

Specifikace díla

Nový autentizační předmět (náhrada SC Schlumberger Cryptoflex)

Úvod:

Cílem projektu je náhrada současných čipových karet (primárně autentizačních čipových karet typu A/S pro KP PCS1) novými čipovými kartami typu java card, pro již certifikované KP PCS1 a KP LANPCS, kdy pro použití nových čipových karet nebude vyžadována žádná změna v certifikovaném prostředku KP PCS1 a KP LANPCS a pouze minimální změny na úrovni střediska klíčů. Tato náhrada je primárně nutná z důvodu nedostupnosti současných čipových karet na trhu a snižujícími se zásobami karet na skladě.

Cíl projektu:

- rychlá náhrada autentizačních karet typu A/S pro KP PCS1 beze změny FW na KP PCS1 a s minimálními změnami pro středisko klíčů
- následná možnost náhrady karet jako nosič klíčů pro současné KP PCS1 a KP LANPCS, pokud dojdou současné čipové karty a ještě nebude vyvinut a schválen nový nosič klíčů (samostatný projekt)

Návrh řešení:

- stanovit minimální funkční a bezpečnostní požadavky na I/A předmět pro KP PCS1 a KP LANPCS v podobě java card (provozní požadavky z pohledu minimálních funkcí na API OS java card, bezpečnostní požadavky včetně požadavků na operace/funkce práce s PINem)
- vyvinout emulační applet Schlumberger Cryptoflex pro standardní java card
- provést výběr fyzické java card pro první období z pohledu dodavatelských, provozních a bezpečnostních požadavků, kde primární podmínkou bude dodávání java card v plně otevřené podobě
- vyřešit inicializaci čipových karet java card (změna výchozích klíčů, nahrání appletu, nastavení jedinečného SN, nastavení výchozích pinů, uchování potřebných informací). Předpokládá se vývoj jednorázové inicializační utility, která se předřadí současnému procesu výroby čipových karet na středisku.
- provedení testů z pohledu funkčnosti řešení a kompatibility s KP PCS1, KP LANPCS a střediska klíčů na nakoupených vzorcích vybraných java card

I. etapa - do 9. 12. 2016

Cíle:

- plně funkční náhrada autentizačních karet typu A/S pro KP PCS1

Výstupy:

- emulační applet Schlumberger Cryptoflex pro standardní java card

- inicializační utilita, která se předřadí současnému procesu výroby čipových karet na středisku
- dodávka 20 ks vybraných java card pro ověření

II. etapa - 10. 12. 2016 - 31. 1. 2017

Cíle:

- ověřovací provoz
- testování z pohledu funkčnosti řešení a kompatibility s KP PCS1, KP LANPCS a střediska klíčů na nakoupených vzorcích vybraných java card
- oponentní řízení