ČESKÁ SPRÁVA SOCIÁLNÍHO ZABEZPEČENÍ
ÚSTŘEDÍ - ÚSEK INFORMAČNÍCH A KOMUNIKAČNÍCH TECHNOLOGIÍ

Křížová 25, 225 08, Praha 5

Standard systémové konfigurace pracovní stanice

Verze 2.20

Změny:

Datum vydání	Verze	Změna proti předchozí verzi	Změnil (jméno)
8.2.2005	0.80	První draft v rámci projektového týmu	Milan Hruška
29.3.2005	0.81	Doplnění informace o omezeném zápisu uživatele do registry klíčů	Milan Hruška
29.3.2005	0.81	Doplnění verze a nastavení IE	Libor Šmíd
16.5.2006	1.0	Změna verze .NET Framework, doplnění konfigurace HW	Libor Šmíd
13.7.2006	1.10	Upravena kapitola 4 – kontakt pro testování na lokalitě	Libor Šmíd
20.3.2007	1.11	Doplněno JRE	Libor Šmíd
30.3.2009	1.12	Aktualizována tabulka v kapitole 2	Jiří Rybáček
3.4.2009	1.12	Aktualizována kapitola 2 a 3	Milan Zapletal
14.5.2009	1.13	Aktualizována kapitola 2	Jiří Rybáček
23.6.2009	1.14	Aktualizována tabulka v kapitole 2	Jiří Rybáček
29.6.2009	1.15	Aktualizována tabulka v kapitole 2 (602 XML Filler 2.62)	Jiří Rybáček
20.7.2009	1.16	Aktualizována tabulka v kapitole 2 (TrueCrypt)	Pavel Šmejkal
30.7.2010	1.17	Aktualizována tabulka v kapitole 2 (TrueCrypt)	Jiří Rybáček
31.1.2011	1.18	Aktualizována tabulka v kapitole 2	Jiří Rybáček
2.8.2011	1.19	Změna verze a nastavení IE v kapitole 3, přidána příloha: GPO šablona pro IE8	Jiří Rybáček
26.10.2011	1.20	Aktualizována tabulka v kapitole 2	Jiří Rybáček
8.11.2011	2.00	Rozšíření standardu PC o operační systém Windows 7 v rámci projektu NDOS	Jiří Rybáček
4.3.2014	2.10	Aktualizace verzí programů	Jiří Rybáček
2.12.2014	2.20	Aktualizace verzí programů + přidán FormApps Plug-in verze 1.9 v kapitole 2 Změna nastavení IE v kapitole 4 Změna v příloze: GPO šablona pro IE8	Jiří Rybáček

Obsah

1. ÚVOD

Cílem dokumentu je specifikovat základní požadavky na provoz aplikací ČSSZ na desktopu v konfiguraci *Windows 7 Enterprise* v prostředí Windows 2003 Active Directory.

2. ZÁKLADNÍ POŽADAVKY KLADENÉ NA PROVOZ APLIKACÍ V PROSTŘEDÍ WINDOWS XP

Podpora operačního systému Windows XP v prostředí ČSSZ byla ukončena ke dni 8.4.2014. Provoz aplikací pod systémem Windows XP není od tohoto data v prostředí ČSSZ podporován.

3. ZÁKLADNÍ POŽADAVKY KLADENÉ NA PROVOZ APLIKACÍ V PROSTŘEDÍ WINDOWS 7

Základní požadavky lze shrnout do několika následujících bodů:

- Desktopy jsou konfigurovány tak, že mají celý disk naformátován jako jedinou partition , tj. pouze disk C
- Na desktopu bude instalován operační systém Microsoft Windows 7 Enterprise SP1 česká verze (vypnutý firewall)
- Na každém desktopu bude standardně instalován následující systémový SW:

Poř. Číslo	**Název aplikace**
1	Symantec Endpoint Protection 12.1
2	Client SCCM
3	Microsoft Office Professional Plus 2010 SP1 CZ
4	Microsoft Windows Media Player 12 CZ
5	Microsoft .NET Framework 1.1, Hotfix .NET Framework 1.1(KB928366), .NET Framework 4
6	WinRar 5.11 CZ
7	Adobe Reader 11 CZ
8	ASPI klient verze 2014 CZ
9	WTA Print
10	Sun ODF Plugin for Microsoft Office 3.1 (podpora dokumentů Open Office pod MS Office)
11	Crystal Reports for .NET Framework 2.0 (x86)
12	Adobe Flash Player 15.0.0.170
13	602 XML Filler 4.51.09
14	Java Runtime Environment (JRE 7.51)
15	Cryptoplus Pro ID 2.3.14 (SW pro práci s čipovými kartami + program pro obnovu certifikátů)

Poř. Číslo	Název aplikace
16	TrueCrypt 6.1a – omezeno pouze na stanice určené pro provoz: • aplikace PSL od firmy Navidata • aplikace KOC • aplikace KLM
17	PDF-XChange 4 Pro
18	FormApps Plug-in 1.9

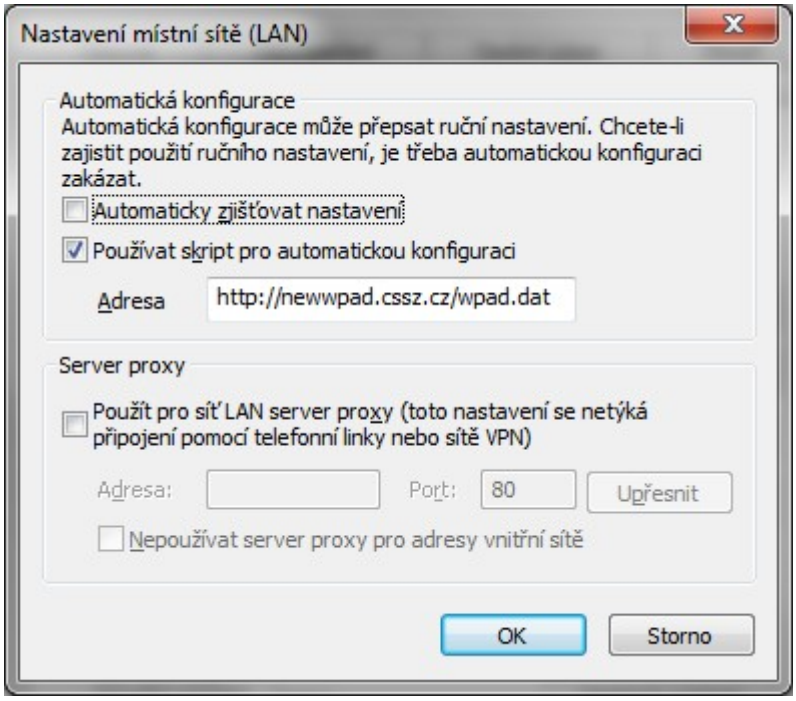
- Klient elektronické pošty MS Outlook 2010 má kopii schránky (*.OST), popřípadě offline složky (*.PST) uloženy v adresáři **%USERPROFILE%\DATA**
- Pro ukládání uživatelských dat jsou k dispozici dvě úložiště „ Dokumenty síťové " (**\\sizz06\Home$\%USERNAME%**) a „ Dokumenty lokální " (**%USERPROFILE%\data**)
- Umístění aplikace bude pouze v rámci složky **C:\Program Files** (dané proměnnou %PROGRAMFILES%)
- V programovém kódu aplikace nesmí být uvedena konkrétní struktura jmen objektů (počítač, doména, organizační jednotka apod.) a jejich umístění v Active Directory, ani IP adresa některého počítače či lokality
- Je garantováno, že instalace aplikace bude prováděna v bezpečnostním kontextu účtu s právy lokálního Administrátora na stanici
- Je garantováno, že instalace aplikace je možná bezobslužně v tichém módu pomocí systému pro distribuci software Microsoft SCCM.
- Provozování aplikace bude v bezpečnostním kontextu běžného uživatele - privilegia lokální skupiny **Users** (jen právo čtení ve složce %PROGRAMFILES%). Výchozí přístupová práva k souborovému systému i k registry jsou v rámci operačního systému Windows 7 Enterprise navržena tak, že členové skupiny Users nemají možnost modifikovat systémové adresáře, systémové soubory. Přístup k registry klíčům je značně omezen (jen zápis do části HKEY_CURRENT_USER).
- Ukládání uživatelských konfigurací bude povoleno jen v konkrétním profilu uživatele v rámci struktury dané proměnnou %USERPROFILE%. Například dočasné soubory jsou směrovány do složky dané proměnnou %TEMP%, %TMP%, která ukazuje do složky v lokálním uživatelském profilu. Pro ukládání aplikačních dat je k dispozici skrytá složka **C:\ProgramData .**

4. NASTAVENÍ APLIKACE INTERNET EXPLORER

Na stanicích bude nainstalován Internet Explorer verze 8.0 (MSIE) včetně aktuálních oprav vydaných společností Microsoft. Konfigurace MSIE odpovídá standardní instalaci, zvláště však upozorňujeme, že musí být nastaven na automatické zjišťování existence novějších verzí uložených stránek. Pokud jsou používány ActiveX komponenty, je vyžadováno jejich zabezpečení elektronickým podpisem.

Nastavení IE jsou řízeny centrální skupinovou politikou v Active direktory

- **Nastavení místní sítě LAN**



- **Blokování automaticky otevíraných oken** - Změna v zabezpečení v IE pro Intranet **-** Vlastní úroveň. Zakázáno „Blokování automaticky otevíraných oken". Aplikace tak mohou vytvořit nové okno a v něm ovládací prvky potlačit.

- **Nastavení zabezpečení**:

  - **Zóna servery s omezeným přístupem** – vysoké

  - **Zóna internet** – středně vysoké – povoleno automatické přihlášení pouze do zóny intranet

  - **Zóna důvěryhodné servery** – střední – povoleno automatické přihlášení pouze do zóny intranet

  - **Zóna intranet** – středně nízké – povoleno automatické přihlášení pouze do zóny intranet
    - + Initialize and script ActiveX controls not marked as safe **Enabled**
    - + Download unsigned ActiveX controls **Enabled**

- **Export GPO šablony pro IE 8 viz Příloha 1 na konci dokumentu**

5. ZPŮSOB TESTOVÁNÍ PROVOZOVANÝCH APLIKACÍ V PROSTŘEDÍ WINDOWS 7

V této části je naznačen způsob testování aplikací:

- Vytvořit prostředí na desktopu podle základních požadavků uvedených v kapitole 1
- Otestovat funkčnost aplikace včetně všech výstupů a periferií (soubor, tiskárna, skener)

- Pro místně provozované aplikace může testování probíhat přímo v provozované lokalitě. Pokud to nebude technicky možné je nutné z lokality předat instalační média k otestování v Ústředí ČSSZ – odbor systémové, komunikační a technické podpory.

6. ODPOVĚDNOST ZA FUNKČNOST APLIKACÍ V PROSTŘEDÍ WINDOWS 7

Odpovědnost za bezproblémovou funkčnost aplikace v prostředí Windows7 má vždy příslušný Garant aplikace.

7. ZÁVĚR

Dokument je důležitým materiálem pro Garanty aplikací, kteří podle něj budou zajišťovat testování aplikací ČSSZ v konfiguraci desktopu na platformě Windows 7.

8. PŘÍLOHA 1: GPO ŠABLONA PRO IE 8

Internet Settings

Internet Explorer 8: Internet Explorer 8 (Order: 1)

Security

Securitylevels

Internet	**Medium-high**
Local Intranet	**Medium-low**
	+ Initialize and script ActiveX controls not marked as safe **Enabled**
	+ Download unsigned ActiveX controls **Enabled**
Trusted	**Medium**
Restricted	**High**

Connections

Dial-up settings

Connectionbehavior	Neverdial a connection

Programs

Default web browser

Tellmeif Internet Explorer is not the default web browser	Enabled

Advanced

Accessibility

Alwaysexpand ALT text forimages	Disabled
Movesystemcaretwithfocus/selectionchanges	Disabled

Browsing

Automaticallycheckfor Internet Explorer updates	Disabled
Closeunusedfolders in History and Favorites (requires restart)	Disabled
DisableScript debugging (Internet Explorer)	Enabled
DisableScript debugging (Other)	Enabled
Display a notificationabouteveryscripterror	Disabled
Enable FTP folderview (outsideof Internet Explorer)	Enabled
Enablepagetransitions	Enabled
EnablePersonalizedFavorites Menu	Disabled
Enablethird-party browser extensions (requires restart)	Enabled
Enablevisualstyles on buttons and controls in web pages	Enabled
Enablewebsites to use thesearch pane	Disabled
Forceoffscreencompositingevenunder Terminal Server (requires restart)	Disabled
Notifywhendownloadscomplete	Enabled
Reusewindowsforlaunchingshortcuts	Enabled

Show Friendly HTTP Errormessages	Enabled
Underlinelinks	Always
Use inlineAutoComplete	Disabled
Use most recentorderwhenswitchingtabswithCtrl+Tab	Disabled
Use Passive FTP (for firewall and DSL model compatibility)	Enabled
Use smoothscrolling	Enabled

HTTP 1.1 settings

Use HTTP 1.1	Enabled
Use HTTP 1.1 throughproxyconnections	Enabled

International

Always show encodedaddresses	Disabled
Send IDN server names	Enabled
Send IDN server namesfor Intranet addresses	Disabled
Send UTF-8 URLs	Enabled
Use UTF-8 formailtolinks	Disabled

Multimedia

Always use ClearTypefor HTML	Disabled
EnableAutomatic Image Resizing	Enabled
Play animations in web pages	Enabled
Play sounds in web pages	Enabled
Show image downloadplaceholders	Disabled
Show pictures	Enabled
Smart image dithering	Enabled

Printing

Print background colors and images	Disabled

SearchfromtheAddress bar

Whensearching	Just display theresults in themainwindow

Security

AllowactivecontentfromCDs to run on My Computer	Disabled
Allowactivecontent to run in files on My Computer	Enabled
Allow software to run orinstallevenifthesignatureis invalid	Disabled
Checkforpublisher'scertificaterevocation	Enabled
Checkfor server certificaterevocation (requires restart)	Enabled
Checkforsignatures on downloadedprograms	Enabled
Do not saveencryptedpages to disk	Disabled
EmptyTemporary Internet Filesfolderwhen browser isclosed	Disabled
EnableIntegrated Windows Authentication (requires restart)	Enabled
Enablenative XMLHTTP support	Enabled
PhishingFilter	Turnoffauto maticwebsit echecking
Use SSL 2.0	Disabled
Use SSL 3.0	Enabled
Use TLS 1.0	Enabled
Warnaboutcertificateaddressmismatch	Enabled
Warnifchangingbetweensecure and not secure mode	Disabled
Warnif POST submittalisredirected to a zonethatdoes not permitposts	Enabled