ČESKÁ spořitelna

Technická příručka Bankovního Datatrezoru České spořitelny

Obsah

1 Datatrezor

Přístup ke službě a k zabezpečení dat je podobný jako ve fyzickém světě u bezpečnostních schránek. Zajišťujeme bezpečné místo pro uložení Vašich cenností, a to ověřením Vaší identity a autentizací digitálním klíčem, abychom mohli garantovat přístup do Datartezoru pouze Vám.

2 Přihlášení a autorizace

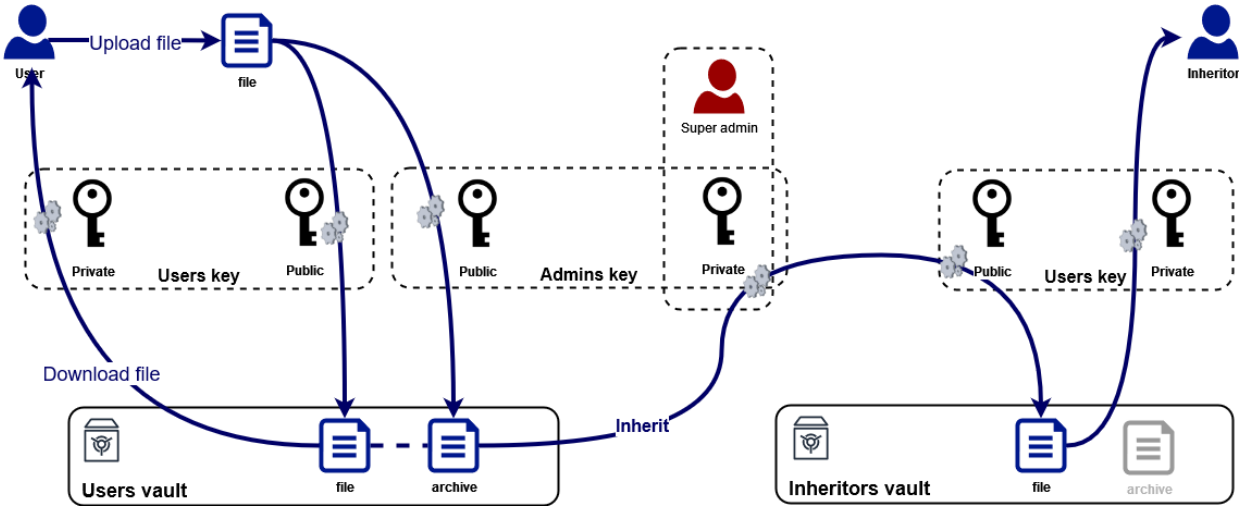
Ověření identity uživatele a přihlášení k Datatrezoru je zajištěno na základě kvalifikovaného systému elektronické identifikace s úrovni záruky **ZNAČNÁ.**

Uživatel se hlásí ke službě Datatrezor stejně, jako kdyby se hlásil do jakékoliv banky na českém trhu. I když se jedná o službu České spořitelny, je možné se přihlásit pomocí řešení jiné banky, která je akreditovaným poskytovatelem bankovní identity. Díky požadavku na úroveň záruky je zajištěna odpovídající síla ověření uživatele a přihlášení, kterou pravidelně kontroluje audit Ministerstva vnitra České republiky. Podrobné informace jsou k dispozici zde.

Autorizace přístupu na data je zajištěna na základě identifikovaného a ověřeného uživatele s využitím JWT tokenů. Tím je zajištěna integrita záznamu propojení dané identity s asymetrickými klíči, kterými jsou chráněna uložená data. Použité kryptografické algoritmy odpovídají doporučení NUKIB, jehož znění je dostupné zde: Doporučení v oblasti kryptografických prostředků (nukib.cz).

3 Uložení dat

Data jsou uložena ve službě cloudového poskytovatele MS Azure v datových centrech umístěných na území EU. Každý trezor, ve kterém jsou uložena uživatelská data, je veden jako oddělený kontejner v datovém úložišti se specifickým nastavením přístupových oprávnění. Soubory v trezoru jsou uloženy v denormalizované podobě, bez názvu souboru a informací o obsahu. Pro každý trezor je při jeho založení vytvořena sada asymetrických klíčů (privátní a veřejný klíč). Privátní klíč je bezpečně uložen v auditovaném úložišti klíčů mimo aplikaci Datatrezor. Veřejný klíč slouží k zašifrování souboru pro uložení do kontejneru trezoru. Takto zašifrovaný soubor je možné přečíst jen při použití privátního klíče, který není bez předchozí autorizace uživatele dostupný.



4 Řešení a bezpečnostní požadavky

Na řešení jsou aplikovány bezpečnostní požadavky vycházející

- ze standardu Minimální bezpečnostní standard – podpůrný materiál pro subjekty, které nespadají pod zákon o kybernetické bezpečnosti,
- ze zákona č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Jeho znění naleznete zde.

Řešení pravidelně prochází testy zranitelností a penetračními testy, jako jsou OWASP, CWE, OSSTMM, PTES a další.