



EURÓPSKA ÚNIA

Európsky sociálny fond
Európsky fond regionálneho rozvoja



OPERAČNÝ PROGRAM
ĽUDSKÉ ZDROJE



Modul 7: Základy práce online

Pojmy z oblasti prezerania webu

1 Pojmy z oblasti prezerania webu

1.1 Kľúčové pojmy

1.1.1 Rozumieť, čo je internet, čo je web (World Wide Web, www), čo je jednoznačný lokalizátor zdrojov – (Uniform Resource Locator, URL) a hypertextový odkaz (hyperlink).

Internet – rozľahlá verejná celosvetová počítačová sieť navzájom poprepájaných počítačov, sieť sietí. Rozprestiera sa okolo celej zemegule a prepája veľký počet lokálnych sietí. Užívatelia počítačov pripojených k internetu majú možnosť navzájom komunikovať, prenášať rôzne údaje.

Internet poskytuje pomerne veľké množstvo služieb. Medzi tie najznámejšie patria: elektronická pošta, World Wide Web, elektronické konferencie, diskusné skupiny, FTP, chat, Telnet...

Pripojenie k internetu. Pripojenie počítača k internetu zabezpečujú spoločnosti, ktoré sa nazývajú poskytovatelia pripojenia (provider). Zabezpečia pripojenie vášho počítača alebo siete k svojmu serveru, ktorý je pripojený k internetu. Pripojenie môže byť realizované rôznym spôsobom.

World Wide Web (WWW, web) – v slovenskom preklade to znamená celosvetová pavučina. Umožňuje nám prístup k pomerne veľkému a rozsiahlemu množstvu informácií. Tieto informácie sú zverejnené vo forme webových dokumentov – webových stránok.

WWW je najpopulárnejšia a stále najrýchlejšie rastúca služba internetu a pravdepodobne aj najviac využívaná. Na webe máme k dispozícii veľké množstvo informácií z rôznych oblastí ľudskej činnosti. Dokumenty – webové stránky, ktoré sú zverejnené na webe sú písané najčastejšie špeciálnym jazykom **HTML** (HyperText Markup Language – hypertextový značkovací jazyk). Najčastejšie majú príponu htm, html, php... Ide o graficky orientované spracovanie informácií. Webové stránky obsahujú informácie vo forme textu, obrázkov, multimediálnych záznamov (zvuky, videoklipy)... Od bežných dokumentov sa webové stránky odlišujú predovšetkým tým, že sú medzi sebou prepojené pomocou **hypertextových odkazov**. Tieto nám umožňujú medzi jednotlivými dokumentmi umiestnenými kdekoľvek na webe prechádzať. Takto prepojenému textu hovoríme tiež **hypertext**.

Pre prácu s webovými stránkami používame špeciálny program – prehliadač webových stránok. Na akýsi štandard webu, webových stránok dohliada a snaží sa ho aj ustanovovať do praxe organizácia W3C Consortium - **www.w3c.org**.

Aby boli všetky stránky zverejnené na webe kedykoľvek prístupné, sú uložené na takzvaných **webových serveroch**. Ide o počítače, ktoré neustále pracujú a na ich diskoch sú uložené webové stránky a ďalšie dokumenty dostupné v sieti Internet.

Definovanie pojmov: HTTP, URL, hypertextový odkaz (hyperlink), ISP, FTP

HTTP – **HyperText Transfer Protocol**. Typ prenosového protokolu. Umožňuje komunikáciu medzi našim počítačom (klient) a počítačom na ktorom sú umiestnené webové stránky (serverom). Zaisťuje prenos obsahu vybraných stránok zo serveru na náš počítač. Je to najdôležitejší protokol na webe.

URL – **Uniform Resource Locator**. V slovenskom preklade to znamená - jednoznačný identifikátor zdroja. Skratkou URL sa označuje internetová adresa webovej stránky. Jedinečným spôsobom identifikuje súbor na internete. Na internete by nemali existovať dve stránky, ktoré majú rovnakú adresu.

Hypertextový odkaz (hyperlink) – linka, odkaz. Časť textu, obrázok, časť obrázku v dokumente, ktorý odkazuje na iný súbor (dokument, obrázok, súbor atď.). Zvyčajne je farebne alebo inak zvýraznený (podčiarknutie, rámček...). Kliknutím myšou aktivujeme súbor, na ktorý odkaz ukazuje.

ISP – **Internet Service Provider**. Skrátene sa používa názov provider. Ide o organizáciu, spoločnosť, ktorá zabezpečuje pripojenie počítača, lokálnej siete, k internetu. Pripojenie môže byť realizované prostredníctvom telefónnej linky, satelitným alebo pevným pripojením.

FTP – **File Transfer Protocol**. Druh interaktívneho prenosu súborov medzi lokálnym počítačom a vzdialeným počítačom (serverom). Používa sa na prenos väčšieho množstva dát najmä na internete. Takto môžeme zo servera ukladať údaje na náš počítač a tiež z nášho počítača nahrávať na server.

1.1.2 Rozumieť tvaru a štruktúre webovej adresy. Vedieť identifikovať bežné typy domén: geografické, organizačné (.org, .edu, .com, .gov).

Webové stránky sú dokumenty uložené na diskoch webových serverov. V sieti Internet je takýchto serverov pomerne veľa a je na nich uložené značné množstvo dokumentov s informáciami z rôznych oblastí. Aby sme sa dostali ku stránke, s ktorou chceme pracovať, musíme poznať jej adresu. Každá stránka má svoju jednoznačnú adresu – **URL** (Uniform Resource Locator).

Každý počítač pripojený do siete Internet má pridelenú svoju adresu. Hovoríme jej tiež **IP adresa**. Zatiaľ je zložená zo štyroch trojčísel oddelených bodkou (napr.: 158.197.16.80). Postupne sa začína zavádzať aj nový typ IPv6, ktorý bude obsahovať 8 skupín hexadecimálnych (šestnástkových) čísel. IP adresu majú aj webové servery, na ktorých sú uložené webové stránky. Takéto čísla sa samozrejme ťažko pamätajú a preto je každej IP adrese pridelený jeden alebo viac symbolických názvov. Vyššie uvedenej číselnej IP adresy servera je pridelený názov **www.science.upjs.sk**.

Adresa webovej stránky je vždy spravidla v celku, neobsahuje medzery a ani diakritické znaky (niektoré domény 1. stupňa už umožňujú použitie diakritiky/národných znakov v doménovej adrese, ale táto možnosť je zatiaľ využívaná minimálne).

Adresa webovej stránky môže vyzerat' napríklad takto:
`http://ccv.upjs.sk/formulare/prihlaska_na_kontinualne_vzdelavanie.php`.

Je rozdelená na 4 časti.

http: - označuje protokol, ktorým náš počítač komunikuje s webovým serverom - počítačom, na ktorom je hľadaná stránka. Protokol http slúži na prenos webových stránok.

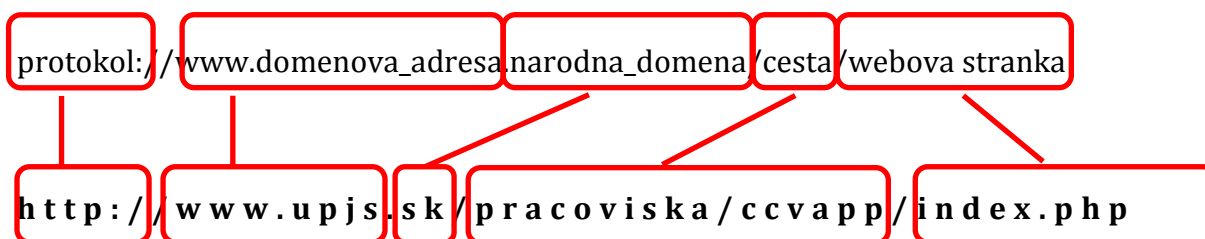
Časť adresy umiestnená medzi // a /, v našom prípade **ccv.upjs.sk** sa nazýva **doménová adresa**. Určuje server, na ktorom je stránka umiestnená. Môže to byť niekoľko slov oddelených bodkou.

Doménová adresa sa číta odzadu. Posledná skupinka znakov označuje spravidla krajinu, kde sa server nachádza – **národná doména**. Nazýva sa tiež **doména 1. stupňa**. Pre Slovenskú republiku je to **.sk**, pre Nemecko **.de**, pre Rakúsko **.au**,... Okrem národných existujú **nadnárodné domény**, ktoré sa spočiatku používali len v Spojených štátoch amerických - **.com**, **.net**, **.org**, **.edu**, ... Tieto domény boli pôvodne určené presne definovaným subjektom na základe oblasti, ktorej sa venujú (stránky venované vzdelávaniu **.edu**, stránky vládnych inštitúcií **.gov**, komerčných firiem **.com**, neziskové organizácie **.org**). V súčasnosti sa už od toho viac-menej upustilo. Iba domény **.name**, **.coop**, **.pro**, **.museum**, **.aero** sú určené pre registráciu len presne špecifikovaným subjektom.

Druhá časť doménovej adresy – **doména 2. stupňa** označuje zvyčajne organizáciu, ktorej server patrí - **upjs**. Ak chceme mať aj my počítač pripojený na internet a umiestniť naň webové stránky, môžeme si takúto doménu zaregistrovať.

S časťou adresy webovej stránky umiestnenej za / sa nemusíme stretnúť vždy. Ak je v adrese uvedená, určuje meno konkrétneho dokumentu (stránky) a jeho umiestnenie na disku webového servera. V našom príklade slovo **formulare** označujú adresár a **prihlaska_na_kontinualne_vzdelavanie.php** je konkrétna webová stránka.

Adresa webovej stránky má teda nasledovnú štruktúru:



1.1.3 Vedieť, čo je webový prehliadač (browser) a vymenovať najbežnejšie webové prehliadače.

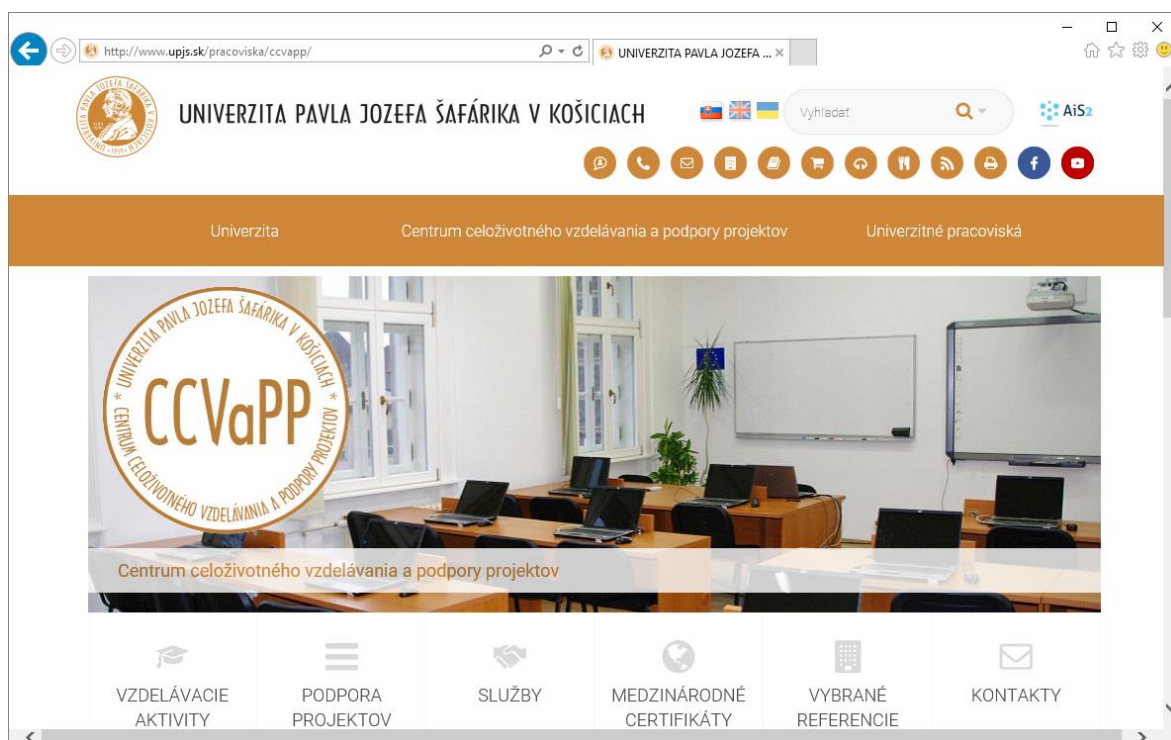
Webový prehliadač (browser, browse angl. prezerat' si, listovat') je špeciálny program, ktorý slúži na prezeranie webových stránok. Prezeraniu webových stránok hovoríme tiež surfovanie, browsovanie, túlanie po internete...

Webový prehliadač zabezpečuje komunikáciu so serverom, na ktorom je stránka umiestnená a slúži okrem zobrazovania webovej stránky aj na prácu so stránkou (uloženie, tlač, vyhľadávanie...). Ide o komunikáciu medzi našim počítačom = klient a počítačom, na ktorom sú uložené webové stránky = server.

Ako užívateľ a nás nemusí zaujímať priebeh a forma komunikácie medzi klientom a serverom. Našou úlohou, alebo to čo musíme zvládnuť, je práca s prehliadačom webových stránok, s browserom.

S operačným systémom Windows je nainštalovaný webový prehliadač firmy Microsoft – **MS Internet Explorer** (alebo **MS Edge** pre Windows 10).

Okno prehliadača Internet Explorer vyzerá spravidla takto:



Existujú však i iné pomerne rozšírené prehliadače – **Mozilla Firefox, Google Chrome, Opera...** Ponúkajú v podstate rovnaké služby, odlišujú sa v užívateľskom prostredí a v niektorých špeciálnych funkciách.

Aj keď rozdiely medzi jednotlivými prehliadačmi nie sú veľké, každý z nich si našiel medzi používateľmi internetu svojich priaznivcov.

Okrem samotného prezerania webových stránok niektoré obsahujú v sebe editor na tvorbu webových stránok, klienta na správu a prácu s elektronickou poštou...

1.1.4 Mať prehľad o rôznych činnostiach na internete ako: vyhľadávanie informácií, nakupovanie, učenie sa, publikovanie, elektronické bankovníctvo, využívanie služieb štátnej správy, zábava, komunikácia.

Na internete je možné vykonávať rôzne činnosti. Cez učenie sa, publikovanie, elektronické bankovníctvo, využívanie služieb štátnej správy, zábavu, komunikáciu až

nakupovanie. V tom množstve informácií je však potrebné sa vedieť orientovať. Na vyhľadávanie potrebných informácií je najlepšie použiť tzv. vyhľadávací stroj.

Vyhľadávacie stroje si pomocou špeciálnych programov vytvárajú svoje databázy stránok podľa kľúčových slov. Programy (vyhľadávacie roboty) každodenne prechádzajú webové stránky na celom svete a zaznamenávajú si o stránkach informácie. Každý vyhľadávací stroj má svoje špecifiká. Stroje získavajú informácie z titulku stránky, z textu na stránke, z kľúčových slov, ktoré do stránky dal sám autor... Na základe týchto informácií robot indexuje webovú stránku a uloží ju do svojej databázy. Samotné vyhľadávanie - zadávanie hľadaných pojmov prebieha pri všetkých podobným spôsobom.

My pri vyhľadávaní napíšeme do príslušného políčka slovo. Vyhľadávací stroj sa snaží nájsť všetky stránky, ktoré má indexované týmto slovom. Musíme však rátať s tým, že nie všetky odkazy budú relevantné.

Pri zadaní jednoduchých požiadaviek môžeme priamo uviesť pojem, ktorý vyhľadáme. Pri viacslovných pojmoch, nájde vyhľadávací stroj stránky, obsahujúce aspoň jedno z uvedených slov. Ak chceme, aby našiel celé slovné spojenie, dáme ho do „úvodzoviek“.

Pri finančných transakciách musíme byť obozretní a overiť si vždy, či pristupujeme k svojej banke zo zabezpečenej webovej stránky, aby nemohlo dôjsť k presmerovaniu našej komunikácie a nakoniec k zneužitiu našej identity.

Pojem cookie, vyrovnávacia pamäť (cache)

Cookie.

Jedná sa o malý, zvyčajne textový súbor, ktorý vznikne komunikáciou medzi serverom WWW a prehliadačom. Pri komunikácii servera s klientom vytvorí server súbor s informáciami o klientovi. Tieto informácie zašle ku klientskému počítaču, ktorý si ich môže (ale nemusí) uložiť na svojom pevnom disku a sprístupniť ich serveru vždy pri ďalšom pripojení. Cookie môže obsahovať užitočné informácie pre „obidve strany“ - prihlasovacie meno a heslo, užívateľské nastavenia... Vo väčšine prehliadačov sa dá prijímanie cookie zakázať. V drvivej väčšine prípadov sú však cookie užitočnou pomôckou, ktorá skrakuje a zjednodušuje komunikáciu medzi klientom a serverom.

Cache (vyrovnávacia pamäť).

Rýchla pamäť medzi hlavnou pamäťou a procesorom počítača. Do cache pamäte sa priebežne ukladajú dáta čítané z hlavnej pamäte (napr. webové stránky). Pri požiadavke na prečítanie ďalších dát sa najskôr prezrie rýchlejšia pamäť cache. Ak žiadané dáta cache pamäť obsahuje, načítajú sa oveľa rýchlejšie než z hlavnej pamäte. Ak dáta vo vyrovnávacej pamäti nie sú, načítajú sa štandardným spôsobom z hlavnej pamäte alebo média.

NAKUPOVANIE NA INTERNETE

V dobe Internetu ľudia viacej porovnávajú pri nákupoch a to často z pohodlia svojej obývačky. Záujem o nákup v internetových obchodoch a nákupná aktivita internetovej populácie rastie. Niektoré z komodít sú pre takýto nákup vhodnejšie (Knihy, cestovné lístky vrátane leteniek a vstupenky na rôzne udalosti) iné menej vhodné (oblečenie, potraviny,...). Počet internetových obchodov jedného ale i druhého druhu rastie a užívatelia si čoraz viac zvykajú i na túto formu nákupov.

Internetové stránky so zameraním na internetový obchod je možné rozdeliť do štyroch skupín:

- **Internetový obchod** zameraný na predaj výrobkov z jednej vybranej oblasti (elektronika, záhradné potreby, oblečenie, hobby, ...).
- **Internetový obchodný dom**, ktorý ponúka výrobky z viacerých oblastí tak ako je to bežné i v obchodných domoch.
- **Katalóg internetových obchodov/obchodných domov**, ktorý tvorí akýsi rozcestník prostredníctvom ktorého môžeme nájsť pre nás vhodný obchod alebo obchodný dom na internete kde by sme nami hľadanú vec mohli nájsť. (napr. www.jahoda.sk)
- **Nákupný radca**, ktorý slúži na vyhľadanie a porovnanie hľadaného výrobku. Medzi takéhoto nákupného radcu patri portál Heureka.sk.

Spôsobov ako si objednať vybraný tovar je viacero. Medzi najpoužívanejšie patrí formou e-mailu (nahrádza posielanie objednávky v papierovej forme) alebo formou vyplnenia elektronického formulára priamo na stránke e-shopu. V tomto prípade si pridávame produkty, množstvo do virtuálneho košíka a vyplnením údajov doručenia odosielame objednávku.

Spôsoby platby

Platba pri prevzatí tovaru (dobierka) - Tovar hradíte v hotovosti vodičovi dopravnej spoločnosti alebo poštovému doručovateľovi.

Pri platbe prevodom vopred - Ak si zvolíte platbu klasickým bankovým prevodom, automaticky vám na e-mail pošleme zálohovú faktúru. Po pripísaní platby na náš účet na ten istý e-mail obdržíte daňový doklad.

Platba kartou sú jednou z najpopulárnejších platobných metód na svete. Obchodníci môžu prijímať platby kartami od zákazníkov z celého sveta. Nemusíte mať u seba hotovosť ani vyberať z bankomatu, stačí použiť vašu kreditnú kartu a tovar zaplatiť on-line. Po dokončení objednávky budete presmerovaní na stránky platobného portálu pre dokončenie platby. Priradenie k vašej objednávke prebehne v priebehu niekoľkých minút po úhrade.

PayPal – je tak isto online platba ale cez účet PayPal, k tomuto účtu môže byť pripojený alebo viacero účtov. Výhodou tohto typu platby je, že údaje potrebné pre identifikáciu kartou sa nedostávajú priamo k cieľovému subjektu.

Spôsoby dodania

Kuriér – využíva pre dodanie rôzne kuriérske spoločnosti – DPD, UPS DHL,... Niektoré spoločnosti umožňujú sledovanie zásielky kde sa nachádza podľa kódu zásielky

Poštou – Slovenská pošta doručí tovar na adresu dodania.

Balíkomat /BalikoBox - Slovenská pošta pri tomto type dopravy nedoručuje zásielku adresátovi na adresu, ale uloží balík na pošte, alebo do BalikoBOXu.

Zásielkovňa – dodanie tovaru na výdajné miesto siete Zásielkovňa, kde si zákazník môže prevziať tovar

Osobné prevzatie – prevzatie tovaru priamo v predajni alebo na výdajnom mieste.

Reklamácie

Ak ste si objednali cez internet tovar, a po jeho doručení a rozbalení ste prišli na to, že Vám z určitých dôvodov nevyhovuje, takýto tovar budete chcieť vymeniť alebo dokonca vrátiť s tým, že rátate s vrátením peňazí.

V prípade, že chcete internetovému obchodu tovar vrátiť, predávajúci ale aj kupujúci sa riadia Zákonom č. 102/2014 Z. z. o ochrane spotrebiteľa pri predaji tovaru alebo poskytovaní služieb na základe zmluvy uzavretej na diaľku alebo zmluvy uzavretej mimo prevádzkových priestorov predávajúceho. Tento zákon upravuje práva spotrebiteľov a povinnosti predávajúcich pri predaji tovaru alebo poskytovaní služieb na základe zmluvy uzavretej na diaľku alebo zmluvy uzavretej mimo prevádzkových priestorov predávajúceho, podmienky organizovania predajných akcií a predaja tovaru alebo poskytovania služieb na predajných akciách a pôsobnosť orgánov dohľadu pri kontrole dodržiavania tohto zákona.

Podľa tohto zákona je spotrebiteľ oprávnený aj bez uvedenia dôvodu odstúpiť od zmluvy uzavretej na diaľku alebo od zmluvy uzavretej mimo prevádzkových priestorov predávajúceho do 14 dní odo dňa prevzatia tovaru, uzavretia zmluvy o poskytnutí služby alebo uzavretia zmluvy o poskytovaní elektronického obsahu nedodávaného na hmotnom nosiči. (§7 Odstúpenie od zmluvy, ods. 1-3). Lehoty na odstúpenie od zmluvy sa môžu upraviť v prípade, že (ne)bola poskytnutá informácia predávajúcim o práve spotrebiteľa odstúpiť od zmluvy, podmienkach, lehote a postupe pri uplatňovaní práva na odstúpenie od zmluvy; predávajúci zároveň poskytne spotrebiteľovi formulár na odstúpenie od zmluvy (§3, ods. 1 pís. h).

Povinnosti predávajúceho pri odstúpení od zmluvy a spotrebiteľa upravujú §9 a §10 spomínaného zákona.

Výhody a nevýhody nakupovania cez Internet

Výhody

- Najväčšou výhodou pre potencionálneho zákazníka je možnosť nakupovať priamo cez počítač, s ktorým pracuje v domácnosti.
- Z pohľadu prevádzkovateľa takéhoto obchodu je hlavnou výhodou jednoduchá a rýchla manipulácia s cenami a samotným sortimentom.

- Výhodný je aj bezhotovostný platobný styk, kde je dôležitá dôvera zákazníka voči virtuálnemu obchodu.
- Využitie Internetu má tieto výhody - široké spektrum dostupných informácií, možnosť osloviť globálny trh, ľahká aktualizácia informácií, možnosť monitorovania aktivít
- Nakupovanie na Internete nie je časovo obmedzené.
- Tovar je lacnejší tým, že nie je umiestnený v predajni, ale na sklade, preto nevznikajú skladovacie náklady.
- Rýchlosť – elektronické zásielky sú doručené do niekoľkých hodín.

Nevýhody

- Zákazník tovar fyzicky nevidí pred nákupom, ale až po nákupe. Preto prípadná reklamácia výrobku je zdĺhavejšia.
- Nedodržanie dodacej lehoty. Niektorí predajcovia nevedia dostatočne rýchlo aktualizovať dostupnosť jednotlivých druhov tovaru. Niekedy sa stane, že nám tovar vôbec nedôjde. Preto je dobré sa bližšie informovať o stave objednávky.
- U niektorých produktoch je nedostatočné uvedenie podrobných informácií o produkte. Vtedy je lepšie si vyhľadať na Internete podrobnejšie informácie.
- Nie všetky produkty sa predávajú rovnako. Elektronický obchod je viac úspešný s predajom nízkodotykového tovaru ako sú počítače, CD, knihy, ktoré zákazníci nepotrebujú vidieť a dotknúť sa ich oproti vysokodotykovému tovaru ako je oblečenie.

Pri uzatváraní objednávok cez internet by mali byť splnené náležitosti. Náležitosti nákupu môžeme rozdeliť do troch skupín a to:

1. Údaje identifikačné: meno kupujúceho, jeho adresa (v niektorých prípadoch aj doručovacia adresa, keď nie je totožná s adresou pobytu), emailová adresa (na potvrdenie nákupu), samozrejme identifikačné údaje predávajúceho.
2. Údaje týkajúce sa tovaru: druh tovaru, jednotková cena, množstvo tovaru
3. Údaje o podmienkach nákupu: obchodné, platobné a dodacie podmienky ako aj súhlas s nimi, pri zadávaní osobných údajov súhlas s ich spracovaním.

Typy platobných kariet:

Debetná karta je platobná karta pevne viazaná na bankový účet, ktorou možno čerpať prostriedky do výšky (často aj povoleného záporného) zostatku na bankovom účte.

Kreditná karta je druh platobnej karty, opak debetnej karty. Je to platobná karta s prideleným kreditom poskytnutým bankou alebo inou úverovou spoločnosťou, možným na prečerpanie.

Embosovaná platobná karta (angl. Embossed Payment Card) je typ platobnej karty, na ktorej sú (embossing) vyrazené údaje o vlastnej karte aj o jej majiteľovi (jeho

meno, ďalej číslo platobnej karty a doba jej platnosti). Vďaka embosovaným údajom je možné kartou platiť tiež v prevádzkach nevybavených elektronickým platobným terminálom, kde sa tak používa mechanické snímacie zariadenie nazývané imprinter. Ten pri platení embosované informácie z karty otláči na účtenku, ktorú následne zákazník podpíše.

Neembosovaná platobná karta (elektronická) tieto karty je možné použiť len pre online transakcie, výbery z bankomatov, či platby v obchodoch vybavených platobným terminálom.

Kombinovaná platobná karta je typ karty, ktorá spojuje obe predchádzajúce a tým umožňuje širšie využitie karty.

Nakupovanie zo zahraničia

Dodávky tovarov z Európskej únie a zvyšku sveta sa líšia. Pri nákupe v krajinách zjednoteného trhu prebehnú všetky zdanenia priamo v krajine, z ktorej tovar kupujete. Bez ohľadu na cenu nákupu špedičná spoločnosť doručí zásielku priamo k vašim dverám.

Od 1.mája 2017 vstúpili do platnosti nové pravidlá pre dovoz tovaru z krajín mimo EU. Ak si občan objedná tovar pre vlastnú potrebu „z tretej krajiny, v hodnote nad 22 eur, prostredníctvom súkromnej kuriérskej spoločnosti“, colné konanie vybaví už len elektronicky. Pre potreby elektronického colného konania občan potrebuje kvalifikovaný elektronický podpis (KEP). Procesom musí prejsť akýkoľvek tovar dovezený do EÚ, pokiaľ bola hodnota objednávky viac ako 22 eur. Nakupujúci musí v takom prípade dodatočne zaplatiť DPH, pričom je vymeriavací základ pre výpočet dane tvorený súčtom hodnoty tovaru a poplatkov za dopravu.

Clo (spolu s DPH) zaplatí v prípade, že hodnota objednávky prekročila sumu 150 eur. Pripomeňme však, že na viaceré druhy tovaru platia výnimky, respektíve nulový colný výmer. Jednou z takýchto kategórií sú aj mobilné telefóny a smartfóny.

ELEKTRONICKÉ BANKOVNÍCTVO

Elektronické bankovníctvo nám umožní rýchly a pohodlný spôsob ako obsluhovať bankové účty, karty, úvery a investície cez internet. Bezpečný prístup do Internet Bankingu máme 24 hodín denne, 7 dní v týždni, po celý rok teraz už z ľubovoľného počítača. Výhody, ktoré nám Internet Banking prináša: (prevzaté z webstránky <http://www.vub.sk/informacie-internet-bankingu/>)

- úsporu na poplatkoch za transakcie,
- nonstop prístup z pohodlia domova, práce alebo zahraničia,
- jednoduché ovládanie s najčastejšie využívanými možnosťami vždy na dosah jedným klikom,
- bezpečnosť transakcií posilnená SMS autorizáciou alebo novými bezpečnostnými prvkami Token a Mobilný Token,

- prehľad o pohyboch na účte, nastavených inkasách, pravidelných platbách, či využívaných službách v rámci Flexiúctu, Start konta alebo Senior konta,
- kontrola nad účtom a platbami kartou cez SMS/E-mail upozornenia,
- rýchle platby do iných bánk, či platby v cudzích menách,
- nový Mobile Banking

V rámci elektronického bankovníctva rozlišujeme:

internet banking – užívateľ používa webové rozhranie pre správu účtu

mobile banking – užívateľ využíva mobilné zariadenia ako napríklad smartphone alebo tablet prostredníctvom aplikácie od svojej banky

Funkcionalita Internet Bankingu je u rôznych poskytovateľov dosť podobná, my si v materiáli priblížime podrobnejšie demo formu Internet Bankingu VUB banky a tiež si vyskúšame simulátor Internet Bankingu Slovenskej sporiteľne.

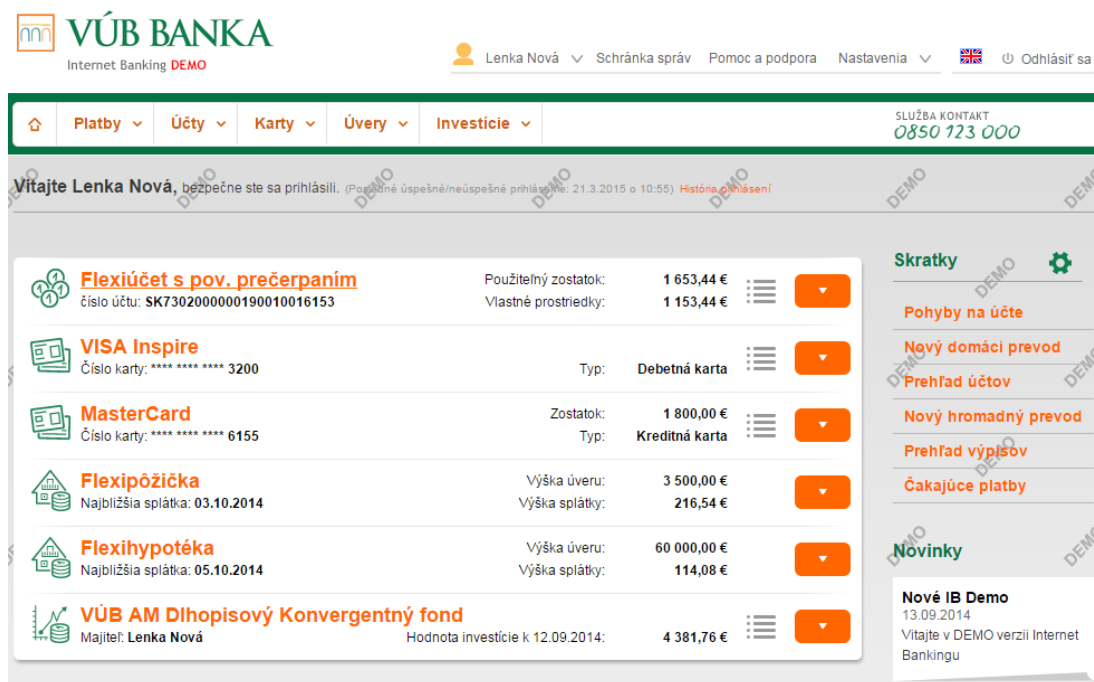
Demo verzia VUB banky je voľne prístupná a môžeme si na nej bez problémov vyskúšať ako funguje zadávanie platieb, inkasa ale i platenie poplatku za kreditnú kartu. (<http://nibdemo.vub.sk/login.html>)

Úvodná stránka demo verzie je zhodná s reálnou stránkou aktuálneho Internet Bankingu VUB banky. Pre prihlásenie je potrebné zadať identifikačné údaje, v prípade demo sú prednastavené. V reálnom Internet Bankingu tieto údaje získame pri aktivácii Internet Bankingu a jedná sa o 10 miestny číselný kód, v niektorých prípadoch o rodné číslo užívateľa.

Aby bolo prihlásenie bezpečné, používa sa dvojstupňová verifikácia klienta. Druhým krokom je v našom prípade overenie pomocou kódu, ktorý nám dôjde na mobil.

V našom prípade sa ten kód sám vyplní. V reálnom Internet Bankingu, sa po kliknutí na Vyžiadať SMS kód odpošle na telefónne číslo ktoré sme uviedli pri aktivácii Internet Bankingu SMS kód. Preto ak by niekto sa chcel dostať do vášho Internet Bankingu, potrebuje mať po ruke i váš telefón. Vygenerovaný kód je platný obmedzený čas, niekoľko minút, konkrétne tu sú to 3 minúty. Potom je neplatný a tak by verifikácia zlyhala.

Po prihlásení sa dostávame na stránku kde je prehľad o všetkých aktuálnych možnostiach tohto konkrétneho Internet Bankingu. Máme tak pod drobnohľadom všetky svoje účty v banke. Možnosť požiadať o pôžičku a celkovo spravovať všetky financie.

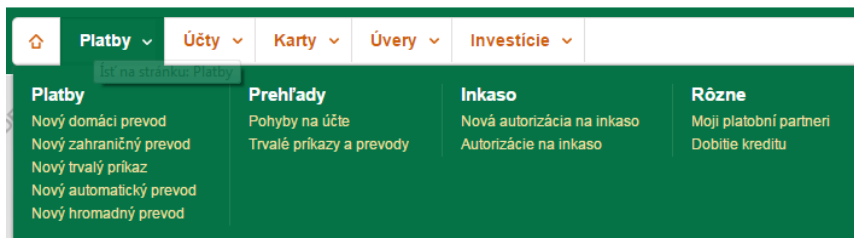


The screenshot shows the VUB BANKA Internet Banking DEMO interface. At the top, there's a navigation bar with the bank's logo and name, and a user profile section for 'Lenka Nová'. Below this is a main menu with categories like 'Platby', 'Účty', 'Karty', 'Úvery', and 'Investície'. The main content area displays a list of accounts and services for 'Lenka Nová', including:

- Flexiúčet s pov. prečerpaním**: Použiteľný zostatok: 1 653,44 €, Vlastné prostriedky: 1 153,44 €
- VISA Inspire**: Číslo karty: **** * 3200, Typ: Debetná karta
- MasterCard**: Zostatok: 1 800,00 €, Typ: Kreditná karta
- Flexipôžička**: Výška úveru: 3 500,00 €, Výška splátky: 216,54 €
- Flexihypotéka**: Výška úveru: 60 000,00 €, Výška splátky: 114,08 €
- VÚB AM Dlhopisový Konvergentný fond**: Hodnota investície k 12.09.2014: 4 381,76 €

On the right side, there's a sidebar with 'Skratky' (Shortcuts) and 'Novinky' (News). The 'Skratky' section includes links like 'Pohyby na účte', 'Nový domáci prevod', 'Prehľad účtov', 'Nový hromadný prevod', 'Prehľad výpisov', and 'Čakajúce platby'. The 'Novinky' section shows a 'Nové IB Demo' announcement dated 13.09.2014.

V karte platby máme viaceré možnosti prevádzania platieb cez domáce platby tak i zahraničné platby ale i nastavenie trvalého príkazu, respektíve inkasného príkazu na niektorú zo služieb (telefón, internet, SIPO, ...), ktoré vo svojom živote využívame.



The screenshot shows the 'Platby' (Payments) section of the VUB BANKA Internet Banking DEMO interface. It features a green header with the word 'Platby' and a sub-header 'Platby'. Below this, there are four main categories of payment services:

- Platby**: Nový domáci prevod, Nový zahraničný prevod, Nový trvalý príkaz, Nový automatický prevod, Nový hromadný prevod
- Prehľady**: Pohyby na účte, Trvalé príkazy a prevody
- Inkaso**: Nová autorizácia na inkaso, Autorizácie na inkaso
- Rôzne**: Moji platobní partneri, Dobíte kreditu

Viac užívateľských funkcií si môžeme vyskúšať experimentovaním v rámci dema. Prevod, ktorý vykonáme, je len fiktívny a teda sa nemusíme báť, že niečo pokazíme. Pozor však, v reálnom Internet Bankingu to neplatí a preto je potrebné dávať si veľký pozor pri písaní čísla účtu a podobne. Je to rovnako ako keď niečo posielame poštou, adresa je dôležitá. A tu je adresou číslo účtu.

Rôzne formy zneužitia Internet Bankingu

Bezpečnú elektronickú komunikáciu medzi bankami a ich klientmi ohrozuje najmä neopatrnosť samotných užívateľov služby Internet Banking. Tí veľakrát nedodržiavajú základné bezpečnostné zásady, čím ohrozujú predovšetkým vlastné peniaze. Asi najznámejším porušovaním bezpečnosti je zaznamenávanie si prihlasovacích údajov na papierik, ktorý si uchovávame pri počítači. Okrem neopatrného zaobchádzania s prihlasovacími údajmi je nebezpečné aj zvolenie príliš jednoduchých alebo ľahko uhádnuteľných hesiel, ale rovnako aj používanie nezabezpečených počítačov. Do Internet Bankingu by sme nemali pristupovať na neznámych počítačoch, a ak sme prihlásení v nezabezpečenej wifi sieti, tak ani prostredníctvom nej. Nebezpečný môže byť samozrejme aj domáci počítač, ak sa nestaráme o jeho aktualizácie antivírusových programov.

Phishing je väčšinou falošný e-mail, ktorý vyzerá, ako by ho zaslala banka, v ktorej máme svoj účet. V takejto elektronickej správe vás zdvorilo žiada o overenie totožnosti a ďalších údajov (napr. čísla kreditnej karty či prístupových kódov). Phishing môže byť aj súčasťou aplikácie, ktorú sme si nainštalovali do svojho mobilného telefónu. Phishing môže obsahovať skrytý vírus, ktorý sa bez vedomia užívateľa nainštaluje do počítača, poškodzuje programy, mení nastavenia a odosiela rôzne údaje bez vášho vedomia.

Pharming využíva špeciálne počítačové programy, ktoré užívateľa pri prihlásení do internetového bankovníctva presmerujú na stránky, ktoré vyzerajú ako stránky jeho banky, ale v skutočnosti sú iba ich napodobeninou. Tie vytvorili hackeri, ktorí chcú získať dôverné údaje. Dizajn stránok je podobný alebo skoro rovnaký ako oficiálna stránka banky. Návštevník stránky preto ani nemusí zistiť, že má otvorenú falošnú webovú stránku.

Vishing je podvodný postup s využitím telefonického rozhovoru, pomocou ktorého sa útočník snaží od klienta získať citlivé údaje (osobné údaje, prístupové heslá do Internetbankingu, čísla platobných kariet a pod.). Útočník klientovi pošle SMS so stručnou informáciou, že bola zistená podozrivá transakcia na jeho účte. Súčasťou SMS správy je aj telefónne číslo, z ktorého ho bude útočník kontaktovať, resp. klient má ihneď kontaktovať toto telefónne číslo. Následne sa útočník predstaví ako jeho banka. Aby si získal dôveru klienta, opýta sa ho na pozíciu, resp. niekoľko pozícií z GRID karty alebo sa opýta na autorizačný kód práve doručenej SMS. Tieto údaje neskôr, resp. okamžite využije na podvodné získanie finančných prostriedkov z účtu klienta. Útočník ukončí hovor s tým, že rýchlym konaním banky sa podozrivá transakcia neuskutočnila a klientove peniaze sú v bezpečí.

E-GOVERNMENT

Od 1. novembra 2013 je účinný zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente). Tento zákon upravuje niektoré informačné systémy pre výkon pôsobnosti orgánov verejnej moci v elektronickej podobe, elektronické podanie, elektronický úradný dokument a niektoré podmienky a spôsob výkonu verejnej moci elektronicky a elektronickej komunikácie, elektronické schránky a elektronické doručovanie, identifikáciu osôb a autentifikáciu osôb, autorizáciu, zaručenú konverziu, spôsob vykonania úhrady orgánu verejnej moci.

Pre zabezpečenie elektronickej komunikácie sú zavádzané komunikačné rozhrania tzv. prístupové miesta. Môžu to byť:

- **Ústredný portál verejnej správy** je informačný systém verejnej správy, prostredníctvom ktorého je možné centrálnne vykonávať elektronickú úradnú komunikáciu s ktorýmkoľvek orgánom verejnej moci a prístupovať k spoločným modulom, a to najmä prostredníctvom siete internet.
- **Špecializovaný portál** je informačný systém verejnej správy, prostredníctvom ktorého je možné vykonávať elektronickú úradnú komunikáciu s jedným alebo viacerými orgánmi verejnej moci, ktoré ho zriadili, a to najmä prostredníctvom siete internet. Špecializovaný portál zriaďuje orgán verejnej moci, na elektronickú úradnú komunikáciu s ktorým má tento portál slúžiť, pričom orgány verejnej moci môžu po dohode zriaďiť špecializovaný portál aj na spoločný prístup k elektronickej úradnej komunikácii s viacerými orgánmi verejnej moci.
- **Integrované obslužné miesto** slúži na asistovanú elektronickú úradnú komunikáciu fyzických osôb a právnických osôb s orgánmi verejnej moci pri výkone verejnej moci elektronicky.
- **Ústredné kontaktné centrum** slúži na telefonické poskytovanie informácií o výkone verejnej moci elektronicky a o činnosti orgánov verejnej moci s tým súvisiacej, ak takéto poskytovanie informácií nie je v rozpore s osobitnými predpismi.

Správca ústredného portálu verejnej správy zabezpečuje komunikačné rozhrania na zabezpečenie elektronickej komunikácie a to **spoločnými modulmi**, ktoré sú:

Modul elektronických schránok je modul určený pre správu elektronických schránok a zabezpečenie fungovania elektronických schránok.

Autentifikačný modul na základe identifikátora osoby a autentifikátora zabezpečuje autentifikáciu osoby

Platobný modul sprostredkúva vykonanie úhrady a poskytnutie informácie o úhrade.

Modul centrálnej elektronickej podateľne zabezpečuje funkcie elektronickej podateľne a službu časovej pečiatky na spracovanie elektronických podaní a vytváranie elektronických úradných dokumentov.

Modulu elektronických formulárov zabezpečuje programové nástroje na tvorbu elektronických formulárov, vedenie platných elektronických formulárov, ako aj elektronických formulárov so zrušenou platnosťou, sprístupňovanie elektronických formulárov podľa požiadaviek na typ elektronického formulára a dobu platnosti,

Modul elektronického doručovania zabezpečuje elektronické doručovanie a jeho prostredníctvom sa vykonáva doručenie elektronickej správy odosielanej orgánom verejnej moci osobe, ktorá nie je orgánom verejnej moci, alebo v konaní alebo vo veci, v ktorej sa doručuje, nevystupuje v postavení orgánu verejnej moci.

Notifikačný modul zabezpečuje zasielanie notifikácií.

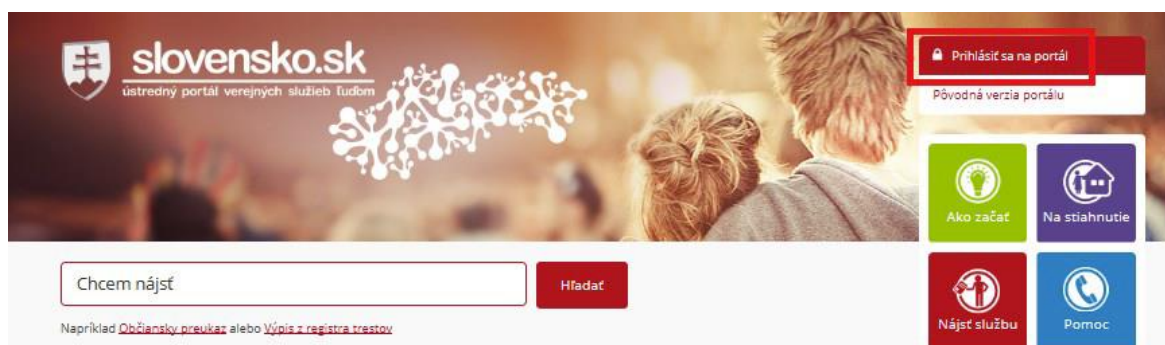
Modul úradnej komunikácie zabezpečuje prostredie pre elektronickú komunikáciu medzi agendovými systémami a inými informačnými systémami v správe rôznych orgánov verejnej moci pri výkone verejnej moci elektronicke a poskytuje funkciu podpory petícií.

Modul dlhodobého uchovávania zabezpečuje dlhodobé uchovávanie elektronických dokumentov a elektronických správ podľa tohto zákona.

Elektronické schránky

Elektronické schránky sa zriaďujú orgánu verejnej moci, právnickej osobe, fyzickej osobe, podnikateľovi, subjektu medzinárodného práva. Elektronická schránka sa zriaďuje bezodplatne. Každému je možné zriadiť len jednu elektronickú schránku pre jedno právne postavenie.

Postup pri prihlásení sa na Ústredný portál verejnej správy prostredníctvom občianskeho preukazu s čipom Na titulnej stránke portálu na adrese www.slovensko.sk kliknete na ikonu vpravo hore „Prihlásiť sa na portál“



Ak nemáte pripojenú čítačku čipových kariet zobrazí sa vám okno, v ktorom budete vyzvaní na jej pripojenie. Následne budete vyzvaní na vloženie občianskeho preukazu s čipom (eID karty) do čítačky čipových kariet Občiansky preukaz s čipom je dôveryhodným a bezpečným nosičom identifikačných údajov občana a slúži na preukazovanie totožnosti občana v elektronickom prostredí. Proces overenia identity

osoby sa nazýva autentifikácia. Na úspešnú identifikáciu a autentifikáciu osoby je potrebné zadať 6 – miestny bezpečnostný osobný kód (BOK)

Aplikácia eID klient

Elektronická identifikácia

Zadajte BOK k vášmu občianskemu preukazu s čipom (6 číslí):

1 2 9

4 3 6

8 5 7

← 0 OK

Rozloženie klávesnice
☐ usporiadané ☒ náhodné

Údaje z vášho čipu poskytnete subjektu
Národná agentúra pre sieťové a elektronické služby
[viac informácií](#)

Poskytované údaje:
[viac informácií](#)

Zrušiť

Zostávajúci čas: 9:48

Systém overí váš zadaný bezpečnostný osobný kód a dokončí autentifikáciu osoby. Po úspešnej autentifikácii budete presmerovaní na úvodnú stránku portálu alebo sa vám zobrazí stránka s ponukou výberu subjektu na prihlásenie. Po potvrdení výberu subjektu budete presmerovaní na úvodnú stránku portálu.

Kvalifikovaný elektronický podpis v elektronickom svete nahrádza vlastnoručný podpis pri papierovom úradnom vybavovaní. Podania na orgány verejnej správy musia byť podpísané kvalifikovaným podpisom.

Kvalifikovaný elektronický podpis vytvoríte aplikáciou na podpisovanie. Na ústrednom portáli sú na podpisovanie voľne dostupné aplikácie. Na vytvorenie kvalifikovaného elektronického podpisu potrebujete vlastniť kvalifikovaný certifikát, ktorý je momentálne jednoduché získať pri vydaní občianskeho preukazu s čipom alebo následne o neho požiadať po vydaní občianskeho preukazu na oddelení dokladov Okresného riaditeľstva Policajného zboru.

Občiansky preukaz s čipom

Občiansky preukaz s čipom – je nový typ občianskeho preukazu s elektronickým čipom, ktorý sa vydáva od decembra 2013. Služí, tak ako doteraz, na preukazovanie totožnosti občana SR pri osobnom styku s úradmi a inštitúciami. Navyše obsahuje elektronický čip a tým umožňuje preukazovanie totožnosti občana v elektronickom prostredí pri využívaní elektronických služieb verejnej správy (e-Government služieb). Občiansky preukaz je na zadnej strane vybavený elektronickým kontaktným čipom, v ktorom sú uložené údaje uvedené na občianskom preukaze (meno, priezvisko, bydlisko, dátum narodenia atď.).

V prípade, že sa občan rozhodne využívať ho na prístup k elektronickým službám, zadá si pri podaní žiadosti o jeho vydanie resp. pri preberaní občianskeho preukazu s

čipom alebo kedykoľvek počas jeho platnosti svoj bezpečnostný osobný kód – BOK. Bezpečnostný osobný kód je kombináciou šiestich ľubovoľných číslic.

Občanovi vystavením občianskeho preukazu s čipom a zadaním bezpečnostného osobného kódu nevzniká povinnosť využívať dostupné elektronické služby, iba mu dáva možnosť komunikovať elektronicky.

Čo je potrebné ešte vedieť pre vytváranie kvalifikovaného elektronického podpisu **ZEP-PIN**. Ten slúži podobne ako pri telefónoch na blokovanie, overovanie majiteľa podpisu. ZEP PIN je teda bezpečnostná ochrana občianskeho preukazu pred vytvorením kvalifikovaného elektronického podpisu neoprávnenou osobou.

Ďalšou bezpečnostnou ochranou vytvárania kvalifikovaného elektronického podpisu prostredníctvom občianskeho preukazu je limitovaný počet nesprávne zadanej hodnoty ZEP PIN-u. Po troch nesprávne zadanych hodnôt ZEP PIN-u sa zablokuje možnosť použitia súkromného kľúča na vytvorenie podpisu. Odblokovanie je možné len prostredníctvom **ZEP PUK**-u.

Dĺžka ZEP PIN kódu je 6 číselných znakov a ZEP PUK je 8 číselných znakov.

1.2 Bezpečnosť a ochrana

Počítačová bezpečnosť je oblasť vedy o počítačoch, ktorá sa zaoberá odhaľovaním a eliminovaním rizík spojených s používaním počítača.

Cieľom počítačovej bezpečnosti je zabezpečiť:

- ochranu pred neoprávneným manipulovaním s dátami a so zariadeniami počítačového systému,
- ochranu pred nelegálnou tvorbou kópií dát,
- bezpečnú komunikáciu a prenos dát,
- integritu a nepodvrhnutelnosť dát.

Koncepcia počítačovej bezpečnosti spočíva v troch krokoch:

- prevencia - ochrana pred hrozbami,
- detekcia - odhalenie neoprávnenej činnosti a slabého miesta v systéme,
- náprava - odstránenie slabého miesta v systéme.

Malware je všeobecné označenie škodlivého softvéru.

Patria sem napríklad vírusy, červy, trójske kone (spyware, adware, ransomware, dialer, rootkit, back door, botnet). Malware sa do počítača v dnešnej dobe dostáva zvyčajne cez Internet, hlavne pri prezeraní škodlivých stránok s nedostatočne zabezpečeným systémom.

1.2.1 Rozoznávať spôsoby svojej ochrany počas online prítomnosti na internete: nakupovať zo zabezpečených a overených webových sídiel (stránok), vyhýbať sa odkrytiu osobných a finančných informácií, odpojenie sa od webového sídla.

Vírus – nesamostatný počítačový program. Od normálnych programov sa líši najmä tým, že je schopný „neviditeľne“ sa šíriť s inými programami. Pripojí sa k ich programovým súborom. Vírusy môžu byť neškodné, ale môžu mať tiež úplne deštruktívne účinky na dáta na disku. Všeobecne však ide o nežiadúce prvky v našom počítači a mali by sme sa snažiť vyhnúť sa nakazeniu nášho počítača vírusom.

Okrem infikovania počítača vírusom prostredníctvom USB, CD (DVD) nosiča alebo elektronickej pošty, existuje riziko nakazenia počítača z lokálnej siete, prostredníctvom súborom stiahnutým z webu, z niektorých webových stránok.

Preto je veľmi dôležité skontrolovať súbory stiahnuté z internetu spoľahlivým antivírusovým programom, ktorý by sme mali pravidelne aktualizovať.

Bez ohľadu na spôsob, akým sa môže dostať vírus do nášho počítača, je dôležitá prevencia a dodržiavanie zásad, ktoré by nakazeniu počítača mohli zabrániť. Čiže kvalitný a spoľahlivý antivírusový program, pravidelná aktualizácia, kontrolovať USB, stiahnuté súbory...

Stále najúčinnnejšou ochranou proti vírusom je zabrániť ich prieniku do počítača.

Pri počítačových systémoch platí to, čo tvrdia všetci lekári. Najlepšou liečbou je prevencia. Je to tak preto, pretože i počítačové vírusy môžu zmutovať a ich liečbou môžeme napáchať viac škody ako úžitku. Odporúčania sú tieto:

- Zálohujte všetky svoje údaje na disky chránené proti zápisu. Zálohovaním dát sa vyhniete i strate konzistencie dát následkom výpadku prúdu alebo tvrdého reštartu.
- Zabezpečte svoj počítač proti neoprávnenému vniknutiu. Tento krok môžete urobiť použitím tzv. **Firewallu**, ktorý vytvára ochrannú hrádzu medzi vašim počítačom a potenciálne škodlivým obsahom na Internete. Je to veľmi účinná zbraň proti počítačovým červom. Môže byť buď hardvérový (zariadenie) alebo softvérový (program). Takýto softvérový firewall je i súčasťou Windows 10.
- Nenavštevujte nebezpečné stránky a nestahujte programy na sťahovanie hudby, filmov a programov. Snažte sa vyhnúť stránkam s pornografiou, stránkam s mp3 hudbou, filmami, licenčnými kľúčmi a podobne. Nestahujte žiadne programy, ktorých činnosť by mohla byť v rozpore s autorskými zákonmi.
- Pred stiahnutím každého Freeware programu si pozorne prečítajte podmienky používania programu a vyhnite sa všetkým programom, ktoré podmieňujú svoju inštaláciu nainštalovaním tzv. THIRD PARTY COMPONENTS (komponenty od tretích strán). V niektorých prípadoch programy obsahujú komponenty od tretích strán, ktoré sa dajú počas inštalácie vypnúť. Pri

inštalácia buďte preto vždy opatrný a pozorne sledujte možnosti na každej obrazovke prebiehajúcej inštalácie.

- Nezverejňujte svoju emailovú adresu. Používajte radšej niekoľko adries (jednu pre priateľov a druhú na vyplňovanie do formulárov).
- Neotvárajte neznáme prílohy. Pred otvorením podozrivej prílohy emailu si radšej overte či Vám ju dotýčný chcel poslať.
- Nepripájajte neoverený zásuvný modul ActiveX. V súčasnosti sa moduly podpisujú digitálnym podpisom. Preto si pred jeho spustením overte platnosť digitálneho podpisu a nikdy si nepripojte neznámy prvok.
- Nespúšťajte neoverené makrá v dokumentoch. V súčasnosti sa i makrá podpisujú digitálnym podpisom. Preto si pred jeho spustením overte platnosť digitálneho podpisu a neaktivujte neznáme makro.
- Udržujte všetky súčasti systému aktuálne, používajte najnovšiu verziu prehliadača a poštového klienta. Aktualizovaním súčastí systému odstraňujete jeho nedostatky, ktoré by škodlivé programy mohli využiť.
- Chráňte svoj počítač aktuálnym antivírovým systémom. Antivírový systém Vás ochráni pred väčšinou starších hrozieb a niektorými z najnovších. Aby bola ochrana účinná, antivírové systémy sa aktualizujú i niekoľkokrát za deň. Najznámejšie antivírové program sú NOD, Avast, AVG...
- Chráňte svoj počítač proti špiónážnym programom. Na ochranu proti takýmto programom sú najvhodnejšie programy Windows Defender priamo od spoločnosti Microsoft, Ad-Aware SE Personal Edition, Spybot Search&Destroy, Spyware Terminator. Tieto programy sa aktualizujú rovnako ako antivírové systémy, preto ich treba udržiavať vždy aktuálne.
- Nikdy nepracujte s internetom a poštou s oprávneniami správcu počítača. Oprávnenie správcu počítača umožňuje trójskym koňom dokonalé maskovanie. Svoje oprávnenie môžete znížiť vytvorením nového konta s obmedzenými právami. Pod takto vytvoreným kontom nebudete mať právo inštalovať nové programy do počítača a meniť niektoré nastavenia systému. Ak tak budete chcieť urobiť, tak sa odhláste zo systému a prihláste sa opäť pod kontom správcu. Pod kontom správcu však nechod'te na internet ani nečítajte poštu.
- Zvážte, ktoré priečinky budete zdieľať v sieti. Nastavte na všetky zdieľané priečinky príslušné oprávnenia a chráňte k nim prístup heslom.
- Vypnite automatické spúšťanie programu po vložení média (CD, DVD, USB DISK).

Riziká pri použití kreditnej (platobnej) karty na platbu prostredníctvom internetu

Na Slovensku sa elektronický obchod zatiaľ len rozmáha a stáva sa pre ľudí stále obľúbenejší. Umožňuje im totiž pohodlný nákup, vybavenie rôznych platieb... So

zlepšovaním prístupu na internet ja aj možnosť platieb cez internet bližšia širokej verejnosti.

Nie len v zahraničí je bežné uhrádzanie rôznych platieb pri nákupe, rezervácií prostredníctvom kreditných kariet.

Ľudia si uvedomujú, že elektronická platba je efektívnejšia ako platba v hotovosti.

Avšak pri týchto pomerne závažných úkonoch na sieti treba veľmi myslieť na bezpečnosť. Ide predsa o prácu s peniazmi, osobnými údajmi, rôznymi prístupovými kódmi... Treba si vždy overiť dôveryhodnosť organizácie, s ktorou takouto elektronickou formou komunikujeme. Na to slúžia certifikáty. Tiež treba dbať na zabezpečenie komunikácie cez https protokol.

Aj keď všetka komunikácia je šifrovaná, používatelia = klienti bánk majú pridelené užívateľské mená, heslá, rôzne prístupové kódy, ktoré majú zabezpečiť ich overenie a identifikáciu, mali by sme byť veľmi opatrní. Vždy si treba naozaj rozmyslieť, kde zverejníme číslo svojho účtu, svoje osobné údaje a pod.

Pojem stena (firewall)

Internet je rozľahlá verejná celosvetová počítačová sieť. Z dôvodov bezpečnosti je preto nanajvýš vhodné použiť prostriedky na akési bezpečnostné oddelenie lokálnej siete od internetu. Využiť môžeme technológie hardvérové alebo softvérové a tak zabrániť neautorizovanému preniknutiu do nášho počítača. Spoločne ich nazývame - **firewall**.

Firewall slúži na oddelenie jednej siete od druhej z dôvodov bezpečnosti. Aby nikto bez príslušných práv prístupu nemohol získať prístup k počítačom v lokálnej sieti.

Hardvérový firewall sa niekedy označuje tiež ako firewall machine, softvérový firewall ako firewall code.

1.2.2 Vedieť, čo je šifrovanie (encryption, decryption).

V súčasnej dobe sa stále aktuálnejšou stáva otázka elektronického podpisu a šifrovania. Stále obľúbenejšie sú u používateľov služby, ktoré im prostredníctvom internetu šetria čas a urýchľujú vybavovanie rôznych úradných a administratívnych úkonov – bankové prevody... V oblasti elektronického bankovníctva je bezpečnosť veľmi dôležitá.. Komunikácia medzi klientom a bankou prebieha šifrované.

Šifrovanie je „znečitateľnenie“ dokumentu pre toho, komu nie je určený, je to vlastne utajenie obsahu.

Nemali by sme si však mýliť šifrovanie s kódovaním, čo je ukladanie informácií zvyčajne v číselnej reprezentácii a uľahčenie ich prenosu. Na odkódovanie nám stačí poznať postup. Avšak na odšifrovanie správy musíme poznať aj akési heslo a kľúč.

Rozlišujeme **symetrické** a **asymetrické šifrovanie**. Pri symetrickom šifrovaní používame jediný kľúč, ktorým možno správu zašifrovať i odšifrovať. Môžeme to prirovnať k trezoru, ktorý môže otvoriť každý, kto má od neho kľúč. Pri asymetrickom šifrovaní používame dvojicu kľúčov (key pair). Ak jedným správu

zašifrujeme, odšifrovať ju môžeme jedine druhým. Obidva kľúče boli spolu vygenerované, spolu matematicky súvisia, ale znalosťou jedného si nevieme odvodiť druhý.

Digitálny certifikát je digitálne podpísaný verejný kryptografický kľúč, vydaný certifikačnou autoritou, v asymetrickej šifrovaní, ktorý obsahuje (okrem iného) informácie o držiteľovi verejného kľúča a emitentovi certifikátu (výrobca digitálnych podpisov, tj certifikačná autorita). Certifikáty sa používajú na identifikáciu protistrany pri vytváraní zabezpečeného pripojenia (HTTPS, VPN atď.). Na základe princípu prenosu dôvery je možné dôverovať neznámym certifikátom, ktoré podpísali dôveryhodná certifikačná autorita.

Certifikačná autorita (CA skratka) je v asymetrickej kryptografii, ktorá vydáva digitálne certifikáty (elektronické podpisovanie šifrovaním verejným kľúčom), a tým uľahčuje používanie infraštruktúry verejných kľúčov (PKI) potvrdením pravosti údajov. Na základe zásady prevodu dôvery (pozri nižšie) môžeme dôverovať údajom uvedeným v digitálnom certifikáte za predpokladu, že dôverujeme samotnej certifikačnej autorite.

Kvalifikovaný certifikát osoby spája identitu vlastníka súkromného kľúča s verejným kľúčom slúžiacim na overenie jeho pečatí alebo podpisov, pričom všetky údaje obsiahnuté v kvalifikovanom certifikáte boli v čase jeho vydania poskytovateľom certifikačných služieb overené ako platné.

Kvalifikovaný certifikát fyzickej osoby podľa § 3 ods. 4 vyhlášky NBÚ č. 131/2009 Z. z. musí obsahovať minimálne:

- krstné meno v givenName, priezvisko v surname alebo pseudonym v pseudonym a
- doplňujúci identifikátor zabezpečujúci jednoznačnosť identifikačných údajov držiteľa kvalifikovaného certifikátu v serialNumber vo forme „PNO“ (SK legislatíva) a môže obsahovať aj (legislatíva EÚ - eIDAS) „IDC“ a „PAS“.

Dôveryhodnosť zaručeného elektronického podpisu je zabezpečovaná tzv. **stromom dôvery**. Základňa stromu je tvorená držiteľmi kvalifikovaných certifikátov, stred akreditovanými certifikačnými autoritami (ACA) a na vrchole stromu dôvery je koreňová certifikačná autorita (KCA) spravovaná odborom prevádzky sekcie informačnej bezpečnosti a elektronického podpisu Národného bezpečnostného úradu. Pomocou verejného kľúča koreňovej certifikačnej autority je možné overiť pravosť certifikátu kvalifikovanej dôveryhodnej služby a pomocou verejného kľúča kvalifikovaného poskytovateľa dôveryhodnej služby je možné overiť pravosť kvalifikovaného certifikátu klienta a jeho totožnosť.

Certifikačná cesta sa zostavuje od certifikátu koncovej entity až po dôveryhodnú koreňovú CA. Teda certifikačné cesty pozostávajú z certifikátu koncového užívateľa a certifikátov certifikačných autorít.

Elektronický podpis sú elektronické identifikačné údaje autora (odosielateľa) elektronického dokumentu, pripojené k nemu.

Elektronický podpis je digitálny podpis, ktorým podpisujúci potvrdzuje, že je skutočne ten, za ktorého sa vydáva, a že súhlasí s obsahom podpísaného elektronického dokumentu. Pričom elektronickým dokumentom je číselne kódovaný dokument uchovávaný na fyzickom nosiči, prenášaný alebo spracúvaný pomocou technických prostriedkov v elektrickej, magnetickej, optickej alebo inej forme. Podľa zákona je elektronický podpis informácia pripojená alebo inak logicky spojená s elektronickým dokumentom. Kvalifikovaný elektronický podpis je, v zmysle zákona č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu (zákon o dôveryhodných službách), zdokonalený elektronický podpis vyhotovený s použitím kvalifikovaného zariadenia na vyhotovenie elektronického podpisu a založený na kvalifikovanom certifikáte pre elektronické podpisy.

Kvalifikovaný elektronický podpis je elektronický podpis v podobe, kde je možné overiť pravosť dokumentov a autentifikáciu podpísaného. Toto je zaručené spravidla kryptografickými metódami. Zaručený elektronický podpis môže byť vyhotovený iba pomocou certifikovanej aplikácie, bezpečného zariadenia na vyhotovenie elektronického podpisu a kvalifikovaného certifikátu. Zaručený elektronický podpis dokumentu zabezpečuje:

- autenticitu – možno overiť pôvodnosť (identitu subjektu, ktorému patrí elektronický podpis),
- integritu – možno preukázať, že po podpísaní nedošlo k žiadnej zmene, súbor nie je úmyselne alebo neúmyselne poškodený,
- nepopierateľnosť – autor nemôže tvrdiť, že podpísaný elektronický dokument nevytvoril (napr. nemôže sa zriecť vytvorenia a odoslania výhražného listu)

Rozdiel medzi jednoduchým a zaručeným elektronickým podpisom je podobný rozdielu medzi úradne neovereným a overeným vlastnoručným podpisom, pričom možnosť, obťažnosť a spoľahlivosť písomznaleckej analýzy neovereného vlastnoručného podpisu možno prirovnáť k možnosti, obťažnosti a spoľahlivosti overenia autenticity nezaručeného elektronického podpisu.

Kvalifikovaný elektronický podpis a vlastnoručný podpis

Pomocou kvalifikovaného elektronického podpisu je možné elektronicky realizovať právne úkony, ktoré v papierovom svete vyžadujú písomnú formu (§ 40 ods. 4 zákona č. 40/1964 Z. z. Občiansky zákonník), t. j. takýto elektronický podpis v tomto prípade nahrádza písomnú podobu vlastnoručného podpisu. Z uvedeného dôvodu je nevyhnutné jeho použitie pri niektorých úkonoch uskutočňovaných v rámci komunikácie s orgánmi verejnej moci a komerčným sektorom.

Kvalifikovaný elektronický podpis elektronického dokumentu zabezpečuje: autenticitu – možno jednoznačne overiť identitu subjektu, ktorý podpis vytvoril, integritu – možno preukázať, že po podpísaní dokumentu nedošlo k žiadnej úmyselnej alebo neúmyselnej zmene obsahu dokumentu, aký bol v čase jeho podpisovania, nepopierateľnosť – autor nemôže tvrdiť, že nevyhotovil daný podpis

elektronického dokumentu. Podpis môže obsahovať časovú pečiatku, ktorá jednoznačne preukazuje dátum a čas podpísania dokumentu. Časová pečiatka je ekvivalentom pečiatky na dokumente ako informácia pripojená alebo inak logicky spojená s elektronickým dokumentom, ktorá musí spĺňať tieto požiadavky:

- a) nemožno ju efektívne vyhotoviť bez znalosti súkromného kľúča určeného na tento účel a bez elektronického dokumentu,
- b) na základe znalosti verejného kľúča patriaceho k súkromnému kľúču použitému pri jej vyhotovení možno overiť, že elektronický dokument, ku ktorému je pripojená alebo s ním inak logicky spojená, je zhodný s elektronickým dokumentom použitým na jej vyhotovenie,
- c) vyhotovila ju akreditovaná certifikačná autorita použitím súkromného kľúča určeného na tento účel,
- d) možno ju vyhotoviť len použitím bezpečného zariadenia na vyhotovovanie časovej pečiatky,
- e) na verejný kľúč patriaci k súkromnému kľúču použitému na jej vyhotovenie vydala akreditovaná certifikačná autorita certifikát,
- f) umožňuje jednoznačne identifikovať dátum a čas, kedy bola vyhotovená.

V obchodnom styku platí zmluvná voľnosť aj vo vzťahu k formátu elektronického dokumentu. V administratívnom styku sa však môžu používať iba vybrané druhy formátov dokumentov.

Obchodným stykom je odoslanie, prijatie alebo potvrdenie odoslania, alebo potvrdenie prijatia dokumentu v elektronickej podobe (ďalej len „elektronický dokument“) vo vzťahoch, ktoré vznikajú pri elektronickom obchode medzi poskytovateľom služieb informačnej spoločnosti a ich príjemcom alebo spotrebiteľom.

Administratívnym stykom je odoslanie, prijatie alebo potvrdenie odoslania, alebo potvrdenie prijatia elektronického dokumentu podpísaného platným elektronickým podpisom alebo kvalifikovaným elektronickým podpisom medzi orgánmi verejnej moci alebo medzi orgánom verejnej moci a fyzickou osobou, alebo medzi orgánom verejnej moci a právnickou osobou.

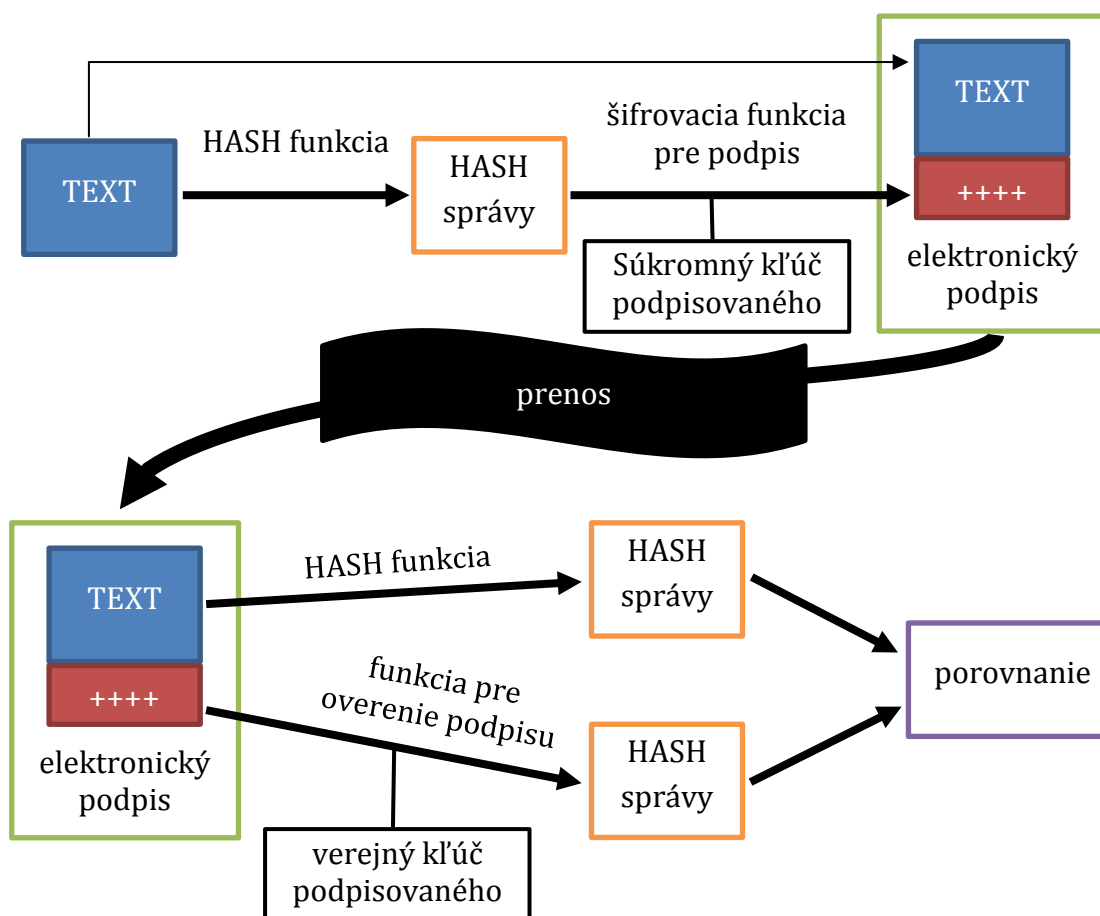
Občan môže využiť kvalifikovaný elektronický podpis pri komunikácii s orgánmi verejnej moci prostredníctvom ústredného portálu verejnej správy (www.slovensko.sk) napr. pri použití služby "Všeobecná agenda", služieb obchodného registra alebo služieb živnostenského registra. Ďalej je ho možné využiť napr. pri komunikácii s finančnou správou SR (daňové úrady, colné riaditeľstvo), pri komunikácii so súdmi v SR.

Na vyhotovenie kvalifikovaného elektronického podpisu musí mať občan k dispozícii:

- elektronický dokument,

- **súkromný kľúč** uložený na bezpečnom zariadení, (Súkromný kľúč je tajná informácia, ktorá slúži na vyhotovenie elektronického podpisu alebo zaručeného elektronického podpisu elektronického dokumentu.)
- **verejný kľúč** patriaci k súkromnému kľúču, na ktorý bol vydaný akreditovanou certifikačnou autoritou kvalifikovaný certifikát, (Verejný kľúč je informácia dostupná overovateľovi, ktorá slúži na overenie správnosti elektronického podpisu alebo zaručeného elektronického podpisu vyhotoveného pomocou súkromného kľúča patriaceho k danému verejnému kľúču.)
- prostriedok na vyhotovenie elektronického podpisu certifikovaný NBÚ SR.

Elektronické podpisovanie správy prebieha tak, že sa pomocou jednocestnej funkcie (hash funkcie) vytvorí tzv. digitálny odtlačok správy, ktorý je zašifrovaný tajným (súkromným) kľúčom a pridaný k tejto správe. Je to kryptografická charakteristika – Message Digest, ktorá charakterizuje spracovávaný dokument. Prijemca dešifruje získaný zašifrovaný odtlačok verejným kľúčom (obsiahnutým v certifikáte) a opäť pomocou hash funkcie vygeneruje z prijatej správy alebo dátového súboru nový odtlačok, pričom oba porovná a v prípade, že sú totožné, je elektronický podpis platný. Účinnosť podpisu závisí na kvalite jednocestnej hash funkcie a na účinnosti šifrovania tohto hash-a.



Hash-ovanie je postup spracovania, ktorý využíva vlastnosti špeciálnych tried matematických funkcií nazvaných jednosmerné funkcie, alebo kryptografické

hash-ovacie funkcie, ktoré umožňujú priradiť elektronickému informačnému reťazcu charakteristickú hodnotu tak, že výsledok spracovania je pre daný reťazec jednoznačnou hodnotou. Zároveň platí, že na základe znalosti charakteristickej hodnoty získanej spracovaním informačného reťazca hash-ovacou funkciou nie je možné zrekonštruovať pôvodný informačný reťazec. Je to teda matematická funkcia, ktorú je možné v jednom, priamom smere jednoducho spočítať, zatiaľ čo v opačnom smere (inverznom zobrazení) prebiehajú výpočty veľmi obtiažne.

Hash je v podstate miniatúrny odtlačok obsahu dokumentu. Výsledkom hash funkcie je 128 alebo 160 bitov dlhá sekvencia jednoznačne charakterizujúca vstupný blok dát.

1.2.3 Rozpoznať zabezpečené webové sídla napr. podľa šifrovaného prenosového protokolu https a symbolu zámky.

V súvislosti s bezpečnosťou na sieti si treba počítač uchrániť pred prenikaním všetkého druhu a pred neoprávneným prístupom k údajom, ktoré odosielame z počítača alebo ich na náš počítač prijímame.

Jednou z úloh správcu je zabrániť prístupu neautorizovaných používateľov internetu k počítaču, webovému sídlu a dátam všeobecne.

Webové stránky firiem, organizácii ale aj osobné stránky sa stávajú terčom útokov niektorých ľudí zvonku. Preto sa dôraz kladie na bezpečnosť stránok a dokumentov, ktoré sa prípadným útokom môžu dostať do rúk nepovolanych osôb.

Každý užívateľ počítača, počítačovej siete, by mal mať na svoju identifikáciu tzv. **užívateľské meno** a k nemu **heslo**. Menom a heslom by sa mal identifikovať používateľ sieťových tlačiarň a pod.

Z hľadiska ochrany dát v sieti Internet, aby sa predišlo počítačovej kriminalite, mnohé firmy zabezpečujú prístup k dátam pre svojich klientov a zamestnancov pomocou užívateľského mena a hesla.

Zabezpečeným sídlom môžeme napríklad chápať stránky bánk (časť internetbanking), kde prevádzame naše transakcie. Vstup ku kontu je možný až po prihlásení sa – **identifikácia**.

Užívateľské meno. Meno alebo prezývka používateľa, ktorý si ho zvolil resp. mu bolo užívateľské meno pridelené. Skladá sa z alfanumerických znakov, špeciálnych znakov ako podčiarkovník atď...väčšinou bez diakritických znakov, bez medzier. Sú systémy, ktoré nekladú žiadne podmienky na tvar, formu a dĺžku užívateľského mena.

Heslo. Vytvorené k príslušnému užívateľskému menu. Heslo si vytvorí osoba, ktorej bolo pridelené užívateľské meno alebo nám heslo pridelia spolu s týmto menom. Heslo, ktoré nám je pridelené, by sme mali hneď po prvom prihlásení zmeniť. Pri vytváraní alebo zmene hesla by sme mali dodržiavať základné pravidlá, aby nebolo naše heslo ľahko „uhádnuteľné“. Heslo zadávame väčšinou „naslepo“ = pri písaní sa na obrazovke neobjaví. Sú však situácie, keď si vieme pozrieť nami zadané heslo

napríklad na mobilných zariadeniach alebo vedľa poľa hesla je symbol oka, ktorý nám zobrazí heslo. Systém, do ktorého sme sa prihlásili menom a heslom, dvojicu „meno – heslo“ porovná a v prípade súladu so skôr nadefinovanou tabuľkou hesiel nám umožní prístup. Na základe správcom nadefinovaných právomocí nám systém môže umožniť prístup len k istým prostriedkom, programom, funkciám...

Komunikácia na zabezpečených stránkach používa protokol **https**. **https** = **http over SSL/TLS**:

- potvrdzuje identitu servera (aby sme vedeli, že komunikujeme s tým správnym),
- zabezpečuje šifrovanie prenášaných údajov (nie je možné získať informácie odpočúvaním),
- zabezpečuje kontrolu integrity prenášaných údajov (nie je možné nepozorovane zmeniť prenášané informácie),
- využíva asymetrické šifrovanie.

1.2.4 Vedieť, čo je digitálny certifikát webového sídla.

Digitálny certifikát nazývame tiež Digital ID. Je to akási elektronická verzia našej identifikácie, digitálna obdoba občianskeho preukazu alebo pasu. Používa sa na preukázanie našej identity, alebo našich práv pri elektronickej komunikácii, alebo pri prístupe k informáciám a službám on-line.

V použití so šifrovaním poskytuje Digitálny Certifikát kompletné bezpečnostné riešenie, a zaisťuje identitu všetkých zúčastnených strán na danej transakcii.


Digitálny certifikát vystavuje certifikačná autorita. **Certifikačná autorita** ručí za totožnosť majiteľa certifikátu. Ak vlastníme certifikát, môžeme napríklad posilať digitálne podpísané e-mailové správy. Certifikát umožňuje tiež výmenu šifrovaných správ. Je to modrený nástroj komunikácie, lebo digitálny podpis nemožno sfaľovať.

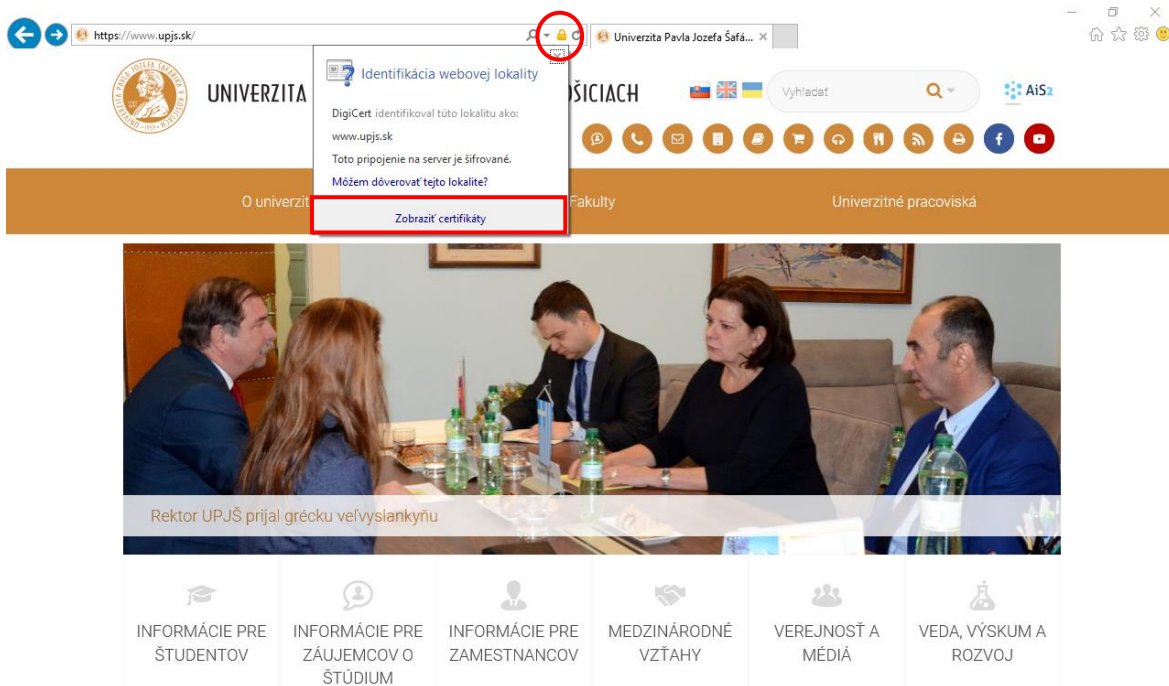
Certifikačnú autoritu všetci považujú za dôveryhodnú. Takouto certifikačnou autoritou je napríklad D. Trust Certifikačná Autorita, Prvá Slovenská Certifikačná Autorita.

Digitálny certifikát obsahuje: verejný kľúč majiteľa, meno majiteľa, dobu platnosti, názov certifikačnej autority, ktorá digitálny certifikát vydala, sériové číslo...

Na vystavenie certifikátu je potrebné zaslať osobné údaje. Certifikát býva vystavený po overení totožnosti, čo môže trvať niekoľko dní.

Digitálny certifikát môžeme použiť pri vykonávaní komerčných transakcií, pri zabezpečení a podpisovaní našich e-mailov, môžeme sa identifikovať na webových stránkach a získať tak prístup k zabezpečeným informáciám. Organizácie využívajú certifikáty na šifrovanie, dešifrovanie, podpisovanie správ...

Preto je dôležité si skontrolovať pri činnostiach na internete platnosť a dôveryhodnosť vystaveného certifikátu. Na to slúži ikonka zámku .



1.2.5 Poznať možnosti kontroly používania internetu ako: dohľad (supervision), obmedzenia na prezeranie webových stránok a obmedzenia na sťahovanie z internetu.

Systém Windows obsahuje funkciu **Rodičovská kontrola**, ktorou môžu rodičia obmedziť aktivity svojich detí pri počítači. Rodič môže presne určiť stránky, ktoré budú môcť ich deti navštevovať, a z ktorých budú môcť sťahovať dáta. Rodič môže kontrolovať čas, ktorý stráví dieťa pred počítačom tým, že softvérovo určí čas, v ktorom bude môcť dieťa využívať počítač. Rodič bude môcť blokovat prístup k jednotlivým programom, taktiež hrám, ktoré nie sú určené pre vekovú skupinu, v ktorej sa dieťa nachádza. Rodič môže zistiť aktivity dieťaťa na PC pomocou výpisov – logov, v ktorých bude zaznamenané, aké stránky dieťa navštívilo, koľko emailov prijalo, s kým bolo v kontakte pri číťovaní prostredníctvom programov (Skype, Messenger, Hangout, atď.).

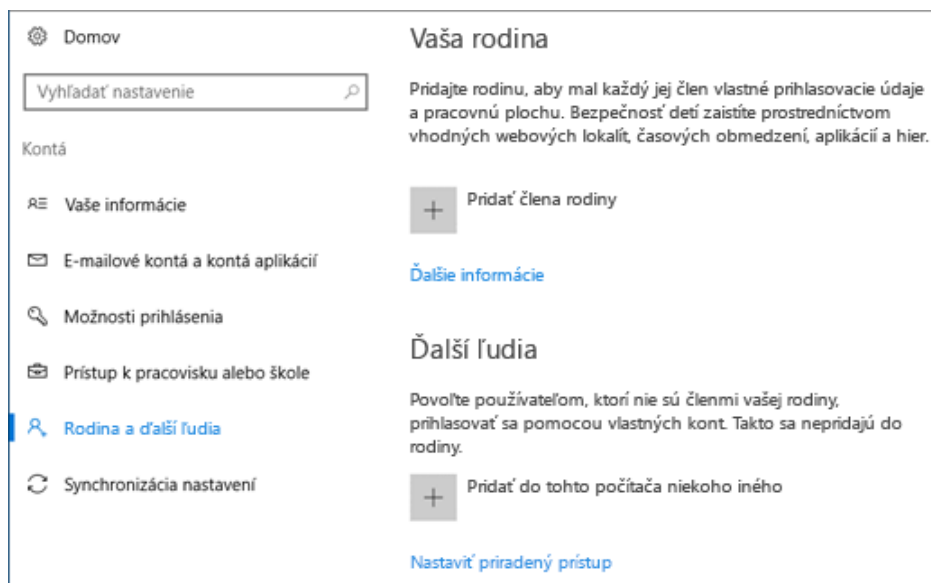
Treba mať na mysli, že žiadny filter nie je taký dokonalý, aby dokázal blokovat všetky nevhodné stránky. Okrem toho sa obsah na internete mení a dopĺňa tak rýchlo, že sa filtrovacie programy iba veľmi ťažko môžu stíhať aktualizovať. Preto je nutné, aby sa deti vzdelávali aj v oblasti používania internetu a vedeli reagovať v prípade nebezpečenstva, nevhodného obsahu stránok a podobne. Rodičia by nemali podobné riešenia vnímať ako náhradu za prístup k deťom, tieto riešenia by mali byť pre nich len pomocníkom pre získanie prehľadu v návykoch ich detí pri surfovaní na internete.

Ak chcete otvoriť Rodičovskú kontrolu, kliknite na tlačidlo **Štart, Ovládací panel** a v časti **Používateľské kontá a bezpečnosť rodiny** kliknite na položku **Nastaviť rodičovskú kontrolu**. Vyžaduje sa oprávnenie správcu. Ak sa zobrazí výzva na zadanie hesla správcu alebo potvrdenie, zadajte heslo alebo potvrdte akciu. Kliknite na štandardné používateľské konto, pre ktoré chcete nastaviť rodičovskú kontrolu. Ak

štandardné používateľské konto ešte nie je vytvorené, kliknutím na položku Vytvoriť nové používateľské konto vytvorte nové konto. V časti **Rodičovská kontrola** kliknite na položku **Zapnutá, presadiť aktuálne nastavenie**. Po zapnutí rodičovskej kontroly pre štandardné používateľské konto môžete upraviť nasledujúce jednotlivé nastavenia, ktoré chcete riadiť:

- Časové obmedzenia. Nastavením časových obmedzení môžete určiť, kedy majú deti povolené prihlásiť sa do počítača. Časové obmedzenia bránia deťom v prihlásení sa v určitých hodinách. Pre každý deň v týždni môžete nastaviť iné prihlasovacie hodiny. Keď je dieťa prihlásené v čase, keď sa skončí vyhradený čas na prihlásenie, dieťa bude automaticky odhlásené. Ďalšie informácie nájdete v téme Určenie času, v ktorom môžu deti používať počítač.
- Hry. Môžete mať pod kontrolou prístup k hrám, vybrať úroveň hodnotenia podľa veku, vybrať typy obsahu, ktorý chcete blokovať, a rozhodnúť, či chcete blokovať nehodnotené alebo konkrétne hry. Ďalšie informácie nájdete v téme Výber hier, ktoré môžu deti hrať.
- Povolenie alebo zablokovanie konkrétnych programov. Deťom môžete zabrániť v spúšťaní programov, ktoré im nechcete dovoliť používať.

Pridávanie člena rodiny sa robí pomocou **Štart→Nastavenie→ Kontá→Rodina a ďalší ľudia**



1. V počítači Windows 10 vyberte tlačidlo **Štart**, potom vyberte položku **Nastavenia** > **Kontá** > **Rodina a ďalší ľudia**. (Je nutné prihlásiť sa s kontom Microsoft.)
2. Vyberte položku **Pridať člena rodiny**.
3. Vyberte položku **Pridať dieťa** alebo **Pridať dospelú osobu**.
4. Zadáte e-mailovú adresu, na ktorú sa danej osobe odošle pozvánka na pridanie. Ak táto osoba nemá e-mailovú adresu, vyberte položku **Osoba, ktorú chcem pozvať, nemá e-mailovú adresu**, a podľa pokynov nastavte nové konto.

5. Keď táto osoba prijme e-mailovú pozvánku, vyzvite ju, aby sa prihlásila do systému Windows 10 použitím tej istej e-mailovej adresy, na ktorú ste odoslali pozvánku.

Správa nastavení rodiny

Po pridaní dieťaťa do svojej rodiny vo Windowse môžete jeho aktivity spravovať takto.

1. Prejdite na lokalitu account.microsoft.com/family a prihláste sa pomocou svojho konta Microsoft.
2. V zozname detí v rodine vyberte dieťa, ktorého nastavenie chcete spravovať. Ak vaše deti používajú aj službu Bezpečnosť rodiny v starších verziách Windowsu alebo službu Moja rodina v starších telefónoch s Windowsom, zobrazí sa ich zoznam podľa zariadenia.
3. Vyberte súčasti konta dieťaťa, ktoré chcete zapnúť alebo zmeniť:
 - **Nedávne aktivity** – toto nastavenie umožňuje vidieť, ktoré webové lokality deti navštívili, ktoré aplikácie a hry používali a koľko času strávili používaním svojich zariadení.
 - **Prehľadávanie webu** – toto nastavenie umožňuje vybrať webové lokality, ktoré môže vaše dieťa zobrazovať.
 - **Aplikácie a hry** – toto nastavenie umožňuje obmedziť aplikácie a hry, ktoré môže vaše dieťa sťahovať z Windows Obchodu. Umožňuje tiež odblokovat všetky aplikácie a hry, ktoré ste predtým zablokovali.
 - **Čas používania počítača** – tu môžete nastaviť čas, ktorý môžu deti stráviť používaním svojich zariadení.

1.2.6 Ovládať a dodržať odporúčané postupy pri on-line komunikácii

- Od neznámych užívateľov neprijímať správy.
- Nezdierať dôverné, napr. finančné informácie.
- Neprijímať poskytnuté informácie a fakty bez overenia.
- Dodržať zásady ochrany osobných údajov.
- V on-line komunitách
 - používať prezývky (nickname),
 - vedieť rozlíšiť súkromný a verejný profil,
 - nastaviť osobné údaje ako súkromné,
- Nastaviť obmedzenia pre sťahovanie súborov, t.j. prevenciu pred mimoriadnymi výdavkami za prenos)
- Nakupovať on-line len z bezpečných on-line obchodov.
- Navštevovať len dôveryhodné stránky.