

Security-Portal.cz má podepsaný SSL certifikát

Vložil/a [cm3l1k1](#) [1], 18 Leden, 2011 - 21:41

- [SP News](#) [2]

Vzhledem k tomu, že náš poskytovatel webhostingu spustil službu Server Name Indication ([SNI](#) [3]), tak jsme mohli nasadit podepsaný SSL certifikát pro doménu portálu bez nutnosti rezervace IP adresy. (asi jsem je neprudil sám :))

Současný standard pro HTTPS komunikaci totiž trpí chybou designu, kdy se šifruje komunikace ještě před předáním HTTP hlaviček (Host), takže nebylo možné zvolit správný certifikát při virtualním hostingu.

SNI tento problém řeší, ale je třeba podpory jak na straně klienta, tak serveru. Na výše uvedeném odkazu na wiki si můžete přečíst více.

CN je www.security-portal.cz [4], takže na subdoménách browser zahlásí chybu, ale stále se jedná o ten samý. Wildcard CN stojí desetkrát tolik...

Njoy!



URL článku:

<https://www.security-portal.cz/clanky/security-portalcz-m%C3%A1-podepsan%C3%BD-ssl-certifik%C3%A1t>

Odkazy:

- [1] <https://www.security-portal.cz/users/cm3l1k1>
- [2] <https://www.security-portal.cz/category/tagy/sp-news>
- [3] http://en.wikipedia.org/wiki/Server_Name_Indication
- [4] <http://www.security-portal.cz>