

Príloha č. 1 - Projekt

Názov projektu: Vývoj a návrh hardvéru(elektroniky) inteligentného dverového zámku

Skratka projektu: KEY.VI - HW

Žiadateľ :

- **Obchodný názov:** rogainformatika s.r.o.
- **Adresa:** Janka Kráľa, 44/17, 93601, Šahy
- **Štatutárny orgán:** Ing.Robert Gašparík, konateľ, Tel.0907/746-548, e-mail:
rgasparik@rogainformatika.eu)
- **Vedúci projektu:** Ing.Robert Gašparík, konateľ, Tel.0907/746-548, e-mail:
rgasparik@rogainformatika.eu)
-

Termín riešenia: 10/2014

Cena riešenia celkom: 5100€

z toho - oprávnené náklady: 5100€

- vlastné zdroje:100€

- dotácia:5000€

Popis Projektu

1. Ciele riešenia

Cieľom riešenia je návrh a výroba prototypu mikoelektroniky- (schéma + prototyp dosky + elektrotechnické komponenty) inteligentného elektronického zámku.

2. Základné parametre riešenia

Používateľ pristúpi k dverám, smartfón pomocou mobilnej aplikácie(Android, iOS, WindowsPhone) naviaže komunikáciu so zámkom. Zámok(HW) v tejto komunikácii figuruje ako master a bude iniciovať komunikáciu. Smartfón bude figurovať ako slave pri komunikácii. Štruktúra vymenených dát medzi zámkom a smartfónom bude nasledovná:

A) Generovanie key.vi kľúča v smartfóne: Samotná správa napr. „otvor“ zahashovaná algoritmom SHA. Podpisovač-softvér, ktorý správu elektronicky podpíše. Podpísaná správa (podpis) je vždy iný string(retazec). Pošle sa balík v zložení správa „otvor“ + hash správy („otvor“, vždy rovnaký string) + podpis (vždy unikátny string) + certifikát VK (verejný kľúč, vždy rovnaký string). Užívateľ zadáva PIN k certifikátu VK. Takto vytvorený key.vi kľúč sa pošle cez NFC (nebude to viac ako 1000KB) do Zámku(HW)

B) Práca s key.vi kľúčom na hardvéri:

1. Príjem správu „otvor“ – (hash1)

2.Odšifrujem podpis s VK a dostanem sa k SHA hash-u (hash2)

3.Porovnam hash1(originál) ?= hash2(čo prišlo). Či nedošlo k zmene údajom (man in the middle útok)

4.Skontrolujem platnosť certifikátu VK, aktuálne CRL-ko(black list/white list) zámok dotiahne cez wifi. Zámok sa pýta: Je tento certifikát podpísaný certifikačnou autoritou, kt dôverujem? Tj či vystavený certifikát nie je na blackliste.

Ak sú body 1-4 splnené pošli signál na otvorenie zámku. Vyhodnotí OK, pustí elektronika signál na otvorenie zámku + LED signalizácia zelená + bzučiak.

5. Vyhodnotí NOK, + LED signalizácia červená. CRL súbor sa bude aktualizovať 1x denne (scheduler).

Napájanie zariadenia bude cez 4xAAA batérie, kt sú už standardne obsiahnuté v elektromechanickom zámku.

Variant A: Elektronika bude obsahovať Wifi chip, kde po pripojení sa cez wifi router bude posilať informácie o časovej stope a ID zámku, kedy bol zámok otvorený. Rovnako bude automaticky v zadaných časových intervaloch sťahovať-aktualizovať súbor CRL.

3. Charakteristika projektu, postup riešenia,

Podrobný popis návrhu riešenia: V prvej časti projektu sa zameriame na riešenie bezpečnosti používania key.vi kľúčov. Ich generovanie, šifrovanie, elimináciu rizika zneužitia key.vi kľúčov (použijeme bezpečnostnú technológiu elektronického podpisu), ich posielanie do zámku(HW) key.vi a následné spracovanie. Existujúce riešenia sa vyberú so zreteľom na cieľ projektu. . V ďalšom kroku sa vyberie riešenie elektro-mechanických zámkov (len čisto elektromechanická časť zámku) so zreteľom na cieľ projektu. (napr. blokovanie kľučky, panic funkcia, bzučiak, info ledky na zámku). Ďalší krok spočíva vo výbere dodávateľa elektrotechnických komponentov (napr. mikrokontroller, bezpečnostné moduly, nfc chip, wifi chip, SIM modul, CMOS pamäť, zdroj napájania poprípade záložný zdroj napájania) so zreteľom na manipuláciu s generovaným key.vi kľúčom. Následne sa navrhne základná doska elektroniky, tak aby ju bolo možné zabudovať do elektromechanického zámku spolu so zdrojom napájania. Vyberú sa správne komponenty, navrhne sa ich rozmiestnenie na doske a naprogramuje sa mikrokontroller.

Varianty riešenia:

Variant A: Elektronika bude obsahovať Wifi chip, kde po pripojení sa cez wifi router bude posielat informácie o časovej stope a ID zámku, kedy bol zámok otvorený. Rovnako bude automaticky v zadaných časových intervaloch sťahovať-aktualizovať súbor CRL.

Prínosy riešenia: Podstatne zvýšený komfort pri otváraní dverí, žiadny zväzok kľúčov, stačí nosiť smartfón vo vrecku a priblížiť sa k dverám. Podstatne zvýšená bezpečnosť generovaných kľúčov (elektronické kľúče sa nestratia a nedajú sa okopírovať vďaka technológiám elektronického podpisu) a nie je potrebná výmena zámku pri strate smartfónu. Posielanie informácií kto a kedy otváral zámok cez sms. Jednoduché a bezpečné zdieľanie kľúčov. Očakávaný ekonomický rast nakoľko toto riešenie sa bude predávať aj v zahraničí – export. S tým súvisí tvorba nových vysokokvalifikovaných pracovných miest v našej spoločnosti.

4. Realizačné výstupy

Predpokladaným výsledkom riešenia je funkčný prototyp hardvérovej časti key.vi, ktorý spĺňa funkčnú špecifikáciu opísanú v časti Charakteristika projektu.

5. Harmonogram riešenia

- **názov čiastkovej úlohy (etapy) – I. Elektronické kľúče (generovanie, mazanie, zdielanie)**

- **termín začatia / ukončenia – November 2014 / 28.02.2015**

- **riešiteľ** (Katedra mechatroniky a elektrotechniky Žilinskej univerzity v Žiline)

- Kontrolné body riešenia - Výber elektrotechnických komponentov, Návrh elektrotechnickej schémy, programovanie softvéru kontrollera , 31.12.2014

- **názov čiastkovej úlohy (etapy) – II. Elektronický zámok**

- **termín začatia / ukončenia – November 2014 / 28.02.2015**

- **riešiteľ** (Katedra mechatroniky a elektrotechniky Žilinskej univerzity v Žiline)

Kontrolné body riešenia - Elektrotechnický plošný spoj-modul osadený komponentmi, Zabudovaný v zámku, schopný spracovať a vyhodnotiť prijatý NFC signál, 31.01.2015

- **názov čiastkovej úlohy (etapy) – III. Návrh elektroniky a programovanie kontrollera**

- **termín začatia / ukončenia – November 2014 / 28.02.2015**

- **riešiteľ** (Katedra mechatroniky a elektrotechniky Žilinskej univerzity v Žiline)

Kontrolné body riešenia - Kontrola kvality riešenia, užívateľské testy, ladenie prototypu, 28.02.2015

6. Financovanie riešenia projektu	Rok	2014	2015	2016
Cena projektu celkom: (v tis. EUR)		2550€	2550€	0€
z toho - oprávnené náklady celkom:		-50€	-50€	-0€
- vlastné zdroje				
- štátna dotácia		-2500€	-2500€	-0€

7. Stručná charakteristika doterajšej činnosti žiadateľa

2014 - Elektronizácia služieb vyšších územných celkov (VucTT,VucNR,VucBB,VucPO,VucKE) na Slovensku – operačný program informatizácia

2014 - Elektronizácia služieb miest a obcí na Slovensku - – operačný program informatizácia

2013 – 2014: Vývoj online e-learningových portálov do Južnej ameriky

2012 – 2013: Vývoj softvéru pre elektronické verejné obstarávanie

8. Stručná charakteristika doterajšej činnosti vedúceho projektu

2014:Softvérový architekt na projekte Elektronizácia služieb vyšších územných celkov na Slovensku

2014:Softvérový architekt na projekte Elektronizácia služieb miest a obcí na Slovensku

2013–2014:Projektový manažér na projekte Vývoj online e-learningových portálov do Južnej ameriky

2012 – 2013: Projektový manažér na projekte Vývoj softvéru pre elektronické verejné obstarávanie

V Šahách dňa 28.10.2014

<i>Odtlačok pečiatky žiadateľa</i>	<i>Podpis štatutárneho orgánu žiadateľa</i>