Autentifikácia certifikátom do systému XMtrade[®]/ISZO a XMtrade[®]/ISOT





sféra, a.s. • Továrenská 14 • 811 09 Bratislava tel.: +421 2 502 13 142 • fax: +421 2 502 13 262

© **sféra**, a.s., 2014

OBSAH

1	ÚVOD.		. 3
	1.1 Au	tentifikácia certifikátom pomocou SSL	3
	1.1.1	Internet Explorer	. 3
	1.1.2	Google Chrome	. 4
	1.1.3	Safari	. 4
	1.1.4	Firefox	. 4
	1.1.5	Opera	. 7
	1.2 Au	tentifikácia Java Appletom	. 7
2	ZOZNA	M OBRÁZKOV	. 8



1 ÚVOD

Systém XMtrade[®]/ISZO a XMtrade[®]/ISOT vyžaduje autentifikáciu menom, heslom a certifikátom. Certifikát musí byť nainštalovaný na stanici, z ktorej sa používateľ prihlasuje. Prihlasovanie sa vykonáva v dvoch krokoch. Najskôr používateľ zadá meno a heslo, ak autentifikácia prebehne úspešne, potom sa vykoná autentifikácia s certifikátom. Počas autentifikácie s certifikátom musí používateľ zvoliť certifikát, následne sa vykoná digitálny podpis, ktorý sa odošle do systému XMtrade[®]/ISZO a XMtrade[®]/ISOT. Digitálny podpis sa vykonáva lokálne na stanici, z ktorej sa používateľ prihlasuje.

Systém XMtrade[®]/ISZO a XMtrade[®]/ISOT podporuje dve možnosti autentifikácie certifikátom:

- 1) Pomocou protokolu SSL a prehliadačom (odporúčané).
- 2) Pomocou Java Appletu.

1.1 Autentifikácia certifikátom pomocou SSL

Autentifikácia certifikátom pomocou protokolu SSL a prehliadača je odporúčaný a najjednoduchší spôsob. Digitálny podpis sa vykonáva pomocou prehliadača, preto nie je nutné inštalovať ďalší softvér. Výnimkou je Firefox, kde je potrebné nainštalovať ovládač od certifikačnej autority, ktorá vydala certifikát na autentifikáciu. Dialóg na výber certifikátu sa líši v závislostí na prehliadači.

Tento spôsob autentifikácie podporujú tieto prehliadače:

- Internet Explorer,
- Google Chrome,
- Safari,
- Firefox.

Opera aktuálne tento spôsob autentifikácie nepodporuje.

1.1.1 Internet Explorer

Internet Explorer ponúka certifikáty z úložiska operačného systému. Certifikáty musia byť určené na autentifikáciu.



Obrázok 1 Dialóg pre výber certifikátu – Internet Explorer 11



1.1.2 Google Chrome

Google Chrome ponúka certifikáty z úložiska operačného systému. Certifikáty musia byť určené na autentifikáciu.

Select a certificate	×
Select a certificate to authenticate yourself to test-certificate.okte.sk:443	
Sfera TEST User (Sfera TEST CA)	
Certificate information OK Cancel	

Obrázok 2 Dialóg pre výber certifikátu – Google Chrome

1.1.3 Safari

Safari ponúka certifikáty z úložiska operačného systému. Certifikáty musia byť určené na autentifikáciu.

Windows Security	X	J
Confirm Ce Confirm this co click Cancel.	ertificate ertificate by clicking OK. If this is not the correct certificate,	
	Sfera TEST User Issuer: Sfera TEST CA Valid From: 8. 10. 2013 to 8. 10. 2014 Click here to view certificate prope	
	OK Cancel	

Obrázok 3 Dialóg pre výber certifikátu – Safari

1.1.4 Firefox

Firefox ponúka certifikáty z vlastného úložiska certifikátov. Certifikáty, ktoré obsahujú privátny kľuč (nekvalifikované) sa musia naimportovať aj s privátnym kľúčom do prehliadača.

Postup importu certifikátu s privátnym kľúčom (.pfx, .p12) do Firefoxu:

Zvolí sa hlavné menu prehliadača pomocou klávesy F10. Následne sa zvolí **Tools** (Nástroje)/**Options** (Nástroje), potom sa zvolí záložka **Advanced** (Spresnenie), ďalej záložka **Certificates** (Certifikáty).



Options							x
		۵.		90	A	\bigcirc	Ĩ
General	Tabs	Content	Applications	Privacy	Security	Sync	Advanced
General Da	ata Choice	s Network	Update Certifi	cates			
When a s	server requ	iests my per	sonal certificate				
○ Select	t one auto	omatically	Ask me even	ry t <u>i</u> me			
		A P L P		D :			
View Ce	ertificate <u>s</u>	Validati	Security	Devices			
				ОК	Cance		Help

Obrázok 4 Dialóg nastavenia prehliadača Firefox

Označí sa možnosť **Ask me every time**. Zvolí sa tlačidlo **View Certificates** (Certifikáty), následne pomocou tlačidla **Import...** sa môže vložiť certifikát do úložiska. Podporované sú formáty **.pfx** a **.p12**. Počas importu bude výzva na zadanie hesla, ktorým bol export privátneho kľúča zabezpečený.

	ger							
Your Certificates	People	Servers	Authorities	Others				
You have certit	ficates fro	om these	e organizatio	ns that i	dentify you:			
Certificate Na	me	Secu	urity Device		Serial Number	Expires	On	EŞ.
▲Sfera TEST C	A							
<u>V</u> iew	Back	up	Bac <u>k</u> up All	I	I <u>m</u> port	Qelete		
<u>V</u> iew	Back	up	Bac <u>k</u> up All		I <u>m</u> port)elete		

Obrázok 5 Úložisko certifikátov prehliadača Firefox

Postup inštalácie ovládača pre Firefox:

Ak sa používa certifikát, ktorého privátny kľuč je uložený na bezpečnostnom zariadení (SmartCard, USB token), je potrebné nainštalovať ovládač zariadenia do prehliadača.

Zvolí sa hlavné menu prehliadača pomocou klávesy F10. Následne sa zvolí **Tools** (Nástroje)/**Options** (Možnosti), potom sa zvolí záložka **Advanced** (Spresnenie), ďalej záložka **Certificates** (Certifikáty).



Options		Opti	ons							×
General Tabs Content Applications Privacy Security Sync	Advanced	6	General	Tabs	正 页 Content	Applications	Privacy	Security	Sync	Advanced
General Data Choices Network Update Certificates		Ge	eneral Da	ata Choice	s Network	Update Certifi	icates			
When a server requests my personal certificate: Seject one automatically Ask me every time 		When a s	server requ ct one auto	uests my per omatically	sonal certificate	s ry t <u>i</u> me				
View Certificates Validation Security Devices			View Ce	ertificate <u>s</u>	Validati	on	Devices			
OK Cancel	Help						ОК	Cance	el 🗌	<u>H</u> elp

Obrázok 6 Dialógy nastavenia prehliadača Firefox

Ďalej sa zvolí tlačidlo **Security Devices** (Zariadenia), následne sa zobrazí dialóg s podporovanými bezpečnostnými zariadeniami.

Device Manager			
Security Modules and Devices	Details	Value	Log I <u>n</u>
▲NSS Internal PKCS #11 Module			Log Out
Generic Crypto Services			Change Pareword
Software Security Device			
A New PKCS#11 Module			Load
Builtin Roots Module Builtin Object Taken			Unload
Builtin Object Token			Enable FIPS
			ОК

Obrázok 7 Dialóg pre bezpečnostné zariadenia prehliadača Firefox

V nasledujúcom zozname sa nachádzajú návody pre používanie certifikátu, pre niektoré akreditované certifikačné autority:

- <u>http://www.ica.cz/Pouzivani-certifikatu</u>
- <u>http://www.disig.sk/index.php?id=60</u>
- <u>http://www.psca.sk/podpora/navody</u>



User Identification Request
This site has requested that you identify yourself with a certificate:
*.okte.sk (:443)
Organization: "OKTE, a.s."
Issued Under: "DigiCert Inc"
Choose a certificate to present as identification:
5c5abc6a6eef7e631950f670bd8f708f_f0809fa9-7fdc-47a1-b624-0108862364a3 [38:66:C0:76:00:00:00:00:00:00:68]
Details of selected certificate:
Issued to: E=info@sfera.sk;CN=Sfera TEST User,OU=ÚV,O="sféra, a.s.",L=Bratislava,ST=Slovakia,C=SK Serial Number: 38:66:C076000000000068 Valid from 8.10.03312:32:123 to 8.10.2014 12:41:23 Certificate Key Usage: Signing,Non-repudiation,Key Encipherment,Data Encipherment Email: info@sfera.sk
Issued by: CN=Sfera TEST CA,DC=sfera,DC=sk
Stored in: Software Security Device
✓ Remember this decision
OK

Obrázok 8 Dialóg pre výber certifikátu – Firefox

1.1.5 Opera

Opera (aktuálne verzia 18) nepodporuje tento typ autentifikácie, systém XMtrade[®]/ISZO a XMtrade[®]/ISOT automatický rozpozná prehliadač a ponúkne alternatívny spôsob prihlásenia pomocou Java Appletu.

1.2 Autentifikácia Java Appletom

Autentifikácia Java Appletom je možná pre všetky stanice, na ktorých je nainštalovaná posledná verzia Javy. Táto možnosť autentifikácie je k dispozícii na adrese:

- pre produkčné prostredie XMtrade[®]/ISZO https://www.iszo.sk/portal/Pages/Login/Default.aspx?certapplet=true
- pre produkčné prostredie XMtrade[®]/ISOT https://www.isot.sk/portal/Pages/Login/Default.aspx?certapplet=true
- pre testovacie prostredie XMtrade[®]/ISZO
 <u>https://www.test.iszo.sk/portal/Pages/Login/Default.aspx?certapplet=true</u>
- pre testovacie prostredie XMtrade[®]/ISOT
 <u>https://www.test.isot.sk/portal/Pages/Login/Default.aspx?certapplet=true</u>

Java Applet sa spúšťa priamo v prehliadači a pomocou neho sa vykoná digitálny podpis, ktorý sa odošle do autentifikačnej služby.

Stone TEST Hace			12055-0 1
Stera iESI USEr			(3000CU)
	Assess	Consol	1
	Accept	Cancel	

Obrázok 9 Java Applet pre výber certifikátu

Tento spôsob autentifikácie podporujú tieto prehliadače:

- Internet Explorer,
- Google Chrome,
- Safari,
- Firefox,
- Opera.

Java Applet je podpísaná aplikácia, ktorá musí byť povolená pre spustenie v prehliadači.



2 ZOZNAM OBRÁZKOV

Dialóg pre výber certifikátu – Internet Explorer 11	. 3
Dialóg pre výber certifikátu – Google Chrome	4
Dialóg pre výber certifikátu – Safari	. 4
Dialóg nastavenia prehliadača Firefox	5
Úložisko certifikátov prehliadača Firefox	5
Dialógy nastavenia prehliadača Firefox	6
Dialóg pre bezpečnostné zariadenia prehliadača Firefox	6
Dialóg pre výber certifikátu – Firefox	. 7
Java Applet pre výber certifikátu	7
	Dialóg pre výber certifikátu – Internet Explorer 11 Dialóg pre výber certifikátu – Google Chrome. Dialóg pre výber certifikátu – Safari. Dialóg nastavenia prehliadača Firefox Úložisko certifikátov prehliadača Firefox Dialógy nastavenia prehliadača Firefox. Dialóg pre bezpečnostné zariadenia prehliadača Firefox Dialóg pre výber certifikátu – Firefox Java Applet pre výber certifikátu.

