Dodatek č. 2

ke Smlouvě o mimozáručním servisu č. 2004/05/06/2062/3 ze dne 21.5.2004

uzavřený níže uvedeného dne, měsíce a roku, označenými smluvními stranami

1. Smluvní strany

SMS spol. s r. o.
Sídlo: Smetanova 9, 602 00 Brno
IČ: 63477475
DIČ: CZ63477475
Statutární zástupce: Doc. Ing. Jan Münz, CSc., jednatel společnosti
Bankovní spojení: HVB, Brno
Číslo účtu: [redacted]
Obchodní rejstřík: KS v Brně, oddíl C, vložka 20563

dále jen Zhotovitel

a

Sdružení zdravotnických zařízení II Brno, příspěvková organizace
Sídlo: Zahradníkova 2-8, 611 41 Brno
IČ: 00344648
Statutární zástupce: MUDr. Kateřina Vomelová, ředitelka
Bankovní spojení: Komerční banka, a.s.
Číslo účtu: [redacted]
Obchodní rejstřík: KS v Brně, oddíl Pr., vložka 8

dále jen Objednatel

2. Předmět dodatku

2.1. Tímto dodatkem smluvní strany sjednávají níže uvedené změny smlouvy.

3. Ochrana osobních údajů a informací

3.1. Smluvní strany jsou si vědomy toho, že v rámci plnění této smlouvy:

a) si mohou vzájemně úmyslně nebo i opomenutím poskytnout osobní údaje nebo informace, které budou považovány za důvěrné (dále jen důvěrné informace),

b) mohou jejich zaměstnanci získat vědomou činností druhé strany nebo i jejím opomenutím přístup k důvěrným informacím druhé strany.

3.2. Veškeré důvěrné informace zůstávají výhradním vlastnictvím předávající strany a přijímající strana vyvine pro zachování jejich důvěrnosti a pro jejich ochranu stejné úsilí, jako by se jednalo o její vlastní důvěrné informace. Při plnění této smlouvy, se obě strany zavazují neduplikovat žádným způsobem důvěrné informace druhé strany, nepředat je třetí straně ani svým vlastním zaměstnancům s výjimkou těch, kteří s nimi potřebují být seznámeni, aby mohli plnit tuto smlouvu. Obě smluvní strany se zároveň zavazují nepoužít důvěrné informace druhé strany jinak než za účelem plnění této smlouvy.

3.3. Nedohodnou-li se smluvní strany výslovně jinak, považují se za důvěrné informace všechny informace, které jsou a nebo by mohly být součástí obchodního tajemství, tj. například nejenom popisy nebo části popisů technologických procesů a vzorců, technických vzorců a technického know-how, informace o provozních metodách, procedurách a pracovních postupech, obchodní nebo marketingové plány, koncepce a strategie nebo jejich části, nabídky, kontrakty, smlouvy, dohody nebo jiná ujednání s třetími stranami, informace o výsledcích hospodaření, o vztazích s obchodními partnery, o pracovněprávních otázkách, o zpracovávání osobních údajů v souvislosti s poskytováním zdravotní péče. Jedná se o osobní údaje podle zákona č. 20/1966 Sb., o péči o zdraví lidu v platném znění a dále podle zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění zákona č. 227/2000 Sb., a všechny další informace, jejichž zveřejnění přijímající stranou by předávající straně mohlo způsobit škodu.

3.4. Pokud jsou důvěrné informace poskytovány v písemné podobě a nebo ve formě textových souborů na počítačových médiích, je předávající strana povinna upozornit přijímající stranu na důvěrnost takového materiálu jejím vyznačením alespoň na titulní stránce.

3.5. Bez ohledu na výše uvedená ustanovení se za důvěrné nepovažují informace, které:

a) se staly veřejně známými, aniž by to zavinila záměrně či opomenutím přijímající strana,

b) měla přijímající strana legálně k dispozici před uzavřením této smlouvy, pokud takové informace nebyly předmětem jiné, dříve mezi smluvními stranami uzavřené smlouvy o ochraně informací,

c) jsou výsledkem postupu, při kterém k nim přijímající strana dospěje nezávisle a je to schopna doložit svými záznamy nebo důvěrnými informacemi třetí strany.

3.6. Ustanovení tohoto dodatku není dotčeno ukončením účinnosti této smlouvy z jakéhokoliv důvodu a jeho účinnost skončí nejdříve jeden (1) rok po ukončení účinnosti této smlouvy. Pokud se jedná o osobní údaje, které budou v držení SMS spol. s r.o. ať již v tištěné formě nebo zpracované výpočetní technikou je povinností SMS spol. s r.o. je neprodleně vrátit druhé smluvní straně.

3.7. Za zaměstnance druhé smluvní strany se považuje osoba, která byla v pracovním poměru ke druhé smluvní straně v době účinnosti této smlouvy. Každá ze smluvních stran této smlouvy je povinna proškolit příslušné zaměstnance, aby byla zajištěna ochrana důvěrných informací, které jsou uvedeny v odst. 3.3 tohoto dodatku.

3.8. Smluvní strany této smlouvy si sjednávají pro případ porušení některé i jednotlivé povinnosti, které jsou uvedené v tomto dodatku smluvní pokutu ve výši 20.000,-Kč za každou porušenou povinnost.

3.9. Smluvní pokuta je splatná do 15 dnů poté, co bude písemná výzva jedné strany v tomto směru druhé straně doručena. Povinností zaplatit smluvní pokutu, jak je specifikováno v bodě 3. 8, není dotčeno právo na náhradu škody, a to ani co do výše, v niž případně náhrada škody smluvní pokutu přesáhne. Povinnost zaplatit smluvní pokutu může vzniknout i opakovaně, její celková výše není omezena.

3.10. Povinnost zaplatit smluvní pokutu, jak je specifikována v bodě 3.8, 3.9, trvá i po skončení smlouvy, jakož i poté, co dojde k odstoupení od ní některou ze smluvních stran či oběma stranami.

4. Vzdálené připojení

4.1. Objednatel se zavazuje umožnit vzdálený přístup pracovníků Zhotovitele k IS prostřednictvím Internetu za podmínek stanovených směrnicí Zhotovitele „Vzdálený přístup k NIS", která je přílohou č. 1 tohoto dodatku.

5. Závěrečná ujednání

5.1. Ostatní ustanovení smlouvy se nemění a zůstávají nadále v platnosti. Smluvní strany shodně prohlašují, že s obsahem tohoto dodatku před jeho podpisem se seznámily a že tento dodatek byl uzavřen podle jejich pravé a svobodné vůle, určitě, vážně a srozumitelně, nikoliv v tísni za nevýhodných podmínek a je nedílnou součástí původní smlouvy.

5.2. Dodatek smlouvy nabývá platnosti dnem podpisu dodatku oběma stranami.

5.3. Nedílnou součástí tohoto dodatku je jeho příloha č. 1 - Vzdálený přístup k NIS.

5.4. Dodatek smlouvy je vyhotoven ve čtyřech provedeních, z nichž každá ze smluvních stran obdrží po dvou stejnopisech.

Za Objednatele	Za Zhotovitele
V Brně dne 23. listop. 2006	V Brně dne 24. 11. 2006
MUDr. Kateřina Vomelová Ředitelka SZZ II Brno	Doc. Ing. Jan Münz, CSc. jednatel SMS spol. s r. o.

Sdružení zdravotnických zařízení II
BRNO, p.o.
Zahradníkova 2/8, 611 41 BRNO
MUDr. Kateřina VOMELOVÁ
ředitel

SMS spol. s r.o.
Smetanova 9, 602 00 Br...

Výtisk č.: X

Vzdálený přístup k NIS

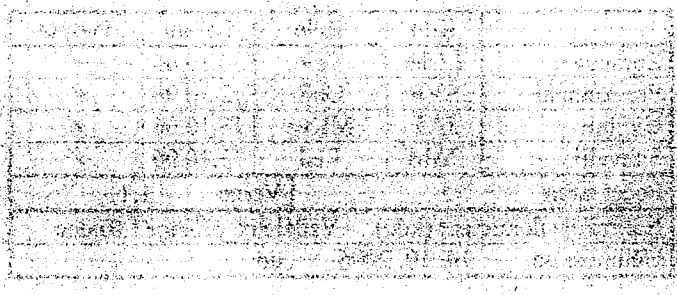
Příloha č. 1 k dod. č.2 smlouvy č. 2004/05/06/2062/3

SMS, spol. s r. o.
se sídlem Smetanova 9
602 00 Brno
IČO: 63477475

	Kdo	Role	Datum	Podpis
Zpracoval	LUM	TeŘ	10.10.06	✓
Přezkoumal	SVB	ObŘ	12.10.06	✓
Uvolnil	JAT	MKva	13.10.06	✓
Schválil	JAM	Řed	13.10.06	✓
Počet stran	5		Verze	1.1
Nahrazuje dokument (kód)		Vzdálený_přístup(1.0).doc		
Účinnost od	14. 10. 2006	do		

Změnový list dokumentu

Verze	Datum	Obsah změny typ: kap(str) –text (typ: R-rozšíření, O-oprava, Z-zrušení)
1.0	10.08.01	R: Zpracování první verze dokumentu
1.1	10.10.06	O: 1.1 – upřesnění systémů SMS R: 1.2 – způsoby připojení O: 2.1 – použitý SW R: 2.4 - drobné změny 1. věty



1. Účel

1.1 Těmito pravidly se řeší způsob vzdáleného přístupu (prostřednictvím modemu nebo po Internetu) do systémů CLINICOM, CLINICOM-PL, DSS a S4M , popřípadě k jiným systémům instalovaným u zákazníka, které jsou udržovány a podporovány firmou SMS Účelem je vyřešit jak bezpečnost dat zákazníka, tak i bezpečnost vlastního chodu systému.

1.2 Pro zajištění vzdálené správy NIS musí zákazník zajistit připojení NIS po dohodě s SMS jedním z níže uvedených způsobů:

- zabezpečeným Internetovým spojením dle níže uvedených parametrů
- přístupem prostřednictvím modemu
- VPN

2. Technické zabezpečení

2.1 Použitý SW

Pro zajištění bezpečné šifrované komunikace mezi firmou SMS a zákazníkem bude používán OpenSSH. Tento SW využívá knihovny OpenSSL a ZLIB. Je nutné udržovat uvedený SW v aktuálních verzích, neboť jinak hrozí bezpečnostní riziko. OpenSSH zahrnuje protokol SSH1 i protokol SSH2. Vzhledem k tomu, že protokol SSH1 používá autentizaci RSA a protokol SSH2 autentizaci DSA bude pro komunikaci použit protokol SSH2. Každý počítač je jednoznačně identifikován DSA klíčem. Bezpečnost je zajištěna Diffie-Helmanovým klíčem. Komunikaci je možné šifrovat pomocí algoritmů Blowfish, 3DES, CAST128, Arcfour. Navíc integrita relace je zajištěna autentizačním kódem (hmac-shal, hmac-md5) – toto je výhoda oproti protokolu SSH1, který neobsahuje mechanismus pro silné zajištění integrity relace. Autentizace uživatelů je založena na veřejném/soukromém klíči. Pro ověření klíče je rovněž použit DSA algoritmus.

2.2 Umístění OpenSSH

OpenSSH může být nainstalován buď přímo na firewallu (doporučeno) nebo na libovolném počítači v síti. Doporučen je OS unixového typu. K zajištění bezpečnosti sítě je vhodné nastavit přístup pouze pro specifikovanou IP adresu. V případě instalace OpenSSH na jiný počítač než firewall, je vhodné nastavit firewall za využití NAT, PAT takovým způsobem, aby IP adresa počítače nebyla zveřejněna na Internetu.

2.3 Použití OpenSSH

Teprve spuštěním daemona sshd je umožněno vytváření relací přes Internet. Jeho ukončením tato možnost zaniká. Je možné rovněž zakázat vytváření relací vytvořením souboru /etc/nologin (neplatí pro uživatele root).

2.4 **Účty uživatelů**

Pro každého uživatele, který bude mít povolen přístup přes Internet k zákazníkovi, bude vytvořen pod OS počítače s nainstalovaným OpenSSH účet (kvůli bezpečnosti mohou být práva účtu omezena). V rámci tohoto účtu bude vytvářena bezpečná šifrovaná relace. Tímto bude jednoznačně identifikováno, kdo v daný okamžik využívá spojení přes Internet. Zároveň bude do systémového logu zaznamenáno kým a kdy byla daná relace vytvořena a kdy byla ukončena.

2.5 Vhodným nastavením parametrů daemona sshd je možné dosáhnou následujícího:

- povolení pouze protokolu SSH2,
- zákaz možnosti komunikace přes Internet pro uživatele root,
- vytvoření seznamu uživatelů, kteří jako jediní budou mít možnost komunikovat přes Internet ,
- vytvoření seznamu uživatelů, kteří budou mít zákaz komunikace přes Internet ,
- je možné specifikovat šifrovací algoritmy, které budou povoleny (3DES, Blowfish, Arcfour, Cast128).

2.6 Při vytváření bezpečné šifrované relace nejprve proběhne autentizace počítačů. Teprve v případě úspěchu dochází k autentizaci uživatele. Pokud tato proběhne úspěšně, dojde k vytvoření bezpečné šifrované relace. Při autentizaci je použito veřejných/soukromých klíčů.

3. Vzdálený přístup

3.1 Každý pracovník SMS musí mít individuální přístup, za který plně odpovídá. Pracovník SMS nesmí používat hromadné neidentifikovatelné přístupy typu SMS, root a pod. Rozsah práv těchto přístupů je definován v přiložených tabulkách. Individuálním přístupem se myslí přístup na firewall, login do operačního systému a login do aplikačního systému.

3.2 Vzdálený přístup do NIS zákazníka se děje na základě následujících příčin:

- zásahy objednané zákazníkem,
- zákroky související s analýzou či odstraněním závady nebo havárie hlášené zákazníkem,
- zásahy předem projednané se zákazníkem,
- plánované zákroky (profylaxe).

4. Vytvoření přístupu

4.1 Za vznik a údržbu příslušných účtů u zákazníka odpovídá po dohodě se správcem systému zákazníka vedoucí projektu SMS pro daného zákazníka.

5. Evidence přístupů

5.1 Každý vzdálený přístup do systému zákazníka je zaevidován. Evidence se provádí pomocí vnitrofiremního mailu SMS - Lotus Notes. Mail je adresován na skupinu CZ.Activity.XXX, kde XXX je kód zákazníka. Z tohoto místa je automaticky odeslán mail zákazníkovi. Seznam mailových adres, na které bude informace k zákazníkovi odeslána, definuje vedoucí projektu zákazníka.

5.2 Mail musí obsahovat datum (pokud se shoduje s datem zápisu mailu, tak datum není nutné), čas připojení, délku připojení a důvod/provedená práce. Např.: *Dnes jsem byl připojen do nemocnice ABC- 10:15-10:40, nastavení instalačních parametrů dle požadavků vedoucího projektu.*

5.3 Pokud se během krátké doby (max. v rozsahu jednoho dne) pracovník připojuje několikrát, stačí pouze jedna zpráva, kde se uvede informace o opakovaném připojení: *23.2. jsem se v období 15:40 - 18:20 opakovaně připojil do nemocnice DEF- kontrola nahrání NV.*