POŽADAVEK NA ČERPÁNÍ MD / ZMĚNOVÝ POŽADAVEK Č. 41

Poskytovatel služby	Pasante s.r.o. Hybernská 1007/20, 110 00 Praha 1
Správce IS	Správa základních registrů, 130 00 Praha 3 Na Vápence 14
Objednatel	Správa základních registrů, 130 00 Praha 3 Na Vápence 14
Smlouva	Smlouva o poskytování služeb podpory provozu a rozvoje RAZR, č.: SZR-1658-17/OEM-2017
Číslo RFC SZR	**1164**
Název RFC SZR	RAZR - Nastavení přímého přístupu ke službám CA pro vydávání certifikátů
Kategorie RFC	**Change**
Číslo tiketu (Service Desk)	122167
Katalogový list	**RAZR10 - objednávka**
Typ odstávky	Zero

1. Identifikace vzniku požadavku

RAZR přijímá žádosti o vydání i o odvolání certifikátů pro přístup do základních registrů a ISSS. Žádosti předává na Service Desk (SD) SZR a od SD přijímá výsledky. Pracovníci SD se připojí k CA SZR a požádají o vydání, respektive odvolání certifikátů. Dělají to tak, že spustí proceduru (batch) s příslušnými příkazy.
Vydané certifikáty uloží do adresáře na disku, který je pro RAZR přístupný, RAZR si je odtud přečte a automaticky je spáruje s příslušnými žádostmi.
Proces tedy obsahuje manuální činnosti, které vykonává SD SZR.

2. Zadání požadované změny

Nahradit manuální zpracování požadavků na vydání a odvolání certifikátu komunikací aplikace RAZR s Certifikačními autoritami pro vydávání certifikátů do produkčního a testovacího prostředí ZR a ISSS.

3. Popis zajištění změny

Změny požadované po Pasante jsou ty, které nejsou kurzívou.

3.1 Změny

- Uzpůsobit informační sytém RAZR tak, aby realizoval případy užití (use case) uvedené v tomto dokumentu.
- Zrušit posílání požadavků na SD SZR e-mailem.
  Nastavit zpracování žádosti, která obsahuje žádost o certifikát:
  - Ruční zpracování.
  - Automatické zpracování.
- Nahradit stávající postup, kdy RAZR kopíruje žádosti o certifikáty na sdílený disk a čte vydané certifikáty, novým postupem, který je popsaný v tomto dokumentu.
  Odstranit službu, která kopíruje soubory na síťové úložiště a ze síťového úložiště.
  - Zadat požadavek na zrušení síťového prostupu.

- Ke komunikaci mezi RAZR a CA použít webové služby a protokol HTTPS.
  - *Na straně CA bude použitý web server IIS.*
    Instalaci a konfiguraci IIS na serverech CA zajistí SZR ve spolupráci s dodavatelem.
  - RAZR bude volat webovou službu vystavenou na serveru CA.
- Pro komunikaci s CA bude použit endpoint webové služby, který bude vystavený na serveru CA, RAZR ho bude v pravidelných intervalech volat.
- Endpoint Webové služby bude obsahovat tyto metody:
  - PodepsatZadost - use case Žádost o vydání certifikátu.
  - ZneplatnitCertifikat - use case Žádost o odvolání certifikátu.
  - OdeslatLog - odešle logy endpointu za zadané období.
- Jednotlivé metody budou spouštět na straně CA příkazy, které pracuji s certifikační autoritou. *Jako příklad mohou sloužit procedury, které jsou v kapitole "Proof of Concept" tohoto dokumentu.*
- RAZR bude volat služby automaticky v naplánovaném čase.
- V konfiguraci RAZR bude možné automatické volání služeb vypnout a zapnout.
- RAZR bude obsahovat možnost (funkční tlačítko / tlačítka) pro manuální spouštění procedur. Bude je možné ručně spouštět přímo z formuláře konkrétního certifikátu, nebo z konkrétní žádosti o certifikát.
- Není možné během vývoje testovat proti CA pro testovací prostředí ZR. Proto je nutné připravit 2 nové CA a propojit je s RAZR-test.
  - *Vytvořit ve virtuálním prostředí SZR 2 nové tenanty. Zajistí SZR.*
  - *Vytvořit v každém tenantu 1 virtuální server. Zajistí SZR.*
  - Nainstalovat na virtuální servery OS MS Windows Server.
    Licence zajistí SZR. Je možné využít 180 denní možnost provozovat MS Windows Server bez licence.
    Instalaci OS zajistí Pasante.
  - Nainstalovat a nakonfigurovat na každý virtuální server MS Certifikační autoritu.
    Zajistí Pasante.
  - Nainstalovat a nakonfigurovat na každý virtuální server (IIS, .NET Framework)IIS.
    Zajistí Pasante.
  - Na obou virtuálních serverech vytvořit uživatele "razr".
    Bude použitý pro spouštění příkazů pro vydání a odvolání certifikátů – bude pod ním spuštěn endpoint WS.
    Zajistí Pasante.
  - *Zajistit síťovou konektivitu mezi Interním modulem RAZR-test a vytvořenými CA.*
    Zajistí SZR.

3.2 Parametry webové služby

- Typ služby: REST API
- Zabezpečení
  - Na serveru CA bude SSL certifikát (použijeme self signed certifikát) – volání jen přes HTTPS (443)
  - Každé volání bude autentizováno pomocí klíče (GUID) zaslaného v hlavičce volání
  - Služba bude dostupná jen z INT serveru RAZR – síťový prostup mezi servery na portu 443

3.3 Žádost o vydání certifikátu - use case

Požadovaná změna je v těch krocích, které nejsou kurzívou.

- *Správce AIS zadá do KIVS modulu RAZR žádost, která obsahuje požadavek na vydání certifikátu pro AIS a jako přílohu přidá technickou žádost ve formátu PKCS10.*
- *KIVS modul předá žádost Internímu modulu RAZR.*
- *Interní uživatel žádost schválí.*
- Interní modul RAZR označí záznamy s žádostí o certifikát (část žádosti) ke zpracování pomocí webových služeb.
- Interní modul RAZR zavolá pro všechny označené technické žádosti webovou službu endpointu na CA serveru pro produkční, respektive pro testovací prostředí ZR (bude rozlišeno podle prostředí, pro které je žádost vystavená).
- Webová služba na serveru CA přijme požadavek na vydání certifikátu a spustí procedury, které obsahují volání služeb CA. Každá procedura požádá o vydání certifikátů (příkazem certreq) na základě žádostí předaných webovou službou.
- CA pro každou žádost buď vrátí certifikát, nebo vrátí chybovou zprávu – předá se jako odpověď volání WS.
- Pokud CA vrátí certifikát, RAZR ho dostane v odpovědi na žádost o vydání certifikátu a uloží certifikát k příslušné žádosti.
- Pokud CA certifikát nevydá, vrátí webová služba chybové hlášení CA - návratový kód certutil.
- V případě, že CA není dostupná, RAZR se ji pokouší kontaktovat opakovaně.
- Interní uživatel RAZR má možnost žádost zamítnout. RAZR v takovém případě už CA dále pro tuto žádost nekontaktuje.
- Interní uživatel RAZR má možnost žádost převést do stavu Chyba a následně někdy stav Chyba zrušit. Po dobu stavu Chyba RAZR CA pro příslušnou žádost nekontaktuje.
- Interní modul RAZR ukládá certifikáty vrácené webovou službou CA do formuláře Certifikáty (stávající součást žádosti).
- *RAZR dokončí zpracování část žádosti s požadavkem na vydání certifikátu.*

3.4 Žádost o odvolání certifikátu - use case

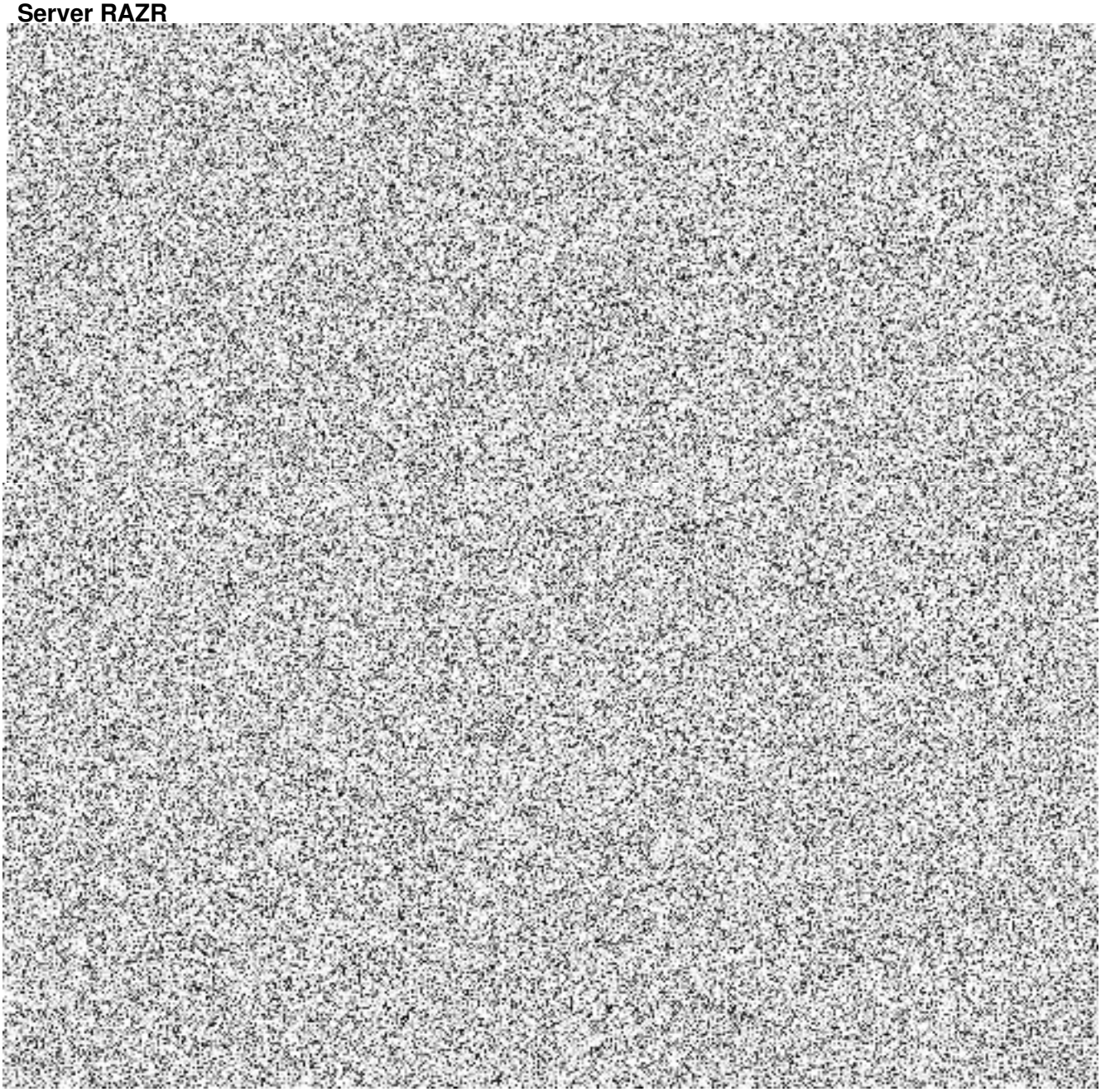
Požadovaná změna je v těch krocích, které nejsou kurzívou.

- *Správce AIS zadá do KIVS modulu RAZR žádost o odvolání certifikátu, zadá jeho sériové číslo a případně důvod odvolání.*
- *KIVS modul předá žádost Internímu modulu RAZR.*
- *Interní uživatel žádost schválí.*
- Interní modul RAZR označí záznamy s žádostí o odvolání certifikátu (část žádosti) ke zpracování pomocí web služby.
- Interní modul RAZR zavolá web službu CA a předá jí sériová čísla odvolávaných certifikátů.
- Endpoint WS na serveru CA spustí odvolání certifikátů (příkazem certutil).
- CA pro každou žádost vrátí výsledek zpracování, ten je vrácen v (response) odpovědi webové služby.
- Pokud CA vrátí, že certifikát je odvolaný RAZR zapíše do příslušné části žádosti, že je vyřízena.
- Pokud CA certifikát neodvolá, zapíše RAZR do příslušné části žádosti chybový stav a zastaví zpracování celé žádosti.
- V případě, že CA není dostupná, RAZR se ji pokouší kontaktovat opakovaně.
- Interní uživatel RAZR má možnost žádost zamítnout, RAZR v takovém případě už CA dále pro tuto žádost nekontaktuje.
- Interní uživatel RAZR má možnost žádost převést do stavu Chyba a následně někdy stav Chyba zrušit. Po dobu stavu Chyba RAZR CA pro příslušnou žádost nekontaktuje.
- *RAZR dokončí zpracování žádosti.*
- V případě automaticky generovaných žádostí o odvolání certifikátu je postup stejný.

3.5 Proof of Concept komunikace mezi RAZR a CA

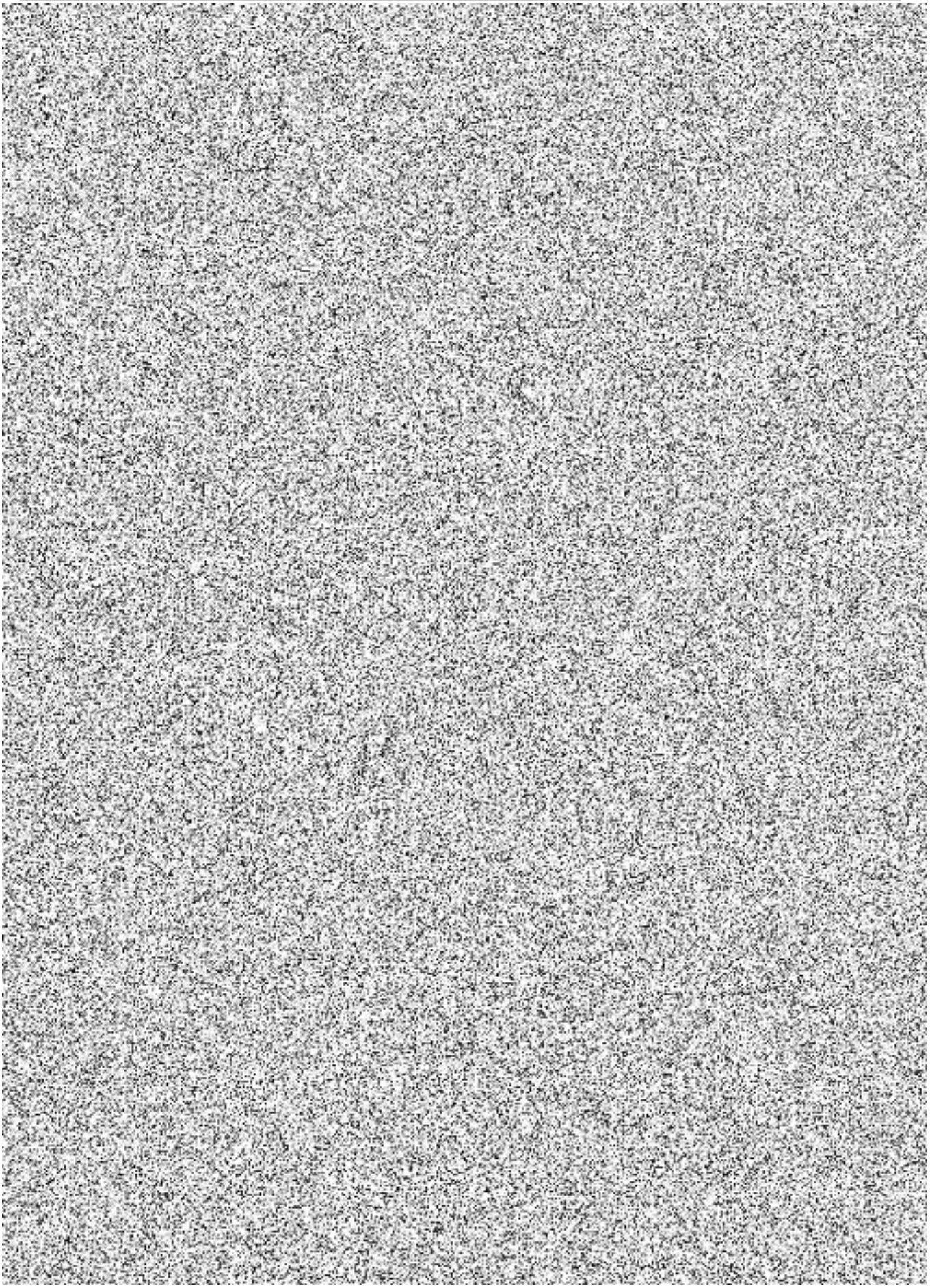
V této kapitole je demonstrována realizovatelnost navrženého způsobu komunikace mezi aplikací RAZR a Certifikační autoritou a realizovatelnost navrženého způsobu vydávání a odvolávání certifikátů. Nejedná se kompletní řešení, zejména chybí ošetření chyb a různých mimořádných stavů.
Proof of Concept je realizovaný s použitím protokolu SSH. Řešení s HTTPS je analogické.
Certutil bude volán webovou službou na serveru CA s níže popsanými příkazy.

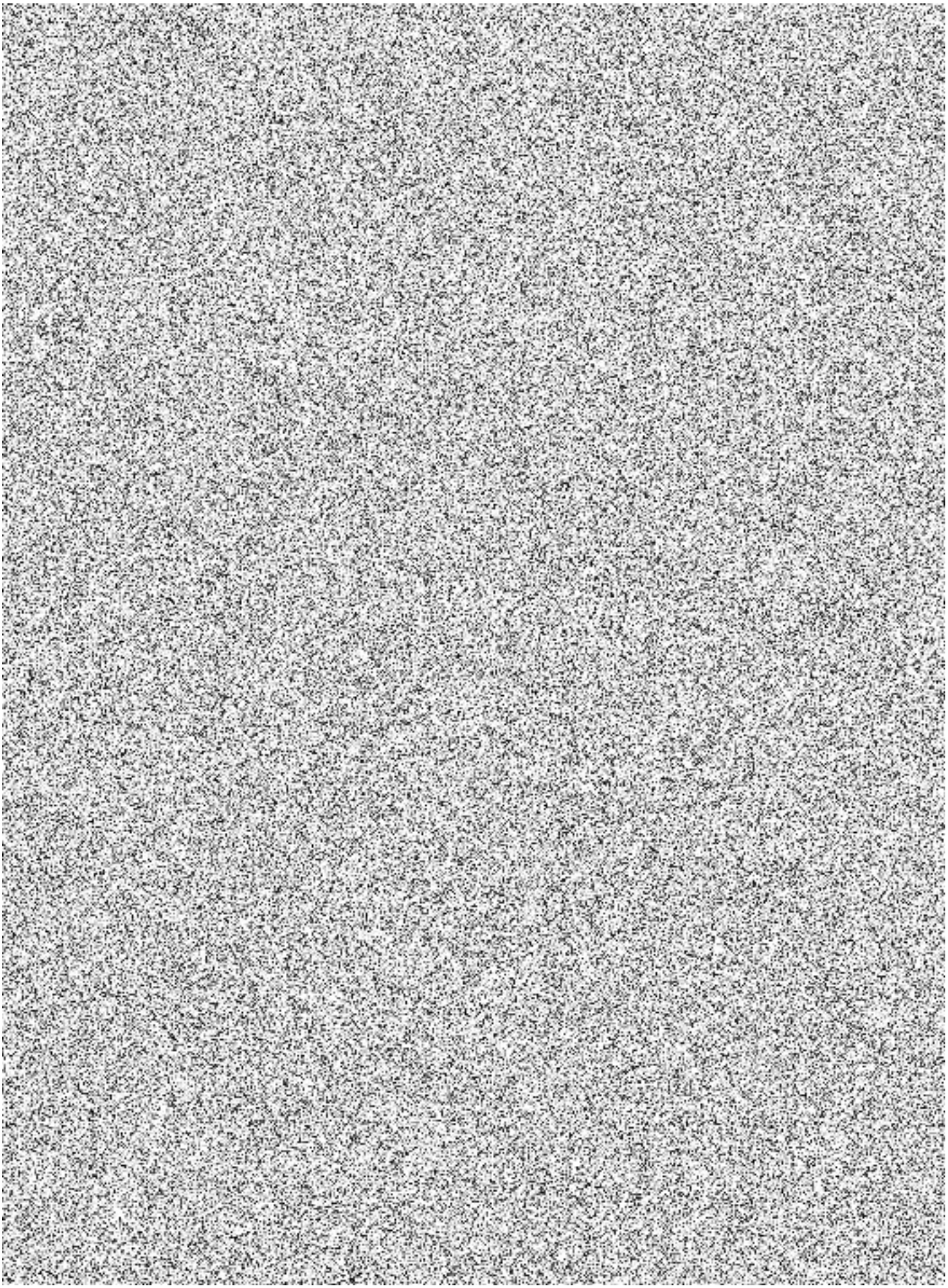
Server RAZR

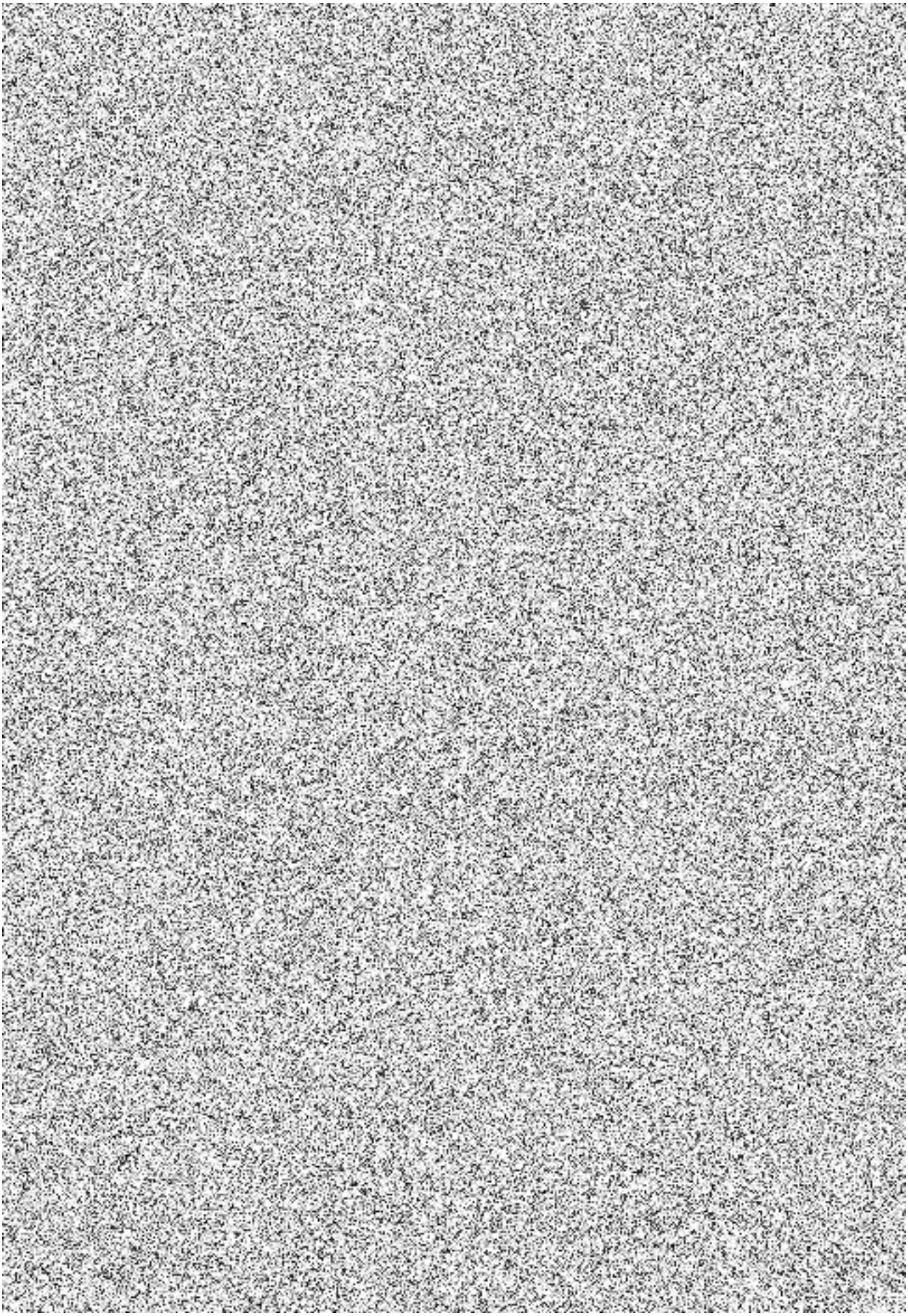


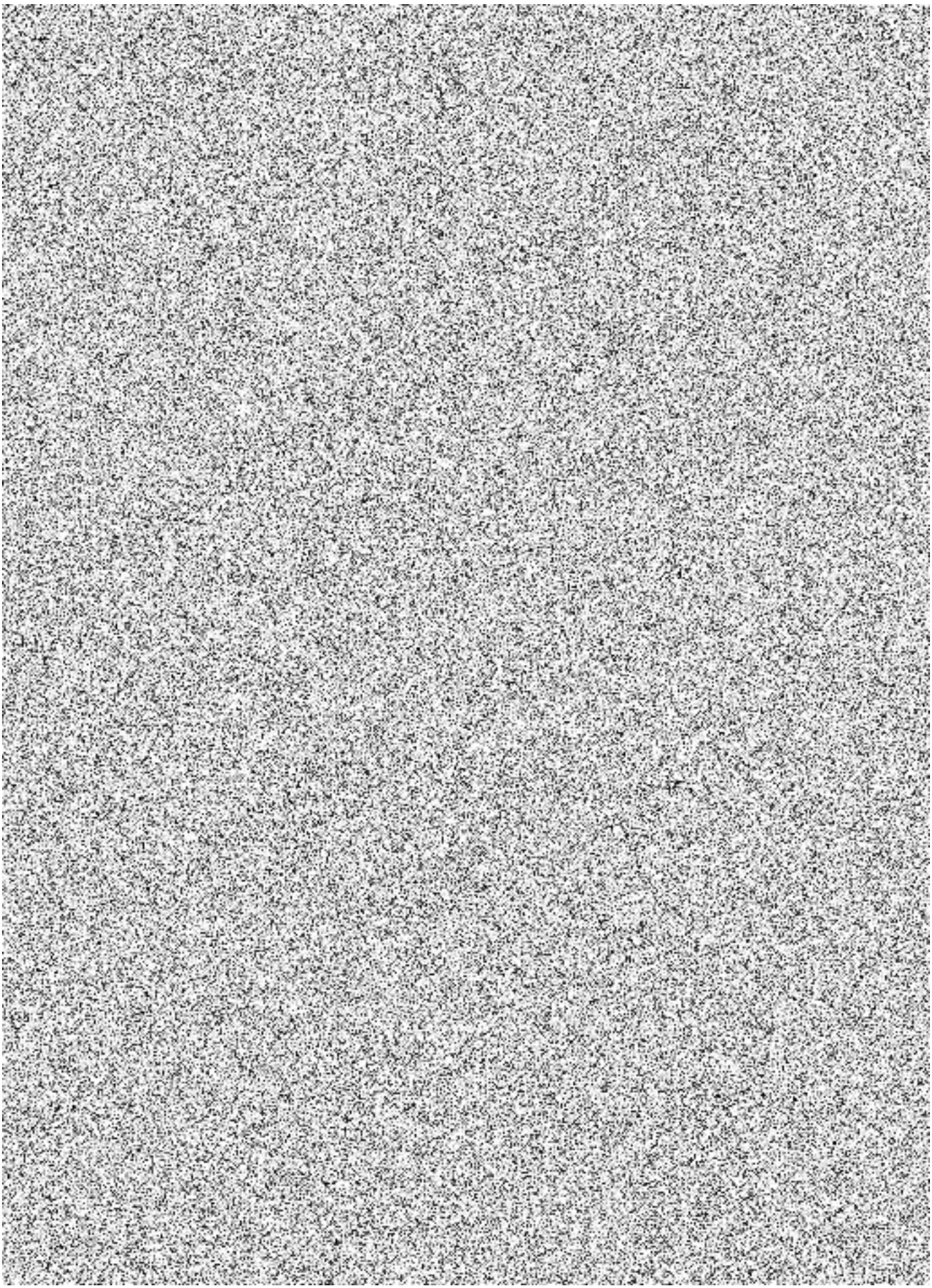
Komunikace RAZR - CA

Veškerá komunikace mezi RAZR a CA probíhá protokolem SSH.
Mezi RAZR a CA jsou firewally. Na nich musí být povolený prostup z RAZR na CA na TCP / 22.
A na CA serveru musí být povolená příchozí spojení SSH (v lokálním firewallu).









4. Pracnost

- Analýza – [redacted]
    - Návrh řešení.
    - Zjištění, jak funguje Windows CA a jak se konfiguruje.
- Implementace
    - Instalace testovacího prostředí (2x WIN server + konfigurace CA a IIS) [redacted]
    - Řešení problémů s prostupy, testování [redacted]
    - Vytvoření endpointu a jeho instalace na CA (2x na vývojové prostředí 2x na produkční prostředí (prod a test). [redacted]
    - Zjistit, jak CA funguje a jak správně volat certutil, čtení výstupů certutil [redacted]
    - Volání služeb endpointu z RAZR. [redacted]
    - Změna procesů ve zpracování žádosti. [redacted]
        - Změna zpracování části žádosti Certifikáty.
            - Část: Manuální zpracování.
            - Část: Automatické zpracování.
        - Zobrazení logů a vyhodnocování odpovědi CA – zpřístupnit pro uživatele.
        - Zrušení stávajícího způsobu předávání.
- Testování [redacted]
- Úprava dokumentace – [redacted]
- Release – [redacted]

Celkem: [redacted]

Celková pracnost: [redacted] **403 000,- Kč bez DPH, tj. 487 630,- Kč s DPH**

Poznámka: Článek 5.1.2 Smlouvy „Cena služeb na objednávku“, Katalogový list RAZR10 „Optimalizace parametrů poskytovaných služeb ZR“ – tento KL v rámci tohoto PnČ neslouží k pracím, které vedou k navýšení stávajících funkcionalit, a tedy k technickému zhodnocení IS dle vyhlášky č. 410/2009 Sb., k provedení zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů pro vybrané jednotky. V rámci PnČ 2023-41 nebudou prováděny žádné rozvojové činnosti.

Poskytovatel služby (dále jen „Pasante“) bere na vědomí, že předmět plnění tohoto PnČ č. 41 je spolufinancován z fondů Evropské unie, konkrétně z programu Národní plán obnovy (dále jen „NPO“), v rámci pilíře Digitální transformace, pro projekt, který byl zahrnut do projektu s názvem „Budování referenčního rozhraní propojeného datového fondu“ (dále jen „projekt“) s registračním číslem projektu: CZ.31.1.01/MV/22_22/0000022. Pasante v této souvislosti bere na vědomí, že je povinen plnit některé další povinnosti vyplývající z podmínek realizace projektu, a to uchovávat veškerou dokumentaci související s realizací poskytnutého plnění dle tohoto PnČ č. 41, včetně všech účetních dokladů, nejméně po dobu 10 let ode dne schválení závěrečné zprávy o projektu, s tím, že o datu jejího schválení bude Pasante ze strany SZR informován po skončení projektu. Faktura za plnění dle tohoto PnČ č. 41 bude obsahovat údaje o názvu projektu a registrační číslo projektu, viz identifikace výše.

5. Harmonogram změnového požadavku

Den D = Přijetí SD požadavku na zapracování požadavku

Analýza: do D + 15 dní

Úprava systému a testování: D + 90 dní

Nasazení do produkčního: do D + 120 dní

Termín dodání: nejpozději do 15.6.2023

Termín dodání může být prodloužen v případě neposkytnutí nezbytné součinnosti dle bodu 9. tohoto PnČ, nebo z dalších důvodů na straně objednatele. Nejzazší termín dodání je však 30.9.2023.

6. Testovací scénáře

- Vydat několik certifikátů.
- Odvolat několik certifikátů.
- Nasimulovat chybové stavy:
  - Nedostupnost CA.
  - Chybu při vydávání certifikátu (CA odmítne vydat certifikát).
  - Chybu při odvolání certifikátu (CA odmítne odvolat certifikát).
- Manuální spouštění procedur.

7. Výstupy změnového požadavku

Aktualizovaná verze Interního modulu RAZR s funkcemi uvedenými v tomto dokumentu.
Procedury pro přenos souborů mezi servery RAZR a servery CA ISZR.
Procedury pro vydávání a odvolávání certifikátů.

8. Akceptační kritéria, způsob ověření na produkci

Akceptační kritéria:

- Úspěšné otestování změn v testovacím prostředí RAZR napojeném na testovací Certifikační autority, které byly vytvořeny nově na základě tohoto změnového požadavku.
- Technická dokumentace RAZR odpovídá skutečnému stavu po implementaci změnového požadavku.

Způsob ověření na produkci:

- Kontrola přítomnosti změn v produkčním prostředí RAZR.
- Vydání a odvolání certifikátu pro AIS RAZR-test (AIS 8625) pro přístup do testovacího prostředí ZR s použitím RAZR-produkce.

9. Požadavky na součinnosti

- Připravit dvě testovací Certifikační autority a propojit je s RAZR-test.
  Při vývoji není možné použít existující CA pro testovací prostředí ZR. Na tuto CA je napojený RAZR-produkce. RAZR-test není dosud napojený na žádnou CA.
  - Vytvořit ve virtuálním prostředí SZR 2 nové tenanty. Zajistí SZR.
  - Vytvořit v každém tenantu 1 virtuální server. Zajistí SZR.
  - Nainstalovat na virtuální servery OS MS Windows Server.

Licence zajistí SZR. Je možné využít 180 denní možnost provozovat MS Windows Server bez licence.
Instalaci OS zajistí Pasante.

- Nainstalovat a nakonfigurovat na každý virtuální server MS Certifikační autoritu.
  Zajistí Pasante.
- Nainstalovat a nakonfigurovat na každý virtuální server IIS.
  Zajistí Pasante.
- Na obou virtuálních serverech vytvořit uživatele "razr".
  Zajistí Pasante.
- Zajistit síťovou konektivitu mezi Interním modulem RAZR-test (RAZR2T-INT) a vytvořenými servery CA. Musí být povolené spojení HTTPS ve směru z RAZR na servery CA.
  Zajistí SZR.
- Po testování ponechat virtuální servery pro budoucí využití.

- Na serveru s CA pro testovací prostředí ZR a na serveru s CA pro produkční prostředí ZR vytvořit uživatele "razr".
  Bude použitý pro kopírování souborů mezi RAZR a CA a pro spouštění příkazů pro vydání a odvolání certifikátů pro testovací, respektive produkční prostředí ZR.
  Zajistí SZR ve spolupráci s Autocontem.
- Instalace a konfigurace IIS na serveru s CA pro testovací prostředí ZR a na serveru s CA pro produkční prostředí ZR.
  Zajistí SZR ve spolupráci s Autocontem.
- Na obou serverech CA povolit (v lokálním firewallu) příchozí HTTPS spojení.
  Zajistí SZR ve spolupráci s Autocontem.
- Na obou serverech CA nainstalovat IIS a potřebné komponenty pro endpoint WS.
  Zajistí SZR ve spolupráci s Autocontem.
- Na oba servery CA nainstalovat endpoint WS.
  Zajistí SZR ve spolupráci s Pasante a Autocontem.
- Zajistit síťovou konektivitu mezi Interním modulem RAZR-produkce (RAZR2P-INT) a CA SZR pro testovací prostředí ZR a mezi Interním modulem RAZR-produkce (RAZR2P-INT) a CA SZR pro produkční prostředí ZR.
  Veškerá komunikace mezi RAZR a CA probíhá protokolem HTTPS.
  Mezi RAZR a CA jsou firewally. Na nich musí být povolený prostup z Interního modulu RAZR-produkce na CA na TCP / 443.
  Zajistí SZR.

10. Dopady do provozu / dopady do provozní dokumentace

- Úprava technické a procesní dokumentace - Pasante
- Úprava Příručky RAZR pro SZR – SZR

Služby definované v čl. 3. „Popis zajištění realizace změny“ tohoto PnČ nebudou generovat další dodatečné finanční prostředky na podporu provozu daného IS.

11. Dopady na bezpečnost IS / dopady do bezpečnostní dokumentace

Nemá dopad na bezpečnost IS.

Změny nemají vliv na bezpečnostní dokumentaci.