

ČSOB v tomto dokumentu popisuje bezpečnostní aspekty používání aplikace Flexims.

Zabezpečení

System Flexims je navržen tak, aby byla zajištěna integrita, důvěrnost a dostupnost informací. Vnitřní mechanismy aplikace chrání data před ztrátou a neoprávněnou změnou. Autentizační technologie chrání vstup do aplikace a zabraňují tak neautorizovanému používání systému.

Zabezpečené spojení

Služby jsou poskytovány prostřednictvím veřejných komunikačních a datových linek. Za jejich zabezpečení ČSOB neodpovídá, a proto nemůže ovlivnit skutečnost, pokud Klientovi vznikne škoda v důsledku zneužití přenášených zpráv, byť na straně systému Flexims byla přijatá veškerá možná opatření k zajištění důvěrnosti dat.


Komunikační tok mezi počítačem klienta a aplikací Flexims je kódován za použití definovaných matematických algoritmů. Aplikací kódovacích technik je zajištěna důvěrnost přenášených informací mezi systémy, tj. neoprávněná osoba není schopná informace sledovat během přenosu.

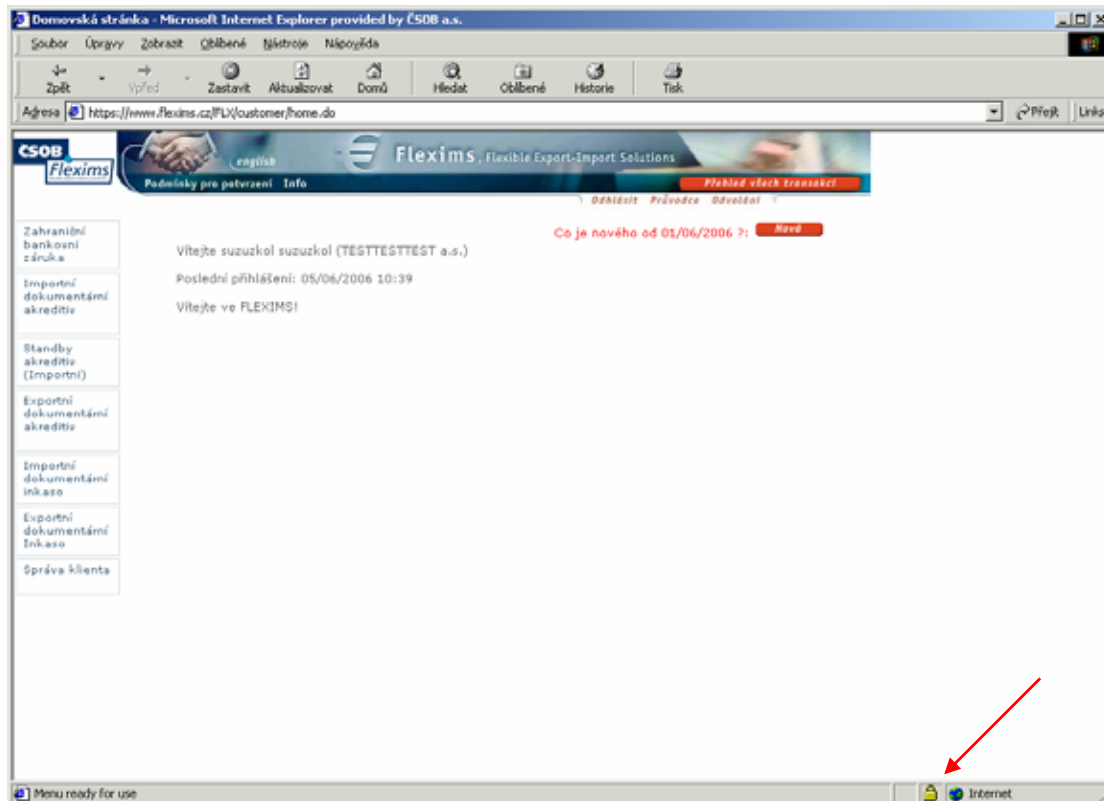
Komunikace mezi počítačem klienta a aplikací Flexims je zabezpečena použitím komunikačního protokolu SSL za použití certifikátu. Certifikát slouží k ověření osoby (zákazníka) a zaručuje, že pouze držitel certifikátu je schopen komunikovat se serverem (aplikací) Flexims.

Pro nastavení zabezpečeného kanálu SSL musí ČSOB vlastnit tzv. serverový certifikát, který je vystaven vrcholným orgánem tzv. certifikační autoritou. Certifikační autorita (pro ČR je to I.CA, více na www.ica.cz) vystavuje certifikáty pouze na základě důkladného prověření osoby, pro kterou je certifikát vystavován. Zároveň certifikační autorita podrobně zkoumá důvěryhodnost této osoby. Serverový certifikát je obdobou občanského průkazu v digitálním světě a zaručuje, že protistrana se kterou klient komunikuje je důvěryhodná. Certifikáty, podobně jako občanské průkazy, mají omezenou časovou platnost. ČSOB má tyto certifikáty vystavené a jsou pravidelně obnovovány.

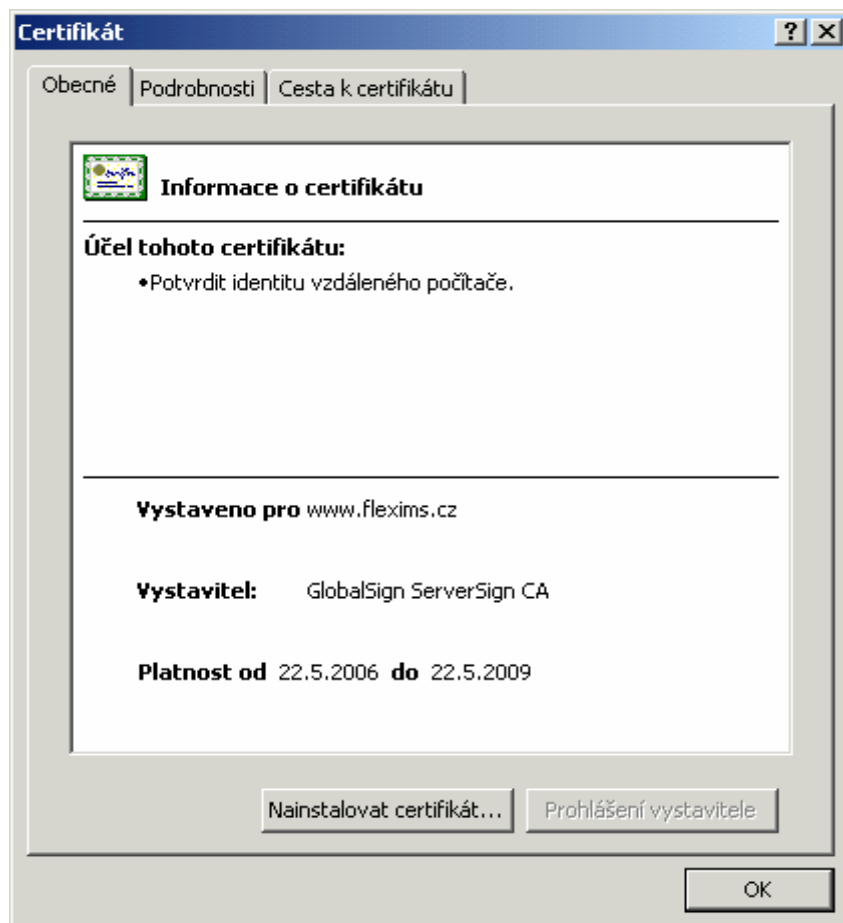
Použitím kanálu SSL a aplikací klientských a serverových certifikátů (digitálních občanských průkazů) klient získává jistotu, že informace, které obdržel pocházejí od důvěryhodného a ověřeného zdroje.

Indikátory zabezpečeného komunikačního kanálu jsou:

- v řádku Adresa vašeho prohlížeče je na počátku adresy uvedeno https://, kde „s“ znamená secure (bezpečný)
- v pravém dolním rohu obrazovky vidíte malý obrázek žlutého záměčku 



Pokud na obrázek žlutého záměčku poklepete myší, objeví se informace o serverovém certifikátu (občanském průkazu systému, ke kterému se připojujete).



Požadavky na prohlížeč sítě Internet pro používání zabezpečeného spojení SSL:

prohlížeč sítě Internet musí podporovat protokol SSL (SSL3)

- instalovaný certifikát authority, která slouží pro potvrzování identity vzdáleného systému (I.CA)

Pokud dojde k přerušení komunikace mezi prohlížečem sítě Internet a aplikací Flexims, uživatel obdrží hlášení o chybě a nebude moci nadále aplikaci používat. Po navázání spojení je nutné do aplikace se znovu přihlásit.

Firewalls

Bezpečnostní prvek, tzv. firewall, slouží k ochraně sítí a stanic před útoky, které jsou vedené pomocí počítačových sítí.

Firewall je bezpečnostním zařízením, které pracuje na principech kontroly vstupního a výstupního toku dat mezi počítačem a Internetem. Lze jej přirovnat k bezpečnostní bráně. Firewall by měl chránit počítač před vnějším napadením.

Zabezpečení

ČSOB podniká nezbytné kroky k zajištění IT bezpečnosti. Specializované vnitřní útvary a externí partneři pravidelně provádějí audit všech bezpečnostních prvků systému.

V ČSOB působí vnitřní útvar bezpečnosti IS, který řídí a monitoruje úroveň bezpečnosti systémů. Naši specialisté rychle reagují na signály o potenciálních slabínách v IT bezpečnosti.

Chraňte si svůj PIN

Neprozrazujte svůj PIN kolegům. Pokud i oni chtějí používat Flexims, požádejte o další osobní přístupové kódy.

Nezaznamenávejte si PIN a nenechávejte ho volně na stole. Neopouštějte počítač, dokud jste se neodhlásili z Flexims (i když budete po několika minutách nečinnosti v systému automaticky odhlášeni).

Zabezpečení vložených dat

Byla učiněna opatření k ochraně vložených dat, avšak z bezpečnostních důvodů podrobnosti přijatých opatření neuvádíme.

Přihlášení

Použitý systém garantuje bezpečnost zpracovávaných dat a umožňuje uživatelům v rámci aplikace nabývat různá oprávnění v rámci svých pravomocí. Za tímto účelem musíme znát a identifikovat každého uživatele.

Pro práci s aplikací Flexims je časové omezení. Po přibližně 15 minutách nečinnosti je uživatel automaticky odhlášen a pro pokračování v práci se musí opětovně přihlásit.

Uživatel je zodpovědný za správné a přísně osobní používání přístupového PIN.

Technické vybavení

- Prohlížeč: Internet Explorer min. verze 5.5. nebo Netscape min. verze 6.0
- Prohlížeč musí akceptovat „cookies“
- Podpora pro Javascript
- Root Certifikát I.CA (Globální certifikát autority)
- Prohlížeč musí umožňovat stahování a ukládání zabezpečených dokumentů.