# IV. odborné setkání – implementace nařízení EU o certifikaci kybernetické bezpečnosti IKT

6.4.2022

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

# IV. odborné setkání k CSA



## Organizační pokyny

- Prosím, vypněte si kamery a mikrofony, pokud nemluvíte k účastníkům.

- Na závěr setkání budou otázky a odpovědi.
  Po každé části bude prostor na krátké otázky a odpovědi k jednotlivým tématům.
  Pro interaktivní komunikaci bude využito webové aplikace SLICO.COM pod #4CSA.
  Pokud nebudou otázky zodpovězeny na tomto setkání, budou odpovědi zaslány emailem na všechny zúčastněné.

- Pokud bude v průběhu prezentace uváděn odkaz na nějakou dokumentovanou informaci dostupnou na webových stránkách, je link připraven v seznamu odkazů ve SLIDO pod #4CSA.

- S ohledem na plánovanou délku trvání tohoto setkání neplánujeme přestávku.

slido

# Join at slido.com
# #4CSA

ⓘ Start presenting to display the joining instructions on this slide.

# IV. odborné setkání k CSA



**Program:**

- Úvodní slovo
- Blok 1:
  - Přehled schémat EUCC a EUCS (ENISA)
  - Metodika hodnocení pro schéma EUCS (ENISA)
  - Příležitosti pro ITSEF a CB u schématu EUCC (ENISA)
  - Q&A (ENISA)
- Blok 2:
  - Zřízení rámce pro evropskou digitální identitu aneb eIDAS2 (MVČR)
  - Regulace využívání cloud computingu veřejnou správou (NÚKIB)
  - European Cyber Resilience Act (NÚKIB)
  - Vzdělávací a osvětové aktivity (NÚKIB)
- Q&A
- Závěr

# IV. odborné setkání k CSA



## Úvodní slovo

**Ing. Jaroslav Šmíd**
**Náměstek ředitele, Sekce informační bezpečnosti**

THE EU CYBERSECURITY AGENCY

# ACCREDITION OF CABs FOR THE EUCC CYBERSECURITY CERTIFICATION SCHEME

## Presentation to CZ stakeholders

Philippe Blot
MCS Unit, HoS certification & EUCC AHWG Chair

06 | 04 | 2022

# Background

ENISA has developed with the support of the EUCC AHWG the candidate EUCC scheme for the certification of ICT products according to the Common Criteria - CC - (ISO/IEC 15408).

The scheme provides a mapping between the assurance levels of the CSA and the assurance component AVA_VAN. of the CC: AVA_VAN.1 and 2 map to CSA level substantial, AVA_VAN.3 to 5 map to CSA level high.

The notification of CABs is intended to be based, for this scheme:

- For the level substantial of the CSA, on the accreditation of CBs according to ISO/IEC 17065 and of related ITSEFs according to ISO/IEC 17025
- For the level high of the CSA, on the accreditation of CBs according to ISO/IEC 17065 and of related ITSEFs according to ISO/IEC 17025, plus their authorisation by a NCCA.

# Background

Differences between accreditation and authorization:

In a nutshell and based on SOG-IS practices related to the authorization of CBs and the licensing of ITSEFs, it is foreseen that EUCC authorization will complement accreditation with a review by the NCCA of the CB assessment that their related ITSEFs are capable to:

- Perform penetration testing for assurance components AVA_VAN.3 and above, (according to methodology not in the public domain nor published standards),
- Protect the security of information (according to stricter requirements than the ones applying for their accreditation, currently under definition).

Note: in addition to existing requirements defined in the Annexes of the candidate scheme, we have developed guidance to assess the capabilities of ITSEFs performing AVA_VAN.3 evaluations.

# Background

In parallel, in order to ease the harmonization of MSs practices, at all possible levels, ENISA with the support of the EUCC AHWG develops guidance, including interpretations of accreditation requirements.
The first step was to address the requirements for the accreditation of the testing laboratories (ITSEFs) according to ISO/IEC 17025, for the substantial level (up to and including AVA_VAN.2).

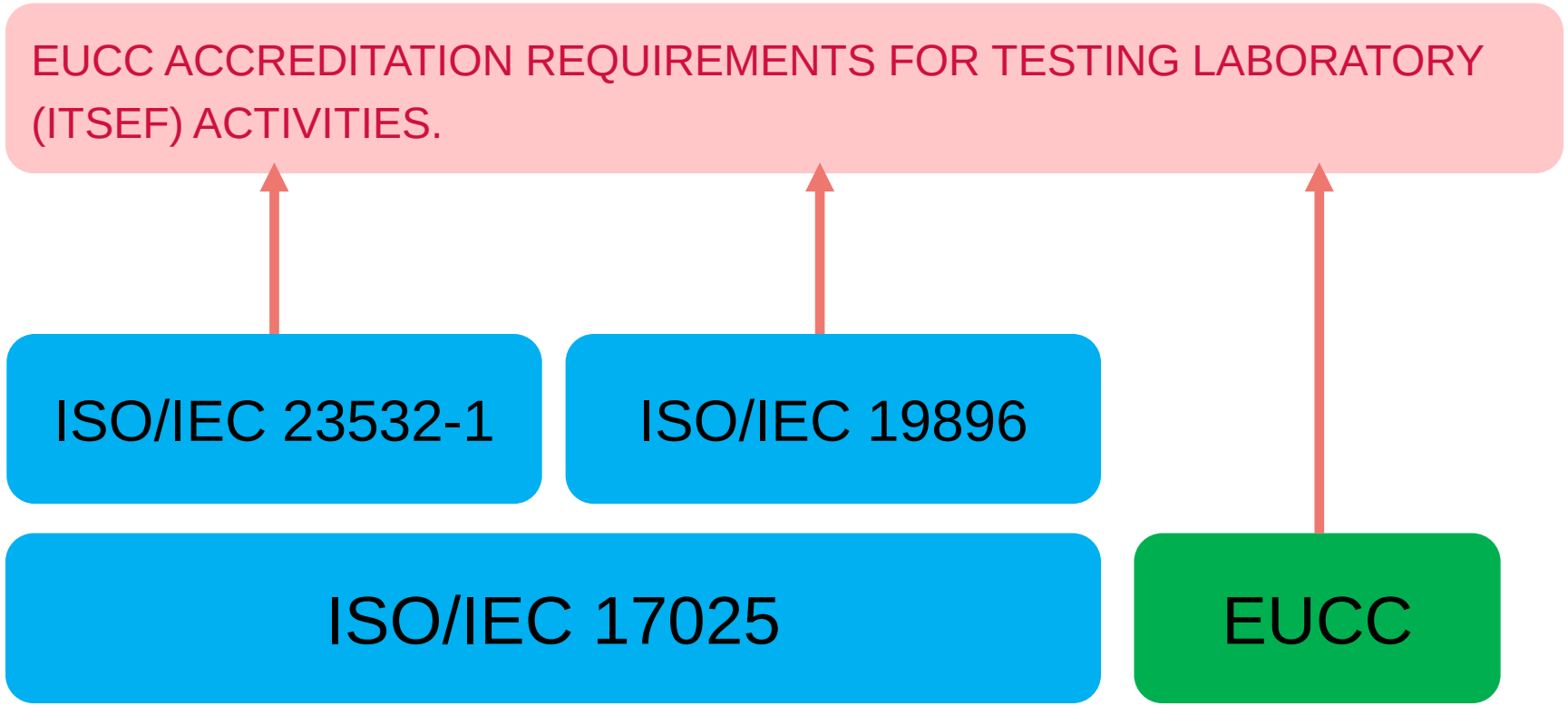
Then we're addressing the requirements for the accreditation of the:

- CBs according to ISO/IEC 17065, for the substantial level (up to and including AVA_VAN.2),
- ITSEFs according to ISO/IEC 17025, for the level high (from AVA_VAN.3),
- CBs according to ISO/IEC 17065, for the level high (from AVA_VAN.3).

# Background

Ultimately, we will provide consolidated documents (for example where a CAB has both CB and ITSEF activities), but for the moment, we separate the activities as current practices under the SOG-IS have such a separation in place.

# Outcome of current work: EUCC interpretations of accreditation requirements for ITSEFs activities



# EUCC interpretations of accreditation requirements for ITSEFs activities


TECHNICAL SPECIFICATION

ISO/IEC TS 23532-1

First edition
2021-11

Information security, cybersecurity and privacy protection — Requirements for the competence of IT security testing and evaluation laboratories —

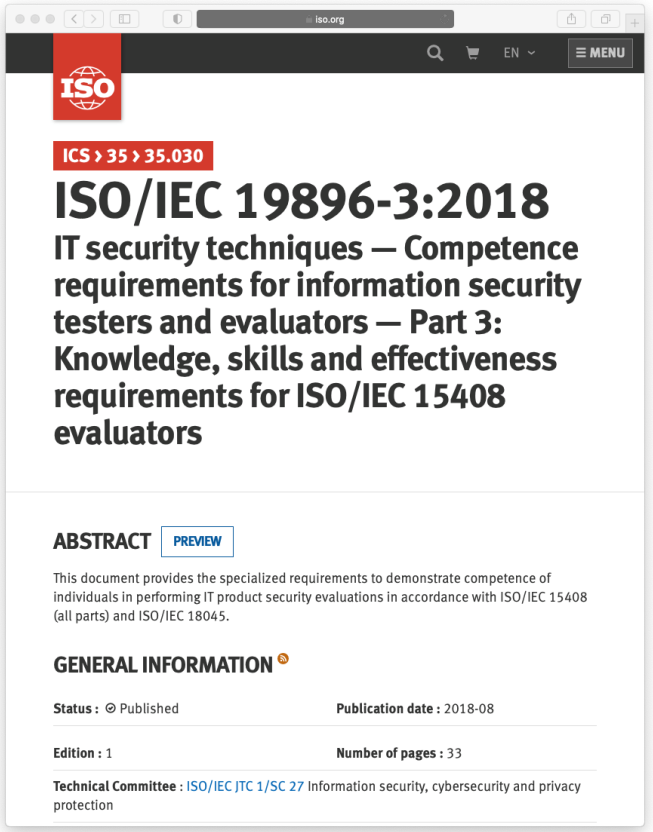
Part 1:
Evaluation for ISO/IEC 15408

*Sécurité de l'information, cybersécurité et protection de la vie privée — Exigences relatives aux compétences des laboratoires d'essais et d'évaluation de la sécurité TI —*

*Partie 1: Évaluation pour l'ISO/IEC 15408*

Reference number
ISO/IEC TS 23532-1:2021(E)

© ISO/IEC 2021


iso.org

EN

MENU

ICS › 35 › 35.030

ISO/IEC 19896-3:2018

IT security techniques — Competence requirements for information security testers and evaluators — Part 3: Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators

ABSTRACT PREVIEW

This document provides the specialized requirements to demonstrate competence of individuals in performing IT product security evaluations in accordance with ISO/IEC 15408 (all parts) and ISO/IEC 18045.

GENERAL INFORMATION

Status : Published

Publication date : 2018-08

Edition : 1

Number of pages : 33

Technical Committee : ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection

# EUCC interpretations of accreditation requirements for ITSEFs activities

Interpretations relate to:

- Confidentiality
- Competence
- Subcontracting
- Non-compliance
- Retention of records
- Quality process
- Composite evaluations
- Monitoring compliance
- Patch management

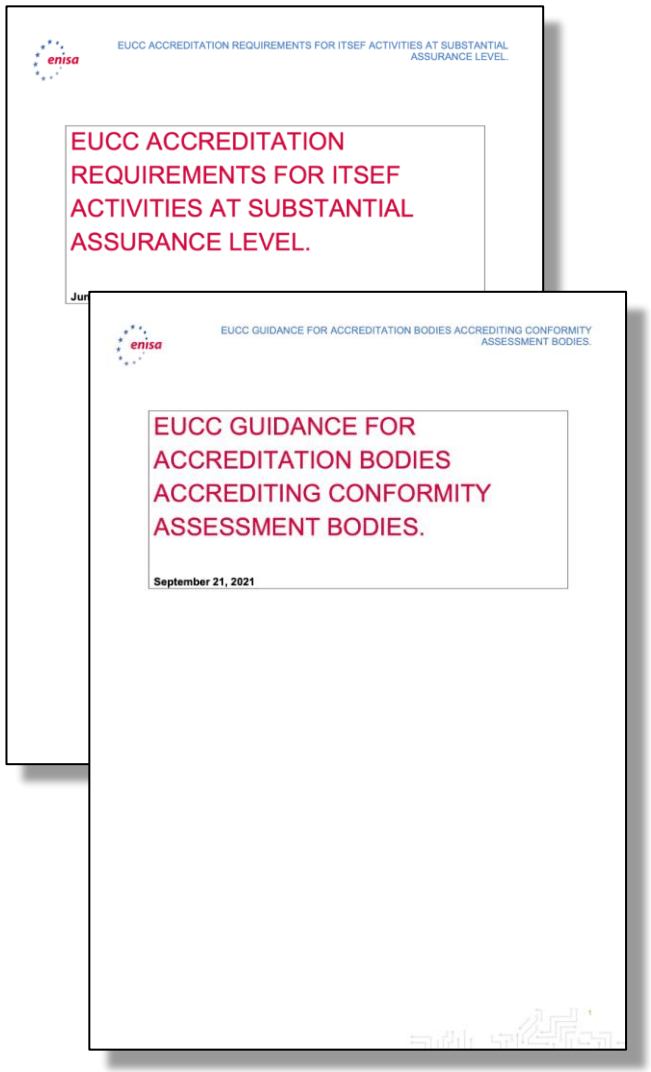
They also provide recommendations to the NABs.

# EUCC interpretations of accreditation requirements for ITSEFs activities

This guidance document has been submitted to the ECCG and EA for review, ENISA is considering, as a good way forward, to submit these elements as a new work item to CEN/CLC TC 13. But we are of course open to other options!

In addition, we have engaged in 2021 into pilots to experiment some on the new features introduced by the EUCC with regards to the SOG-IS, including the accreditation of ITSEFs, we're getting feedback right now.

# Latest version of the document




Based on the contributions from EA, the text has been updated, and split into two documents:

- The EUCC requirements for ITSEF accreditation;
- Guidance for NABs complementing ISO/IEC 17011.

# THANK YOU FOR YOUR ATTENTION

**European Union Agency for Cybersecurity**

+30 28 14 40 9711

info@enisa.europa.eu

www.enisa.europa.eu

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

# METODIKA HODNOCENÍ PRO SCHÉMA EUCS

# *ASSESSMENT METHODS IN EUCS*

Eric Vetillard, Ph.D.
Lead Certification Expert, ENISA

06 | 04 | 2022

# AGENDA

# WHERE ARE WE ON EUCS?

**ENISA is finalizing the candidate scheme before to submit it to the Commission.**

We have a pre-final draft candidate scheme

- It will be sent to the ECCG for their formal opinion this month
- ENISA will then “take utmost account of the opinion of the ECCG” to finalize the candidate scheme

Then, the Commission will take over

- Drafting an Implementing Act for the scheme
- Organizing a public review of the Implementing Act
- Then going for formal approval from Member States through a comitology process
- Finally, publishing and adopting the scheme

# CHAPTER 1

# THE SCHEME TODAY

# A GENERIC SCHEME

## All capabilities

Based on ISO/IEC 22123-1

All cloud capabilities are supported: Infrastructure, Platform, Application

Preferred for clarity to references to IaaS, PaaS, SaaS, XXaaS

No mention of deployment model

## Horizontal

Defines a baseline of requirements that are applicable to all services.

Enables the same methodology for all services

Does not assess the security of product-specific security features (Security as a Service)

## 3 assurance levels

As defined in the European Cybersecurity Act

‘basic’ → CS-Basic

‘substantial’ → CS-Substantial

‘high’ → CS-High

All levels based on an assessment by an accredited third-party

# TECHNICAL CHALLENGES

## Which requirements?

There is no clear standard, so we need to define a list of controls, drawing from existing schemes, and adding the notion of assurance levels

## Which assessment?

Several assessment methods, mostly based on ISO270xx and on ISAE standards, and an ability to combine with both assessments

## Which assurance levels?

Assurance levels must bring added value and be simple enough to understand in order to bring a clear message

## How to make results matter for customers?

Started with allowing customers to make informed choices (transparency, documentation), and shifted to sovereignty discussions.

# 3 ASSURANCE LEVELS

## CS-Basic level

Minimise the **known basic** risks of incidents and cyberattacks

- Limited assurance
- Review of CSP evidence
- Focus on the definition of procedures and mechanisms
- Few constraints

## CS-Substantial level

Minimise **known** cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with **limited skills and resources**

- Reasonable assurance
- Design effectiveness
- Operating effectiveness

## CS-High level

Minimise the risk of **state-of- the-art** cyberattacks carried out by actors with **significant skills and resources**

- Same as substantial, plus
- Stronger requirements, including automated monitoring
- Penetration testing

# ONE SET OF REQUIREMENTS

## A variety of sources, from standards to national schemes

We used the German C5 criteria to provide a sound basis

- This has been the basis for the CS-Substantial level (with inputs from ISO270xx, SecNumCloud)
- The CS-Basic level is defined by removing constraints from the requirements
- The CS-High level is defined by adding constraints and additional requirements (with inputs from SecNumCloud)

But this remains a very open scheme

- Many transparency requirements (also for location of data storage and processing, up to CS-Substantial)
- The scheme is very careful not to mandate specific technologies, focuses mostly on results to achieve
- The scheme remains focused on cybersecurity, not contractual issues or data protection

# TWO ASSESSMENT METHODS

## Limited assurance

For the Basic level only, as initially proposed by CSP-CERT:

- Mostly a review of evidence provided by the CSP
- In fact, a self-assessment reviewed by a 3rd party
- Fully integrated in the main scheme, certificate lifecycle, maintenance, *etc*.
- Mostly for vendors with no certification

## Reasonable assurance

For the Substantial and High levels:

- "Normal" audit of a cloud service
- Focus on the ISMS and processes, but some interest in the "product" underlying the service
- Following a specific methodology, fully defined in the scheme
  - Compatible with both ISO17021 and ISAE3402
- Vendors can keep their certification strategy

# CHAPTER 2

# ASSESSMENT PRINCIPLES

# THE METHODOLOGY IS DEFINED IN THE EUCS

**The EUCS is using a hybrid methodology, which draws both from ISO7065 and from ISAE assessments.**

The structure of the CAB work follows the ISO 17065 organisation

- Application, audit planning, audit, review, certification
- Also reusing basic rules on independence, competences, …

The audit is strongly influenced by ISAE principles

- Definition of audit as limited assurance or reasonable assurance
- Verification of operating effectiveness of the controls (for CS-Substantial and CS-High)

The dependency analysis is the main EUCS add-on

- To provide a full-stack coverage independently of the actual implementation
- Requiring an analysis of the assurance documentation available on carved-out subservice providers

# THE DEPENDENCY ANALYSIS

**In the EUCS, assurance documentation must be provided for the full stack, whether or not it is implemented by the CSP or by a subservice provider.**

Composition is the preferred way to achieve this

- Using a subservice provider that has itself been certified with the EUCS
- This is encouraged by mandatory documentation that ease composition

But composition is not always possible

- Not all subservice providers are cloud providers
- At least during transition, some subservice providers have not been certified yet

Dependency analysis is the solution for such cases

- Possibility to rely on other kinds of assurance documentation (ISO 27001 certificates, SOC2 reports, …)
- BUT this documentation needs to meet some criteria

# SOME OF THE CRITERIA

## Auditor / Evaluator

The auditor must be trusted

- Accredited CAB
- Public auditor

Following rules of conduct from a known institution

- NABs, ISAE, …

## Quality of Information

From a known framework

- ISO27001 schemes
- SOC2 or similar schemes

With proper information

- SOC2, but most likely not SOC3
- Evaluation report elements required for ISO 27001

## Requirement coverage

Coverage derived from CSP's declarations

- CSOCs defined by the CSP
- Some EUCS requirements

Mappings may be used

- To map a report based on different requirement structure

# CHAPTER 3

# ASSESSMENT AT LEVEL CS-BASIC

# PRINCIPLES OF THE ASSESSMENT

**At evaluation level CS-Basic, the objective is to validate that the CSP is on the right path to full good cybersecurity practices.**

Requirements cover a wide range of topics, with only limited depth

- All areas of cybersecurity need to be covered
- The requirements in most cases do not include any constraints on the kind of coverage

The assessment is intended to be efficient

- Focus on documentation of process and existence of an implementation
- No need to demonstrate a regular/systematic application of the controls
- Assessment based on the result of an internal audit
- Assessment driven by a questionnaire

I4

# Questions on requirements

Questions related to some requirements, organized by chapters and categories

*OPS-10 to OPS-16 : Logging and Monitoring*

| Requirement | QID | Question | Expected evidence | Answer | Evidence doc. | Evidence pointer | CSP Comment | Validation | CAB Comment |
|---|---|---|---|---|---|---|---|---|---|
| OPS-10.1B | 01 | Does the CSP document policies and procedures that govern the logging and monitoring of events on system components under its responsibility? | - Documented policies and procedures | Yes | OPS Policy | page 24 | | OK | |
| OPS-10.1B | 02 | Does the CSP implement policies and procedures that govern the logging of events on system components under its responsibility? | - Logging configuration<br>- Logs | Yes | Event log example | | | OK | |
| OPS-10.1B | 03 | Does the CSP implement policies and procedures that govern the monitoring of events on system components under its responsibility? | - Monitoring configuration<br>- Logs with monitoring action | Yes | Monitoring rule example | | | OK | |
| OPS-11.1B | 01 | Does the CSP document policies and procedures that govern the secure handling of derived data? | - Documented policies and procedures | Yes | Data Policy | page 18 | | OK | |
| OPS-11.1B | 02 | Does the CSP implement policies and procedures that govern the secure handling of derived data? | - Records derived from the implementation of the policies and procedures<br>- Configuration items<br>- Application to logs | Yes | Log configuration | | The configuration follows the policies for the handling of derived data. | OK | |
| OPS-12.1B | 01 | Does the CSP monitor log data in order to identify events that might lead to security incidents, in accordance with the logging and monitoring requirements? | - Documented policies and procedures<br>- Monitoring configuration | Yes | Monitoring rule example | | This show that the rules are defined | OK | |
| OPS-12.1B | 01 | Does the CSP monitor log data in order to identify events that might lead to security incidents, in accordance with the logging and monitoring requirements? | - Documented policies and procedures<br>- Monitoring configuration | Yes | Event report example | | This is an example of applying one of the rules | OK | |
| OPS-12.1B | 02 | Are identified events reported to the appropriate departments for timely assessment and remediation? | - Pointer to procedure<br>- Security event notification report | Yes | Event report example | | | Inconclusive | Not fully clear to whom the report was done |
| OPS-13.1B | 01 | Does the CSP store all log data in an integrity-protected and aggregated form that allow its centralized evaluation? | - Pointer to procedure<br>- Extract of centralized log data | Yes | Log configuration | Storage | In the section that starts with the "Storage" comment. | OK | |
| OPS-13.1B | 02 | Is the communication between the assets to be logged and the logging servers authenticated and protected in integrity and confidentiality? | - Pointer to procedures with analysis of the selected protocol<br>- Configuration item | Yes | Log configuration | Communication | In the section that starts with the "Communication" comment. | OK | |
| | | Are log data deleted when it is no longer required for | Reference to procedure | | | | In the section that starts with | | |

# CHAPTER 4

# ASSESSMENT AT LEVELS CS-SUBSTANTIAL AND CS-HIGH

# THE REQUIREMENTS AND METHODOLOGY ARE RATHER DEMANDING

**This is a result of combining the CSP's very large threat surface with the definition of assurance levels from the CSA, based on attackers.**

Assurance level CS-Substantial intends to "minimise the known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources".

- Recent attacks show that this covers a wide range of groups, including the teenagers from Lapsus$
- Able to apply any well-known attack on a not/poorly protected target, so mostly opportunistic

Assurance level CS-High intends to "minimise the risk of state-of- the-art cyberattacks carried out by actors with significant skills and resources".

- For instance resources provided by a nation-state to perform systematic attacks on specific targets
- Able to identify/purchase a 0-day vulnerability or combine known vulnerabilities into an attack path

**This is actually quite demanding, so how can we meet that?**

# A FIXED SET OF REQUIREMENTS

**The requirements on controls are defined for every evaluation level, with increasing details and constraints.**

For CS-Substantial, requirements are comparable to typical frameworks

- Mostly inspired from C5 (Germany), itself drawing from ISO 270xx and more
- All requirements are considered applicable, but may be conditional
  - No Security Target, the requirements are a baseline

For CS-High, requirements are more demanding than for usual frameworks

- Some requirements inspired from SecNumCloud, especially for more specific/detailed requirements
- Many requirements about automated monitoring, an important theme for CS-High
- Also, much stronger requirements on penetration testing

# AN AUDIT IN THREE PARTS

**The requirements apply on controls, which in practice may not necessarily follow the same organization.**

Step 1: Demonstrate that all requirements are covered by a control

- Typically pointing to policies, procedures, configurations, …

Step 2: Demonstrate the existence of an implementation of the control

- Typically pointing to configuration files, logs, and other traces

Step 3: Demonstrate the operating effectiveness of the control

- Typically pointing to logs, workflow history, …
- Demonstrating that the control has been applied as expected over a period of time
- Demonstration based on sampling, depending on the volume

# CHAPTER 5

# AFTER THE INITIAL ASSESSMENT

# CONTINUED COMPLIANCE

**With the Cybersecurity Act, certification is not a “one-shot” activity, since there is a requirement for continued compliance.**

NCCAs are in charge of market surveillance of certified products or services

- Making sure that certified products and service live up to their promise
- Supervising CABs, also performing surveillance assessments on a sample of products

CSPs need to declare identified nonconformities and vulnerabilities to CABs

- In the EUCS, only major nonconformities and critical vulnerabilities
- Other nonconformities and vulnerabilities are reviewed during maintenance assessments

In the EUCS, maintenance assessments are required at least every year

- A limited assessment every year, but with more tasks than in IS027001

# NONCONFORMITIES AND VULNERABILITIES

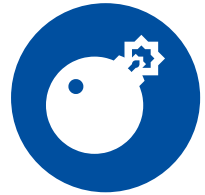
## Nonconformities

The CSP has a process to handle them

- Assessing the significance (minor or major)
- Fixing the nonconformities
- Informing the CAB for major nonconformities

Could lead to some issues

- A suspension could happen, or a withdrawal
- Also, non-compliance could be even worse, if the rules from the scheme are not followed



## Vulnerabilities

The CSP has a process in place

- Assessing the significance
- Informing the CAB of the most significant vulnerabilities, and of the mitigation

Could also lead to some issues

- If the process is not followed
- If the vulnerability leads to/originates from a nonconformity or a non-compliance

# SIGNIFICANT RECURRENT TASKS

**Compared to ISO27001, there are more recurrent tasks every year. But there are still less than for an ISAE assessment.**

Every year, the CSP must demonstrate

- Coverage and existence for modified controls and for a limited subset of controls
- Operating effectiveness for all controls (not applicable for CS-Basic)

Every 3 years, the renewal assessment is the same as the initial assessment

- Simplification will come from the knowledge acquired by the CAB of the CSP's controls

Special assessments may be necessary when events occur

- Significant changes in the cloud service, or identification of vulnerabilities or nonconformities

# CHAPTER 6

# MOVING FORWARD

# ONGOING AND FUTURE WORK

## Ongoing work

Finalization of the scheme

- To be sent to the ECCG for opinion this month

Standardization in CEN-CENELEC JTC13

- A TS in WG2 on the requirements on controls
- A TS in WG3 on the accreditation requirements

Some guidance already initiated

- General guidance on the requirements
- Also, the questionnaire for level CS-Basic

## Future work

More guidance will be required

- Guidance for CABs on the assessment
- Guidance for cloud customers on using the EUCS

A maintenance structure will be set up

- Continuing the work on guidance
- Preparing the future revisions of the scheme

NCCAs and the ECCG will start working on peer assessments and peer reviews

# THANK YOU FOR YOUR ATTENTION

**European Union Agency for Cybersecurity**
Ethnikis Antistaseos 72 & Agamemnonos 14, Chalandri 15231
Attiki, Greece

+30 28 14 40 9711

certification@enisa.europa.eu

www.enisa.europa.eu

slido

# Join at slido.com
# #4CSA

ⓘ Start presenting to display the joining instructions on this slide.

slido

# Audience Q&A Session

ⓘ Start presenting to display the audience questions on this slide.

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

# Zřízení rámce pro evropskou digitální identitu aneb eIDAS2

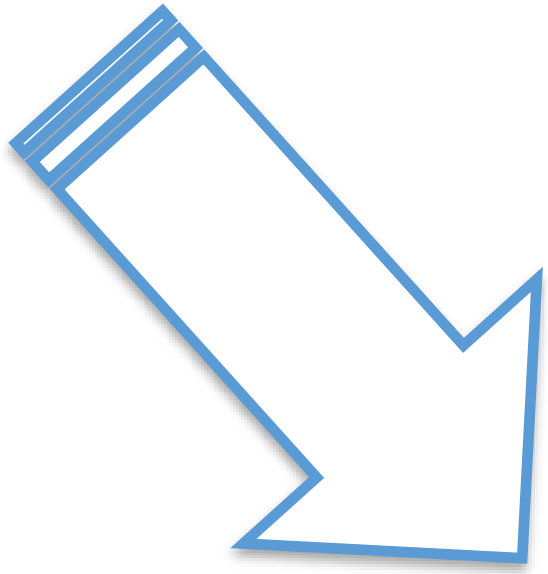
Filip Bílek

# Důvod pro revizi nařízení eIDAS


- **Elektronická identifikace:** Pouze 14 států notifikovalo alespoň jeden systém el. identifikace (jen 59% obyvatel EU má možnost přístupu k důvěryhodným a bezpečným systémům el. identifikace, které lze využít přeshraničně).
- **Služby vytvářející důvěru:** technologická neutralita, různý výklad požadavků.

# Návrh revize nařízení eIDAS

Zveřejněn 3. června 2021.
Obsahuje návrh Evropské digitální identity.
Změny rovněž v oblasti služeb vytvářejících důvěru.
Návrh revize eIDAS musí projít řádným legislativním procesem.



# Evropská digitální identita

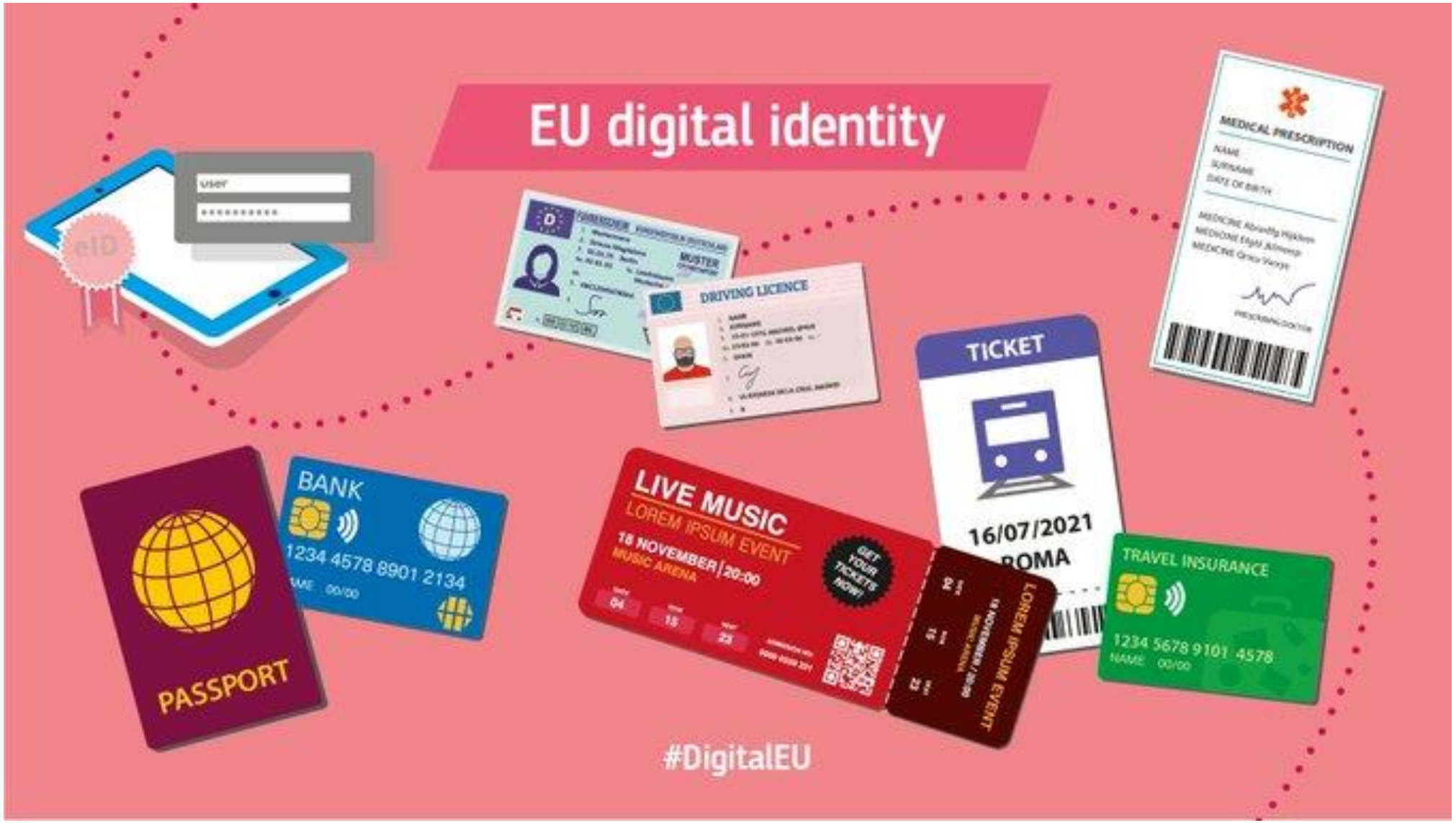

Zdroj:#DigitalEU

Evropská peněženka digitální identity.
Povinnost pro členské státy poskytovat peněženku.
Občan může/nemusí využívat peněženku.
Uživatel rozhoduje, které údaje o sobě poskytne.
Možnost uložit další atributy o své osobě (např. kvalifikace, vzdělání).
Vysoká úroveň záruky.
Umožnění podepsání kvalifikovaným elektronickým podpisem.
Harmonizovaný přístup.

# Evropská digitální identita


Zdroj:#DigitalEU

- Použití jak vůči veřejným online službám, tak vůči soukromoprávním online službám vyžadujícím silné ověření uživatele na základě právního předpisu nebo smluvního závazku.




Zdroj: #DigitalEU

# Certifikace evropské peněženky digitální identity

Nutnost zajistit důvěru, jak ze strany uživatelů, tak ze strany spoléhajících se stran.
Stanovena povinnost, aby peněženky byly certifikované.
Potvrzení, že splňují požadavky na funkčnost a bezpečnost.

# Certifikace systémů elektronické identifikace

Pomocí certifikace eID systému lze nahradit požadavek na provedení procesu vzájemného hodnocení.
Návrh na možnost certifikace celého eID systému reaguje na dosavadní zkušenosti s procesem vzájemného hodnocení.

# Služby vytvářející důvěru

Dohled nad QTSP by měl být více sladěn v rámci celé EU.
Provázanost s NIS2.
Upřesnění ve věci ověření totožnosti při vydání kvalifikovaných certifikátů.
Povinnost akceptace QC pro autentizaci internetových stránek ze strany webových prohlížečů.
Zlepšení interoperability QTS díky přijetí prováděcích aktů (IA).
Omezení platnosti certifikace QSCD prostředků na 5 let s pravidelným hodnocením zranitelnosti.

# Služby vytvářející důvěru

- Elektronické potvrzení atributů
  - souvislost s evropskou peněženkou digitální identity
  - kvalifikované elektronické potvrzení atributů má stejné právní účinky jako potvrzení vydané v tištěné podobě.
  - požadavky na kvalifikované elektronické potvrzení atributů podobně těm pro QC.
  - Atributy například:
    - Věk
    - Adresa
    - Pohlaví
    - Národnost
    - Vzdělání
    - Profesní kvalifikace

# Služby vytvářející důvěru

- Správa kvalifikovaných prostředků pro vytváření el. podpisů/pečetí na dálku
  - Vytváření kvalifikovaných el. podpisů a pečetí na dálku.
- Služba elektronické archivace
  - zachování důvěryhodnosti elektronického dokumentu.
- Elektronická účetní kniha (ledger)
  - Ochrana dat proti pozměnění.
  - S kvalifikovanou elektronickou účetní knihou se pojí právní domněnka jedinečnosti a autentičnosti údajů, které obsahuje, přesnosti jejich data a času a jejich postupného chronologického řazení v této knize.

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

# Děkuji Vám za pozornost.

slido

# Join at slido.com
# #4CSA

ⓘ Start presenting to display the joining instructions on this slide.

slido

# Audience Q&A Session

ⓘ Start presenting to display the audience questions on this slide.

# Regulace využívání cloud computingu veřejnou správou

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

6. dubna 2022
TLP: WHITE

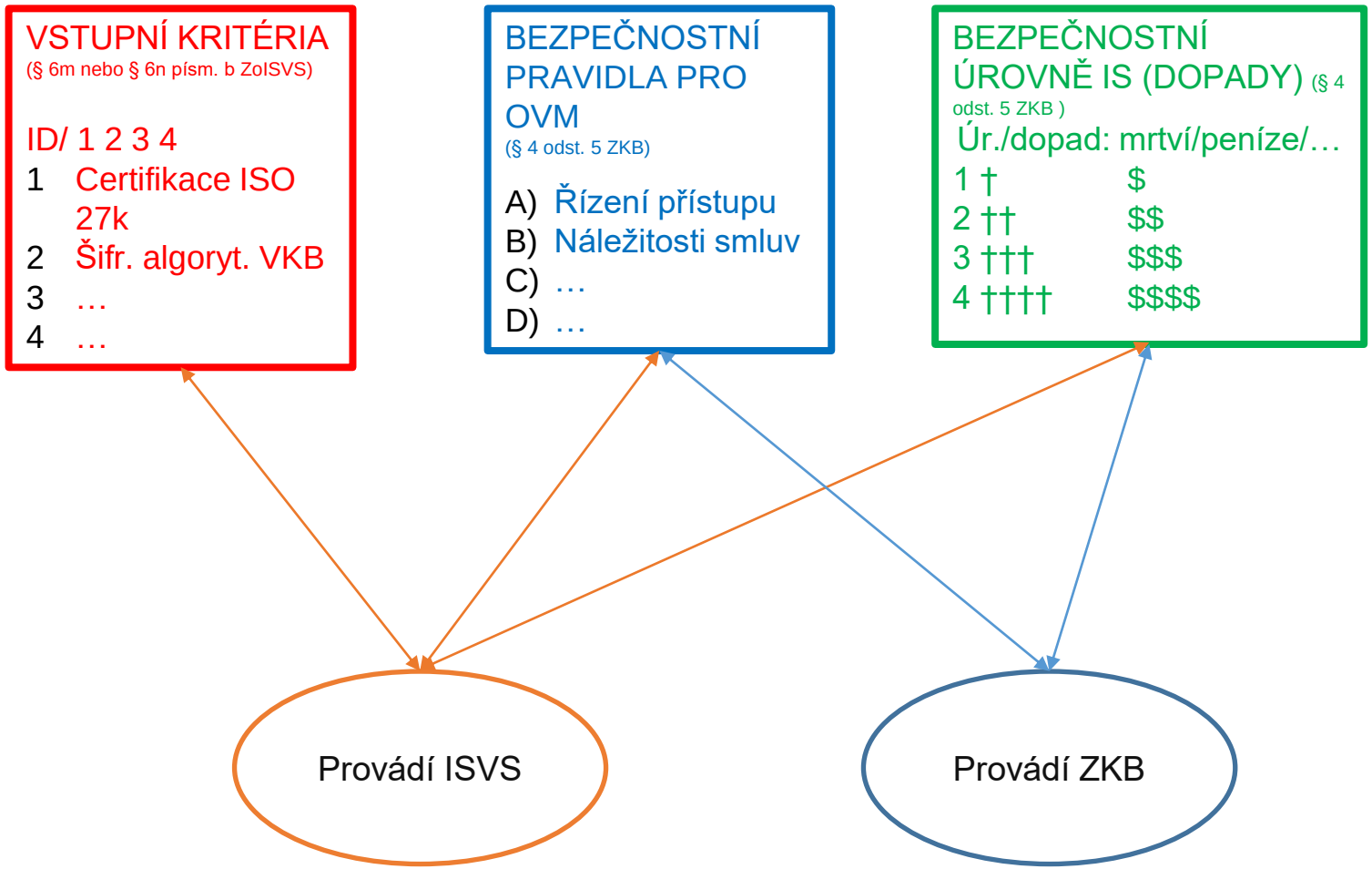
Petr Kopřiva
Odbor regulace

# Provedení regulace cloud computingu

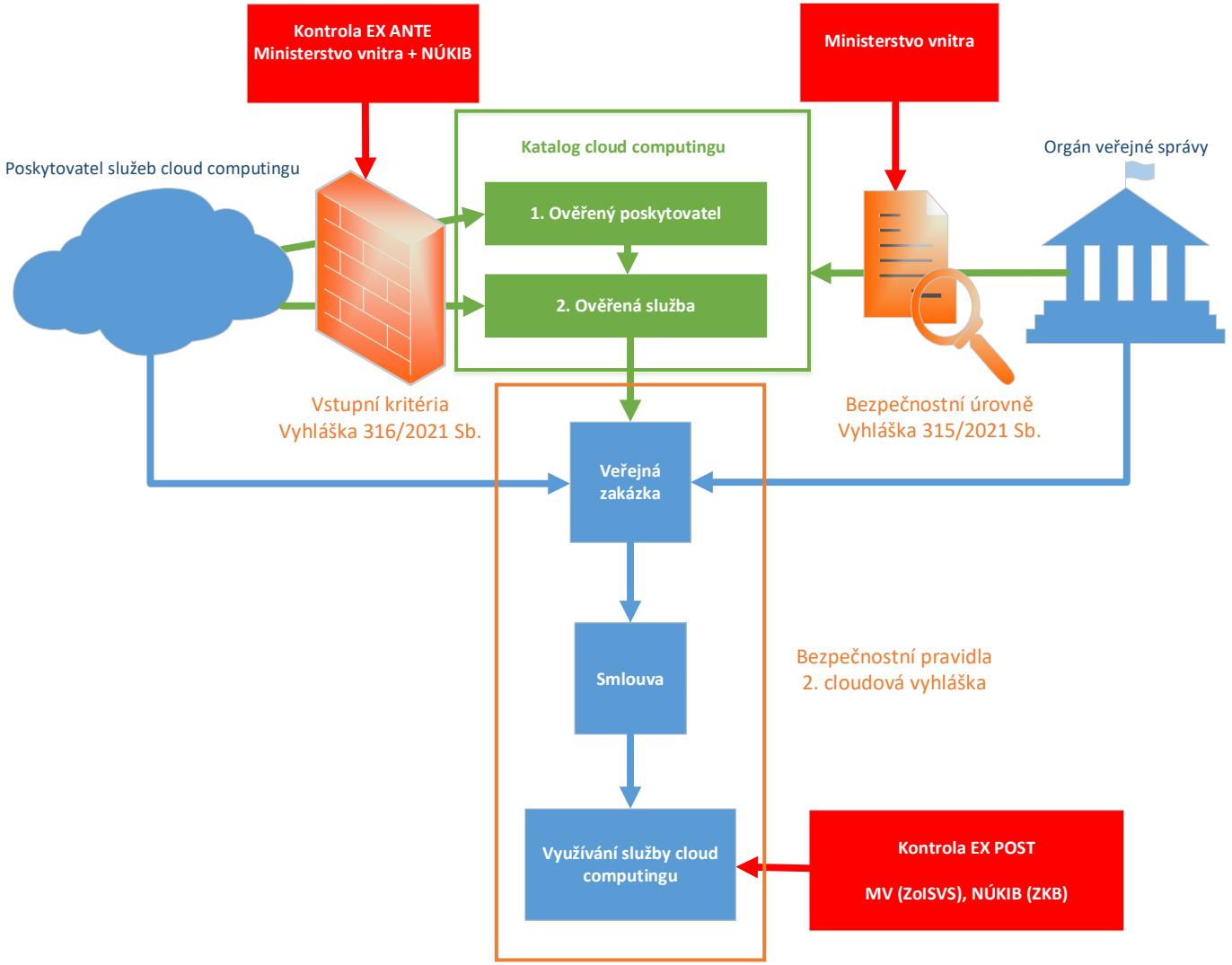
- Regulatorní rámec
  - zákon č. 365/2000 Sb., o informačních systémech veřejné správy (ZoISVS) – garant Ministerstvo vnitra
  - zákon č. 181/2014 Sb., o kybernetické bezpečnosti (ZKB)
- základní úprava od 1. 8. 2020 – řada nedostatků – nutné novelizovat
- novely provedeny zákonem č. 261/2021 Sb., tzv. DEPO účinnost od **1. 9. 2021**.

- v souvislosti s tím NÚKIB vydal dvě vyhlášky a připravuje třetí:
  - vyhláška č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu (tzv. vstupní kritéria)
  - vyhláška č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci (tzv. vyhláška o bezpečnostních úrovních)

# Dva zákony a tři vyhlášky



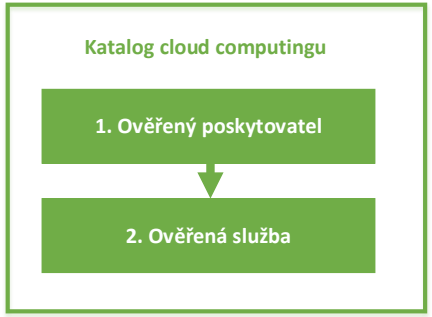
# Schéma regulatorního rámce cloud computingu - ZoISVS



# Požadavky na správce ISVS- ZoISVS

**§ 6l ZoISVS**
**Základní pravidla využívání cloud computingu orgánem veřejné správy**
**(1)** Orgán veřejné správy může využívat pouze cloud computing, který splňuje požadavky podle § 6n a je poskytovaný

**a)** poskytovatelem státního cloud computingu nebo poskytovatelem cloud computingu zapsaným v katalogu cloud computingu na základě nabídky cloud computingu tohoto poskytovatele zapsané v okamžiku jejího přijetí orgánem veřejné správy v katalogu cloud computingu,
**b)** v rámci vertikální nebo horizontální spolupráce podle právního předpisu upravujícího zadávání veřejných zakázek nebo
**c)** v rámci obecné výjimky z povinnosti zadat veřejnou zakázku v zadávacím řízení podle právního předpisu upravujícího zadávání veřejných zakázek. (…)



# Požadavky na správce ISVS- ZoISVS

**§ 6l ZoISVS**

**Základní pravidla využívání cloud computingu orgánem veřejné správy**

**(4)** Odstavce 1 až 3 se nepoužijí v případě cloud computingu, který slouží výlučně

**a)** ke správě a řešení technických potíží nebo diagnostice programových anebo technických prostředků, případně k zabezpečení nebo přenosu s tím souvisejících signálů,

**b)** ke správě nebo využívání prostředků pro elektronickou identifikaci využívajících vícefaktorové autentizace,

**c)** k aktualizaci nebo opravě programového prostředku, nebo

**d)** ke shromažďování nebo výměně provozních údajů,

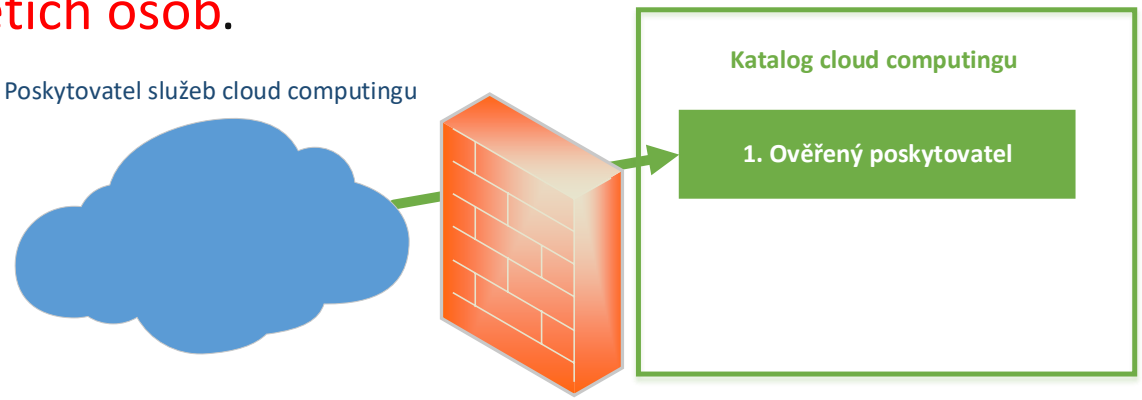
**e)** ke zkušebnímu provozu informačního systému veřejné správy, pokud při něm nebudou využity údaje, které se v informačním systému veřejné správy vedou nebo povedou anebo které jsou nebo budou v souvislosti s poskytováním služby informačního systému veřejné správy využívány.

# Požadavky na poskytovatele cloud computingu - ZoISVS

**§ 6m ZoISVS**

**Požadavky na poskytovatele cloud computingu poskytujícího cloud computing orgánu veřejné správy**

- **(1)** Poskytovatelem cloud computingu poskytujícím cloud computing orgánu veřejné správy může být pouze osoba nebo jiné právní uspořádání, které jsou
- **a)** způsobilé zajistit základní úroveň ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy,
- **b)** bezúhonné v rozsahu bezúhonnosti požadované po kvalifikovaném správci kvalifikovaného systému elektronické identifikace,
- **c)** způsobilé pro poskytnutí cloud computingu orgánu veřejné správy z hlediska veřejného pořádku, bezpečnosti a dodržování práv třetích osob.




Vstupní kritéria
Vyhláška 316/2021 Sb.

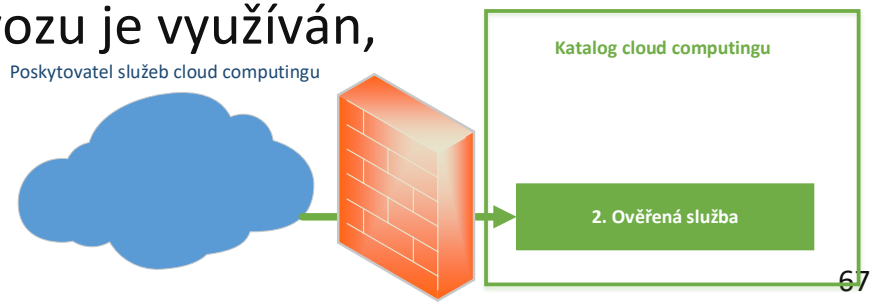
# Požadavky na cloud computingu - ZoISVS

**§ 6n ZoISVS**

**Požadavky na cloud computing využívaný orgánem veřejné správy**

- Orgán veřejné správy může využívat a poskytovatel cloud computingu může orgánu veřejné správy nebo poskytovateli státního cloud computingu poskytovat pouze cloud computing,
- **a)** který umožňuje splnění požadavků kladených na informační systém veřejné správy informační koncepcí České republiky,
- **b)** který umožňuje dosažení alespoň základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy,
- **c)** který umožňuje orgánu veřejné správy postupovat podle bezpečnostních pravidel pro orgány veřejné moci využívající služby cloud computingu podle právního předpisu upravujícího kybernetickou bezpečnost,
- **d)** jehož bezpečnostní úroveň je stejná nebo vyšší než bezpečnostní úroveň informačního systému veřejné správy nebo jeho části, k zajištění jehož provozu je využíván,

**(…)**

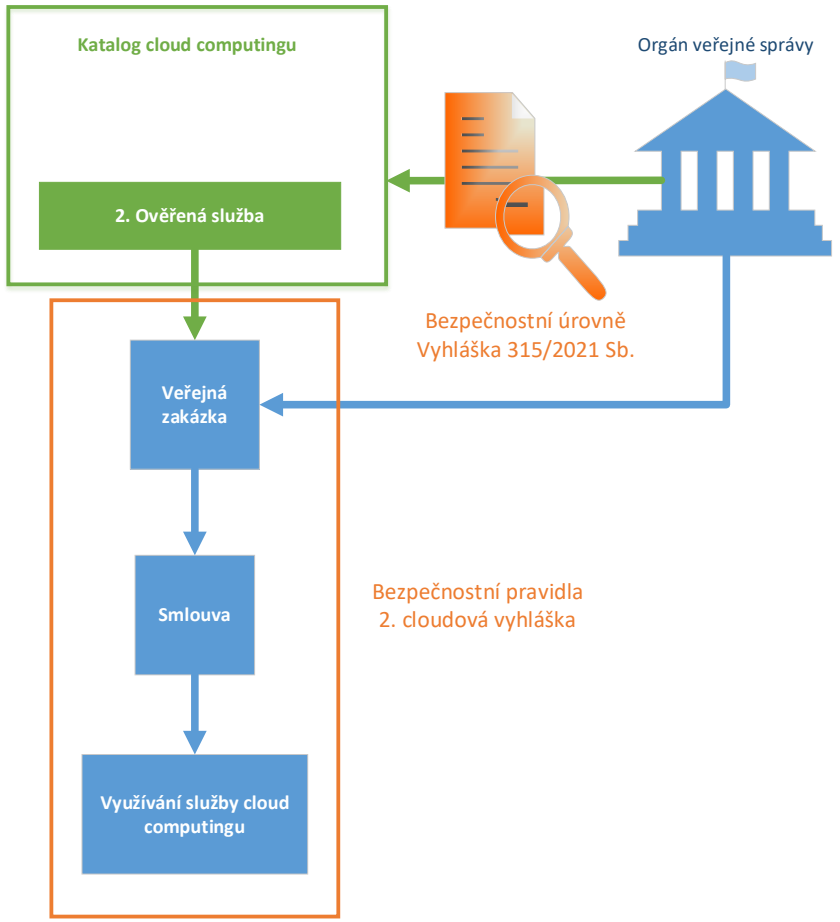


# Požadavky orgán veřejné moci - ZKB

**§ 4 odst. 5 ZKB**
**Požadavky na cloud computing využívaný orgánem veřejné správy**

- Od 1. 9. 2021:

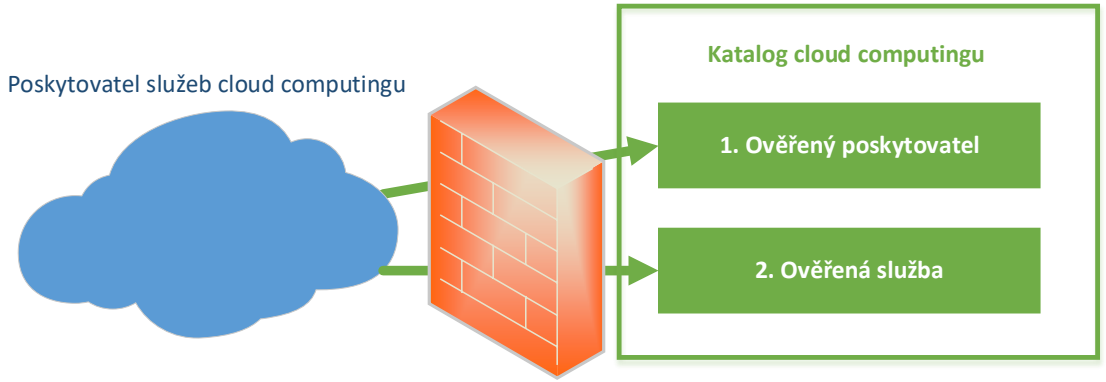
Orgány veřejné moci jsou povinny před uzavřením smlouvy s poskytovatelem služeb cloud computingu zařadit poptávaný cloud computing do bezpečnostní úrovně s ohledem na povahu dotčeného informačního nebo komunikačního systému podle prováděcího právního předpisu a zajistit, že budou dodržována bezpečnostní pravidla pro poskytování služeb cloud computingu stanovená Úřadem (…)



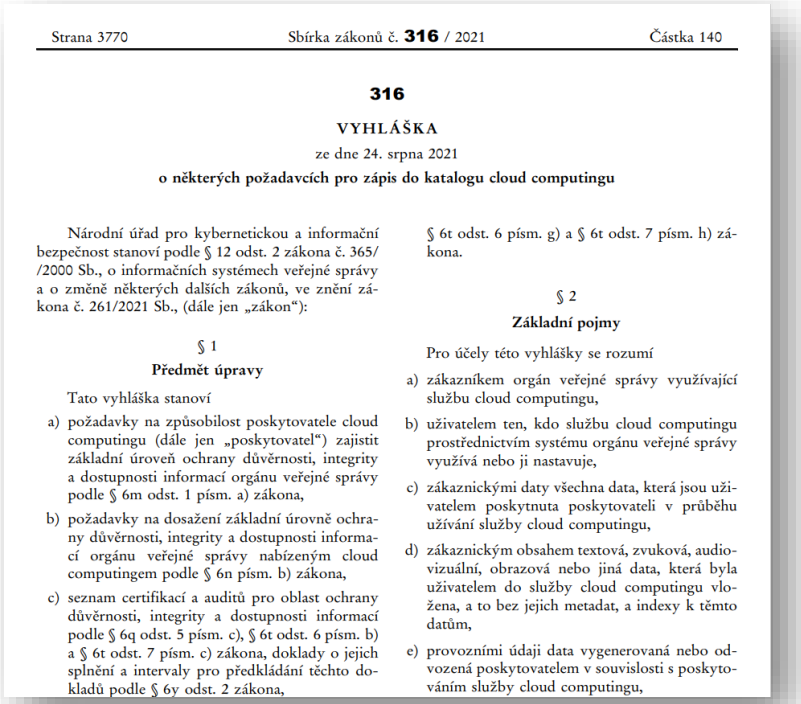
# Tři cloudové vyhlášky I.

## 1. Vyhláška č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu

- ÚČINNÁ OD 1. 9. 2021
- Tzv. vyhláška o vstupních kritériích
- Sada požadavků a podmínek, které musí poskytovatel CC služeb splnit aby mohl dodávat orgánům veřejné správy
- Cloudové služby rozděleny do 4 úrovní podle požadavku na bezpečnost
- Jednotliví dodavatelé služeb musí splnit vstupní požadavky
- Naplnění požadavků posoudí MV a NÚKIB = správní řízení




Vstupní kritéria
Vyhláška 316/2021 Sb.



Strana 3770 Sbírka zákonů č. **316** / 2021 Částka 140

**316**

**VYHLÁŠKA**

ze dne 24. srpna 2021

**o některých požadavcích pro zápis do katalogu cloud computingu**

Národní úřad pro kybernetickou a informační bezpečnost stanoví podle § 12 odst. 2 zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění zákona č. 261/2021 Sb., (dále jen „zákon"):

§ 1

**Předmět úpravy**

Tato vyhláška stanoví

a) požadavky na způsobilost poskytovatele cloud computingu (dále jen „poskytovatel") zajistit základní úroveň ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy podle § 6m odst. 1 písm. a) zákona,

b) požadavky na dosažení základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy nabízeným cloud computingem podle § 6n písm. b) zákona,

c) seznam certifikací a auditů pro oblast ochrany důvěrnosti, integrity a dostupnosti informací podle § 6q odst. 5 písm. c), § 6t odst. 6 písm. b) a § 6t odst. 7 písm. c) zákona, doklady o jejich splnění a intervaly pro předkládání těchto dokladů podle § 6y odst. 2 zákona,

§ 6t odst. 6 písm. g) a § 6t odst. 7 písm. h) zákona.

§ 2

**Základní pojmy**

Pro účely této vyhlášky se rozumí

a) zákazníkem orgán veřejné správy využívající službu cloud computingu,

b) uživatelem ten, kdo službu cloud computingu prostřednictvím systému orgánu veřejné správy využívá nebo ji nastavuje,

c) zákaznickými daty všechna data, která jsou uživatelem poskytnuta poskytovateli v průběhu užívání služby cloud computingu,

d) zákaznickým obsahem textová, zvuková, audiovizuální, obrazová nebo jiná data, která byla uživatelem do služby cloud computingu vložena, a to bez jejich metadat, a indexy k těmto datům,

e) provozními údaji data vygenerovaná nebo odvozená poskytovatelem v souvislosti s poskytováním služby cloud computingu,

# Uložení a zpracování dat - TRANSPARENTNOST

§ 6k odst. 2, písm. c, bod 3 ZoISVS

- údaje o **předpokládaném místu zpracování informací** orgánu veřejné správy a **předpokládané době**, **předpokládaném rozsahu** a **předpokládaném účelu** zpracování informací orgánu veřejné správy v tomto místě, případně o tom, že nabízený cloud computing **vyžaduje dlouhodobé uložení informací orgánu veřejné správy** mimo území Evropské unie,

Příloha č. 2, část 1 vyhlášky 316/2021 Sb.

**ULOŽENÍ NEAKTIVNÍCH ZÁKAZNICKÝCH DAT A SPECIFICKÝCH PROVOZNÍCH ÚDAJŮ**

- Uložení neaktivních dat v EU nebo výjimka uvedená na webu NÚKIB (v jednání informace v Katalogu eGC)

https://www.nukib.cz/cs/uredni-deska/cloud-computing/

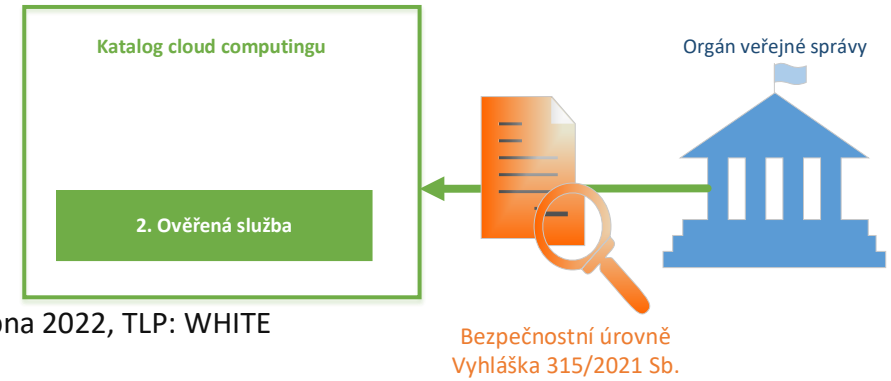
**ZPRACOVÁNÍ ZÁKAZNICKÝCH DAT A SPECIFICKÝCH PROVOZNÍCH ÚDAJŮ**

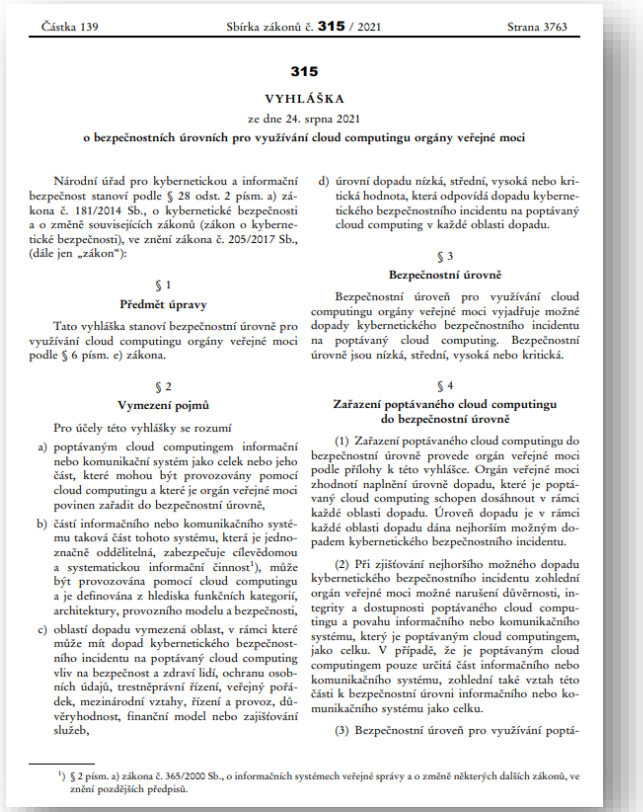
- Buď v EU nebo v Katalogu eGC informace o předpokládaném místě, době, času zpracování

# Tři cloudové vyhlášky II.

## 2. Vyhláška č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci (Vyhláška o bezpečnostních úrovních systémů)

- ÚČINNÁ OD 1. 9. 2021
- Zařazení informačního systému nebo jeho části do bezpečnostní úrovně (BÚ)
- Bezpečnostní úroveň určuje možný dopad narušení bezpečnosti informací
- Rozcestník pro hodnocení důležitosti systémů státní správy a pro určení požadavků na jejich zabezpečení
- Dopadá na všechny orgány veřejné moci
- BÚ jsou 4: nízká, střední, vysoká (= komerční), kritická (= státní)



Částka 139 Sbírka zákonů č. 315 / 2021 Strana 3763

**315**

**VYHLÁŠKA**

ze dne 24. srpna 2021

**o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci**

Národní úřad pro kybernetickou a informační bezpečnost stanoví podle § 28 odst. 2 písm. a) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 205/2017 Sb., (dále jen „zákon"):

§ 1

**Předmět úpravy**

Tato vyhláška stanoví bezpečnostní úrovně pro využívání cloud computingu orgány veřejné moci podle § 6 písm. e) zákona.

§ 2

**Vymezení pojmů**

Pro účely této vyhlášky se rozumí

a) poptávaným cloud computingem informační nebo komunikační systém jako celek nebo jeho část, které mohou být provozovány pomocí cloud computingu a které je orgán veřejné moci povinen zařadit do bezpečnostní úrovně,

b) částí informačního nebo komunikačního systému taková část tohoto systému, která je jednoznačně oddělitelná, zabezpečuje cílevědomou a systematickou informační činnost[1]), může být provozována pomocí cloud computingu a je definována z hlediska funkčních kategorií, architektury, provozního modelu a bezpečnosti,

c) oblastí dopadu vymezená oblast, v rámci které může mít dopad kybernetického bezpečnostního incidentu na poptávaný cloud computing vliv na bezpečnost a zdraví lidí, ochranu osobních údajů, trestněprávní řízení, veřejný pořádek, mezinárodní vztahy, řízení a provoz, důvěryhodnost, finanční model nebo zajišťování služeb,

d) úrovní dopadu nízká, střední, vysoká nebo kritická hodnota, která odpovídá dopadu kybernetického bezpečnostního incidentu na poptávaný cloud computing v každé oblasti dopadu.

§ 3

**Bezpečnostní úrovně**

Bezpečnostní úroveň pro využívání cloud computingu orgány veřejné moci vyjadřuje možné dopady kybernetického bezpečnostního incidentu na poptávaný cloud computing. Bezpečnostní úrovně jsou nízká, střední, vysoká nebo kritická.

§ 4

**Zařazení poptávaného cloud computingu do bezpečnostní úrovně**

(1) Zařazení poptávaného cloud computingu do bezpečnostní úrovně provede orgán veřejné moci podle přílohy k této vyhlášce. Orgán veřejné moci zhodnotí naplnění úrovně dopadu, které je poptávaný cloud computing schopen dosáhnout v rámci každé oblasti dopadu. Úroveň dopadu je v rámci každé oblasti dopadu dána nejhorším možným dopadem kybernetického bezpečnostního incidentu.

(2) Při zjišťování nejhoršího možného dopadu kybernetického bezpečnostního incidentu zohlední orgán veřejné moci možné narušení důvěrnosti, integrity a dostupnosti poptávaného cloud computingu a povahu informačního nebo komunikačního systému, který je poptávaným cloud computingem, jako celku. V případě, že je poptávaným cloud computingem pouze určitá část informačního nebo komunikačního systému, zohlední také vztah této části k bezpečnostní úrovni informačního nebo komunikačního systému jako celku.

(3) Bezpečnostní úroveň pro využívání poptá-

[1]) § 2 písm. a) zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů.

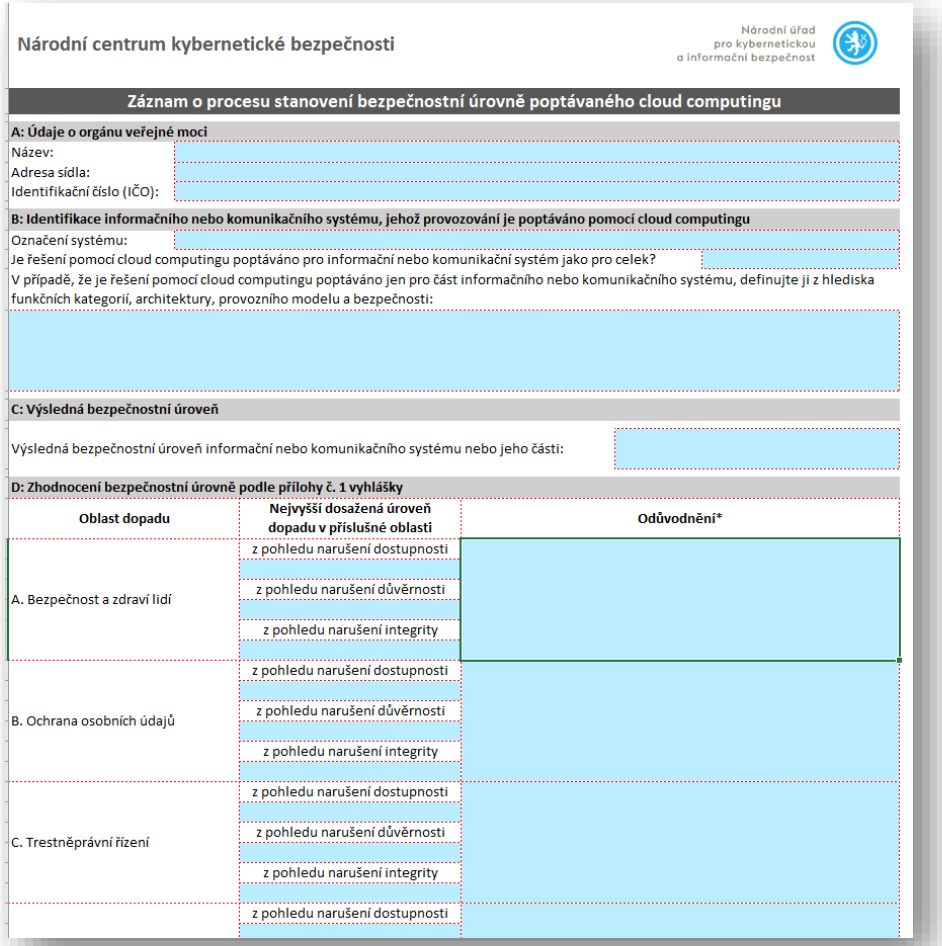
# Tři cloudové vyhlášky II. - formulář

https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/formulare/

**Formulář hodnocení bezpečnostních úrovní**

Pro splnění povinnosti podle § 4 odst. 5 zákona o kybernetické bezpečnosti ve spojení s vyhláškou 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci.

› ke stažení zde



Národní centrum kybernetické bezpečnosti

Národní úřad pro kybernetickou a informační bezpečnost

**Záznam o procesu stanovení bezpečnostní úrovně poptávaného cloud computingu**

**A: Údaje o orgánu veřejné moci**

Název:
Adresa sídla:
Identifikační číslo (IČO):

**B: Identifikace informačního nebo komunikačního systému, jehož provozování je poptáváno pomocí cloud computingu**

Označení systému:
Je řešení pomocí cloud computingu poptáváno pro informační nebo komunikační systém jako pro celek?
V případě, že je řešení pomocí cloud computingu poptáváno jen pro část informačního nebo komunikačního systému, definujte ji z hlediska funkčních kategorií, architektury, provozního modelu a bezpečnosti:

**C: Výsledná bezpečnostní úroveň**

Výsledná bezpečnostní úroveň informační nebo komunikačního systému nebo jeho části:

**D: Zhodnocení bezpečnostní úrovně podle přílohy č. 1 vyhlášky**

| Oblast dopadu | Nejvyšší dosažená úroveň dopadu v příslušné oblasti | Odůvodnění* |
|---|---|---|
| A. Bezpečnost a zdraví lidí | z pohledu narušení dostupnosti<br>z pohledu narušení důvěrnosti<br>z pohledu narušení integrity | |
| B. Ochrana osobních údajů | z pohledu narušení dostupnosti<br>z pohledu narušení důvěrnosti<br>z pohledu narušení integrity | |
| C. Trestněprávní řízení | z pohledu narušení dostupnosti<br>z pohledu narušení důvěrnosti<br>z pohledu narušení integrity | |
| | z pohledu narušení dostupnosti | |

# Tři cloudové vyhlášky II. – podpůrný materiál

https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/

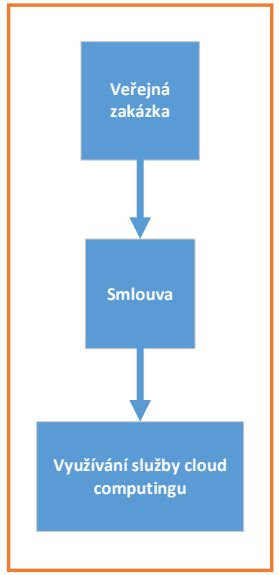
## Cloud computing

**Průvodce zařazením poptávaného cloud computingu do bezpečnostní úrovně**

- Tento podpůrný materiál poskytuje orgánům veřejné moci metodickou podporu pro zařazení informačního nebo komunikačního systému, který si přejí provozovat prostřednictvím služeb cloud computingu, do odpovídající bezpečnostní úrovně dle vyhlášky č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné.
- Stáhnout pdf (v1.0 platná ke dni 03.12.2021)

# Tři cloudové vyhlášky III.

## 3. Vyhláška o bezpečnostních pravidlech




- Ve výrobě – vydání předpokládáme v průběhu roku 2022, v blízké době do MPŘ
- Každá z bezpečnostních úrovní (1-4) bude mít stanovena příslušná bezpečnostní opatření
- Dopadá na všechny orgány veřejné moci
- Obsahově blízké VKB, vychází z německého standardu C5
- Bude obsahovat povinná a volitelná bezpečnostní pravidla – celkem cca 250 pravidel (povinná 46)
- Subjekt zavede povinná pravidla a zváží vhodnost volitelných s ohledem na jejich aplikovatelnost a nezbytnost pro zajištění bezpečnosti informací.
- Možnosti zajištění:
  - Prohlášení poskytovatele
  - Certifikace poskytovatele – ISO 27001, ISO 27017, ISO 27018, C5, SOC 2® Type 2, ISO 20000 nebo ISO 22301, v budoucnu evropská certifikace (EUCS)
  - Smluvní závazek poskytovatele

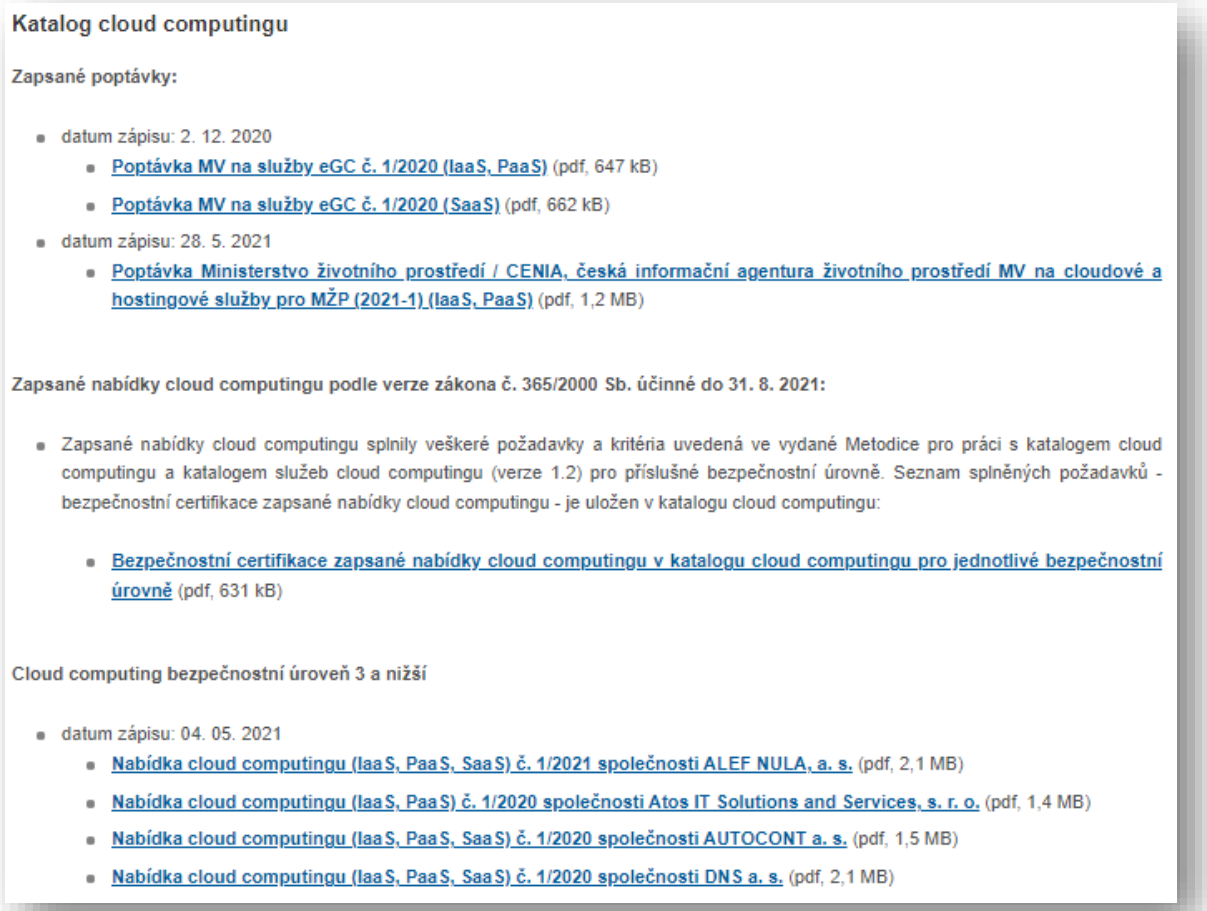
# Přechodná ustanovení

- **Zákon č. 12/2020 Sb. § 17** (novelizován zákonem č. 261/2021 Sb.)
  - OVS musí do 3 měsíců od 1. 8. 2020 zapsat využívaný cloud computing (CC) do katalogu CC
  - OVS využívalo cloud computing k 1. 8. 2020 = může tento CC dále využívat do 1. 1. 2024
- **Zákon č. 261/2021 Sb., Čl. LXXXI**
  - OVS využívalo CC nebo uzavřelo (rámcovou) smlouvu před 1. 9. 2021 = může tento CC využívat do 31. 12. 2023
  - CC v katalogu před 1. 9. 2021/zapsaný dle podmínek před 1. 9. 2021 = může využívat do 31. 12. 2023
  - OVS zahájilo využívaní CC od 1. 9. 2021 do 31. 1. 2022 = může využívat do 31. 12. 2022

pozn. v případě, že daný CC splňuje aktuální podmínky – zapsán v katalogu, splňuje požadavky cloudových vyhlášek – lze využívat bez časového omezení

# Aktuální stav katalogu cloud computingu MV

https://www.mvcr.cz/clanek/egovernment-cloud.aspx?q=Y2hudW09NQ%3D%3D



**Katalog cloud computingu**

**Zapsané poptávky:**

- datum zápisu: 2. 12. 2020
  - Poptávka MV na služby eGC č. 1/2020 (IaaS, PaaS) (pdf, 647 kB)
  - Poptávka MV na služby eGC č. 1/2020 (SaaS) (pdf, 662 kB)
- datum zápisu: 28. 5. 2021
  - Poptávka Ministerstvo životního prostředí / CENIA, česká informační agentura životního prostředí MV na cloudové a hostingové služby pro MŽP (2021-1) (IaaS, PaaS) (pdf, 1,2 MB)

**Zapsané nabídky cloud computingu podle verze zákona č. 365/2000 Sb. účinné do 31. 8. 2021:**

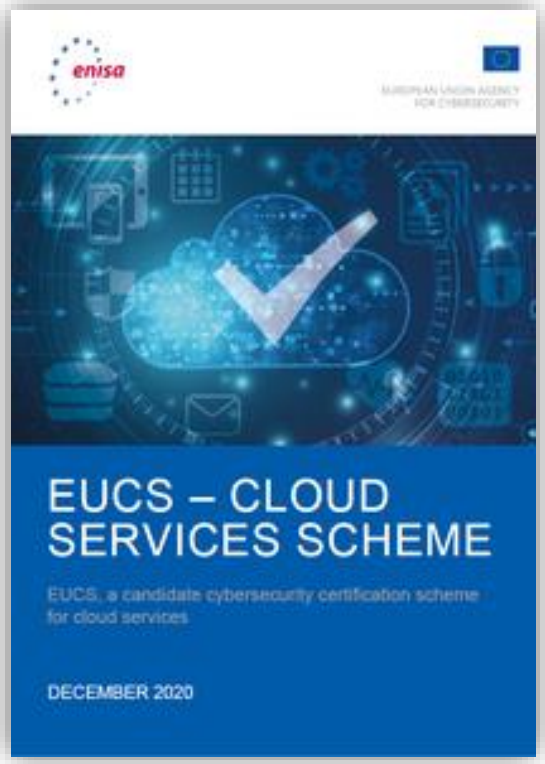
- Zapsané nabídky cloud computingu splnily veškeré požadavky a kritéria uvedená ve vydané Metodice pro práci s katalogem cloud computingu a katalogem služeb cloud computingu (verze 1.2) pro příslušné bezpečnostní úrovně. Seznam splněných požadavků - bezpečnostní certifikace zapsané nabídky cloud computingu - je uložen v katalogu cloud computingu:
  - Bezpečnostní certifikace zapsané nabídky cloud computingu v katalogu cloud computingu pro jednotlivé bezpečnostní úrovně (pdf, 631 kB)

**Cloud computing bezpečnostní úroveň 3 a nižší**

- datum zápisu: 04. 05. 2021
  - Nabídka cloud computingu (IaaS, PaaS, SaaS) č. 1/2021 společnosti ALEF NULA, a. s. (pdf, 2,1 MB)
  - Nabídka cloud computingu (IaaS, PaaS) č. 1/2020 společnosti Atos IT Solutions and Services, s. r. o. (pdf, 1,4 MB)
  - Nabídka cloud computingu (IaaS, PaaS, SaaS) č. 1/2020 společnosti AUTOCONT a. s. (pdf, 1,5 MB)
  - Nabídka cloud computingu (IaaS, PaaS, SaaS) č. 1/2020 společnosti DNS a. s. (pdf, 2,1 MB)

# Pohled do budoucna a EU

**EUCS – Evropská certifikace cloudových služeb**




**Směrnice NIS/2**


- Směrnice NIS
  - Poskytovatelé cloudových služeb = DSP
- Směrnice NIS2 (2022?)
  - Poskytovatelé cloudových služeb = Essential and important entities = povinné osoby dle ZKB?

# Vztah regulace cloudu v ČR a EUCS

- Po zavedení EUCS a vyřešení některých výhrad bude možné přizpůsobit národní regulaci EUCS:
  - úprava VSTUPNÍCH KRITÉRIÍ
    - umožnění předložení EUCS certifikátu + dodatečné požadavky k místu zpracování dat a prověření poskytovatele cloudové služby
  - úprava BEZPEČNOSTNÍCH PRAVIDEL
    - sjednocení znění bezpečnostních pravidel s požadavky na poskytovatele cloudových služeb v EUCS + požadavky týkající se výhradně orgánu veřejné moci

# Cloudové vyhlášky - kde najít informace

- Vyhlášky, včetně odůvodnění:
  - https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/
- Nejčastější dotazy:
  - https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/faq/
- Katalog cloud computingu – zapsané nabídky a poptávky:
  - https://www.mvcr.cz/clanek/egovernment-cloud.aspx?q=Y2hudW09NQ%3d%3d
- Služby, které trvale ukládají data mimo EU – Úřední deska NÚKIB - https://www.nukib.cz/cs/uredni-deska/ - od nové právní úpravy – zatím prázdné

# Dotazy?

## Děkuji za pozornost!

regulace@nukib.cz

slido

# Join at slido.com
# #4CSA

ⓘ Start presenting to display the joining instructions on this slide.

slido

# Audience Q&A Session

ⓘ Start presenting to display the audience questions on this slide.

# Cyber Resilience Act

**Karolína Menšíková**
**odd. Mezinárodních organizací a práva, NÚKIB**

Národní úřad pro kybernetickou a informační bezpečnost

“If everything is connected, everything can be hacked,”

- Ursula von der Leyen, předsedkyně EK

- Předsedkyně Evropské komise ve svém projevu o stavu Unie (SOTEU) dne 15. září 2021 zmínila potřebu přijetí nové evropské legislativy, která by stanovila společné standardy pro zlepšení kybernetické bezpečnosti produktů a služeb na evropském vnitřním trhu.
- Potřeba legislativy již zmíněna ve Strategii kybernetické bezpečnosti EU pro digitální dekádu ze dne 16. prosince 2020.
- Podle pracovního plánu EK pro rok 2022 by měl být návrh **představen v září 2022**, tedy v průběhu CZ PRES.

# Studie na potřebu KB požadavků pro ICT produkty

Study on the need of cybersecurity requirements for ICT products | Shaping Europe's digital future (europa.eu)

- Komplexní studie, která se zabývá kategoriemi ICT produktů a souvisejících služeb a dále přístupem ke KB ICT produktů a souvisejících služeb, jak je také uvedeno ve Výzvě veřejnosti (viz další slides).

# Klíčové výsledky Studie

- Existující EU legislativa je nedostatečné v ohledu KB.
- Nedostačující zabezpečení ICT produktů a souvisejících služeb.
- Dle Studie není možné rizikové ICT produkty a související služby škatulkovat dle ICT kategorie či sektoru (jinými slovy produkty jsou velmi heterogenní/různé v každé kategorii či sektoru).
- Studie se věnuje 5 možným přístup k bezpečnosti ICT produktů a souvisejících služeb (viz Výzva veřejnosti).

# Výzva k vyjádření veřejnosti

Cyber resilience act – new cybersecurity rules for digital products and ancillary services (europa.eu)

- Veřejná konzultace otevřena **do 25. května 2022.**

# Navrhované možnosti regulace/přístupu

I. Zachování současného stavu a stávajících právních předpisů;
II. Zavedení dobrovolných opatření;
III. Regulační zásahy "ad hoc“;
IV. Smíšený přístup;
V. Horizontální regulační zásah

**Zachování současného stavu a stávajících právních předpisů** (např. nařízení v přenesené pravomoci podle nařízení o ochraně osobních údajů, směrnice o rádiových zařízeních, právní předpisy o zdravotnických prostředcích, motorových vozidlech, strojních zařízeních nebo bezpečnosti výrobků atd.), které částečně řeší KB hmotných produktů.

**Zavedení dobrovolných opatření** - dobrovolná certifikační schémata podle CSA by mohly být dále rozvíjena a uplatňována. Zvážit by se mohla také opatření "měkkého práva", jako jsou pokyny, doporučení, iniciativy průmyslu, kodexy chování aj.

**Regulační zásahy "ad hoc"** v oblasti KB digitálních produktů a doplňkových služeb - zásah by se omezil na doplnění a/nebo změnu požadavků na KB v již existujících právních předpisech a na regulaci nových rizik, jakmile se objeví, včetně potenciálně nevestavěných softwarů.

Smíšený přístup zahrnující **závazná a měkká pravidla**, což by zahrnovalo:

a. horizontální regulační zásah zavádějící požadavky na KB pro širokou škálu hmotných digitálních produktů a doplňkových služeb.

S ohledem na postup posuzování shody lze zvážit různé dílčí možnosti:

- vlastní posouzení shody, kdy se prodejci mohou rozhodnout pro posouzení shody třetí stranou, pokud to budou považovat za vhodné; nebo

- předepsané posouzení shody třetí stranou pro určité kategorie výrobků v rámci postupu založeném na posouzení rizik.

b. Co se týče KB nevestavěných softwarů, zvážil by se odstupňovaný přístup, přičemž prvním krokem by byla měkká právní opatření, jako jsou pokyny nebo doporučení, případně následované regulačním zásahem v závislosti na výsledcích implementace takových opatření.

**Horizontální regulační zásah**, který by zavedl požadavky na KB pro širokou škálu hmotných a nehmotných digitálních produktů a souvisejících doplňkových služeb, včetně nevestavěných softwarů.

Alternativní dílčí možnosti by mohly být zváženy, pokud jde o kategorie softwaru, na které se mají vztahovat - buď pouze kritický software nebo veškerý software - a pokud jde o postup posuzování shody, jako v možnosti IV a)

- vlastní posouzení shody, kdy se prodejci mohou rozhodnout pro posouzení shody třetí stranou, pokud to budou považovat za vhodné; nebo
- předepsané posouzení shody třetí stranou pro určité kategorie výrobků v rámci postupu založeném na posouzení rizik.

# ICT produkty a související služby

## Early thinking on scope *(work in progress)*

**In scope:**

- **Hardware products** ("tangible")
- **Ancillary services**
- **Standalone software products** ("non-tangible"), including games

**Outright exclusions:**

- **Open source**
- **Websites**
- **Web apps** and **cloud services** (SaaS)
- **Certain products regulated** under the new and old approach

# Děkuji za pozornost.

Diskuze

Národní úřad
pro kybernetickou
a informační bezpečnost

slido

# Join at slido.com
# #4CSA

ⓘ Start presenting to display the joining instructions on this slide.

slido

# Audience Q&A Session

ⓘ Start presenting to display the audience questions on this slide.

# Vzdělávání a osvěta v oblasti kybernetické bezpečnosti

Nina Adamcová, Oddělení vzdělávání

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

# Kdo jsou naše cílové skupiny?



- Primární skupina – pracovníci veřejné správy, organizace podle Zákona o kybernetické bezpečnosti a směrnice NIS
- Sekundární skupina – zranitelné skupiny (žáci a učitelé, rodiče a děti, senioři) a pracovníci prevence
- Široká veřejnost

# Národní strategie kybernetické bezpečnosti



- Pilíř Odolná společnost 4.0

Kybernetická bezpečnost není jen technická disciplína.

# Online kurzy



- Zakončení testem a certifikátem o absolvování
- Registrace jednotlivců i větších skupin (preferujeme zaměstnavatele/skupiny)
- Pravidelná aktualizace kurzů
- Kurzy vhodné pro širokou veřejnost, IT administrátory a manažery kybernetické bezpečnosti či konkrétní zaměstnání (učitelé, zdravotníci, pracovníci prevence)
- Tvorba dalších kurzů:
  - Například pro krypto pracovníky (neutajovaný obsah)

# Dávej kyber – Základy kybernetické bezpečnosti

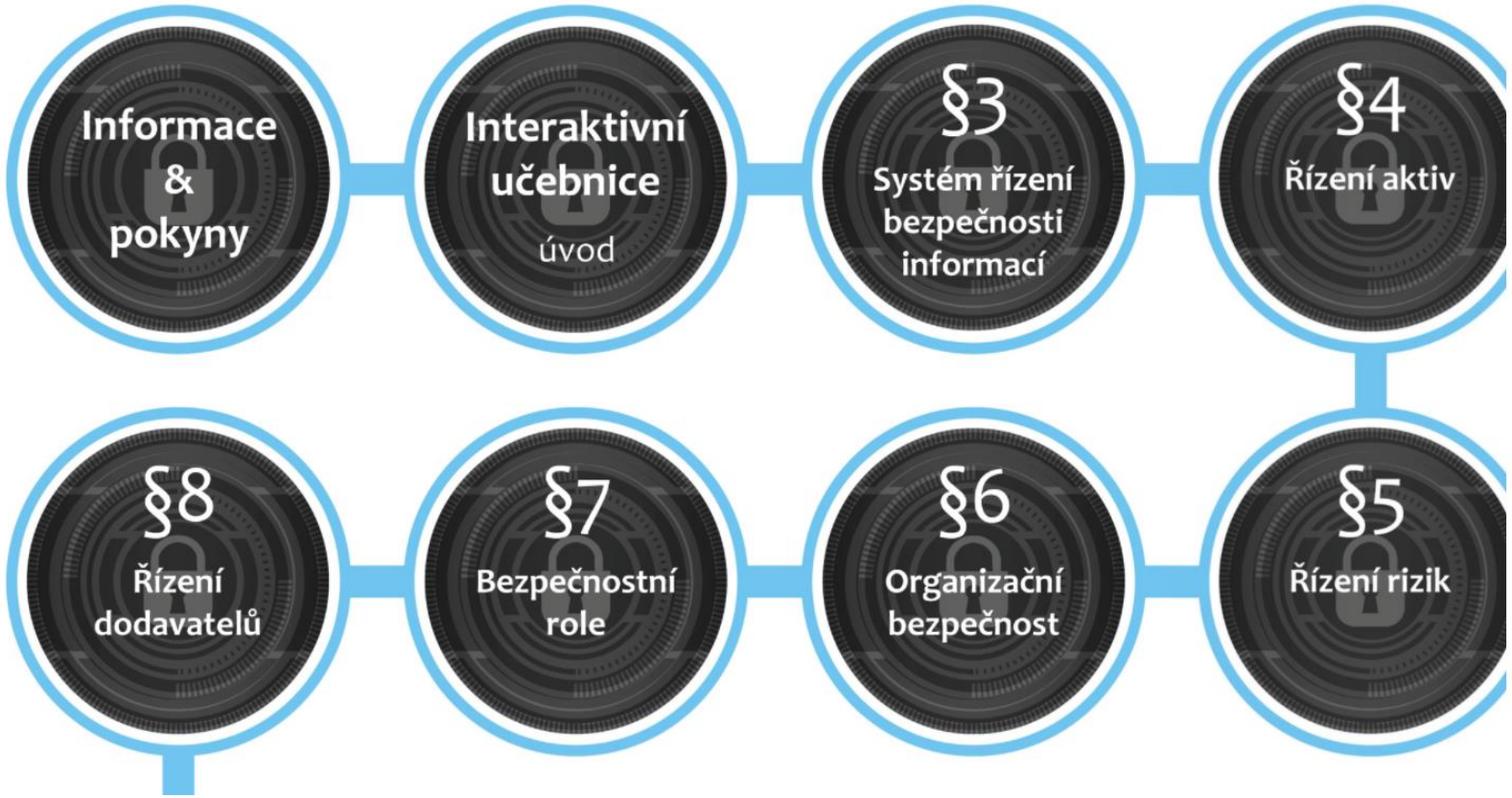
Národní úřad pro kybernetickou a informační bezpečnost

- Kurz vhodný pro každého
- Témata: registrace a přihlašování, e-mail a přílohy, aplikace a služby, zařízení a média, odkazy a weby, připojení a internet
- V roce 2021 kurz absolvovalo 20 546 uživatelů
- 2022 – aktualizace, nový design, nová témata

# Šéfuj kyber



- Kurz vhodný pro manažery kybernetické bezpečnosti a pracovníky IT oddělení.
- Vyhláška o kybernetické bezpečnosti (č. 82/2018 Sb.)

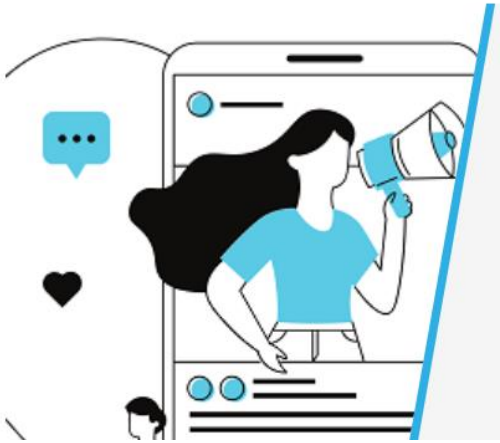


## Základy kybernetické bezpečnosti

Pro zaměstnance škol

## Průvodce portálem

Určeno všem zájemcům o kurzy



## Bezpečná školní ICT infrastruktura

## Minimum kybernetické bezpečnosti

Pro zaměstnance ve

# Jak si vybrat správný kurz?



- Průvodce portálem - doporučení, pro koho jsou vhodné

## Naše nabídka

Všechny potřebné informace o kurzech na jednom místě. Prozkoumejte nabídku našich osvětových a vzdělávacích kurzů.


**Informace o kurzech**

**Otevřít portál**

# Anti-phishingový modul



- V konkrétním období po absolvování kurzu může přijít zaměstnanci testovací phishingový mail
- Maily jsou obecné a veškeré odkazy vedou na vzdělávací stránku k phishingu
- Výsledný report – otevření a rozkliknutí e-mailu

# Osvětové materiály



- Bezpečný pohyb v kybersvětě

Zaměřeno na:

- počítač & smartphone,
- online komunikaci,
- online účty.

- Bezpečnostní doporučení pro administrátory

osveta.nukib.cz
Průvodce kurzy a portálem

moodle@nukib.cz
vzdelavani@nukib.cz
n.adamcova@nukib.cz

slido

# Join at slido.com
# #4CSA

ⓘ Start presenting to display the joining instructions on this slide.

slido

# Audience Q&A Session

ⓘ Start presenting to display the audience questions on this slide.

Národní úřad
pro kybernetickou
a informační bezpečnost

# DĚKUJEME ZA POZORNOST
# A PŘEJEME VÁM KRÁSNÝ DEN

Ing. Markéta Šilhavá
m.silhava@nukib.cz
+420 702 160 590