Hybridná čipová karta na báze čipu Desfire EV1 na Žilinskej univerzite

Ing. Daniel Milučký, Ing. Róbert Orenič,
Doc. Ing. Emil Kršák, PhD.
Žilinská univerzita

Dôvody rozhodnutia pre samostatne vydávané čipové preukazy pri prechode na hybridnú kartu

- *Od roku 2003 boli vydávané čipové preukazy Mifare Standard pomocou program EM-študent od firmy Emtest*
- *Média boli dodávané firmou Emtest už s nastavenými dopravnými aplikáciami –s cenou s dopravnými aplikáciami*
- *Naša úloha pri vydávaní preukazu – zápis dát o študentovi*
- *Nedokázali sme o karte získať žiadne podrobnejšie informácie*
- *Rozhodnutie o zmene bezkontaktnej časti čipovej karty na typ Mifare Desfire EV1 – na základe informácií od firmy EMtest*

Dôvody rozhodnutia pre samostatne vydávané čipové preukazy pri prechode na hybridnú kartu

- *Vytvorenie certifikačného pracoviska na FRI ŽU pre vydávanie elektronických podpisov , ktorých platnosť bude uznávaná na univerzitách v SR*
- *Karty vydávané od roku 2003 – dôraz kladený na multifunkčnosť v oblasti dopravných aplikácii*
- *Neschopnosť vybavovať reklamácie študentov, reklamácie vybavované v dobe 30 dní – v podmienkach univerzity neprípustné. Karta je využívaná nielen na dopravu ale i v mnohých interných aplikáciách univerzity*

Dôvody rozhodnutia pre samostatne vydávané čipové preukazy pri prechode na hybridnú kartu

- *Množstvo reklamácií zapríčinených rôznymi chybami (premazávanie karty čítačkami sprievodcov a revízorov, špatne nastavené dátumy platnosti u prepravcov, ...)*
- *Problémy s ďalším rozvojom využívania čipových kariet v aplikáciách univerzity – využívanie iba čísla karty*
- *Rozhodnutie firmy Emtest posunúť čas prechodu na karty Desfire EV o jeden rok*
- *Interná analýza funkčnosti a logistiky pri vydávaní, opravách, termínov pri reklamáciách nás priviedli k rozhodnutiu – zabezpečiť si vydávanie čipových kariet vlastnými silami*

Dôvody rozhodnutia pre samostatne vydávané čipové preukazy pri prechode na hybridnú kartu

- *Náš cieľ – dodržať štandard, ktoré budú používať univerzity na Slovensku – z toho dôvodu bezkontaktná časť čipových kariet – typ Desfire EV1*
- *Naše rozhodnutie aj do budúcnosti – vyšší dôraz na využitie čipového preukazu v interných aplikáciách univerzity*
- *Dopravná časť – ponechaná na rozhodnutí študenta, či sa rozhodne pre členstvo v Embase za daný ročný poplatok*
- *Spolupráca s Emtestom – ako partnerom v oblasti dopravných aplikácií*

Vývoj vlastného aplikačného programového vybavenia pre vydávanie hybridných čipových kariet

- *Pri vydávaní hybridných čipových kariet bolo potrebná riešiť*
  - *aplikačné programové vybavenie pre potlač karty*
  - *aplikačné programové vybavenie pre zápis dát do karty*
  - *Aplikačné programové vybavenie pre univerzitný terminál*
- *Nové riešenie pre prolongáciu skôr vydaných čipových kariet*
- *Aplikácia programového vybavenia pre zápis elektronického podpisu do kontaktného čipu*
- *Návrh komunikačného riešenia univerzitný terminál – server so SAM modulom pre bezpečnú komunikáciu*

Aplikačné programové vybavenie
Potlač karty - *CardPerson*

Jedna aplikácia ***CardPerson*** *zabezpečuje*

- *evidenciu držiteľov preukazov (údaje podľa Usmernenia MŠ)*
- *fotografovanie (automatický orez, export a import fotky)*
- *pokladňu (fiškálny blok, možnosť bezhotov. platby aj CASH)*
- *potlač preukazov (wisiwig šablóny preukazov, hromadná tlač, ...)*

Možnosť použitia:

- *1. pc pre fotografovanie*
- *2. pc pre tlač kariet*

Aplikačné programové vybavenie
Zápis dát do karty (UNIinfo terminál)

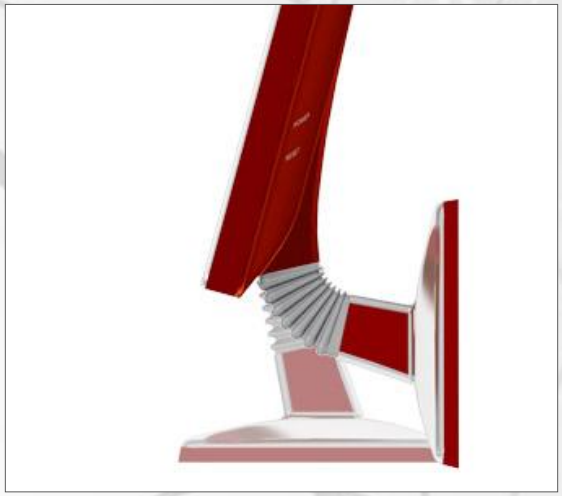
Požiadavky:

1. *online systém bez potreby neustáleho nahrávania údajov*
2. *„sieťová“ distribúcia prístupových kľúčov ku kartám*
3. *viacúčelové zariadenie*
4. *„serverové riešenie“ bez potreby aktualizácii jednotlivých terminálov napr. pri zmene štruktúry dát*
5. *komunikácia okrem bezkontaktu (Classic, DESFire EV1) aj s kontaktom*

Aplikačné programové vybavenie
Zápis dát do karty (UNIinfo terminál)

Terminál je založený na **UniqPC** od fy ELCOM s.r.o. Prešov

- *All-in-one PC* (Intel Atom N270 1.6 GHz, 3xUSB,LAN, možnosť WiFi,...)
- *odolný voči vode a prachu* (IP65 / IP54), **vandalproof** technológia
- *15“ LCD dotykový displej (4:3, 1024x768)*
- *široké možnosti uchytenia*
- *OS MS Windows 7*
- *integrovaná čítacia hlava – **HYBRIDNÁ***



Aplikačné programové vybavenie
Zápis dát do karty (UNIinfoterminál)

Terminál - aplikácia slúži pre:

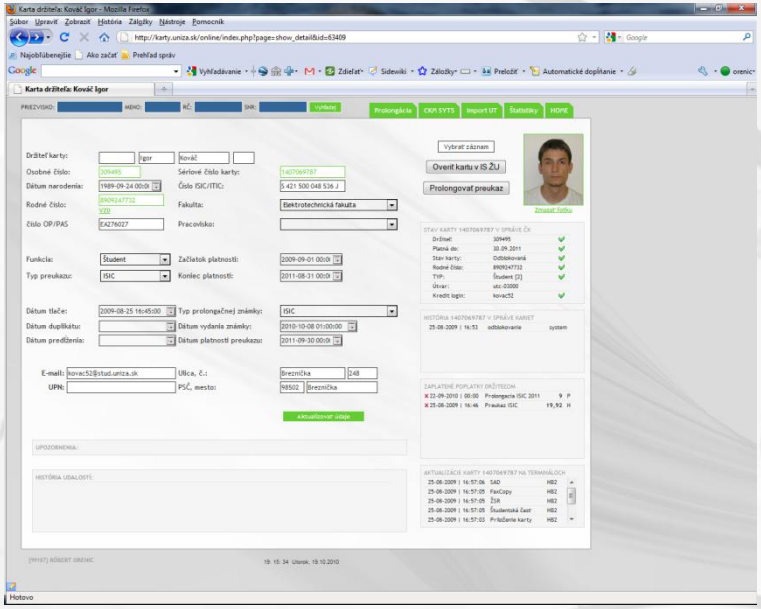
1. *aktualizáciu údajov v čipe podľa Usmernenie MŠ SR + možnosť vytvárania vlastných aplikácii v bezkontaktnom čipe karty*
2. *prácu s elektronickým podpisom E-cert (formátovanie karty, zmena PIN, zmena PUK, žiadosť o následný certifikát)*
3. *overenie funkčnosti karty v jednotlivých IS ŽU (dochádzka, prístupový systém, strava...)*

Web aplikácia

prezeranie údajov, prolongácia čipových kariet

Ide o webovú verziu aplikácie rozšírenú napr. o:

- *prehľad o aktiváciách kariet na terminálov (aj pôvodných Mifare Classic od r. 2006)*
- *umožňuje obsluhe rýchlu kontrolu funkčnosti karty v rôznych systémoch ŽU*
- *porovnanie chýbajúcich preukazov v CKM SYTS online*
- *sub-systém pri urýchlenie prolongácií ČK v novom AR*
- *...*



Web aplikácia

prezeranie údajov, prolongácia čipových kariet

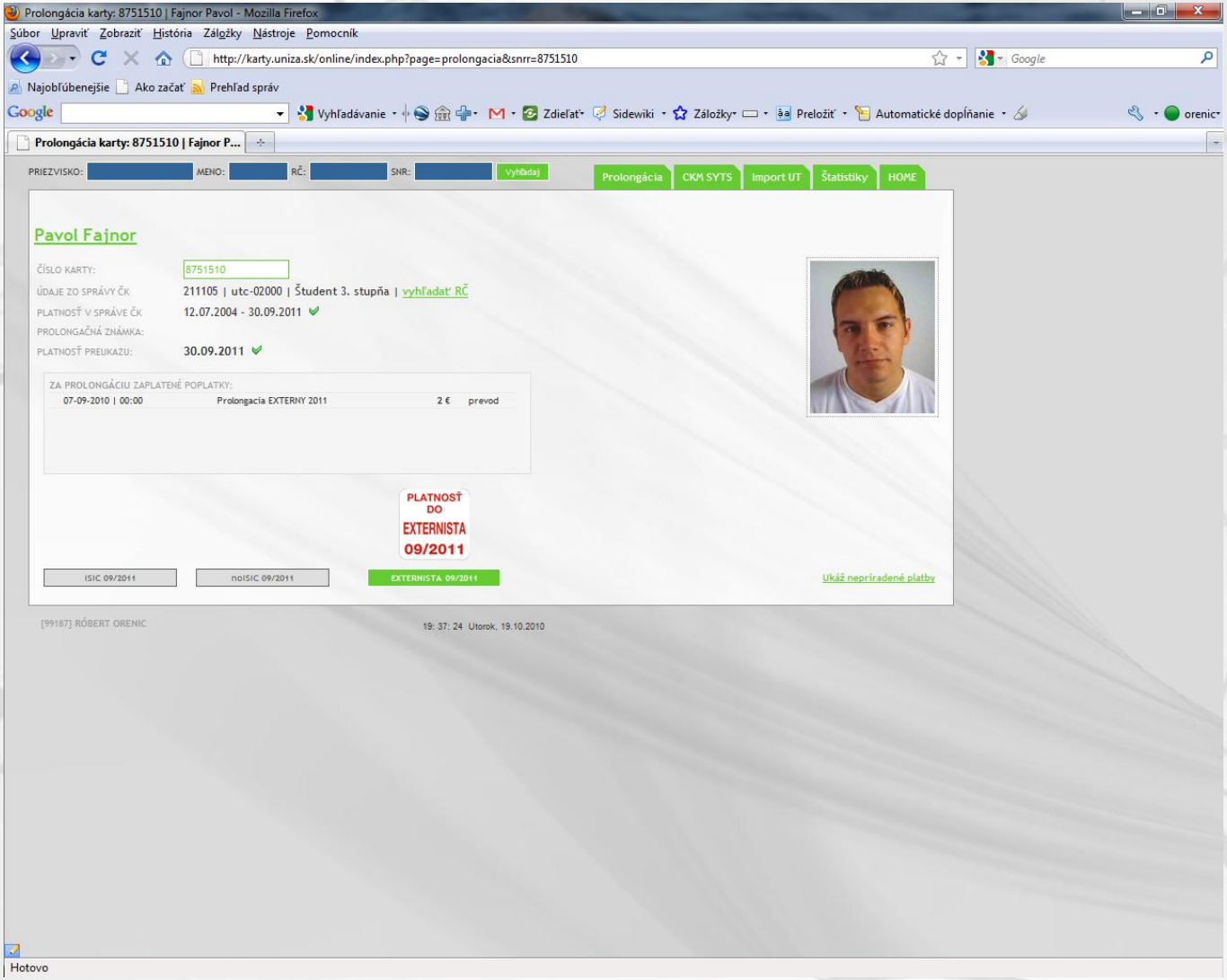
Špeciálne požiadavky pri prolongáciách preukazov:

1. *rýchle vyhľadanie karty pomocou čítačky kariet*
2. *rýchle nasadenie pre viac počítačov*
3. *zobrazenie všetkých potrebných údajov o študentovi*
   - *zaevidovanie bezhotovostnej platby (koľko zaplatil a akú známku si vybral – podľa VS platby)*
   - *reálne zapísanie do vyššom ročníku v IS Vzdelávanie*
   - *nárok na medzinárodný preukaz (ISIC.....)*
   - *...*
4. *„jednotlačítkové“ potvrdenie prolongácie (zapísanie typu prolongačnej známky, dátum vydania známku, zaevidovanie správnej platnosť preukazu)*

Pri splnení podmienok** (zapísanie do ročníka a bezhotovostná platba za prolongáciu)* ***je doba obsluhy 1 študenta cca 20 sec.

Web aplikácia

prolongácia čipových kariet



Certifikačná autorita rezortu školstva

- Vydávanie certifikátov
  - Osobné certifikáty
  - Certifikáty pre servre WWW, LDAP, ActiveDirectory, IMAPS/POP3S, IEEE 802.11x, ...
  - Možnosť ďalších špeciálnych profilov
- Pravidelné vydávanie CRL a delta CRL
- Následný certifikát cez WWW
- Plne automatizované samoobslužné pracovisko pre následné certifikáty (pripravuje sa)
- TSA – server pre časové značky (identifikácia osobným certifikátom)

Osobný certifikát na hybridnej karte

- **Parametre kontaktnej časti**
  - Prístup k privátnym dátam: PIN/PUK
  - RSA kľúče 2048 s certifikátmi: max. 8
  - Samostatná časť pre ZEP
- **Parametre vydávaných osobných certifikátov**
  - Dĺžka platnosti: 14 mesiacov
  - Základné údaje na certifikáte: Meno, organizácia, číslo karty, ďalšie podľa štandardu X509v3
  - Možnosť samostatného profilu pre organizáciu
- **Certifikáty pre servre**
  - Okamžité vydanie certifikátu
  - Prístup k službe na základe osobného certifikátu na karte
  - Delegovanie oprávnení na subdomény

Aplikácie – standalone

- **Štandardné/komerčné**
  - MS Office (Word, Excel, ...)
  - E-mail klienti (Outlook,
  - Neevia PDF
- **Univerzálne aplikácie - ytvorené v rámci E-cert**
  - Univerzálny podpisovač/pečiatkovač
    - Všetky dokumenty pribalením podpisu
    - Plugin pre rôzne typy súborov
  - Podpisovač/pečiatkovač PDF
  - Virtuálna tlačiareň
- **Možnosť okamžitého použitia na VŠ**
  - Internú papierovú komunikáciu elektronizovať
  - Študenti odovzdávajú práce podpísané s časovou pečiatkou
  - Nie je nutné zavádzať plošne pre celú VŠ

Aplikácie – autentifikácia

- **SmartLogon do pracovných staníc v Active Directory**
  - Osobný certifikát vydávaný aj pre SmartLogon
  - Realizácia:
    - všetky PC v laboratóriách FRI ŽU
- **WWW aplikácie**
  - SSL autentifikácia
  - Podpora pre autorizáciu – SNR, UPN, CardID, OpenID
  - Realizácie:
    - Intranet FRI ŽU
      - autentifikácia cez modul
    - AIVS ŽU, ŽU Flow, ...
      - autentifikácia cez autentifikačný server UnizaSSO
      - Podpora rôznych spôsobov autentifikácie (PKI, login/password, OpenID, ...)
- **Prístup do siete**
  - Autentifikácia podľa štandardu IEEE 802.11x
  - Realizácie: WiFi FRI ŽU (WiFri), Ethernet v budove FRI ŽU

Aplikácie – informačné systémy

- **Štandardné/komerčné – Collaborative software**
  - Doména: Katedra, Fakulta, Univerzita
  - SharePoint
  - OpenGroupware
  - Zarafa Groupware, ...
- **Informačné systémy vzdelávania**
  - Doména: Fakulta, Univerzita
  - Eliminácia neoprávnených zásahov do dát IS vzdelávania
  - AISv2 – Akademický informačný systém UPJŠ
    - Implementovaný elektronický podpis
    - Používa väčšina univerzít
    - Podpora zo strany UPJŠ
  - AIVS – Akademický informačný a vzdelávací systém ŽU
    - Implementovaný elektronický podpis
    - Používa ŽU

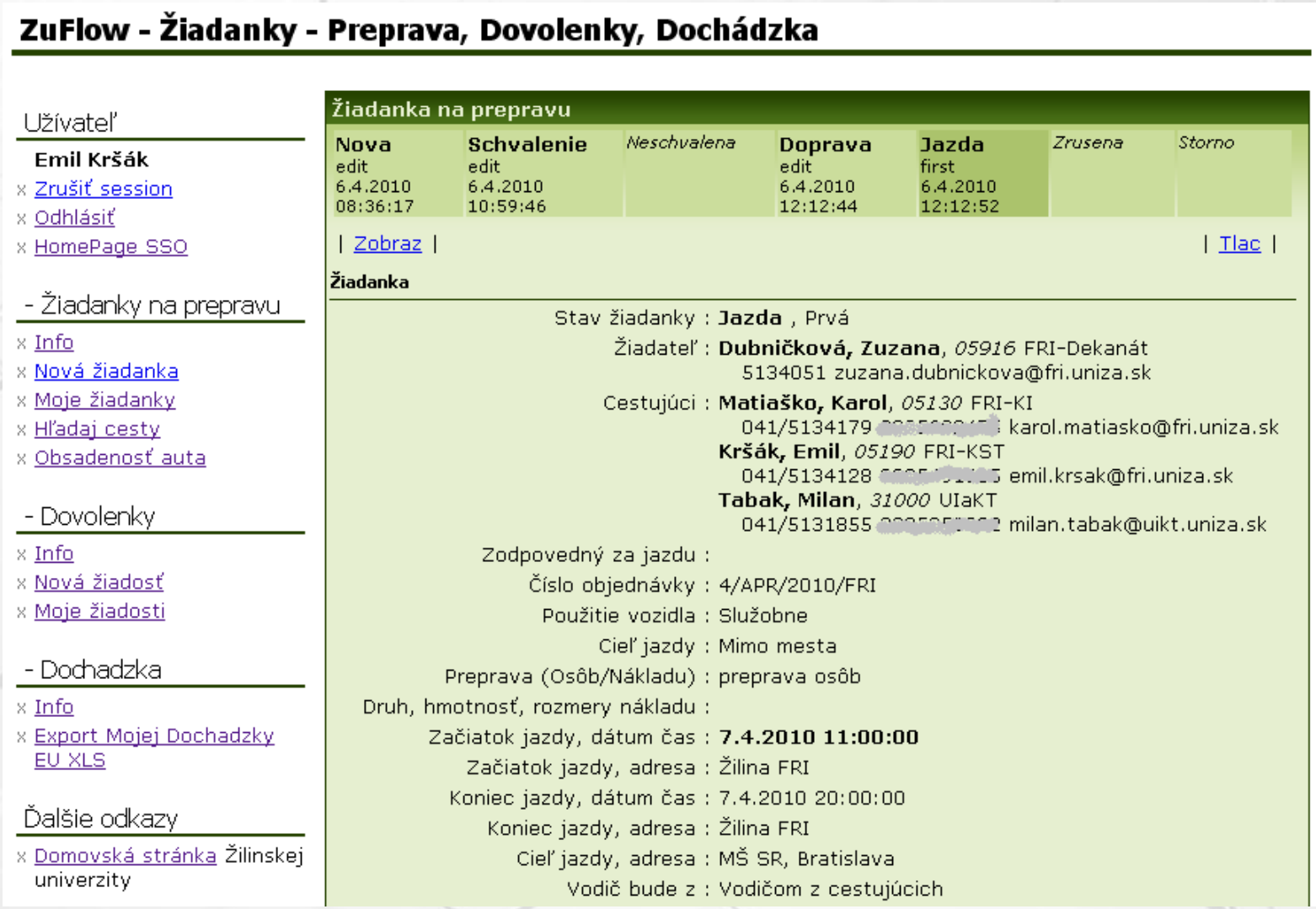
Aplikácie – informačné systémy MŠSR

- **Finančný informačný systém – SOFIA**
  - Doména: Univerzita, MŠ SR
  - Pripravený (zakúpenie modulu SAP – MŠ SR)
- **CREPČ – Centrálny register publikačnej činnosti**
  - Doména: MŠ SR
  - Deklarovaný plán implementácie elektronického podpisu
- **CRZP – Centrálny register záverečných prác**
  - Doména: MŠ SR
  - Deklarovaný plán implementácie elektronického podpisu
- **Dochádzkový systém**
  - Doména: Fakulta, Univerzita
  - SIEMENS (ELAS Prievidza)
    - Deklarovaný plán implementácie elektronického podpisu
    - Možnosť previazať na UnizaSSO
- **Stravovací systém**
  - Doména: Univerzita
  - Možnosť previazať na UnizaSSO ?

Aplikácie – Obeh dokumentov

- Štandardné/komerčné
  - MS Office
  - SharePoint
  - …
- ŽU-Flow – Informačný systém pre elektronický obeh dokumentov na ŽU
  - Framework pre rôzne druhy aplikácií
  - Žiadanky na prepravu
    - Realizované všetky služobné cesty služobnými autami
  - Dochádzka
    - Žiadosti o dovolenku
    - Export dochádzky do projektov EU (napr. Centrá excelentnosti)

ŽU Flow – Obeh dokumentov



Používanie hybridných kariet v súčasnosti

- **Aplikácie pre študentov**
  - IS vzdelávanie
  - E-Learning
  - SmartLogon do PC (v laboratóriách)
  - PKI login do Intranetu FRI
  - Prihlásenie do WIFI
  - Podpisovanie a šifrovanie E-mail
  - Podpisovanie dokumentov (MS Office)
  - Podpisovanie PDF s časovou pečiatkou
- **Navyše pre zamestnancov**
  - SmartLogon do pracovnej stanice
  - ŽU Flow
    - Žiadanky na prepravu
    - Žiadosti o dovolenku
    - Export dochádzky do projektov EU (napr. Centrá excelentnosti)