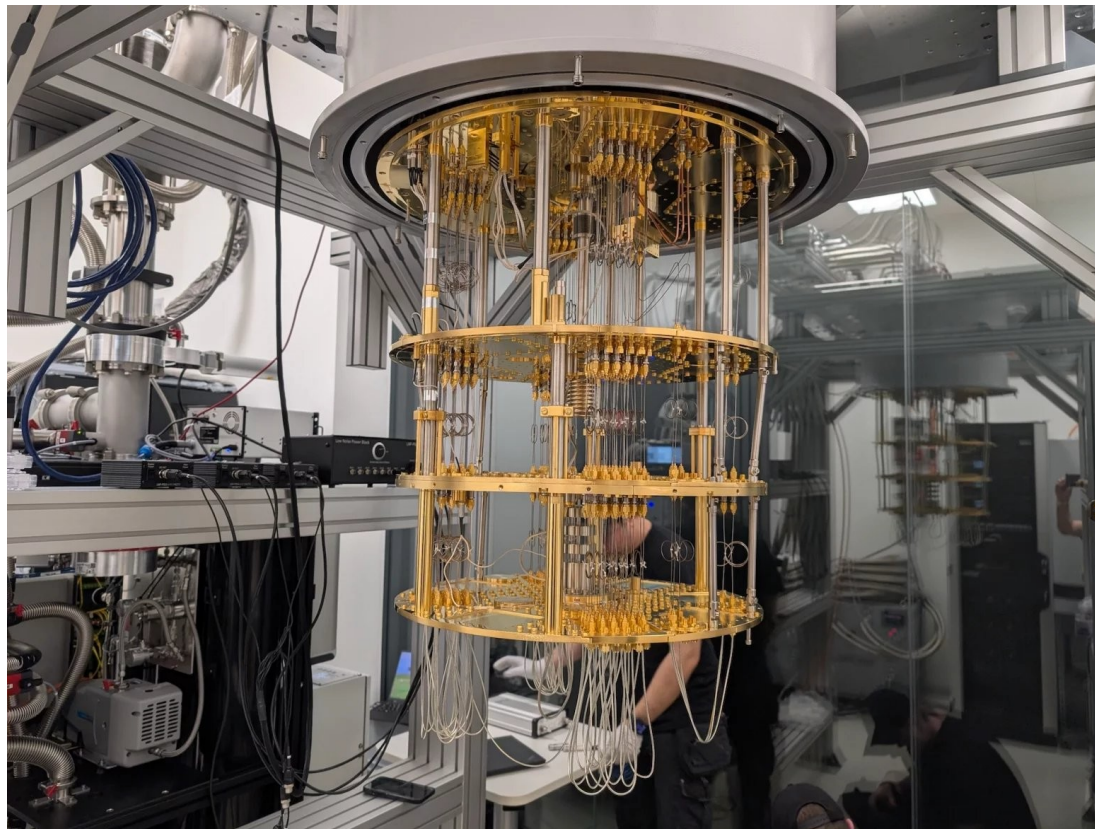


MojID jako první postkvantová digitální identita?

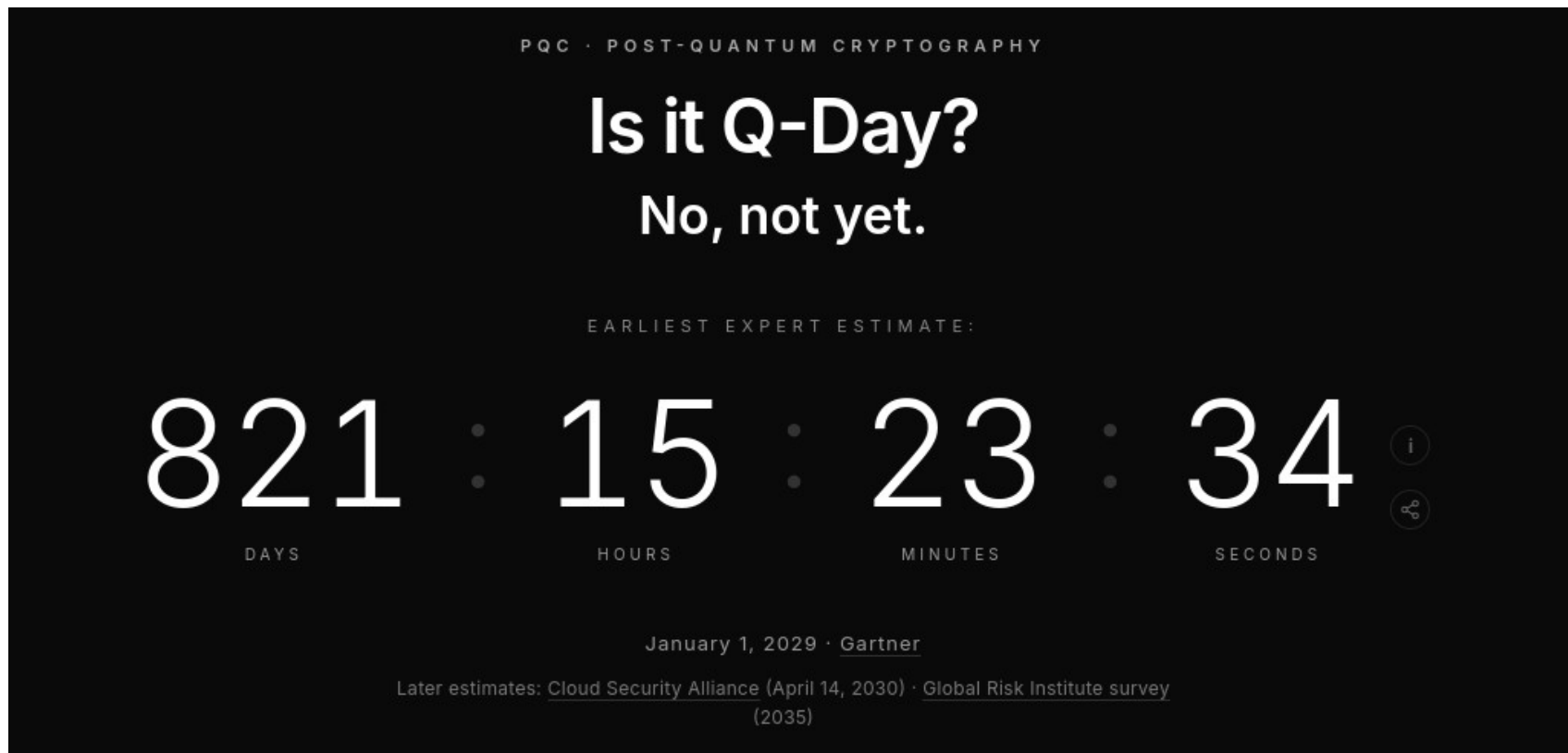
Jaromír Talíř • 3. 10. 2026

cz.nic | SPRÁVCE
DOMÉNY CZ

Kvantové počítače



Den Q - <https://qdayiscoming.com/>



Poskvantová (PQ) kryptografie

- Postkvantové šifrování
 - Chrání už nyní – „Harvest now, decrypt later“
 - ML-KEM / FIPS-203 – standard pro výměnu klíčů
- Postkvantová autentizace
 - ML-DSA / FIPS-204 nebo SLH-DSA / FIPS 205 – standardy pro digitální podpis
 - Kompozitní ML-DSA
 - Merkle Tree Certificates
 - KEM autentizace

MojeID

- Služba digitální identity provozovaná sdružením CZ.NIC
- Nejmodernější autentizační metody
 - FIDO / Passkeys odolné proti phishingu včetně systémových klíčů
 - Mobilní autentizační aplikace MojeID Klíč
- Nejširší spektrum služeb
 - Komerční sektor
 - Státní služby
 - Použití v Evropě v rámci eIDAS
- Nejvyšší úroveň zabezpečení podle eIDAS



Oblasti kryptografie v autentizační službě

TLS

Autentizační prostředky

MojeID
Klíč

FIDO
Passkeys

Autentizační protokoly

OIDC

SAML 2.0

PQ v TLS

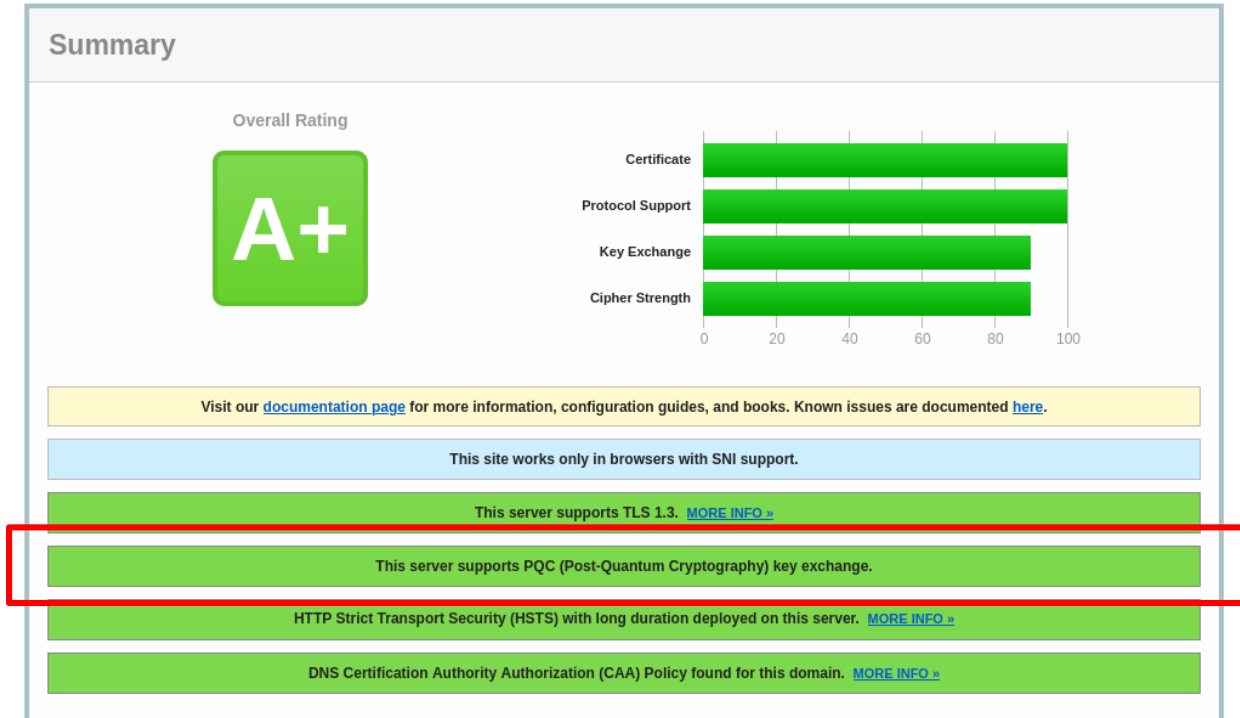
- NGINX - <https://blog.nginx.org/blog/pqc-nginx>
- Debian 13 + zapnutí v konfiguraci
 - Hybridní schéma X25519MLKEM768
- V srpnu konečně vyšlo RFC10024 - *Post-Quantum Traditional (PQ/T) Hybrid Key Agreement Mechanisms for TLS 1.3*
- Většina prohlížečů má podporu implementovanou
- Zatím rozhodně není dominantní na straně služeb

Distribution/ Release	OpenSSL Version Shipped	PQC Available?	Notes
Debian 13 "Trixie"	3.5.x	✓	Current stable release
Debian 12 "Bookworm"	3.0.x	✗*	Current oldstable release – Workaround available
Alpine Linux 3.22	3.5.x	✓	Latest Alpine release
Alpine Linux 3.21	3.3.x	✗	Previous Alpine release
Ubuntu 22.04 (LTS)	3.0.x	✗*	Old LTS – Workaround available
Ubuntu 24.04 (LTS)	3.0.x	✗*	Current LTS – Workaround available
Alma/Rocky/RHEL 10.1	3.5.x	✓	Latest RedHat 10.1 family release
Alma/Rocky/RHEL 10	3.2.x*	✗	Initial RedHat 10 family release – Workaround available
Suse Linux Enterprise (SLES) 16	3.5.x	✓	Latest SLES release

PQ v TLS - <https://www.ssllabs.com/ssltest/>

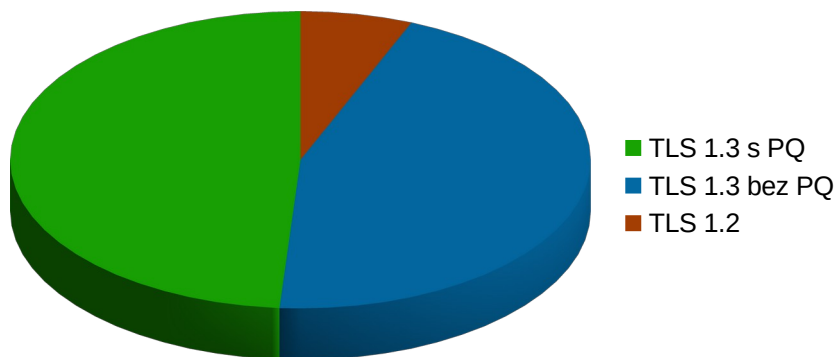
You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [mojeid.cz](#) > 2001:1488:0:4:0:0:0:4

SSL Report: [mojeid.cz](#) (2001:1488:0:4:0:0:0:4)



PQ v TLS - statistiky

MojID



Cloudflare

<https://radar.cloudflare.com/post-quantum>

Post-quantum encryption adoption

Post-quantum encrypted share of HTTPS request traffic ? ⚙️ ...

Traffic type All traffic ▾



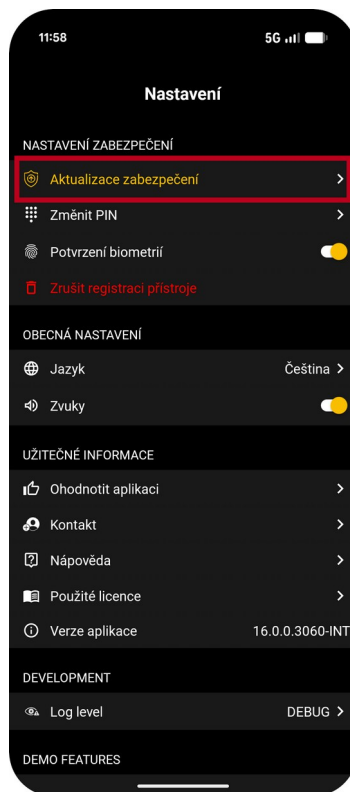
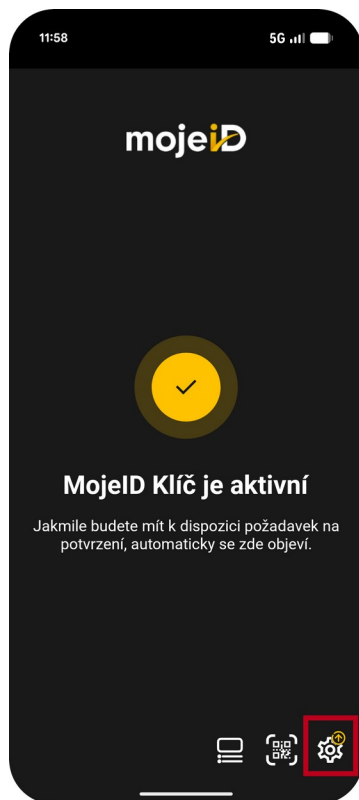
💡 This chart shows the percentage of HTTPS requests using post-quantum key exchange over time. Cloudflare has enabled hybrid post-quantum key agreement on all domains served through its network, including this one. Adoption depends on both client (browser) and server support.

MojID Klíč

- Máme pod kontrolou obě strany komunikace (aplikace na zařízení a backend)
- Vyvíjí pro nás česká společnost Wultra - <https://www.wultra.com/>
- Z velké části open source - <https://github.com/wultra>
- Při přechodu na PQ nutnost aktivního zásahu uživatele pro výměnu klíče
 - K tomu je třeba vždy zadat PIN
- K dispozici od verze aplikace 16.0.0
 - Android vydán před dvěma týdny
 - iOS příští týden



MojeID Klíč



MojeID Klíč

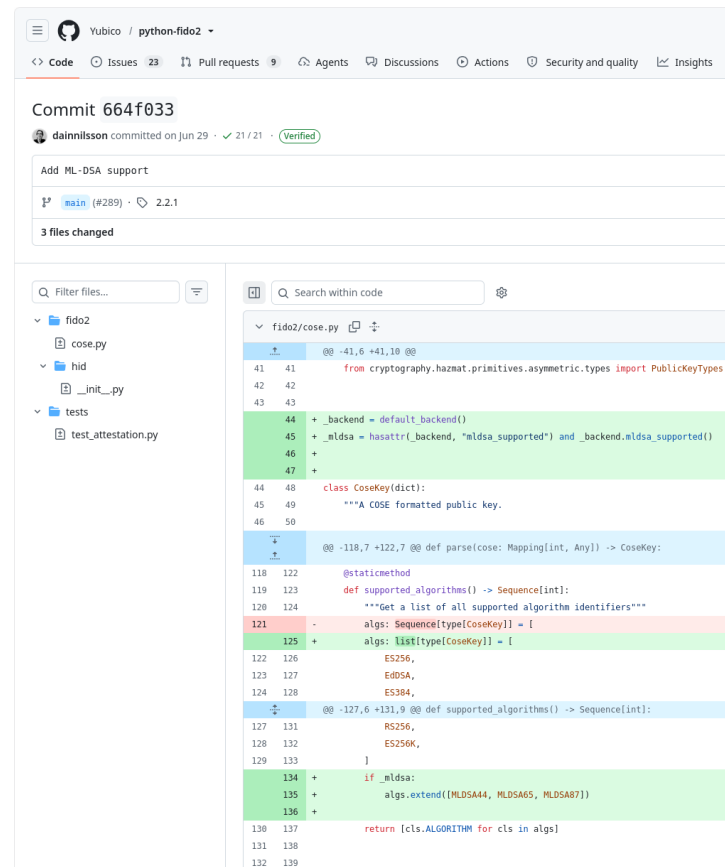
- Dříve se používal NIST P-256
- Novější protokol používá:
 - Pro výměnu klíčů kombinace ECDH s P-384 a ML-KEM 768
 - Pro podepisování ECDSA s P384 a ML-DSA-65 (momentálně v MojeID nevyužíváme)
- Protokol umožňuje v budoucnu přejít na čistě PQ algoritmy
- První použití PQ v mobilních autentizačních aplikacích

FIDO bezpečnostní klíče / Passkeys

- Nemáme pod kontrolou obě strany komunikace, pouze backend. Klíče si pořizuje uživatel vlastní
- Použité protokoly CTAP2 + WebAuthn jsou kryptoagilní, tzn. v zásadě jsou schopné fungovat s libovolným protokolem
 - V květnu vyšlo RFC 9964, která přidává ML-DSA do globálních rejstříků u IANA
- Pracovní skupiny FIDO Alliance pracují na standardizaci dalších prvků jako např. atestačního protokol

Yubico

- Na straně MojeID používáme jako backend knihovnu python-fido2
 - Podporu ML-DSA přidána v nejnovější verzi 2.1:1 letos v červnu
 - Máme nasazeno na testovacím prostředí
- Yubico je zároveň první výrobce, který demonstroval prototyp s ML-DSA
- Tyto klíče budou nejspíš dostupné již v příštím roce



The screenshot shows a GitHub commit titled "Add ML-DSA support" by user dainnilsson, committed on June 29. The commit message is "Add ML-DSA support" and the commit hash is 664f033. The commit is verified and includes a pull request #289. The commit shows 3 files changed. The file explorer on the left shows the directory structure: fido2, cose.py, hid, _init_.py, tests, and test_attestation.py. The code editor on the right shows the file fido2/cose.py. The code includes imports for PublicKeyTypes from cryptography.hazmat.primitives.asymmetric.types. It defines a class CoseKey and a function parse. The code also includes a list of supported algorithms and a function supported_algorithms. The code is highlighted with green and blue background colors.

```
41 41 from cryptography.hazmat.primitives.asymmetric.types import PublicKeyTypes
42 42
43 43
44 + _backend = default_backend()
45 + _mldsa = hasattr(_backend, "mldsa_supported") and _backend.mldsa_supported()
46 +
47 +
44 48 class CoseKey(dict):
45 49     """A COSE formatted public key.
46 50
47 51
48 52
49 53
50 54
51 55
52 56
53 57
54 58
55 59
56 60
57 61
58 62
59 63
60 64
61 65
62 66
63 67
64 68
65 69
66 70
67 71
68 72
69 73
70 74
71 75
72 76
73 77
74 78
75 79
76 80
77 81
78 82
79 83
80 84
81 85
82 86
83 87
84 88
85 89
86 90
87 91
88 92
89 93
90 94
91 95
92 96
93 97
94 98
95 99
96 100
97 101
98 102
99 103
100 104
101 105
102 106
103 107
104 108
105 109
106 110
107 111
108 112
109 113
110 114
111 115
112 116
113 117
114 118
115 119
116 120
117 121
118 122
119 123
120 124
121 125
122 126
123 127
124 128
125 129
126 130
127 131
128 132
129 133
130 134
131 135
132 136
133 137
134 138
135 139
136 140
137 141
138 142
139 143
140 144
141 145
142 146
143 147
144 148
145 149
146 150
147 151
148 152
149 153
150 154
151 155
152 156
153 157
154 158
155 159
156 160
157 161
158 162
159 163
160 164
161 165
162 166
163 167
164 168
165 169
166 170
167 171
168 172
169 173
170 174
171 175
172 176
173 177
174 178
175 179
176 180
177 181
178 182
179 183
180 184
181 185
182 186
183 187
184 188
185 189
186 190
187 191
188 192
189 193
190 194
191 195
192 196
193 197
194 198
195 199
196 200
197 201
198 202
199 203
200 204
201 205
202 206
203 207
204 208
205 209
206 210
207 211
208 212
209 213
210 214
211 215
212 216
213 217
214 218
215 219
216 220
217 221
218 222
219 223
220 224
221 225
222 226
223 227
224 228
225 229
226 230
227 231
228 232
229 233
230 234
231 235
232 236
233 237
234 238
235 239
236 240
237 241
238 242
239 243
240 244
241 245
242 246
243 247
244 248
245 249
246 250
247 251
248 252
249 253
250 254
251 255
252 256
253 257
254 258
255 259
256 260
257 261
258 262
259 263
260 264
261 265
262 266
263 267
264 268
265 269
266 270
267 271
268 272
269 273
270 274
271 275
272 276
273 277
274 278
275 279
276 280
277 281
278 282
279 283
280 284
281 285
282 286
283 287
284 288
285 289
286 290
287 291
288 292
289 293
290 294
291 295
292 296
293 297
294 298
295 299
296 300
297 301
298 302
299 303
300 304
301 305
302 306
303 307
304 308
305 309
306 310
307 311
308 312
309 313
310 314
311 315
312 316
313 317
314 318
315 319
316 320
317 321
318 322
319 323
320 324
321 325
322 326
323 327
324 328
325 329
326 330
327 331
328 332
329 333
330 334
331 335
332 336
333 337
334 338
335 339
336 340
337 341
338 342
339 343
340 344
341 345
342 346
343 347
344 348
345 349
346 350
347 351
348 352
349 353
350 354
351 355
352 356
353 357
354 358
355 359
356 360
357 361
358 362
359 363
360 364
361 365
362 366
363 367
364 368
365 369
366 370
367 371
368 372
369 373
370 374
371 375
372 376
373 377
374 378
375 379
376 380
377 381
378 382
379 383
380 384
381 385
382 386
383 387
384 388
385 389
386 390
387 391
388 392
389 393
390 394
391 395
392 396
393 397
394 398
395 399
396 400
397 401
398 402
399 403
400 404
401 405
402 406
403 407
404 408
405 409
406 410
407 411
408 412
409 413
410 414
411 415
412 416
413 417
414 418
415 419
416 420
417 421
418 422
419 423
420 424
421 425
422 426
423 427
424 428
425 429
426 430
427 431
428 432
429 433
430 434
431 435
432 436
433 437
434 438
435 439
436 440
437 441
438 442
439 443
440 444
441 445
442 446
443 447
444 448
445 449
446 450
447 451
448 452
449 453
450 454
451 455
452 456
453 457
454 458
455 459
456 460
457 461
458 462
459 463
460 464
461 465
462 466
463 467
464 468
465 469
466 470
467 471
468 472
469 473
470 474
471 475
472 476
473 477
474 478
475 479
476 480
477 481
478 482
479 483
480 484
481 485
482 486
483 487
484 488
485 489
486 490
487 491
488 492
489 493
490 494
491 495
492 496
493 497
494 498
495 499
496 500
497 501
498 502
499 503
500 504
501 505
502 506
503 507
504 508
505 509
506 510
507 511
508 512
509 513
510 514
511 515
512 516
513 517
514 518
515 519
516 520
517 521
518 522
519 523
520 524
521 525
522 526
523 527
524 528
525 529
526 530
527 531
528 532
529 533
530 534
531 535
532 536
533 537
534 538
535 539
536 540
537 541
538 542
539 543
540 544
541 545
542 546
543 547
544 548
545 549
546 550
547 551
548 552
549 553
550 554
551 555
552 556
553 557
554 558
555 559
556 560
557 561
558 562
559 563
560 564
561 565
562 566
563 567
564 568
565 569
566 570
567 571
568 572
569 573
570 574
571 575
572 576
573 577
574 578
575 579
576 580
577 581
578 582
579 583
580 584
581 585
582 586
583 587
584 588
585 589
586 590
587 591
588 592
589 593
590 594
591 595
592 596
593 597
594 598
595 599
596 600
600 604
```

OpenID Connect

- Hlavní problémy shrnuje [blogpost](#) vydaný před 2 týdny
 - Velikost podpisů a maximální velikost cookies ~4kB
 - Existující chyby v knihovnách – např. knihovna zahodí data pokud obsahují neznámý algoritmus
 - Obecně nízká podpora PQ algoritmů v knihovnách
 - Lepší podpora ve standardech pro výběr algoritmu při každém dotazu
- Chybějící podpora pro kompozitní schémata:
 - <https://datatracker.ietf.org/doc/draft-ietf-jose-pq-composite-sigs/>

SAML 2.0

- Minimální posun ve standardizaci
 - <https://datatracker.ietf.org/doc/html/draft-eastlake-rfc9231bis-xmlsec-uris-09>
- Chybí podpora v knihovnách
 - pysaml2 a xmlsec1
- SAML 2.0 používáme primárně pro komunikaci s NIA (Identita Občana)
 - Je vysoce pravděpodobné, že dříve zmigrujeme na OpenID Connect

Oblasti kryptografie v autentizační službě

TLS

Autentizační prostředky

MojID
Klíč

FIDO
Passkeys

Autentizační protokoly

OIDC

SAML 2.0

Postkvantový posun v Praze?

- Workshop na téma postkvantové autentizace v Praze
- Organizuje Internet Architecture Board
- Termín 11.-12. října
- CFP bylo do 11. září
- Workshop zřejmě nebude otevřený pro veřejnost
- <https://www.iab.org/announcements/call-for-papers-iab-workshop-on-accelerating-the-deployment-of-post-quantum-authentication-pqws/>

Závěr

- Digitální identita je o důvěře
- Služba MojID se vždy snaží v tomto smyslu jít příkladem
- V tomto roce probíhá hodně změn a příští rok asi nebude jiný
- Postkvantový vývoj budeme nadále sledovat a adekvátně reagovat

Děkuji vám za pozornost!

jaromir.talir@nic.cz