Systém zabezpečení dat

(aktualizace 9. 1. 2017)

Tímto dokumentem se my, společnost Single Case, s.r.o., se sídlem Národní 973/41, Staré Město, 110 00 Praha 1, IČO: 02894815, zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 225059, co do bezpečnosti ukládaných dat řídíme při poskytování služeb v rámci aplikace SingleCase.

1) BEZPEČNOST DAT A POVINNOST MLČENLIVOSTI ADVOKÁTA 2

MÍSTO A ZPŮSOB ULOŽENÍ DAT 2

ZÁLOHOVÁNÍ A EXPORT 2

2) ŘÍZENÍ PŘÍSTUPU K DATŮM A TECHNICKÉ OPATŘENÍ JEJICH ZABEZPEČENÍ 3

VYMEZENÍ POJMŮ 3

SERVER 3

DATABÁZE 4

DOKUMENTY 4

APLIKACE 4

3) KATEGORIE DAT V SINGLECASE A JEJICH ZABEZPEČENÍ ŠIFROVACÍMI KLÍČI V DRŽENÍ KANCELÁŘE6

ZPŮSOB NAKLÁDÁNÍ S ŠIFROVACÍM KLÍČEM V DRŽENÍ KANCELÁŘE 7

4) ŘÍZENÍ BEZPEČNOSTI UVNITŘ FIRMY 9

ACCESS POLICY 9

SECURITY POLICY 9

1) Bezpečnost dat a povinnost mlčenlivosti advokáta

Místo a způsob uložení dat

SingleCase ke svému provozu využívá privátního cloudu umístěného ve Frankfurtu na serverech společnosti Amazon Web Services, Inc. se sídlem 440 Terry Ave N, Seattle, WA, 98109 United States. Systém je tak stále dostupný a díky používaným šifrovacím možnostem také maximálně bezpečný. Dokumenty šifrujeme tak, že klíče k nim má v držení pouze zákazník, nikoli my jako poskytovatel.

V případě zákazníků - advokátů ctíme povinnost mlčenlivosti advokáta dle § 21 zákona o advokacii. SingleCase je místem, kde můžete ukládat data svých klientů (viz také stanovisko trestního kolegia Nejvyššího soudu Tpjn 306/2014). Veškerá data zákazníků spravujeme dle Směrnice 95/46/ES a Zákona o ochraně osobních údajů – Poskytovatel cloudu garantuje, že data nikdy neopustí země Evropského hospodářského prostoru. Pokud se na nás obrátí orgány činné v trestním řízení, informujeme o tom jak zákazníka, tak Českou advokátní komoru.

Zálohování a export

Dokumenty, data vaše i vašich klientů jsou křížově zálohovány na více místech. V nepravděpodobném případě výpadku aplikace nebo dokumentů postupujeme dle transparentních scénářů tzv. *disaster recovery* pro zajistění přístupu v co nejkratším čase. Dokumenty i veškerá data si můžete kdykoli stáhnout přímo z aplikace SingleCase. Rádi vám také budeme posílat plné zálohy vašich spisů – automaticky a na úložiště dle vašeho výběru.

2) Řízení přístupu k datům a technické opatření jejich zabezpečení

Vymezení pojmů

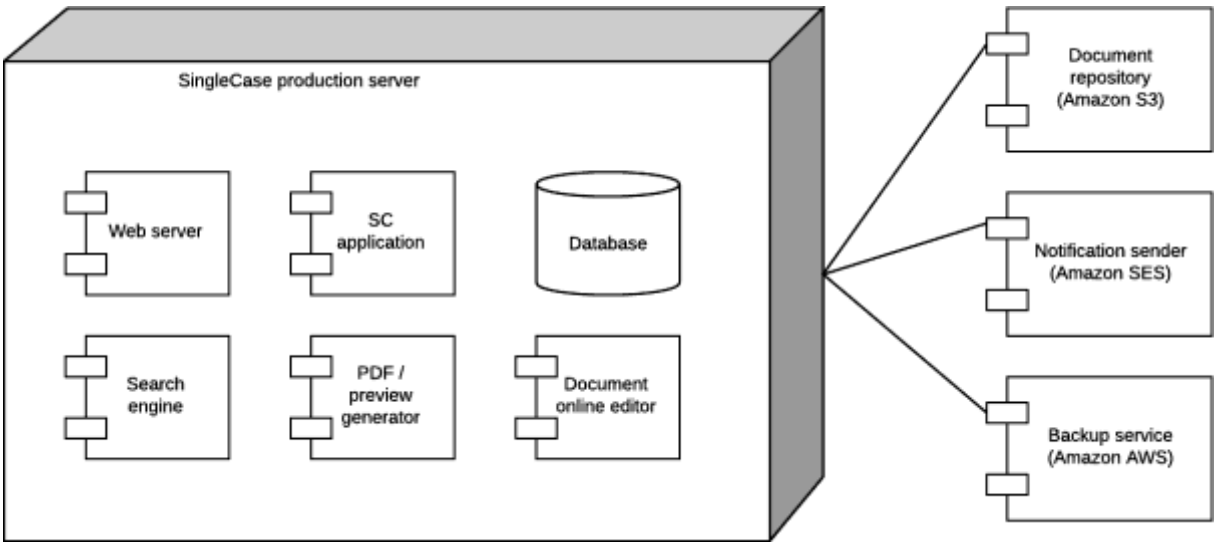
Datové centrum – Místo, kde je fyzicky umístěn server, a které mu poskytuje konektivitu k internetu, fyzické zabezpečení, zálohování a další služby. SingleCase používá datové centrum společnosti Amazon Web Services, Inc. ve Frankfurtu.

Server – Počítač, na kterém běží aplikace SingleCase. Rozlišuje se fyzický server (konkrétní kus hardwaru) a virtuální server (kus pronajaté výpočetní kapacity, HW je typicky velmi výkonný a dělitelný na malé části – případ SingleCase). Kromě samotné aplikace SingleCase (viz níže) běží na serveru také podpůrné aplikace nutné pro její provoz, např. vyhledávací engine, aplikace pro online úpravu dokumentů, databáze, webový server, komponenta pro generování náhledů a jiné.

Aplikace – Počítačový program SingleCase a podpůrné aplikace, které běží na serveru a vykonává operace z pověření uživatele (čtení/zápis do databáze, čtení/zápis do dokumentového úložiště) nebo na pozadí (e-mailové notifikace, příjem pošty, automatická záloha atd.).

Databáze – Struktura, ve které jsou uložena data aplikace.

Dokumentové úložiště – Místo, ve kterém jsou uloženy fyzické dokumenty. Propojeno s aplikací prostřednictvím odkazů na dokumenty z databáze.



Server

Server si pronajímáme prostřednictvím služby *Amazon AWS*, který zabezpečuje jeho fyzickou bezpečnost a dostupnost aplikace. V rámci týmu SingleCase existují dvě osoby s přístupem ke konfiguraci serveru, tím jsou CEO a CTO (vedoucí vývoje). Přístup ke konfiguraci

neznamená automaticky možnost přístupu na server, nicméně prostřednictvím konfigurace lze přístup udělit.

Přístup na samotný server je řízen na úrovni uživatelských účtů konkrétních zaměstnanců SingleCase. K produkčnímu serveru s daty zákazníka mají přístup dvě osoby, a to CTO a senior vývojář (pro zajištění možnosti zásahu v případě absence CTO). Přístupem k serveru získává uživatel možnost přístupu k souborům aplikace vč. přístupovým údajů k databázi

Databáze

Databáze je umístěna přímo na serveru SingleCase. K datům zákazníka mají přístup tři uživatelé s administrátorskými právy – speciální uživatel, pod kterým se hlásí aplikace (více o jejím zabezpečení níže), dále CTO a senior vývojář. **Přístup k datům z naší strany je vždy omezen na konkrétní účty, slouží výhradně k identifikaci a opravě chyby a vždy pouze na dobu nezbytně nutnou**. Podobně jako v případě serveru nepoužíváme z bezpečnostních důvodů účty administrátora, uživatelé se vždy hlásí se svými přístupovými údaji a veškeré jejich operace jsou logovány.

Dokumenty

Dokumenty jsou umístěny na speciálním dokumentovém úložišti *Amazon S3*. Architektura úložiště je postavena na principu malých oddělených úložišť (tzv. *buckets*). Každý *bucket* je šifrován svým vlastním klíčem a znemožňuje vydání dat bez jeho znalosti – tento způsob tedy efektivně zamezuje stažení byť jen zašifrovaných dokumentů bez vědomí vlastníka klíče. Oproti běžnému uložení dokumentů na disku je v *bucketu* oddělen binární obsah dat od jejich popisovače – bucket tedy neobsahuje čitelný název dokumentu. SingleCase využívá metodu, v rámci které je v každém *bucketu* uložen právě jeden dokument – nabytím klíče k jednomu dokumentu tedy nelze získat přístup k jinému.

K přístupu k dokumentu je nutné rozšifrovat soustavu šifrovacích klíčů, přičemž každý z nich odemyká další v řadě. Hierarichie klíčů je následující:

1. **Heslo uživatele** – uloženo v databázi chráněno jednosměrnou 256-bitovou šifrou (SHA-2), chráněno před slovníkovými útoky technologií tzv. solení, vyžadována kvalita hesla (délka i rozsah znaků)
2. **Klíč uživatele** – uložen zašifrovaný v databázi 256-bitovou symetrickou šifrou (AES), generuje se při při vytvoření nového uživatele spolu s jeho heslem, každý uživatel má unikátní klíč
3. **Hlavní klíč firmy**, tzv. *master* klíč, uložen zašifrovaný v databázi 256-bitovou symetrickou šifrou (AES)
4. **Klíč dokumentu** – uložen zašifrovaný v databázi 256-bitovou symetrickou šifrou (AES), je součástí metadat dokumentu spolu s odkazem na *bucket*, každý dokument je umístěn v jiném *bucketu* a tedy má unikátní klíč

Aplikace

Aplikace má při svém běhu přístup k datům, krátkodobě i těm, které jsou při uložení šifrovány (například při synchronizaci pošty se po přihlášení uživatele rozšifrují přístupové údaje ke schránkám, aplikace k nim má přístup do dokončení úlohy). Aplikaci proto podrobujeme pravidelným (2x ročně) bezpečnostním auditům externího partnera – specialisty na bezpečnost aplikací.

Audit je prováděn v těchto fázích:

1. **Audit architektury** – posuzována kvalita návrhu komponent aplikace, systém ukládání šifrovacích klíčů, umístění a ochrana aplikace, databáze i dokumentů
2. **Kontrola zdrojového kódu** – odhaluje potenciální problémy nebo chyby v nakládání s daty při běhu aplikace
3. **Penetrační testy** – testování aplikace v živém provozu s cílem odhalit běžné problémy webových aplikací (např. definovány projektem *OWASP*), které by mohly vést k porušení důvěrnosti informací externím (pokus o prolomení aplikace) nebo interním (pokud o zvýšení práv uživatelem s omezenými právy) útočníkem.

3) Kategorie dat v SingleCase a jejich zabezpečení šifrovacími klíči v držení kanceláře

SingleCase obsahuje systém šifrování s využitím šifrovacích klíčů, které jsou v držení zákazníka. Aktuálně (11/16) se těmito klíči šifrují fyzické dokumenty v úložišti Amazon S3 a přístupové údaje k poštovní schránce uživatelů. V průběhu je přechod na plné šifrování u vybraných kategorií dat, tak aby k nim byl vyloučen jakýkoli přístup Poskytovatele.

Kategorie dat	**Plán šifrování**	**Náročnost / dopady šifrování**
Klient – název	Nelze šifrovat	• E-mailové notifikace (nelze posílat s názvem klienta) • Synchronizace s kalendářem (dtto) • Rychlost filtrování spisů v seznamu • Obecně práce s výkazy, fakturami (pomalý výběr filtru)
Klient – metadata (adresy, fakt. údaje)	Výhledově	• Nemožnost sledování solventnosti (IČO, datum narození / rodné číslo)
Spis – název	Nelze šifrovat	• E-mailové notifikace (nelze posílat s názvem spisu) • Synchronizace s kalendářem (dtto) • Rychlost filtrování spisů v seznamu • Obecně práce napříč aplikací (zpomalení v řádu desítek procent)
Spisy - metadata	Výhledově	• Rychlost filtrování spisů v seznamu
Kontakty (klient, spis)	Výhledově	-
Protistrany	Výhledově	• Rychlost filtrování spisů v seznamu • Nemožnost sledování solventnosti
Sazby (klient, spis)	Výhledově	-
Dokumenty – fyzické	Šifrováno	-
Dokumenty - název	Nelze šifrovat	• Nemožnost hledání v dokumentech stávajícím mechanismem (teoreticky lze s velmi velkým dopadem na rychlost)
Složky - název	Výhledově	• Rychlost výpisu dokumentů

Úkoly a termíny – název	Nelze šifrovat	• Nelze posílat e-mailové notifikace • Nelze synchronizovat úkoly a termíny do kalendáře
Úkoly a termíny – popis	Výhledově	• Nelze zaslat popis úkolu / termínu v notifikaci
Korespondence – předmět	Šifrování v přípravě	• Rychlost výpisu pošty • Rychlost vyhledávání v poště
Korespondence – obsah	Šifrování v přípravě	-
Poznámky ve spisu	Šifrování v přípravě	-
Výkazy – popis	Výhledově	• Rychlost načtení / úpravy faktur • Rychlost přehledu výkazů (zpomalení v řádu desítek procent)
Náklady – popis	Výhledově	• Dtto jako výkazy, pouze s nižším dopadem (menší množství výkazů)
Faktury – celková částka	Nelze šifrovat	• Rychlost načítání přehledu faktur • Kritický vliv na výpočet reportů (nyní se generují při načtení - neukládají se, nutná změna)
Přístupové údaje ke schránce uživatele	Šifrováno	-

Způsob nakládání s šifrovacím klíčem v držení kanceláře

1) Při registraci nového účtu se vytvoří tzv. *master klíč*, kterým šifrujeme dokumenty. Uživateli se také vytvoří jednorázově zobrazí *obnovovací klíč kanceláře*, systém následně vyzve k jeho vytištění a bezpečnému uložení. Klíčem lze obnovit přístup k šifrovacím dokumenty v případě zapomenutí přihlašovacích údajů všemi uživateli aplikace.

2) Po registraci se *master klíč* také použije pro vytvoření hesla prvního uživatele. Následně je zašifrován a již nikdy se v aplikaci neobjeví v nezašifrované podobě.

3) Po přihlášení uživatele se jeho heslo použije ke krátkodobému dešifrování *klíče uživatele* odvozeného z *master klíče*, díky němuž může po dobu svého přihlášení přistupovat k dokumentům, případně zakládat nové uživatele. Bez přihlášení neexistuje žádná možnost, jak se k dokumentům v aplikaci dostat.

4) Změna hesla uživatelů je možná pouze po přihlášení administrátora do aplikace – není tedy kupříkladu možné obnovit heslo uživateli přes e-mailovou adresu.
V případě, že heslo zapomene administrátor, můžeme krátkodobě zvýšit práva

jinému uživateli – ten následně vytvoří nové heslo kolegům.

5) V případě ztráty hesel všech uživatelů přepneme na žádost zákazníka aplikaci do režimu obnovy, kdy je možné zadat *obnovovací klíč*. Po obnovení je možné znovu vytvořit heslo administrátora.

   Upozornění: Použité šifrování neumožňuje, aby se k dokumentům v případě ztráty hesel všech uživatelů dostal kdokoli jiný. Proto je pro případnou obnovu klíčové ponechat si bezpečně uložený klíč vygenerovaný při prvním použití.

4) Řízení bezpečnosti uvnitř firmy

Access policy

Konkrétní způsob řízení přístupů (uživatelů i aplikace) je popsán do většího detailu v dokumentu v dokumentu *SingleCase access policy*, jehož vlastníkem je CTO, který zajišťuje jeho dodržování. Dokument popisuje zejména scénáře přidělení, obnovy a odvolání přístupů a konkrétní způsob realizace.

Security policy

Bezpečnostní standardy nakládání s citlivými informacemi je popsán v dokumentu *SingleCase security policy*, jehož vlastníkem je CEO, který zajišťuje jeho dodržování. Dokument popisuje způsob nakládání s hesly, jejich kvalitu, scénáře jednání vč. těch zakázaných.

Oba dokumenty rádi poskytneme k nahlédnutí.