.news 14 2010 CZ.NIC

Vážení čtenáři,

léto nás už opouští a my opět, někdo pomaleji, někdo rychleji, usedáme k pracovním stolům a monitorům našich počítačů. V tomto čísle našeho čtvrtletníku bychom vás rádi vrátili do druhého čtvrtletí tohoto roku a připomenuli vám aktivity a projekty, které se udály v našem sdružení ještě před letními měsíci.

Na úvod bych se rád zastavil u červnové konference Internet a Technologie 10, kterou CZ.NIC připravil už potřetí. Letošní program jsme rozdělili do dvou dnů. V krásné budově Národní technické knihovny v pražských Dejvicích se v Ballingově sále sešlo každý den více než 100 zájemců o internetové technologie a novinky s nimi spojenými. On-line přenos potom sledovalo více než 1000 lidí u svých počítačů. Hlavním tématem byl letos internetový protokol verze šest. Mezi těmi, kteří se postavili k mikrofonu, byli i odborníci na slovo vzatí, jakými jsou například Jiří Peterka nebo Pavel Satrapa. Více se dozvíte z fotoreportáže na druhé straně.

Jarní měsíce byly bohaté i na dobré zprávy spojené s CZ.NIC a jeho prezentací v zahraničí. Velikou radost máme všichni z ocenění LINX Awards 2010, které je udělováno nejvýše jednou za rok. Letos si tuto významnou mezinárodní cenu odnesl projekt BIRD, na němž pracují zaměstnanci našich laboratoří. Druhá dobrá zpráva přišla až ze Spojených států a týká se kolegy Ondřeje Surého, vedoucího Laboratoří CZ.NIC. Ondřej byl totiž jmenován do prestižní skupiny odborníků, kteří mají dohlížet na fungování technologie DNSSEC na nejvyšší, kořenové úrovni. Více si o Ondřejově funkci Recovery Key Share Holder můžete přečíst na páté straně.

Tento .news má oproti tomu předchozímu zase pět stránek. Proto už vás nebudu zdržovat od dalšího čtení.

Ondřej Filip
*Výkonný ředitel sdružení CZ.NIC*

# České internetové stránky nejsou připraveny na připojení přes IPv6

Podle současných odhadů zmizí za rok v registru IANA veškeré volné bloky IP adres využívajících stávající protokol IPv4. Během první poloviny roku 2012 pak IP adresy postupně dojdou i na regionální úrovni a u jednotlivých poskytovatelů internetového připojení, kteří adresy přidělují koncovým uživatelům. Pokud se včas neuskuteční přechod na protokol IPv6, hrozí vážné problémy s dalším rozšiřováním internetu. Sdružení CZ.NIC proto vyzývá subjekty z řad poskytovatelů internetových služeb, aby se v zájmu bezproblémové budoucnosti českého internetu začaly touto záležitostí odpovědně zabývat. Z internetových stránek s koncovkou .CZ bylo totiž k 30. červnu přístupných přes internetový protokol verze šest pouze jejich zlomek – necelých 12 tisíc (11 813).

IP adresy představují základní stavební prvek internetu, protože bez nich by nebylo propojení počítačů do globální sítě možné. Verze protokolu IPv4 vznikla již v 70. letech 20. století a nabídla kapacitu pro připojení méně než čtyř miliard počítačů. Již několik let je dostupné řešení rapidního úbytku IP adres verze čtyři a to v podobě nové verze internetového protokolu – IPv6. Ten poskytuje prakticky nevyčerpatelnou zásobu nových adres (2^128 – v číselném vyjádření zhruba tři a třicet osm nul), stále ale zůstává nevyužit.

Dnes z původního objemu IPv4 adres zbývá pouhých pět procent a jejich počet klesá rychleji, než se předpokládalo ještě před rokem. Rok 2012 se může zdát daleko, ale kompletní přechod na IPv6

**IPv6**

je záležitost let – co do technologické složitosti jde o proces podobný například digitalizaci televizního vysílání. Lze to stihnout, ale je třeba začít s nasazením řešení co nejdříve, a to ve vzájemné součinnosti zejména poskytovatelů připojení a obsahu, státní správy, ale i koncových uživatelů.

## HOSTILI JSME RIPE 60

Od 3. do 7. května hostil CZ.NIC setkání zástupců evropských doménových registrů, internetových odborníků a zaměstnanců významných internetových společností. Hlavními tématy letošní konference byly IPv6, DNS nebo ENUM.

VÍCE

## MEZINÁRODNÍ OCENĚNÍ PRO NAŠE VÝZKUMNÍKY

Jedno z největších internetových peeringových center na světě, londýnský LINX, udělil v květnu významné ocenění LINX Awards 2010 českému projektu BIRD, za jehož rozvojem stojí zaměstnanci Laboratoří CZ.NIC.

VÍCE

## CZ.NIC ZAVEDL TECHNOLOGII NSEC3

4. června byl zveřejněn plán zavádění technologie NSEC3 do domény .CZ a ENUM. Od tohoto data tak mohou ISP v České republice vyzkoušet na svých DNS resolverech tuto novou verzi technologie DNSSEC.

## VÍTE, ŽE

...registr české národní domény obsahuje již více než 700 tisíc domén s koncovkou .CZ? doména s pořadovým číslem 700 tisíc byla zaregistrována 4. srpna v 10:22 hodin. Průměrný měsíční přírůstek domén .CZ se tak i nadále pohybuje okolo 10 tisíc. Podle statistik CZ.NIC mezi držiteli domén převažují s 87procentním podílem muži a 52procentním podílem firmy a právnické osoby. Doménová jména s koncovkou .CZ nejčastěji obsahují osm znaků.

# Konference Internet a Technologie 10 přinesla řadu zajímavých přednášek a vystoupení

Na začátku června (7. a 8. června) se v Národní technické knihovně v pražských Dejvicích uskutečnil již třetí ročník odborné konference s názvem Internet a Technologie 10. Setkání českých specialistů z oblasti internetu a internetových technologií organizoval i tentokrát správce české domény nejvyšší úrovně. Příspěvky a diskuze se opět věnovaly aktuálním tématům internetového světa, například DNS (podpis kořenové zóny, DNSSEC), doménové bezpečnosti nebo open source. Hlavní pozornost organizátorů si ale tentokrát zasloužila témata spojená s protokolem IPv6. Protože jsme chtěli internetovým tématům věnovat více času a prostoru, rozhodli jsme se letos uspořádat naši konferenci ve dvou dnech. Pro zájemce z řad internetové komunity, novinářů a studentů byly podle všeho největším lákadlem diskuse věnované IPv6. Ve dvou blocích měli návštěvníci v sále i ti, kteří sledovali vše u svých počítačů,

možnost vidět jak odborné prezentace, tak příspěvky se zkušenostmi firem nebo slyšet názory odborníků z praxe. Zajímavá byla jistě také panelová diskuse, v níž vystoupili mimo jiné zástupci největšího českého poskytovatele internetových služeb (Seznam.cz), největšího českého ISP (Telefónica O2) nebo Ministerstva průmyslu a obchodu České republiky. Pozornost si ale jistě zasloužily i jiné přednášky. Z nich si dovolíme vybrat například příspěvky kolegů Ondřeje Surého, který mluvil o podepisování kořenové zóny technologií DNSSEC, a Jaromíra Talíře; ten představil 6to4 relay router pro lepší připojení českých uživatelů internetu.

V průběhu prvního dne konference Internet a Technologie 10 proběhlo také vyhlášení výsledků pátého ročníku ankety Czech Open Source 2010, kterou již tradičně pořádal odborný informační server Root.cz.
Stejně jako v loňském roce byla i letos konference Internet a Technologie 10 streamovaná. Zájemci ji tak mohli sledovat na stránkách akce a nově po oba dva dny také na webu hlavního mediálního partnera serveru Root.cz. On-line přenos nakonec vidělo přes 1000 zájemců. Více než 100 lidí potom sledovalo na místě jednotlivá vystoupení každý den.
Pokud jste neměli možnost vidět vše, co jste chtěli, nebo máte zájem oživit si atmosféru letošní konference, na internetových stránkách najdete jednotlivé prezentace ve formátu PDF a videa z každého vystoupení.
Mediálními partnery letošního ročníku konference byly servery Root.cz (hlavní mediální partner), Lupa.cz, Zdroják.cz, Linuxexpres.cz, měsíčník openMagazín a Český rozhlas Leonardo.

# LINX Awards získal letos projekt BIRD

Jedno z největších internetových peeringových center na světě, londýnský LINX, udělil ocenění LINX Awards 2010 českému projektu BIRD, za jehož rozvojem stojí zaměstnanci Laboratoří CZ.NIC. BIRD je open source software, který v současnosti používá jako route server několik největších světových peeringových center – kromě londýnského LINXu, také například americký PAIX, moskevský MSK-IX, či frankfurtský DE-CIX. LINX ocenění uděluje nejvýše jednou ročně a to vybrané osobnosti nebo organizaci, která se výrazným způsobem podílela na rozvoji přímo centra LINX nebo celého odvětví propojovacích center.

Z ocenění máme velikou radost. LINX Awards platí v rámci celosvětové internetové komunity za jedno z nejrespektovanějších ohodnocení. Představuje velké vyznamenání pro práci jak Laboratoří CZ.NIC, tak i českého propojovacího centra NIX.CZ, které bylo mezi prvními peeringovými centry na světě, jež jej nasadilo jako routovací server.

Open source routovací démon BIRD vznikl na půdě Matematicko-fyzikální fakulty Univerzity Karlovy jako seminární práce tří studentů oboru Informatika. Jedním ze zakladatelů projektu BIRD je právě také Ondřej Filip. K významnému rozvoji projektu došlo před více než rokem, kdy se BIRD stal jednou z prvních aktivit výzkumného a vývojového centra sdružení CZ.NIC – Laboratoří CZ.NIC.

# Nový Řád pro řešení soudních sporů týkajících se domén .CZ

Předvídatelný sazebník poplatků Rozhodčímu soudu, možnost zapojit do sporu tři rozhodce a lepší on-line platforma pro řešení sporů – to jsou hlavní novinky v Řádu pro řešení sporů o domény .CZ. Jeho novou verzi vydal Rozhodčí soud při Hospodářské komoře České republiky a Agrární komoře České republiky v půlce června. Na změnách v řádu se výrazně podílel správce české národní domény .CZ.

Pravděpodobně nejdůležitější změnu představuje nový systém pro výpočet poplatku za řízení. Dosud se poplatek určoval stejně jako u jiných majetkoprávních sporů – procentní sazbou z hodnoty předmětu sporu. Poplatek tak mohl dosáhnout až do výše jednoho milionu korun.

U internetové domény je stanovení hodnoty velmi problematické a nepředvídatelnost poplatku byla hlavním argumentem, proč jinak rychlé a jednoduché rozhodčí řízení k řešení doménových sporů nevyužívat. Nový sazebník vychází z počtu doménových jmen, jichž se spor týká, a z počtu zúčastněných rozhodců. Výpočet nákladů na řízení je tedy zcela transparentní a žalobci se nemusí obávat nepříjemného překvapení způsobeného odlišným názorem rozhodce na hodnotu domény.

Sazebník je k dispozici na internetových stránkách soudu.

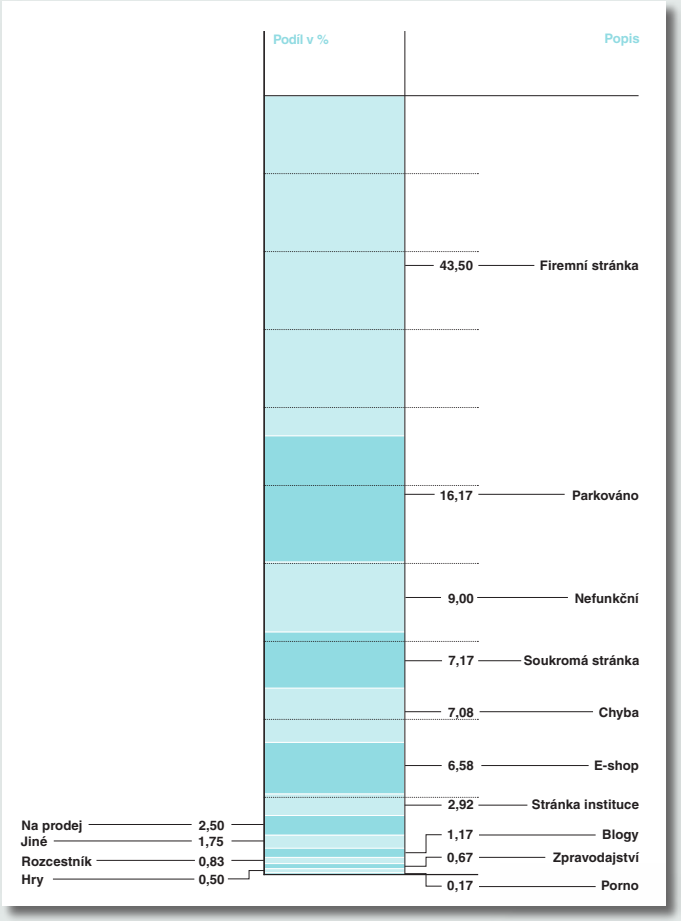
Jakákoli ze stran sporu si nyní může určit, zda spor rozhodne jeden, nebo tři rozhodci. Doposud to byl pouze jeden rozhodce určený předsedou Rozhodčího soudu. Podmínkou takové možnosti je souhlas druhé strany sporu a také uhrazení vyšších nákladů spojených s řízením.

Rozhodčí soud také pro řešení sporů používá novou on-line platformu, která se osvědčila u řešení sporů o evropskou doménu .EU. Oproti té stávající, která byla nasazena v roce 2006, přináší řadu vylepšení, která řízení celkově zjednodušují a zpřehledňují. Přístup k této platformě je možný přes adresu https://domeny.soud.cz/.

# První Domain Report je na světě

Soubor statistik spojený s doménou .CZ, který vydal CZ.NIC na konci května, přináší například informace o držitelích domén nebo o geografickém umístění domén .CZ v České republice, ale i ve světě. Dále se čtenáři z dokumentu dozví více o počtech domén .CZ od roku 2000 do roku 2009 nebo zajímavosti týkající se délky doménových jmen. Domain Report 2009 shrnuje data o doménách .CZ k 31. prosinci loňského roku.

Domain Report 2009, obsah webových stránek:



# 60. setkání RIPE se konalo v Praze

Konferenční centrum Marriott nabídlo od 3. do 7. května přednášky, diskuse, workshopy, veřejná setkání a uzavřené meetingy týkající se IPv4 a IPv6, DNS nebo ENUM. Hostitelem 60. konference RIPE bylo sdružení CZ.NIC. Naši kolegové byli i mezi přednášejícími a vystupujícími v jednotlivých diskusích; Ondřej Surý, vedoucí Laboratoří CZ.NIC, prezentoval o DNSSEC validátorech pro Firefox, Jaromír Talíř, technický ředitel CZ.NIC, představil mezinárodnímu publiku poznatky z budování DNS infrastruktury. Pro CZ.NIC a celou českou internetovou komunitu byla spolupráce na organizaci takovéhoto setkání významnou událostí. Jedno z témat, které bylo na konferenci v centru zájmu, byl podpis kořenové zóny technologií DNSSEC. Právě Česká republika je mezi prvními státy světa, které DNSSEC pro ochranu svých domén používají; v počtu zabezpečených domén jsme dokonce v tuto chvíli první na světě. Podle ředitele RIPE NCC Axele Pavlika představují setkání RIPE jedinečnou příležitost pro každého, kdo se zabývá správou internetových zdrojů a řízením internetu vůbec, aby se zapojil do diskuze o aktuálních problémech, něco se přiučil a setkal se s odborníky z oboru, vlád a technické komunity.


# Testování beta verze PostgreSQL v Laboratořích CZ.NIC

Jako každý rok se i letos komunita uživatelů PostgreSQL podílela na testování připravované nové verze této databáze. K tradiční neorganizované formě testování přibyl v roce 2010 jednodenní testovací maraton, v rámci kterého byla databáze podrobena intenzivnímu zkušebnímu provozu. Česká republika je po Japonsku a Spojených státech teprve třetí zemí, kde se testovací maraton uskutečnil. Organizátory veřejného testování byli správce české národní domény a Sdružení českých a slovenských uživatelů PostgreSQL.
V prostorách výukového centra Akademie CZ.NIC se příznivci PostgreSQL sešli v pátek 21. května v 19 hodin a pod vedením Pavla Stěhuleho z Laboratoří CZ.NIC, který se problematice PostgreSQL věnuje dlouhodobě, testovali až do časných ranních hodin.
Veřejné testování beta verze systému PostgreSQL přesně zapadá do aktivit, které bychom v naší Akademii CZ.NIC rádi viděli i do budoucna. Smyslem učebny vybavené tím nejmodernějším zařízením je vedle pořádání odborných školení také podpora internetových projektů, které slouží k rozvoji znalostí o aktuálních nebo právě začínajících projektech ze světa internetu a jeho technologií.

# Akademie CZ.NIC opět nabízí jedinečná školení

Akademie

Zkušení odborníci vás i v následujících měsících provedou školeními, která byste jinde hledali jen těžko. V Akademii CZ.NIC jsou až do konce listopadu naplánované například kurzy o kryptografii, BGP, DNSSEC, DNS nebo VoIP. Jestli si tedy myslíte, že by pro vás školení na tato témata mohla být užitečná, že by mohla prohloubit vaše znalosti nebo vás seznámit s něčím, o čem třeba jen tušíte a chtěli byste se o tom dozvědět více, potom neváhejte a přihlaste se už teď!

## Nejbližší kurzy v Akademii CZ.NIC

**Problematika infrastruktury veřejných klíčů (PKI)**
15. – 16. září, přednášející: Pavel Vondruška

**Implementace IPv6**
5. října, přednášející: Emanuel Petr

**Směrovací protokol BGP**
12. října, přednášející: Emanuel Petr

**Metody a techniky ochrany proti spamu**
18. října, přednášející: Petr Hruška

**Principy a správa DNS**
3. – 4. listopadu, přednášející: Zbyněk Michl

**DNSSEC - zabezpečení DNS**
5. listopadu, přednášející: Matej Dioszegi

**Metody a techniky ochrany proti spamu**
9. listopadu, přednášející: Petr Hruška

Více informací o těchto a dalších kurzech, stejně jako přihlašovací formulář, jsou na internetové adrese www.nic.cz/akademie.

Publikováno na Root.cz

# Jak jsme podepsali kořenovou zónu

*(Ondřej Surý, vedoucí Laboratoří CZ.NIC, publikováno: 22. června 2010)*

Ve středu 16. června 2010 proběhla první DNSSEC KSK ceremonie, která se konala v chráněném telehousu v americkém městě Culpeper. Tento okamžik patří k jednomu z nejdůležitějších v historii DNS. Na závěr zazněla slova Winstona Churchilla: „Toto není konec, není to ani začátek konce, ale možná je to konec začátku."

Tato první ceremonie byla nejdelší ze všech a trvala celkem osm hodin. Takto dlouhý čas byl zapotřebí, protože se jednalo o úplně první ceremonii, kdy bylo nutné provést vše úplně od začátku.

ICANN má uvnitř telehousu vybudovanou samostatnou místnost, která má několik úrovní zabezpečení. Místnost je obehnána zdmi, které jsou vyztuženy ocelovým výpletem, aby nemohlo dojít ke snadnému probourání se dovnitř. Ke vstupu do místnosti je zapotřebí vstupní karta a kód, případně je možná i autentizace pomocí oční duhovky. Po vstupu do místnosti se ocitnete v menší kleci, kde je zapotřebí se zapsat do knihy návštěv; zde je nutné, aby vás doprovodil někdo se vstupní kartou a kódem dovnitř místnosti, kde jsou připraveny prostory pro účastníky ceremonie. Uvnitř místnosti je umístěna ještě druhá klec s dvěma trezory. Přístup do této klece podléhá ještě přísnějším bezpečnostním pravidlům: pro otevření dveří je zapotřebí dvou autorizovaných osob, dveře této klece mohou být otevřeny maximálně 30 sekund.

Uvnitř této klece jsou umístěny dva trezory s certifikací americké vlády pro přísně tajné dokumenty. Jedna zajímavost o trezorech – zámek má na sobě malý LCD displej, který zobrazuje číselnou kombinaci. Tento displej není napájen baterií, ale mechanicky točením kolečka na zámku, kterým se zároveň volí číselná kombinace. Trezory mají čidla otevření a pokud jsou otevřeny dveře od libovolného z trezorů, nelze otevřít vstupní dveře klece. Zabezpečena je i veškerá kabeláž v místnosti. Všechny kabely jsou vedeny v ocelových trubkách, aby nebylo možné jejich snadné narušení. Aby nebylo možné klec rozšroubovat, jsou všechny použité šrouby zalepeny epoxidovým lepidlem. Celá KSK ceremonie byla nahrávána několika kamerami a po celou dobu byl také sledován prostor trezorové klece.

Ceremonie se kromě zástupců komunity (CO a RKSH) účastnili také další lidé v různých rolích. Jako Master of Ceremony (MC) byl přítomen Rick Lamb za ICANN, který celou akci „moderoval". Hlavní role Ceremony Administrator (CA) připadla Mehmetovi Akcinovi z ICANNu. Mehmet byl v této roli výkonnou složkou celé akce a veškerá činnost byla v jeho rukou. Jako Internal Witness 1 (IW), který figuroval v roli zapisovatele a kontrolora CA, se ceremonie zúčastnil Francisco Arias rovněž z ICANNu.

Akce rovněž přihlíželi další lidé v roli IW (tedy lidé z ICANNu) a External Witness (externí dohližitelé) včetně auditora celé akce. Další důležitá role je Safe Security Controller (SSC), který má na starosti odemčení trezoru. V roli SSC byli přítomni Alexander Kulik a Patrick Jones. Každý z těchto pánů má jednu zálohu a jeden určený trezor. Tedy pro otevření trezoru číslo 1 je zapotřebí SSC1 a trezor číslo 2 může otevřít jen SSC2 (a jeho záloha). Každý trezor obsahuje záznamové archy, kde jsou zaznamenány všechny akce včetně otevření a zavření trezoru.

Protože Alain Aina z Beninu, který měl být jedním z Crypto Officerů, nemohl kvůli zrušenému letadlu dorazit včas, byl nahrazen Christopherem Griffithsem z USA. Aby byl dodržen původní plán, byl na další den (17. června 2010) naplánována ceremonie výměny CO, která také úspěšně proběhla.

Samotný průběh ceremonie byl dlouhý, proto jen ve stručnosti. První úkol čekal Crypto Officery v trezorové kleci. SSC2 otevřel trezor číslo 2, který obsahuje bezpečnostní schránky s přístupy. Každý CO si vybral svou schránku, která je uzamčena dvěma klíči – jeden si z ceremonie odnesl každý CO a druhý je společný a disponuje jím CA. Po kontrole, že klíče fungují a schránky jsou prázdné, opustili všichni trezorovou klec.

Po minutě čekání, což je stanovená minimální doba mezi dvěma otevřeními klece, vstoupili do klece CA, IW1 a SSC1 a otevřeli trezor číslo 1 s vybavením, které čítá dvě HSM, speciální notebook, DVD s operačním systémem a flash disk(y). S HSM je zapotřebí zacházet velmi opatrně, protože neopatrná manipulace může způsobit zničení celého zařízení. Notebook je ve speciální úpravě, kterou používá například americká armáda, a neobsahuje pevný disk, wifi a bluetooth. Veškeré zařízení (a následně i karty) jsou uloženy ve speciálních pytlících pro detekci narušení. Každý pytlík má své evidenční číslo (TEB#).

Toto zařízení bylo vyvezeno ven z trezorové klece a mohla začít inicializace HSM modulů. Notebook byl nabootován z DVD. Jako operační systém používá ICANN Live CD CentOS. Veškerý výstup z HSM a terminálový výstup byl ukládán na flash disk. Nebudu vás zatěžovat všemi detaily inicializace HSM a generování karet – celkem bylo zinicializováno 45 SC karet, takže jen podstatné detaily. Dvě sady sedmi SO (Security Officer) karet.

Tyto karty jsou „hlavním" klíčem k HSM a pro provedení libovolné akce jsou zapotřebí tři libovolné karty. Po počáteční inicializaci budou uloženy v bezpečnostních schránkách (jedna z každé sady pro každého CO) a neměly by být vůbec používány, pokud nebude zapotřebí generovat další karty. Následně byly vygenerovány dvě karty na přesnou kopii nastavení pro druhé HSM, aby bylo možné používat stejné SO karty pro obě HSM. Tyto karty byly po přenesení nastavení nejprve v HSM smazány a následně skartovány.

Po vygenerování SO karet byly vytvořeny dvě sady sedmi karet se zálohou SMK klíče (Storage Master Key) a jedna sada karet Operátora (OP). Pomocí zálohy obsahu HSM a SMK karet (5 ze 7) je možné na libovolném HSM obnovit jeho kompletní obsah. OP karty jsou určeny pro generování klíčů, podpisů a další kryptografické operace.

Dokončení reportáže najdete na Root.cz. ■