

Dodatečné informace k ZD- 1
VZ43/2012 „Podpora provozu aplikačního software eRecept“

Dotaz č. 1:

Prosíme o informaci přesného technického předpisu, resp. postupu vyžadovaného SÚKL pro Generování autorizačních kódů TRGN (bod 7.8.2, druhá odrážka Zadávací dokumentace). Je výstup funkčního požadavku "Generování autorizačních kódů TRGN" ekvivalentní s definicí Autorizačního kódu (autorizačního klíče) v souladu s dokumentem "ERP_v_2_20 změny rozhraní 20110927.doc", kapitolami 1.11.1, 1.11.2 a formátem stanoveným v kapitole 1.11.3., t.j. "Autorizační kód - 5 znaků (26158)"?

Pakliže ano, prosím stanovte detailní technický předpis transformace "náhodně vygenerovaného čísla" (t.j. True Random Generated Number - TRGN) na formát "Autorizační kód - 5 znaků".

Pakliže ne, prosím definujte detailní funkční požadavky "Generování autorizačních kódů TRGN".

V obou případech stanovte prosím požadované statistické vlastnosti využitého generátoru náhodného čísla (TRNG)."

Odpověď:

Přesný technický předpis pro generování autorizačních kódů TRGN je součástí požadovaného plnění „Analýza a návrh řešení“. Informace uvedené v dokumentu „ERP_v_2_20 změny rozhraní 20110927.doc“ mají s ohledem na staří dokumentů pouze informativní význam. Zadavatel očekává, že uchazeč ve své nabídce navrhne takový způsob autorizace elektronických receptů, které na jedné straně zajistí bezpečnost prováděných transakcí, na straně druhé bude navržené řešení v souladu s nejmodernějším poznatky v oblasti ochrany osobních údajů.

Zadavatel nemůže definovat detailní požadavky na generování autorizačních kódů, protože by tím předjímal konkrétní technické řešení. Zadavatel požaduje, aby uchazeč navrhl takové řešení pro generování autorizačních kódů, které bude v souladu s jím definovanými funkčními požadavky, které jsou uvedeny v ZD.

Zadavatel požaduje, aby generátory použité pro generování náhodných čísel splňovaly bezpečnostní normy FIPS 140-2 Level 3 a Common Critéria EAL 4+, které definují minimální požadavky na kvalitu použitých generátorů. Zadavatel nicméně upozorňuje, že kvalita zabezpečení transakcí a tedy i generovaných čísel nemůže být dána pouze implementací jednoho typu algoritmů, i když se jedná o TRNG. Zadavatel předpokládá předložení takové řešení, které bude odolné proti selhání dílčích kryptografických metod.

Zadavatel dále upozorňuje, že navržené řešení musí umožňovat „bezpečnou“ archivaci prováděných transakcí v řádu desítek let.