Myšlenka

Co víme, jak to ověřit a co ještě nevíme

Průvodce programem Konfirmu pro rodiny, učitele, rozhodovací orgány a odborníky.



Ve dvou dokladech je uvedeno, že dorazilo deset krabic. Někdo jde do skladu, spočítá krabice na podlaze a najde jich devět.

Můžeme ověřit, zda se dokumenty shodují. Abychom zjistili, kolik krabic dorazilo, potřebujeme také počet kusů. Jaké doklady byste požádali osobu, která je převzala, aby vám předložila?

Tři úrovně důkazů

Co můžeme zkontrolovat?

Kopie, podpis a počet odpovídají na různé otázky.

01 Máme nějaký spolehlivý zdroj?

Může se jednat o původní soubor nebo o jeho digitální otisk získaný prostřednictvím důvěryhodného kanálu. Uveďte také verzi a zdroj odkazu.

02 Obsahuje kopie stejná data?

Hash je digitální otisk vypočítaný z bajtů v souboru. Ověření digitálního podpisu pomocí důvěryhodného klíče vám také umožňuje ověřit vazbu na klíč podepisujícího.

03 Došlo k události popsané v dokumentu?

Abyste zjistili, co se stalo, možná budete muset spočítat krabice, zkontrolovat rozměry, nahlédnout do oficiálního záznamu nebo požádat někoho kvalifikovaného, aby důkazy posoudil.

Tři možné odpovědi

„Shoda“, pokud se kopie shodují. „Rozdíl“, pokud se liší. „Zatím nevím“, pokud chybí odkaz nebo jiný důkaz.

Můžete offline zkontrolovat, zda vaše zařízení již obsahuje příslušná data, referenční údaje a nástroje. Ztracený originál lze obnovit pouze v případě, že existuje jeho kopie.

Chyby, které jsme se naučili rozpoznávat

Šest zjištění z vědecké zprávy ze dne 25. listopadu. Každý výsledek testu se vztahuje k verzi uvedené v této zprávě.

F1 Limit 95 % může pokrývat menší část

Co jsme zjistili

V tomto příkladu pokrývá horní mez vypočítaná lineární metodou 86,51 % hodnot, ačkoli její nominální úroveň činí 95 %.

Jak to zkontrolovat

Na straně 7 je uvedeno, jak vypočítat pokrytí pro reciprokou hodnotu proměnné s normálním rozdělením, jejíž střední hodnota je 1 a směrodatná odchylka 0,3.

Co to neprokazuje

Výsledek platí pro tento model a tyto mezní hodnoty. Pro jiná měření je třeba provést nový výpočet.

Pro toto vydání byla hodnota F1 přepočítána. Tým tento výpočet zopakoval také 24. listopadu.

F2 Účtenka a velikost šarže

Co jsme zjistili

U některých šarží nebylo možné na dokladu vystaveném ve zkoumané verzi ověřit, kolik položek bylo obsaženo.

Jak to zkontrolovat

Při kontrole by mělo být zaznamenáno, kolik položek dorazilo a jaké důkazy prokazují shodu tohoto počtu s účtenkou.

Co to neprokazuje

To omezuje informace, které účtenka o dané šarži poskytuje. Zpráva neuvádí žádné narušení SHA-256.

Tým 24. listopadu provedl opakovanou kontrolu F2. V poznámce byl tento problém zaznamenán jako nevyřešený ve verzi 3.0.0.

F3 Když zmizí rozdíl v datech

Co jsme zjistili

Uložená podoba ztratila rozlišení, které bylo přítomno ve zdrojových datech. Z účtenky již nebylo možné toto rozlišení zjistit.

Jak to zkontrolovat

Při kontrole by tým měl být schopen prokázat, že záznam zachovává všechny relevantní rozdíly obsažené v originálu.

Co to neprokazuje

Při znázornění dat došlo ke ztrátě tohoto rozdílu. Test neprokazuje kryptografickou kolizi.

Tým 24. listopadu znovu zaznamenal chybu F3. V poznámce byla tato chyba ve verzi 3.0.0 označena jako nevyřešená.

Kdy by se systém měl zastavit

Šest zjištění z vědecké zprávy ze dne 25. listopadu. Každý výsledek testu se vztahuje k verzi uvedené v této zprávě.

F4 Dva ověřovatelé poskytli odlišné odpovědi

Co jsme zjistili

Z interní kontroly vyplývá, že jeden ověřovatel odhalil 7 z 9 změn a druhý odhalil všech 9.

Jak to zkontrolovat

Chcete-li vyhodnotit novou verzi, porovnejte její výsledky s očekávanými a uschovejte si záznamy o testech.

Co to neprokazuje

Na základě devíti příkladů nelze určit, kolik změn by bylo zjištěno v jiné sadě dokumentů.

Chyba F4 byla nahlášena v rámci interního přezkumu dne 24. listopadu. Tým test pro danou poznámku neopakoval.

F5 „OK“, i když pravidlo vyžadovalo zastavení

Co jsme zjistili

Tým identifikoval čtyři situace, ve kterých byla odpověď „OK“, ačkoli pravidlo vyžadovalo „VETO“.

Jak to zkontrolovat

Díky navrhované opravě přestalo 186 z 1 246 testovacích případů vracet výsledek „OK“. Žádný z nich se nezměnil na „OK“.

Co to neprokazuje

V poznámce byl popsán navrhovaný způsob opravy. Potvrzení jeho použití v produkčním prostředí vyžaduje doložení nainstalované verze a provedení příslušných testů.

O F5 bylo informováno 24. listopadu. Dne 25. listopadu bylo v poznámce uvedeno, že oprava ještě nebyla zveřejněna.

F6 Hodnota velmi blízko mezní hodnotě

Co jsme zjistili

V příkladu s mezními hodnotami 2 a 8 vedlo zaokrouhlení naměřené hodnoty na šest desetinných míst k jinému výsledku než při použití vyšší přesnosti.

Jak to zkontrolovat

Při kontrole by měla být uvedena použitá přesnost a dohodnuté pravidlo pro porovnání naměřené hodnoty s mezní hodnotou.

Co to neprokazuje

Tolerance závisí na účelu a příslušném pravidle. Tento příklad nestanovuje tolerance pro jiná použití.

O F6 bylo informováno 24. listopadu. V době sepsání této poznámky se o referenčním pravidle ještě jednalo.

Zdraví a medicína

Nahlížení do zdravotní dokumentace

Tři fiktivní situace, ve kterých může někdo porovnat záznam s důvěryhodným referenčním zdrojem.

01 Očkovací průkaz

Porovnání může odhalit, že kopie byla pozměněna. K prokázání toho, že byla vakcína podána, jsou zapotřebí důkazy z klinického vyšetření. Účinnost vyžaduje vlastní důkazy.

02 Výsledek laboratorního vyšetření

Můžete si ověřit, zda se zpráva, kterou jste obdrželi, shoduje se zprávou uloženou v laboratoři. Výklad konkrétního výsledku by měl provést zdravotnický pracovník.

03 Záznam o dodržování chladicího řetězce

Můžete porovnat kopii protokolu s referenčními údaji. Kalibraci snímače a skutečné skladovací podmínky je třeba zkontrolovat každou zvlášť.

> **Senzor může zaznamenat nesprávnou hodnotu**
>
> Předpokládejme, že snímač zaznamená hodnotu 4 °C. Pokud je snímač vadný, může se skutečná teplota lišit, i když kopie odpovídá původnímu záznamu.

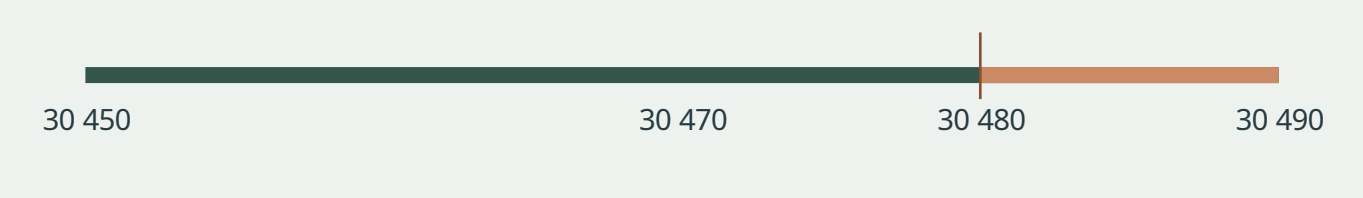
Vědecká poznámka popisuje Konfirmu jako výzkumný prototyp. Nejedná se o zdravotnický prostředek a nebyl navržen pro diagnostiku, léčbu ani pro rozhodování o konkrétních osobách.

Provozní bezpečnost a hlasování

Na platném účtenku může být uvedeno slovo „stop“

Laboratorní zkouška s fiktivním kontejnerem a hypotetickým limitem 30 480 kg.

Naměřená hmotnost 30 470 ± 20 kg



Rozsah hmotnosti v kilogramech · limit 30 480 kg
https://dpsindustrial.nl/konfirmu/guia/pesagem/?lang=cs

Rozsah se pohybuje od 30 450 do 30 490 kg. Tolerance, vypočítaná jako rozdíl mezi limitem a hmotností, se pohybuje v rozmezí od −10 do +30 kg. Na horní hranici hmotnost překračuje limit o 10 kg. Doklad může obsahovat platný podpis (VALID), zatímco pravidlo vyžaduje zastavení (VETO).

A co hlasování?

Kontrola podepsaného zápisu z jednání může odhalit pozdější změny. Přístup voličů, přesnost sčítání hlasů i tajnost hlasování vyžadují každý své vlastní důkazy. Potvrzení, z něhož je patrná volba dané osoby, může ohrozit tajnost hlasování.

Kdo může tuto operaci schválit?

Díky podpisu můžete dokument ověřit. Odpovědné osoby na základě pravidel a údajů týkajících se dané operace rozhodnou, zda v ní pokračovat.

Kontroly na vašem zařízení

Jak si to ověřit sami

Pomocí důvěryhodného referenčního souboru můžete soubor porovnat. Můžete také zopakovat výpočet pokrytí uvedený na straně 3.

V poznámce je uvedena verze jádra Pythonu 3.0.0, revize 90b3968, ze dne 24. listopadu 2026. Kód je licencován pod licencí EUPL-1.2.

Oficiální repozitář kódu

Funkce SHA-256 v jádru jazyka Python, jak je uvedeno v poznámce
`529098c652ee8234960d69383e308f60db6a5df8ea6bdae578b538eb806e80cf`

Umístěte manifest vydání a příslušné soubory do jedné složky. Spusťte příkaz odpovídající vašemu systému.

```
sha256sum -c SHA256SUMS.txt        # Linux
shasum -a 256 -c SHA256SUMS.txt    # macOS
```

Tým uvedl 62 souborů, u nichž byla nalezena shoda, 247 vlastních kontrol a 10 testovaných sad pravidel v systému Linux s Pythonem 3.13. Tyto údaje se vztahují k uvedené revizi.

F1 · Zopakujte výpočet v jazyce Python

```
from statistics import NormalDist
X, Z = NormalDist(1, 0.3), NormalDist()
u = 1 + Z.inv_cdf(.95) * .3
print(u, X.cdf(0) + 1 - X.cdf(1/u))
print(X.cdf(1/.412) - X.cdf(1/1.588))
```

Pro Y = 1/X je horní mez 1,493456088 a pokrytí činí 86,51 %. Tuto mez splňují i záporné hodnoty X. Zveřejněné zaokrouhlené oboustranné meze 0,412 a 1,588 poskytují pokrytí 89,14 %.

Pokrytí představuje pravděpodobnost v rámci tohoto modelu. Poznámka odkazuje na JCGM 100 a 101 týkající se šíření nejistoty.

Otevřete aplikaci prohlížeče · 143 662 B

https://dpsindustrial.nl/konfirmu/app/

Otevřete funkci Porovnat soubory. Vyberte referenční soubor a druhou kopii, poté zvolte možnost A4 · Porovnat.

Compare files → Reference file → Second copy → A4 · Compare

Hodnota SHA-256 souboru HTML aplikace prohlížeče, ověřeno dne 26. listopadu 2026
`0a468ec23401f5125ee1e5399ef536b6fba88beab94771e4df6b7910c9723717`

Meze a další testy

Co zatím nevíme

Každý, kdo obdrží důkazní materiál, si jej může ověřit. To, co tento důkazní materiál prokazuje, závisí na referenčním standardu a použitém testu.

Kdo provedl tyto testy?

Zpráva ze dne 25. listopadu připisuje provedení testů danému týmu a jím použitým systémům umělé inteligence. Nezávislé přezkoumání by mělo určit verzi, zopakovat testy a zaznamenat výsledky, včetně případných nesrovnalostí.

Jaké uznání je zdokumentováno?

Kontrola shody s 295 požadavky normy ECSS-Q-ST-80C Rev.2 byla provedena formou vlastního posouzení. V záznamech i-DEPOT č. 162925 a 164391 je uvedeno, co a kdy bylo uloženo. Kvalita výrobku vyžaduje samostatné posouzení.

Co lze pomocí časového razítka určit?

Chronolex umožňuje čtenářům ověřit integritu záznamu. V poznámce se uvádí, že tato bezplatná veřejná služba pro časové razítko neposkytuje žádnou záruku právní účinnosti. Stále je třeba předložit důkaz o tom, že k události skutečně došlo.

Našli jste nesrovnalost?

Zaznamenejte verzi, očekávaný výsledek a to, co jste pozorovali. Podrobnosti zašlete na adresu

admin@dpsindustrial.nl

Naskenujte nebo klepněte pro otevření

Oficiální webové stránky DPS

Sada s 12 sektory

V archivu ZIP otevřete složku Exemplos/09-Shipping/. Porovnejte soubory 01-original.txt a 02-copia.txt v aplikaci: ve fiktivních záznamech je uvedeno 24 a 29 krabic. Příklad vážení najdete na straně 6.

Primární zdroj · Vědecká poznámka ze dne 25. listopadu 2026

Konfirmu_Scientific_Note.pdf · 88 212 B · SHA-256

`884fde70000fa68dccdb4b6527da7a1bce8a7737b3f44c03340f182ae6100f88`

DPS Industrial & Maritime Services · Konfirmu · KVK 42005886

Enschede, Nizozemsko