Ján Procháska – Profesionálny životopis

Základné údaje

Meno a priezvisko	Ján Procháska	**Titul**	Ing., PhD.
E-mail		**Štátna príslušnosť**	SR

Vzdelanie

Inštitúcia	**Obdobie od–do**	**Najvyšší stupeň vzdelania (I.stupeň Bc, II.stupeň Ing. a pod.)**
STU, Bratislava	2004 – 2009	III. stupeň PhD.
STU, Bratislava	1998 – 2004	II.stupeň Ing.
Certifikácie		
OMG-Certified Expert in BPM 2 – Fundamental Oracle IT Architecture SOA 2013 Certified Architecture Specialist IBM Certified SOA Solution Designer ArchiMate 2 TOGAF 9		

Jazykové znalosti (1 – začiatočník, 2 – pokročilý, 3 - plynulý)

Jazyk	**Čítať**	**Hovoriť**	**Písať**
Anglický	3	2	2
Nemecký	3	2	2

História zamestnania

Zamestnávateľ (názov a sídlo)	**Pozícia a opis pracovnej náplne**	**Od – do (mesiac, rok)**
Archimetes, s.r.o.	**IT Konzultant (špecialista pre problematiku elektronického podpisu, kryptografie a PKI)**	**02/2018 - súčasnosť**
Ensentia s.r.o.	Enterprise architect (návrh architektúry IT riešení, návrh a rozdielové analýzy na jednotlivých vrstvách architektúry: biznis architektúra (podnikové funkcie, kompexné biznisové procesy a služby), aplikačná architektúra (aplikačné funkcie a služby), dátová architektúra, technologická architektúra).	10/2014 – 12/2018
Atos IT Solutions and Services	**Solution Architect (analýza, návrh riešenia, implementácia a test IT riešení pre projekty tzv. jednotných pracovísk Ministerstva vnútra SR (príjem žiadosti o doklady, personalizácia biometrických dokladov s kontaktnými a bezkontaktnými čipmi a vydávanie dokladov ich držiteľom,**	**02/2010 - 09/2014**

	PKI riešenia pre čítanie údajov z dokladov a overovanie intergrity týchto údajov na čipe dokladu)).	
Siemens PSE	IT Integrátor (vyhotovovanie špecifického zákazníckeho IT riešenia na báze existujúcich systémových komponentov (štandardné produkty, odborné alebo referenčné riešenia) a ich napájanie do prostredia a procesov zákazníka).	02/2004 - 12/2009
Siemens PSE	IT Developer (podieľanie sa na vývoji všetkých fáz IT produktu (design, testuj, implementácia, tvorba dokumentácie).	07/2003 - 09/2003
ZSE Slovakia	IT Developer (vývoj software).	01/2002 - 12/2002

Zoznam praktických skúseností

Názov projektu:	Elektronické podpisovanie zmlúv
Identifikačné údaje Objednávateľa/Odberateľa	QCM, s.r.o. (hlavný dodávateľ) / Integrovaná doprava stredočeského kraja (koncový zákazník)
Lehota plnenia predmetu zmluvy/stavby/projektu projekte v tvare od – do (MM/RRRR):	02/2022 -
Stručný opis predmetu plnenia zmluvy/projektu vrátane aktivít a činností, ktoré expert vykonával:	Riešenie pre vytváranie a overovanie kvalifikovaného elektronického podpisu pre zmluvy v systéme pre správu a riadenie obehu dokumentov. Vykonávané činnosti: - analýza a návrh riešenia v rozsahu voľby podpisových formátov a kryptografických algoritmov pre podpisovanie dokumentov (kryptografické funkcie rodiny SHA, podpis založený na využití asymetrických RSA kľúčoch v súlade s nariadením eIDAS a jeho vykonávacím rozhodnutím), - návrh využitia hardwarových zariadení pre vytváranie kvalifikovaného elektronického podpisu a test týchto zariadení prostredníctvom štandardizovaných rozhraní (napr. PKCS#11), - vývoj a test riešenia, - komunikácia so zákazníkom.
Celková zmluvná cena projektu bez DPH:	~ 18 000 EUR
Pozícia na danom projekte:	Špecialista pre problematiku elektronického podpisu, kryptografie a PKI.

Doba vykonávania na vyššie uvedenej pozícií na danom projekte v tvare od – do (MM/RRRR):	02/2022 -

Názov projektu:	MobileID
Identifikačné údaje Objednávateľa/Odberateľa	PosAm, spol. s r. o. / DataCentrum elektronizácie územnej samosprávy Slovenska (DEUS)
Lehota plnenia predmetu zmluvy/stavby/projektu projekte v tvare od – do (MM/RRRR):	02/2020 – 09/2020
Stručný opis predmetu plnenia zmluvy/projektu vrátane aktivít a činností, ktoré expert vykonával:	Softvérové riešenie pre vytváranie elektronického podpisu na serveri pre potreby mID. Vykonávané činnosti: - analýza a návrh riešenia v rozsahu voľby podpisových formátov a kryptografických algoritmov pre podpisovanie dátových viet a dokumentov (kryptografické funkcie rodiny SHA, podpis založený na využití asymetrických RSA kľúčoch v súlade s nariadením eIDAS a jeho vykonávacím rozhodnutím), prenos informácii zabezpčeným TLS kanálom, - návrh využitia hardwarových zariadení pre vytváranie kvalifikovaného elektronického podpisu a test týchto zariadení prostredníctvom štandardizovaných rozhraní (napr. PKCS#11), - vývoj a test riešenia, - komunikácia so zákazníkom.
Celková zmluvná cena projektu bez DPH:	~ 30 000 EUR
Pozícia na danom projekte:	Špecialista pre problematiku elektronického podpisu, kryptografie a PKI.
Doba vykonávania na vyššie uvedenej pozícií na danom projekte v tvare od – do (MM/RRRR):	02/2020 – 09/2020

Názov projektu:	Podpisuj.sk

Identifikačné údaje Objednávateľa/Odberateľa	Archimetes, s.r.o.
Lehota plnenia predmetu zmluvy/stavby/projektu projekte v tvare od – do (MM/RRRR):	02/2018 -
Stručný opis predmetu plnenia zmluvy/projektu vrátane aktivít a činností, ktoré expert vykonával:	Riešenie pre vytváranie a overovanie kvalifikovaného elektronického podpisu pre dokumenty, zaručená konverzia dokumentov a vytváranie osvedčovacích doložiek o autorizácii v zmysle platnej legislatívy. Vykonávané činnosti: - analýza a návrh riešenia pre elektronické podpisovanie a overovanie podpisov dokumentov (kryptografické funkcie rodiny SHA, podpis založený na využití asymetrických RSA kľúčoch v súlade s nariadením eIDAS a jeho vykonávacím rozhodnutím) a súvisiace funkcie ako zaručená konverzia dokumentov a tvorba autorizačných doložiek dokumentov v súlade so zákonom o e-gov a súvisiacou legislatívou, prenos informácii zabezpčeným TLS kanálom, - návrh využitia hardwarových zariadení pre vytváranie kvalifikovaného elektronického podpisu a test týchto zariadení prostredníctvom štandardizovaných rozhraní, komunkikácia s výrobcami týchto rozhraní (napr. PKCS#11), hlásenie bugov, - vývoj a test riešenia, - komunikácia so zákazníkom.
Celková zmluvná cena projektu bez DPH:	~ 100 000 EUR
Pozícia na danom projekte:	Špecialista pre problematiku elektronického podpisu, kryptografie a PKI.
Doba vykonávania na vyššie uvedenej pozícií na danom projekte v tvare od – do (MM/RRRR):	02/2018 -

Názov projektu:	Rozšírenie technického riešenia pre Jednotné pracoviská MV pre zber žiadostí na vydávanie elektronických eID kariet
Identifikačné údaje Objednávateľa/Odberateľa	Hewlett-Packard Slovakia / Ministerstvo vnútra SR

Lehota plnenia predmetu zmluvy/stavby/projektu projekte v tvare od – do (MM/RRRR):	02/2010 – 09/2014
Stručný opis predmetu plnenia zmluvy/projektu vrátane aktivít a činností, ktoré expert vykonával:	Projekt zavedenia elektronickej identifikačnej karty na Slovensku: - rozšírenie personalizačného systému, - rozšírenie centrálnych agendových systémov, - rozšírenie riešenia jednotných pracovísk, - eGovernment služby Vykonávané činnosti: - architekt pre analýzu, návrh a revízie modelov biznisových procesov správnych agend pre zber žiadostí o doklady, spracovanie žiadostí, sledovanie životného cyklu žiadostí a vydávanie dokladov, - návrh riešenia pre šifrovanie osobných údajov pri zbere údajov potrebných pre vydávanie dokladov v teréne (tzv. mobilné pracoviská). Riešenie zahŕňalo symetrickú a asymetrickú kryptografiu na embedded zariadení v súčinnosti s čipovými kartami prostredníctvom štandardizovaných HW a SW rozhraní, prenos informácii zabezpčeným TLS kanálom, vývoj, test, nasadenie a podpora prevádzky.
Celková zmluvná cena projektu bez DPH:	> 10 000 000 EUR
Pozícia na danom projekte:	Architekt, vývojár, tester.
Doba vykonávania na vyššie uvedenej pozícií na danom projekte v tvare od – do (MM/RRRR):	02/2010 – 09/2014

Názov projektu:	Technické riešenie pre samoobslužné pracoviská na kontrolu elektronických osvedčení o evidencii vozidla a biometrických pasov SR
Identifikačné údaje Objednávateľa/Odberateľa	Hewlett-Packard Slovakia / Ministerstvo vnútra SR
Lehota plnenia predmetu zmluvy/stavby/projek	02/2010 – 09/2011

tu projekte v tvare od – do (MM/RRRR):	
Stručný opis predmetu plnenia zmluvy/projektu vrátane aktivít a činností, ktoré expert vykonával:	Technické riešenie pre samoobslužné pracoviská (kiosky) na kontrolu elektronických osvedčení o evidencii a biometrických pasov. Rozšírenie informačného systému Evidencie vozidiel (IS EVO) o funkčnosť realizujúcu zber údajov, vygenerovanie a spracovanie žiadostí na personalizáciu osvedčení o evidencii vozidiel Slovenskej republiky s údajmi o vozidle na kontaktnom čipe. Vykonávané činnosti: - analýza a návrh komponentov pre čítanie údajov z dokladov, pre overenie nepozmenenia údajov z čipov dokladov a zabezpečenie komunikácie medzi čipom dokladu a čítacím komponentom. Riešenie využívalo symetrickú a asymetrickú kryptografiu a SOC (system-on-chip) zariadenia zapustené do dokladov, ktoré boli navrhnuté podľa medzinárodnej, európskej a národnej legislatívy, - vývoj a testovanie komponentov kontroly dokladov. Predmetom projektu Technické riešenie pre samoobslužné pracoviská na kontrolu elektronických osvedčení o evidencii vozidla a biometrických pasov SR (a profesionálnej praktickej skúsenosti experta) bola: 1. Analýza, návrh a implementácia tzv. inšpekčného systému, ktorého predmetom bolo vykonávať tzv. terminálovú autentifikáciu pre čítanie citlivých údajov z biometrických pasov SR. Ide o štandardizované kryptografické riešenie, v ktorom dôveryhodný systém na strane servera (v tomto prípade Ministerstva vnútra) preukáže vlastníctvo privátneho kľúča (prostredníctvom elektronického podpisu) za účelom čítania chránených údajov z čipu dokladu (čip dokladu považuje za dôveryhodné len isté certifikáty resp. systémy, ktoré sa preukážu vlastníctvom privátneho kľúča k týmto certifikátom). Algoritmus podpisu je v tomto prípade založený na eliptických krivkách (ECDSA). Návrh a implementácia kryptografického riešenia využívala eliptické krivky a prebiehala priamo v bezpečnom SoC module (system-on-chip) v spolupráci s výrobcom hardware. Kód bol vykonávaný v chránenej oblasti tohto modulu. 2. Analýza, návrh a implementácia kryptografického riešenia pre overenie integrity a autenticity údajov na čipe dokladu (tzv. pasívna autentifikácia), overenie originality čipu dokladu (tzv. aktívna autentifikácia), vytvorenie zabezpečeného kanála s čipom dokladu (tzv. čipová autentifikácia a secure messaging). Jednotlivé autentifikácie využívajú algoritmy RSA a algoritmy eliptických kriviek ECDSA a sú štandardizované sériou nemeckých noriem spolkového inštitútu pre bezpečnosť (verzia dostupná napr.

	tu https://silo.tips/downloadFile/extended-access-control-eac-password-authenticated-connection-establishment-pace resp. na stránkach BSI - https://www.bsi.bund.de/EN2021/Service-Navi/Publications/TechnicalGuidelines/TR03110/TechnicalGuidelines_03110_node.html). Na doplnenie je uvedené, že praktické skúsenosti (analýza, návrh a implementácia) zhŕňajúce digitálny podpisový algoritmus (DSA - Digital Signature Algorithm) vo vyššie uvedenom projekte (Technické riešenie pre samoobslužné pracoviská na kontrolu elektronických osvedčení o evidencii vozidla a biometrických pasov SR - 02/2010 – 09/2011) zahŕňali pokročilý algoritmus založený na eliptických krivkách (EC - Elliptic Curve) tzv. ECDSA (Elliptic Curve Digital Signature Algorithm). Tento algoritmus bol využívaný pri implementácii inšpekcie biometrického pasu v procese tzv. terminálovej autentifikácie. Ide o štandardizovaný proces (technická norma je uvedená vyššie), ktorým si čip na doklade verifikuje, že čítacie zariadenie (terminál) je oprávnené pristupovať k citlivým údajom (napr. biometrické údaje). Riešenie bolo prevádzkované počas projektu Zavedenie elektronickej identifikačnej karty na Slovensku 02/2010 – 09/2014 a bola k nemu o.i. poskytovaná odborná technická podpora.
Celková zmluvná cena projektu bez DPH:	> 1 000 000 EUR
Pozícia na danom projekte:	Architekt, vývojár, tester.
Doba vykonávania na vyššie uvedenej pozícií na danom projekte v tvare od – do (MM/RRRR):	02/2010 – 09/2011

23.11.2022