



Standard systémové konfigurace pracovní stanice

Verze 2.00

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

Obsah

1. Úvod	3
2. Základní požadavky kladené na provoz aplikací v prostředí Windows XP	3
3. Základní požadavky kladené na provoz aplikací v prostředí Windows 7	4
4. Nastavení aplikace Internet Explorer	6
5. Způsob testování provozovaných aplikací v prostředí Windows XP a Windows 7	6
6. Odpovědnost za funkčnost aplikací v prostředí Windows XP a Windows 7	7
7. Závěr	7

1. ÚVOD

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

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

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 XP česká verze s SP3 (vypnutý firewall)
- Na každém desktopu bude standardně instalován následující systémový SW:

Poř. Číslo	Název aplikace
1	Avast! Verze 4.8
2	Client SCCM
3	Microsoft Office 2003 CZ SP3
4	Microsoft Windows Media Player 11 CZ
5	Microsoft .NET Framework 1.1, 2.0 SP2, 3.0 SP2 3.5 SP1, Hotfix .NET Framework 1.1(KB928366)
6	WinRar 4.1 CZ
7	Acrobat Reader 9.3 CZ
8	ASPI klient verze 13+ CZ
9	Adobe Shockwave Player
10	WTA Print
11	FileFormatConverters (podpora dokumentů Office 2007 pod Office 2003)
12	Sun ODF Plugin for Microsoft Office 1.1 (podpora dokumentů Open Office pod Office 2003)
13	Crystal Reports for .NET Framework 2.0 (x86)
14	Adobe Flash Player 10.3 ActiveX
15	602 XML Filler 4.10.23
16	Java Runtime Environment (JRE 6.23)
17	Cryptoplus Pro ID 2.3.13 (SW pro práci s čipovými kartami + program pro obnovu certifikátů)

Poř. Číslo	Název aplikace
18	TrueCrypt 6.1a – omezeno pouze na stanice určené pro provoz: <ul style="list-style-type: none"> • aplikace PSL od firmy Navidata • aplikace KOC • aplikace KLM

- Klient elektronické pošty MS Outlook 2003 má kopii schránky (*.OST), popřípadě offline složky (*.PST) uloženy v adresáři %USERPROFILE%\DATA
- Pro ukládání uživatelských dat jsou k dispozici dvě úložiště „ Dokumenty síťové “ (\\sizz6\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 XP Professional 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 směřovány do složky dané proměnnou %TEMP%, %TMP%, která ukazuje do složky v lokálním uživatelském profilu. Totéž platí pro složku pro ukládání aplikačních dat, která je specifikována proměnnou %APPDATA%.
- Kompletní technické požadavky pro chování aplikací v prostředí Windows XP jsou uvedeny v příručce Designed for Windows XP spec v2.3.doc volně dostupné na stránkách www.microsoft.com

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	Avast! Verze 4.8
2	Client SCCM
3	Microsoft Office 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 4.1 CZ
7	Acrobat Reader 10.1 CZ
8	ASPI klient verze 13+ CZ
9	WTA Print
10	Sun ODF Plugin for Microsoft Office 1.1 (podpora dokumentů Open Office pod Office 2003)
11	Crystal Reports for .NET Framework 2.0 (x86)
12	Adobe Flash Player 10.3 ActiveX
13	602 XML Filler 4.10.23
14	Java Runtime Environment (JRE 6.23)
15	Cryptoplus Pro ID 2.3.13 (SW pro práci s čipovými kartami + program pro obnovu certifikátů)
16	TrueCrypt 6.1a – omezeno pouze na stanice určené pro provoz: <ul style="list-style-type: none"> • aplikace PSL od firmy Navidata • aplikace KOC • aplikace KLM
17	PDF-XChange 5 Pro

- 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 “ (\\sizz6\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 směřovány do složky dané proměnnou %TEMP%, %TMP%, která ukazuje do složky v lokálním uživatelském profilu. Totéž platí pro složku pro ukládání aplikačních dat, která je specifikována proměnnou %APPDATA%.

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 directory

- **Přístup na internet** - Web proxy klient IE je směřován na proxy soustavu: wpx.cssz.cz port: 8080 s výjimkou pro doménu *.cssz.cz Takto je zajištěna přímá konektivita (mimo proxy soustavu) na aplikace a webové servery, pokud se v URL použije sufix cssz.cz. Příklady: intranet.cssz.cz, ws.cssz.cz
- **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 – vysoke
 - Zóna internet – středně vysoké – povoleno automatické přihlášení pouze do zóny intranet
 - Zóna **důvě**ryhodné servery – střední – povoleno automatické přihlášení pouze do zóny intranet
 - Zóna intranet – středně nízké – povoleno automatické přihlášení pouze do zóny intranet
- Export GPO šablony pro IE 8 viz Příloha 1 na konci dokumentu

5. ZPŮSOB TESTOVÁNÍ PROVOZOVANÝCH APLIKACÍ V PROSTŘEDÍ WINDOWS XP A 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 periférií (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.

V současné době jsou již vytvořeny obrazy cílového desktopu (instalace pomocí WDS), které je možné použít a desktopy, na kterých bude probíhat testování aplikací velice rychle reinstalovat. Výhodou je skutečnost, že na desktopu bude vždy dodržena cílová konfigurace daná projektem NDM a NDOS.

6. ODPOVĚDNOST ZA FUNKČNOST APLIKACÍ V PROSTŘEDÍ WINDOWS XP A WINDOWS 7

Odpovědnost za bezproblémovou funkčnost aplikace v prostředí Windows XP a 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 XP a Windows 7.

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
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 notificationabouteverycripterror 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 through proxy connections	Enabled
International	
Always show encoded addresses	Disabled
Send IDN server names	Enabled
Send IDN server names for Intranet addresses	Disabled
Send UTF-8 URLs	Disabled
Use UTF-8 for mailto links	Disabled
Multimedia	
Always use ClearType for HTML	Disabled
Enable Automatic Image Resizing	Enabled
Play animations in web pages	Enabled
Play sounds in web pages	Enabled
Show image download placeholders	Disabled
Show pictures	Enabled
Smart image dithering	Enabled
Printing	
Print background colors and images	Disabled
Search from the Address bar	
When searching	Just display the results in the main window
Security	
Allow active content from CDs to run on My Computer	Disabled
Allow active content to run in files on My Computer	Enabled
Allow software to run or install even if the signature is invalid	Disabled
Check for publisher's certificate revocation	Enabled
Check for server certificate revocation (requires restart)	Enabled
Check for signatures on downloaded programs	Enabled
Do not save encrypted pages to disk	Disabled
Empty Temporary Internet Files folder when browser is closed	Disabled
Enable Integrated Windows Authentication (requires restart)	Enabled
Enable native XMLHTTP support	Enabled
Phishing Filter	Turn off automatic website checking
Use SSL 2.0	Disabled
Use SSL 3.0	Enabled
Use TLS 1.0	Enabled
Warn about certificate address mismatch	Enabled
Warn if changing between secure and not secure mode	Disabled
Warn if POST submit is redirected to a zone that does not permit posts	Enabled