- **13:05–13:25** Přehled aktuálních výzev v programu Digitální Evropa část Kyberbezpečnost (NKC)
- **13:25–13:45** Přehled aktuálních výzev v programu Horizont Evropa část Klastr 3 kyberbezpečnost (TC Praha)
- **13:45–14:05** Služby a aktivity CzechInvest v pozici Národního kontaktního bodu pro DEP v ČR (CzechInvest)
- **14:05–14:10** Závěr a shrnutí (NKC)
- **14:10–14:30** Diskuse a dotazy účastníků

BLOK 1 - ÚVOD

Nikola Chvátalová

NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

Vymezení NKC

- NKC vzniká na základě Nařízení Evropského parlamentu a Rady (EU) 2021/887 ze dne 20. května 2021, kterým se zřizuje **Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost** a **síť národních koordinačních center**

NKC v ČR

- zajištěním vzniku NKC v ČR byl na základě usnesení Vlády ČR pověřen **Národní úřad pro kybernetickou a informační bezpečnost** (NÚKIB)
- NÚKIB na plnění úkolů NKC spolupracuje s ústavem **CyberSecurity Hub** (CSH)

Úkoly NKC

- definovány v článku 7 nařízení EU 2021/887, například:
  - působit jako **kontaktní místo na vnitrostátní úrovni** pro Komunitu;
  - poskytovat odborné znalosti a přispívat k **plnění úkolů** ECCC;
  - **propagovat účast** subjektů v přeshraničních projektech financovaných EU;
  - **poskytovat podporu** při podávání žádostí o projekty řízené ECCC;
  - zprostředkovávat **finanční podporu třetím stranám**;
  - přispívat k podpoře a **šířit vzdělávací programy** v oblasti kyberbezpečnosti;
  - **posuzovat žádosti** subjektů o členství v Komunitě.

Služby NKC

- NKC poskytuje informační a metodickou podporu a předává informace ohledně:
  - aktualit v oblasti **podpory VaV v kybernetické bezpečnosti** a relevantních akcí na národní i evropské úrovni;
  - aktuálních **činností sítě NKC, ECCC a evropské Komunity**;
  - **aktuálních výzev** v relevantních finančních programech EU v oblasti kybernetické bezpečnosti (primárně Digitální Evropa a Horizont Evropa);
  - **příležitostí k zapojení** do národních i evropských projektů (podpora match-makingových aktivit, tvorby konsorcií atd.).

BLOK 2 – AKTUÁLNÍ VÝZVY DEP KYBERBEZPEČNOST

Nikola Chvátalová a Eliška Chytrá

NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

Struktura DEP a aktuální WPs

- **hlavní pracovní program DEP pro období 2025–2027**
  - investice ve výši cca 1,3 miliardy EUR
  - oblasti podpory – AI, evropská centra digitálních inovací (EDIHs), rozvoj digitálních dovedností
  - první výzvy byly vypsány v dubnu 2025
- **pracovní program DEP část Kyberbezpečnost pro období 2025-2027**
  - rozpočet 390 milionů EUR
  - první výzvy byly vypsány v červnu 2025; další jsou plánovány na podzim 2025

Aktuální pracovní programy DEP

hlavní WP

Kyberbezpečnost

Přehled KB výzev 2025-2027

Areas and topics with indicative allocations (in million EUR)		2025	2026	2027	Total
New technologies, AI & post-quantum transition					**142**
2.1	Cybersecure tools, technologies and services relying on AI	15	15	15	45
2.2	Strengthening cybersecurity capacities of European SMEs with cybersecure AI-powered solutions		20		20
2.3	Deployment of a European testing infrastructure for the transition to PQC in different usage domains	25			25
2.4	Transition to post-quantum Public Key Infrastructures	15			15
2.5	Migration of Cyber Hubs to PQC			7	7
2.6	Uptake of innovative cybersecurity solutions for SMEs	15		15	30
Cyber Solidarity Act Implementation					**121**
2.7	National Cyber Hubs	20	15		35
2.8	Cross-Border Cyber Hubs	20		20	40
2.9	Strengthening the Cyber Hubs ecosystem and enhancing information sharing		2		2
2.10	Coordinated preparedness testing and other preparedness actions	5	15	20	40
2.11	Mutual assistance		2	2	4
Additional actions improving EU cyber resilience					**118**
2.12	Enhancing the NCC Network	10	16	20	46
2.13	Strengthening EU cybersecurity capacities & capabilities in line with legislative requirements		20	12	32
2.14	Dedicated action to reinforce hospitals and healthcare providers	30			30
2.15	Dual-use technologies		10		10
Programme Support Actions		3	3	3	9
TOTAL (in million EUR)		**158**	**118**	**114**	**390**

Plánování KB výzev 2025-2027

- plánovány 2 cally každý rok
- indikativní; může být předmětem úprav

A tentative calendar is included here below for DEP 2025 calls. A similar timeline will be used for 2026 and 2027 calls.

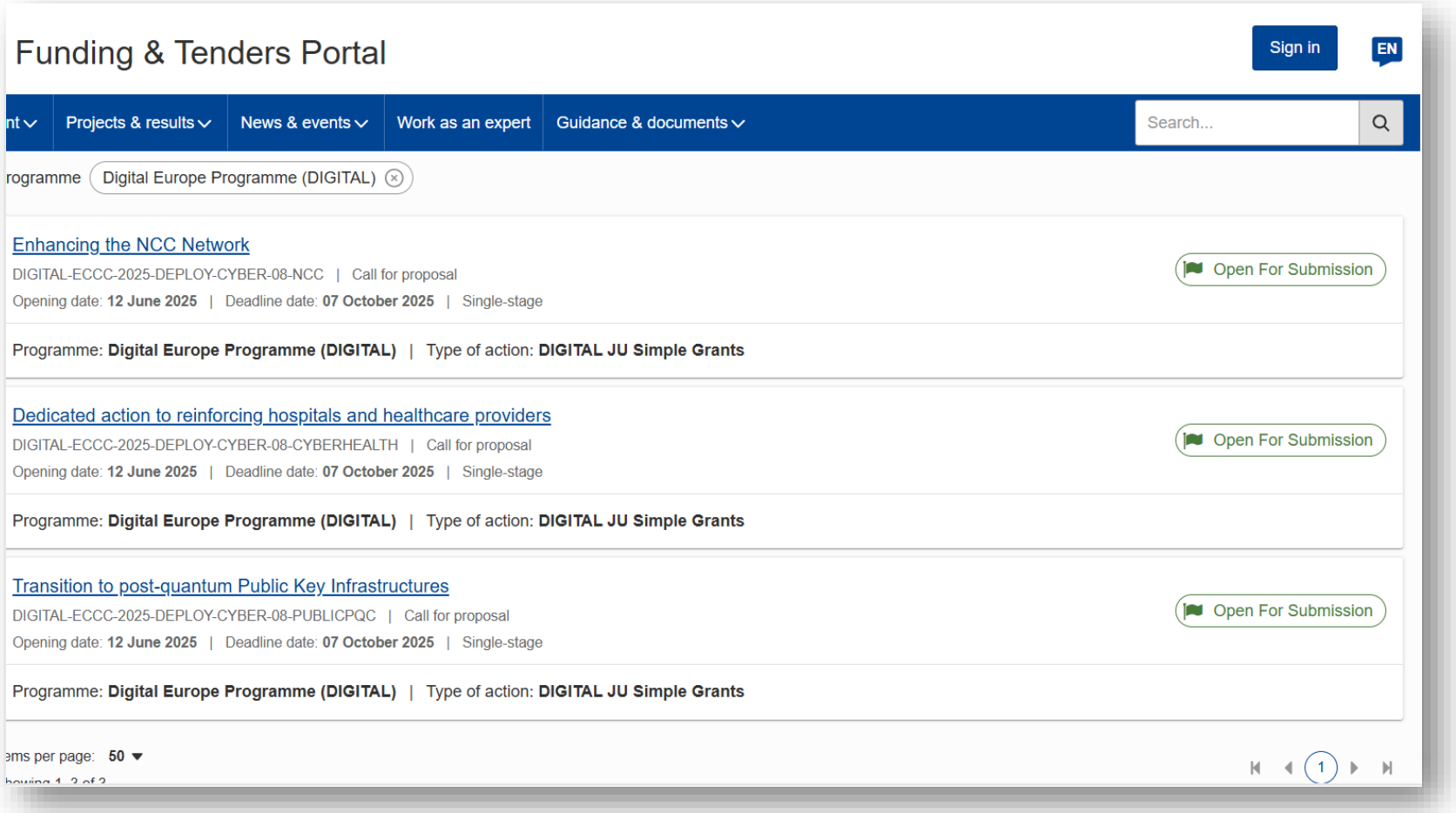
Main tasks	Tentative timeline
Opening	Q2/2025 and Q4/2025
Closing	Q4/2025 and Q1-Q2/2026
Evaluation	Q1/2026 and Q3/2026
Signature of the grants	Q3/2026 and Q1/2027

Přehled KB výzev v roce 2025

- v roce 2025 jsou plánovány **2 výzvy** (8 témat)
- **DIGITAL-ECCC-2025-DEPLOY-CYBER-08** (červen 2025)
  - *Dedicated action to reinforcing hospitals and healthcare providers*
  - *Transition to post-quantum Public Key Infrastructures*
  - *Enhancing the NCC Network*
- **DIGITAL-ECCC-2025-DEPLOY-CYBER-09** (podzim 2025)
  - *Cybersecure tools, technologies and services relying on AI*
  - *Uptake of innovative cybersecurity solutions for SMEs*
  - *National Cyber Hubs*
  - *Cross-Border Cyber Hubs*
  - *Coordinated preparedness testing and other preparedness actions*

DIGITAL-ECCC-2025-DEPLOY-CYBER-08

- 12. června byla otevřena první výzva **Strengthening the cybersecurity ecosystem**



DIGITAL-ECCC-2025-DEPLOY-CYBER-08

- témata výzvy:
  1. **Dedicated action to reinforcing hospitals and healthcare providers** (DIGITAL-ECCC-2025-DEPLOY-CYBER-08-CYBERHEALTH)
  2. **Transition to post-quantum Public Key Infrastructures** (DIGITAL-ECCC-2025-DEPLOY-CYBER-08-PUBLICPQC)
  3. **Enhancing the NCC Network** (DIGITAL-ECCC-2025-DEPLOY-CYBER-08-NCC)
- podmínky výzvy v tzv. call dokumentu


ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Digital Europe Programme (DIGITAL)

Call for proposals

Strengthening the Cybersecurity Ecosystem
(DIGITAL-ECCC-2025-DEPLOY-CYBER-08)

Version 1.0
12 June 2025

Harmonogram výzvy DEPLOY-CYBER-08

Timetable and deadlines (indicative)	
Call opening:	12/06/2025
Deadline for submission:	07 October 2025 – 17:00:00 CET (Brussels)
Evaluation:	November - December 2025
Information on evaluation results:	January - February 2026
GA signature:	June - July 2026

DEPLOY-CYBER-08-CYBERHEALTH

Objectives

This action aims to strengthen the cybersecurity of hospitals and healthcare providers. The goal is to ensure that hospitals and healthcare providers, which are crucial operators in the health sector, can effectively detect, monitor, and respond to cyber threats, particularly ransomware, which pose significant risks, thereby enhancing the resilience of the European healthcare system.
The action will contribute to the EU action plan on cybersecurity in hospitals and healthcare, adopted by the Commission[6] in January 2025.

Targeted stakeholders

This topic targets in particular stakeholders such as regional and/or national clusters associations of hospitals and healthcare providers (such as national healthcare systems, hospitals or associations of hospitals, healthcare providers and/or professional associations of healthcare practitioners), as well as cybersecurity service providers.

Type of action and funding rate

Simple Grants — 50% funding rate

DEPLOY-CYBER-08-CYBERHEALTH

Scope

This action addresses the growing need for continuous cybersecurity monitoring, threat intelligence, and incident response in hospitals and healthcare providers, which often lack dedicated cybersecurity resources to adequately protect themselves from cyber threats.

The action will support pilot projects, which will bring together stakeholders such as regional and/or national clusters associations[7] of hospitals and healthcare providers (such as national healthcare systems, hospitals or associations of hospitals, healthcare providers and/or professional associations of healthcare practitioners), as well as cybersecurity service providers.

The pilot projects will define the state of preparedness of clusters of hospitals and healthcare providers in the European Union, to be able to assess their needs. Based on this analysis, they will prepare an overview of the state-of-the-art cybersecurity solutions and resources needed (technologies, services, tools, human resources, training needs, etc.) for hospitals and healthcare providers to meet the scope of the action. These may include, for example: Security Operation Centres offering real-time monitoring, threat detection, and rapid incident response, and advanced cybersecurity tools, such as Security Information and Event Management (SIEM) platforms, threat intelligence, and automated response capabilities, among others.

The pilots will develop technical plans, tailored to the needs of representative hospitals and healthcare providers (e.g. small or large hospitals, private healthcare providers, etc.) which will also need to include best implementation recommendations and cost estimates for effective deployment.

The pilot projects will conduct a demo implementation of these technical plans to demonstrate their effectiveness in operations at the stakeholders' sites, showcasing different use cases for different user groups at small, medium and large hospitals and healthcare providers, at least in two different Member States.

The pilot projects will serve as demonstration projects and will also provide cybersecurity education and training to the staff of their partner hospitals and healthcare providers, enhancing awareness and ensuring best practices in safeguarding sensitive healthcare information.

Finally, in cooperation with each other, the pilot projects will undertake wide dissemination activities of best practices across the EU, with the specific goal of helping replicate and scale up the pilots' activities as widely as possible.

The pilot projects will support healthcare institutions complying with the NIS 2 Directive.

DEPLOY-CYBER-08-CYBERHEALTH

Expected Outcome

- Mapping of common cybersecurity needs of hospitals and healthcare providers.
- Guidelines for healthcare providers to assess their current state of cybersecurity protection and relevant needs.
- Technical cybersecurity plans to enhance preparedness and cyber resilience: improved detection and response capabilities for healthcare institutions minimising the impact of cyberattacks, particularly for ransomware. This also includes dedicated training courses to staff.
- Pilot cybersecurity demo installations at partner hospitals and healthcare provider sites to ensure hospitals and healthcare providers can maintain operational continuity in the face of cybersecurity incidents. This should be monitored through specific KPIs.
- Wide dissemination campaigns to help scale up preparedness of hospitals and healthcare providers in Europe.

DEPLOY-CYBER-08-PUBLICPQC

Objectives

The aim of this call is to tackle the challenges of an effective integration of PQC algorithms in Public Key Infrastructures (PKIs), which offers efficient migration strategies and strong business continuity guarantees.

The call targets the different actors involved in the PKI ecosystems and supply and value chains, who all have a unique set of diverse needs and interdependencies, such as Certificate Authorities (CAs), intermediate CAs, researchers, end-users in different domains, and vendors.

Targeted stakeholders

This topic targets in particular stakeholders involved in the Public Key Infrastructures (PKIs) chain, Certificate Authorities (CAs), intermediate CAs and other entities with a focus on cryptography and its standardization activities. The topic targets also other actors in PKI chain and entities that can provide use-case studies and real-world applications for deployment.

Submissions from consortia, despite not mandatory, is strongly advised.

Type of action and funding rate

Simple Grants — 50% funding rate

DEPLOY-CYBER-08-PUBLICPQC

Scope

Proposals shall target activities on the following subjects:

- design of digital signature combiners and key encapsulation mechanism combiners.
- the testing of deployment of certificates in protocols that use those certificates.
- the development of novel protocols for Automatic Certificate Management and revocation and of novel protocols for (privacy-friendly) certificate-transparency.
- the development of methods and tools that can be used by experts across various PKI domains, including all aspects of key management of asymmetric systems.

Activities should include some or all of the following:

- Identification of requirements necessary to implement hybrid certificates.
- Development of approaches and techniques for constructing cryptographic combiners for different protocols.
- Testing of the combiners for issuance of new certificates for the different applications, taking into consideration the need to balance the growth of key, signature, and ciphertext sizes, which can lead to compatibility issues with standards, such as PKI certificates, revocation mechanisms, (privacy-friendly) certificate transparency mechanisms, the use of different cryptographic protocols across certificate chains, the applications requirements, such as security level, time-constraints in signing and verification steps, communication/computational and storage overhead, and hardware optimisation requirements.
- Development of and/or further improvement of open-source libraries.
- Development of novel protocols for Automatic Certificate Management and revocation, and of novel protocols for (privacy-friendly) certificate-transparency. Support to standardisation activities.
- Development of recipes for the design and deployment of the new PKIs, with analysis that depends on each component of a given PKI.
- Tests on specialised uses of X.509 certificates other than the core cases using TLS, such as roots of trust, device integrity, firmware signing, and others.
- Design, improvement and testing of X.509 alternatives, such as, among others, Merkle tree ladders, the GNU Name System, older proposals such as SPKI and SDSI and the use of key encapsulation mechanisms for on-demand authentication in place of signatures.
- Awareness and training activities for stakeholders with different profiles, emphasising the interdependencies in the transition and facilitating a broader understanding of the technical standards amongst PKI users.

DEPLOY-CYBER-08-PUBLICPQC

Expected Outcome

- New combiners ensuring that cryptographic schemes provide at least 128-bit security against quantum adversaries.
- Experimental evaluation on hybrid certificates in several standard protocols that use those certificates, also considering options for different cryptographic algorithms at the root Certification Authority level and at the other levels, in terms of security, performance, and backward compatibility. The impact of such certificates in protocols should be tested via open-source libraries.
- New and/or improved open-source libraries for certificate requests, issuance, validation, revocation and (privacy-friendly) certificate transparency.
- Clear procedures taking into account all aspects of key management: requirements for signature generation, in terms of the software and hardware used to create signatures as well as the secure storage and handling of private keys to maintain their authenticity and confidentiality, signature validation, with specification of the data required for verifying signatures and outlining the conditions necessary for a successful signature verification process, signature life-cycle process, and validity status of signatures.
- Test and evaluation of uses of X.509 certificates other than their core uses.
- Tests and evaluation of alternatives to X.509 certificates.
- Awareness activities and training courses.

DEPLOY-CYBER-08-NCC

Objectives

The National Coordination Centres (NCCs) set up by the Regulation (EU) 2021/887 are designed to work together through a network and to contribute to achieving the objectives of the regulation and to foster the Cybersecurity Competence Community in each Member State, by contributing to the acquisition of the necessary capacity. National Coordination Centres can also support priority areas such as the implementation of EU legislation (Directive (EU) 2022/2555, the proposed Cyber Resilience Act and the Cybersecurity Act).

Targeted stakeholders

This call targets National Coordination Centres which have been recognized by the Commission as having the capacity to manage funds to achieve the mission and objectives laid down in the Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres and other private and other private and public entities in consortium with NCCs, including academia and research entities.

Type of action and funding rate

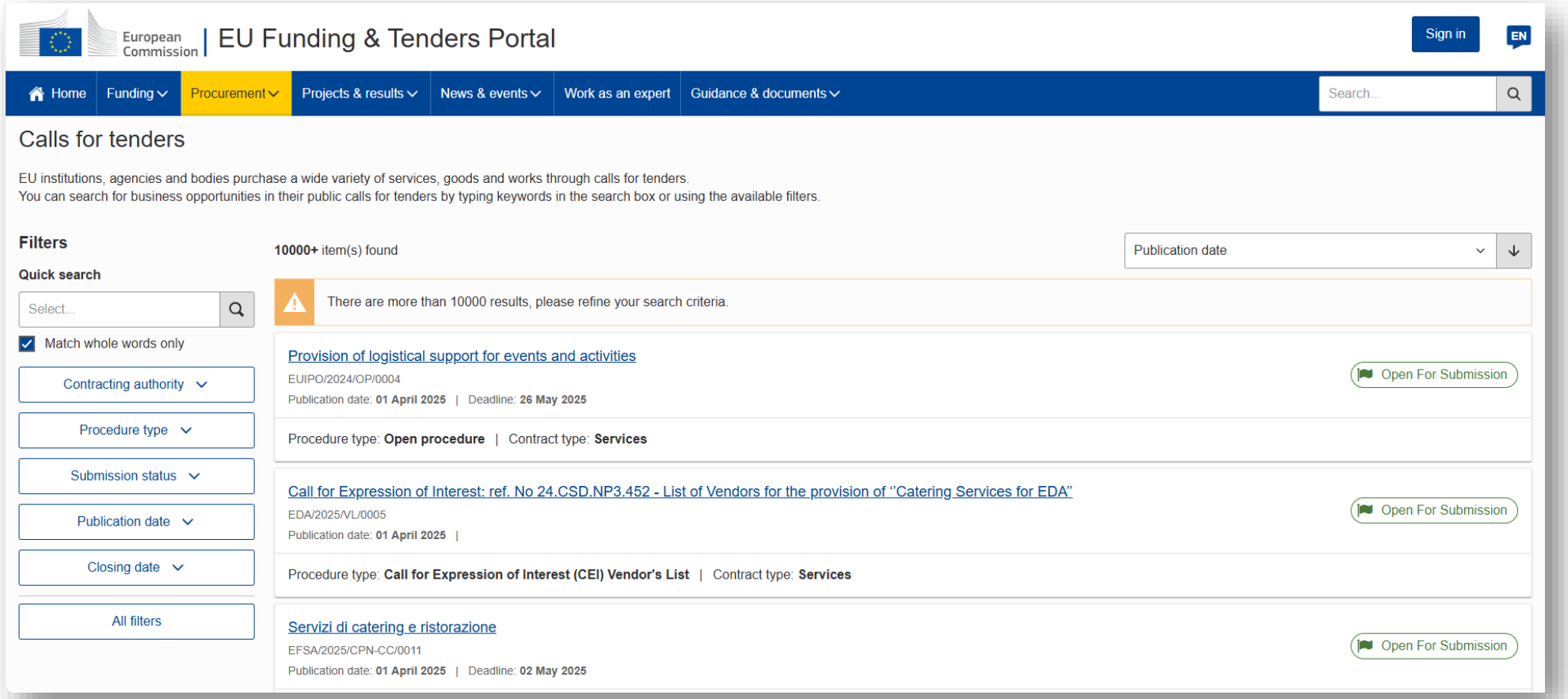
Simple Grants — 50% funding rate

DIGITAL-ECCC-2025-DEPLOY-CYBER-09

- **otevření výzvy:** indikativně září/říjen 2025
- **uzavření výzvy:** indikativně leden 2026
- **témata výzvy:**
  - *Cybersecure tools, technologies and services relying on AI*
  - *Uptake of innovative cybersecurity solutions for SMEs*
  - *National Cyber Hubs*
  - *Cross-Border Cyber Hubs*
  - *Coordinated preparedness testing and other preparedness actions*
- čeká se na zveřejnění call dokumentu a výzev na F&T Portálu

Kde hledat výzvy?

- F&T Portál a web NKC



Aktuální partner search příležitosti

- **DIGITAL-ECCC-2025-DEPLOY-CYBER-08-CyberHEALTH Dedicated action to reinforce hospitals and healthcare providers** – Polská společnost DISKUS Polska Sp. z o.o. hledá partnery do konsorcia. Firma je výrobcem inteligentních a technologicky pokročilých řešení ProDevice je spolehlivým partnerem pro veřejné instituce, korporace a firmy v IT, finančním, zdravotnickém a vládním sektoru. DISKUS Polska/ProDevice může do konsorcia přinést jedinečnou expertízu v oblasti bezpečné likvidace dat a zabezpečení informací na konci životního cyklu. Zájemci o spolupráci se mohou obracet na kontakt: tomasz.filipow@diskus.pl.
- **DIGITAL-ECCC-2025-DEPLOY-CYBER-08-CYBERHEALTH Dedicated action to reinforcing hospitals and healthcare providers** - Maďarský institut HUN-REN SZTAKI v roli koordinátora hledá partnery do konsorcia. Projekt se soustředí na vytvoření bezpečnostního operačního centra (SOC) pro zdravotnické instituce, které bude podporovat sdílení informací, detekci incidentů a správu zranitelností s využitím open-source nástrojů a důrazem na nízké náklady. HUN-REN SZTAKI má zájem zejména o nemocnice a další poskytovatele zdravotní péče, kteří by se zapojili do pilotního testování řešení, a dále o národní či regionální koordinátory ve zdravotnictví, kteří mohou přispět náborem dalších subjektů a zkušenostmi s fungováním systémů. Zájemci se mohou obracet na Ernő Rigóa na e-mailové adrese erno.rigo@sztaki.hun-ren.hu.
- **DIGITAL-ECCC-2025-DEPLOY-CYBER-08-CYBERHEALTH Dedicated action to reinforcing hospitals and healthcare providers** - Portugalská společnost Paldata, S.A. (PIC: 89342694) hledá partnery do konsorcia. Jako středně velká IT firma s dlouholetými zkušenostmi ve zdravotnictví (prostřednictvím své dceřiné společnosti Quattro) plánuje navázat na úspěšný projekt HISC4ALL a zapojit se do mezinárodního konsorcia (v roli project leader, WP leader, nebo participant) s cílem posílit kybernetickou odolnost nemocnic a poskytovatelů zdravotní péče. Projekt se zaměřuje na budování rámce pro kontinuální kybernetický monitoring, threat intelligence a reakci na incidenty v prostředí zdravotnických zařízení. Výsledkem má být metodika pro hodnocení a návrh technických plánů v souladu s požadavky směrnice NIS2. Zájemci o spolupráci se mohou obracet na paulo.domingos@paldata.pt.

BLOK 3 A 4 – PREZENTACE TECHNOLOGICKÉHO CENTRA PRAHA A CZECHINVEST

Lenka Švejcarová, David Mićević

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

BLOK 5 – ZÁVĚR

NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

Kde získám další informace?

Národní úřad pro kybernetickou a informační bezpečnost

Co sledovat:

- web NKC – https://nkc.nukib.gov.cz/
- web ECCC – http://cybersecurity-centre.europa.eu/
- web a sociální sítě Úřadu – https://nukib.gov.cz/
- web CSH – https://www.cybersecurityhub.cz/
- odběr novinek NKC – ncc@nukib.gov.cz
- odběr newsletteru Aktuality ve výzkumu – vyzkum@nukib.gov.cz, https://cyris.cz/

BLOK 6 – DISKUZE A DOTAZY

NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

Diskuze a dotazy

- **dotazy** je možné psát do chatu
- doplňující informace jsou na webu:
  - NKC
  - TC Praha a Horizont Evropa
  - CzechInvest
- kontaktujte nás na ncc@nukib.gov.cz

NCC-CZ
CZECHIA CYBERSECURITY COORDINATION CENTRE

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Spolufinancováno Evropskou unií

DĚKUJEME ZA ÚČAST

NÚKIB
Národní úřad pro kybernetickou a informační bezpečnost