

BPC-AKR - zadání projektů

Průběh projektu:

- 3. týden – Zveřejnění zadání projektů
- 4. týden – Zadání projektů (maximálně **DVĚ** skupiny na jedno zadání)
- 6. týden – Odevzdání studie
- 7. týden – Hodnocení studie
- 11. týden - Odevzdání projektu
- 12./13. týden – Obhajoba projektu

Bodové hodnocení projektu:

- Studie problematiky – 4b
- Realizace programu – 6b
- Obhajoba projektu – 5b

Do 6. týdne semestru je povinnost odevzdat studii problematiky, která bude obsahovat:

- úvod a popis projektu,
- cíle projektu, kterých by mělo být dosaženo,
- teoretickou část popisující vybrané téma,
- aktuální stav řešení (popis v jaké fázi se projekt nachází a jak bude dále pokračovat.
!!!!Stěžejní část studie!!!!)
- představit autory a uvést jejich pracovní přínos do projektu.

Dokument musí obsahovat náležitosti technického dokumentu (**titulní strana, obsah, úvod, závěr, přílohy, literatura (dle ISO 690)**), rozsah je stanoven na **5 – 7 normostran** (dle složitosti problematiky).

Níže jsou uvedeny jednotlivé projekty, které budou zadány skupinám dle registrace v online dokumentu. Odevzdání studie a kódu projektu bude probíhat v elearningu (bude zveřejněno v průběhu semestru) v archivovaném souboru ve formátu zip s číslem skupiny . Odevzdání provede jen jeden člen ze skupiny.

Zabezpečení dat pomocí elektronického podpisu

Nejdříve nastudujte problematiku týkající se elektronických podpisů a jejich možnosti vložení do souboru (např. do metadat). Poté vytvořte aplikaci, která načte vstupní data a zabezpečí je pomocí elektronickým podpisem. Jako vstupní data využijte vámi vytvořený textový, obrázkový nebo jiný soubor. Poté v aplikaci vytvořte funkci pro ověření integrity dat (na základě certifikátu) a demonstруйте funkčnost pro různé situace (změna certifikátu, změna textového souboru atd.).

Samotný podpis je možné realizovat ve dvou variantách:

- Podpis bude součástí textového souboru – Podpis bude vložen přímo do textového souboru, ale zároveň neovlivní možnost číst daný soubor.
- Podpis bude samostatný soubor – Podpis bude realizován jako samostatný soubor a při ověření integrity se bude načítat podpis i textový soubor.

V tomto zadání je možné použít knihovny zaměřené na tvorbu heše a certifikátu. Nesmí se použít přímo knihovny na tvorbu podpisu. Součástí programu bude i možnost vytváření certifikátů (Certifikační autorita bude součástí programu).

Preferována je verze, kdy je podpis SOUČÁSTÍ souboru. Druhou variantu volte v případě, že vám první nepůjde realizovat (Nutné doložit v kontrolní studii nebo při obhajobě proč první varianta nefungovala).

[1] Introduction to digital seals, (<https://www.signicat.com/blog/blog-introduction-digital-seals/>)

[2] Digitální certifikát, (https://cs.wikipedia.org/wiki/Digit%C3%A1ln%C3%AD_certifik%C3%A1t)