NAKIT
Národní agentura pro komunikační a informační technologie, s. p.

SPRÁVA ZÁKLADNÍCH REGISTRŮ

Příloha č. 1

Dílčí smlouvy č. 4 k Rámcové dohodě na rozvoj a rozšíření MORIS,

č.j. SZR-1083-58/Ř-2015, 2018/262 NAKIT, uzavřené dne 31. července 2018

Technická specifikace Díla

Mobilní elektronický prostředek (vč. úpravy GG)

1 Úvod

Tato příloha č. 1 (dále také je „dokument“) popisuje zadání pro použití Mobilního klíče ISDS jako dalšího přihlašovacího nástroje pro NIA dle požadavků MV.

Dokument je rozdělen na tři sekce:

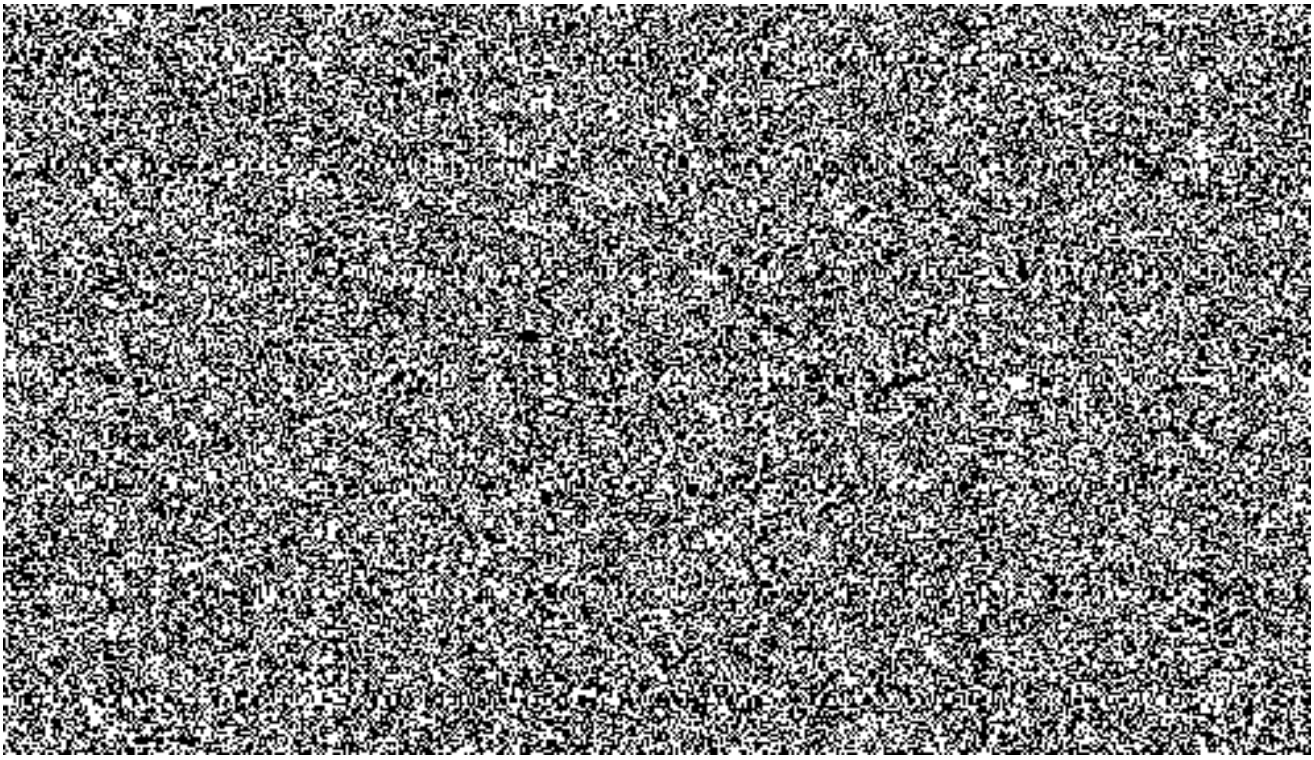
- Popis stávajícího Mobilního klíče a komunikačního rozhraní mezi mobilní aplikací a serverem (kapitoly 3 a 4).
- Popis navrhovaných změn na úrovni business zadání (kapitola 5).
- Technický popis navrhovaných změn (kapitoly 6 až 8).

Tato technická specifikace popisuje celkové řešení Mobilního elektronického prostředku (MEP), součástí dodávky NAKIT nejsou úpravy aplikace Mobilní klíč.

Technická specifikace popisuje obecné principy, po schválení ze strany Zadavatele může dojít k implementačním změnám.

2 Zadání

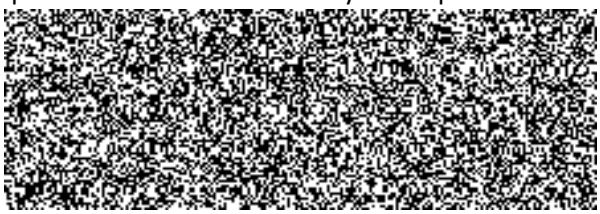
MV požaduje upravit aplikaci Mobilní klíč tak, aby (při zachování stávajícího fungování s identitami ISDS) mohla fungovat také s identitami v NIA, jako nový samostatný IdP. Upravená aplikace by se měla chovat tak, že podle toho, který QR kód (buď ISDS nebo NIA) uživatel oskenuje, s takovým zdrojem identity bude v daném sezení pracovat. V aplikaci Mobilní klíč budou dva nezávislé klíče, dvě nezávislé "identity". Bude umožněn příjem notifikací ze dvou nezávislých kanálů.



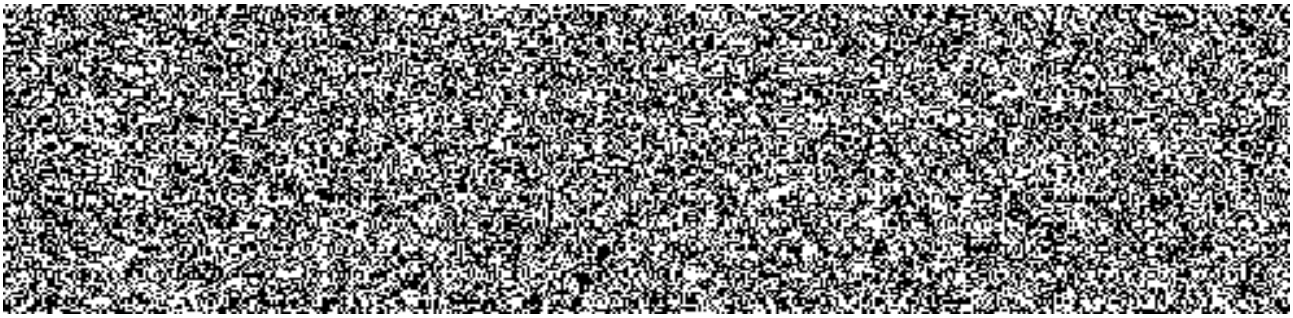
Části zadání:

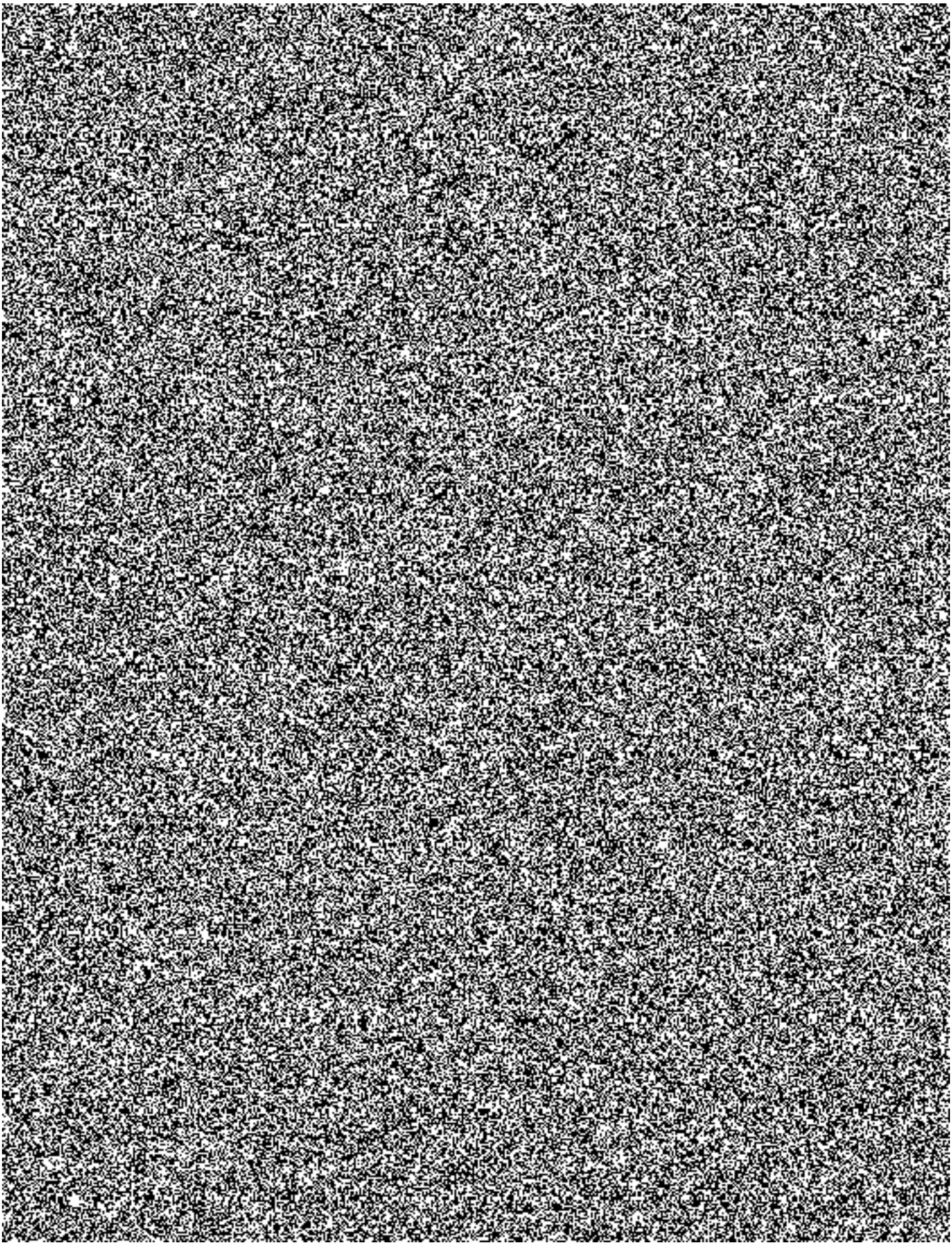
- Realizace IdP „Mobilní klíč eGovernmentu“ (dále MK) zajišťující komunikaci s mobilní aplikací a realizující veškeré procesy spojené s životním cyklem identifikačního prostředku, včetně požadavků zákona 250/2017 Sb. na evidenci prostředků kvalifikovaného správce.
- Realizace backend služeb přístupu kvalifikovaného správce k této evidenci.
- Implementace dalšího elektronického komunikačního kanálu MK
- Implementace mobilního BOK pad založeného na aplikaci MK
- Realizace autorizačního SP pro výdej dat na základě požadavku MK

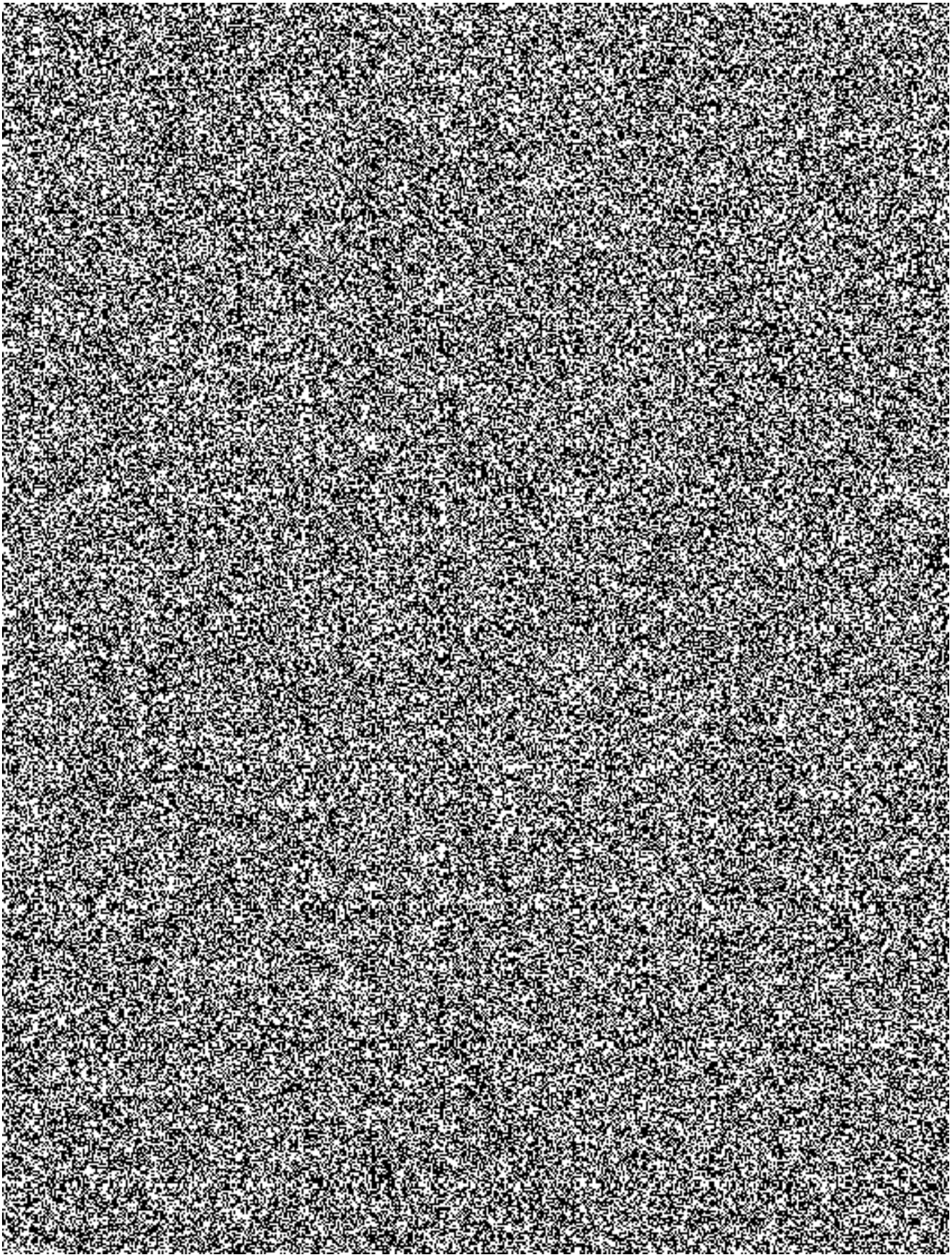
Předpokládá se realizace podle dále uvedených způsobů užití. Jednotlivé části budou vystaveny na separátních adresách chráněných TLS protokolem. Předpokládaná doménová jména:

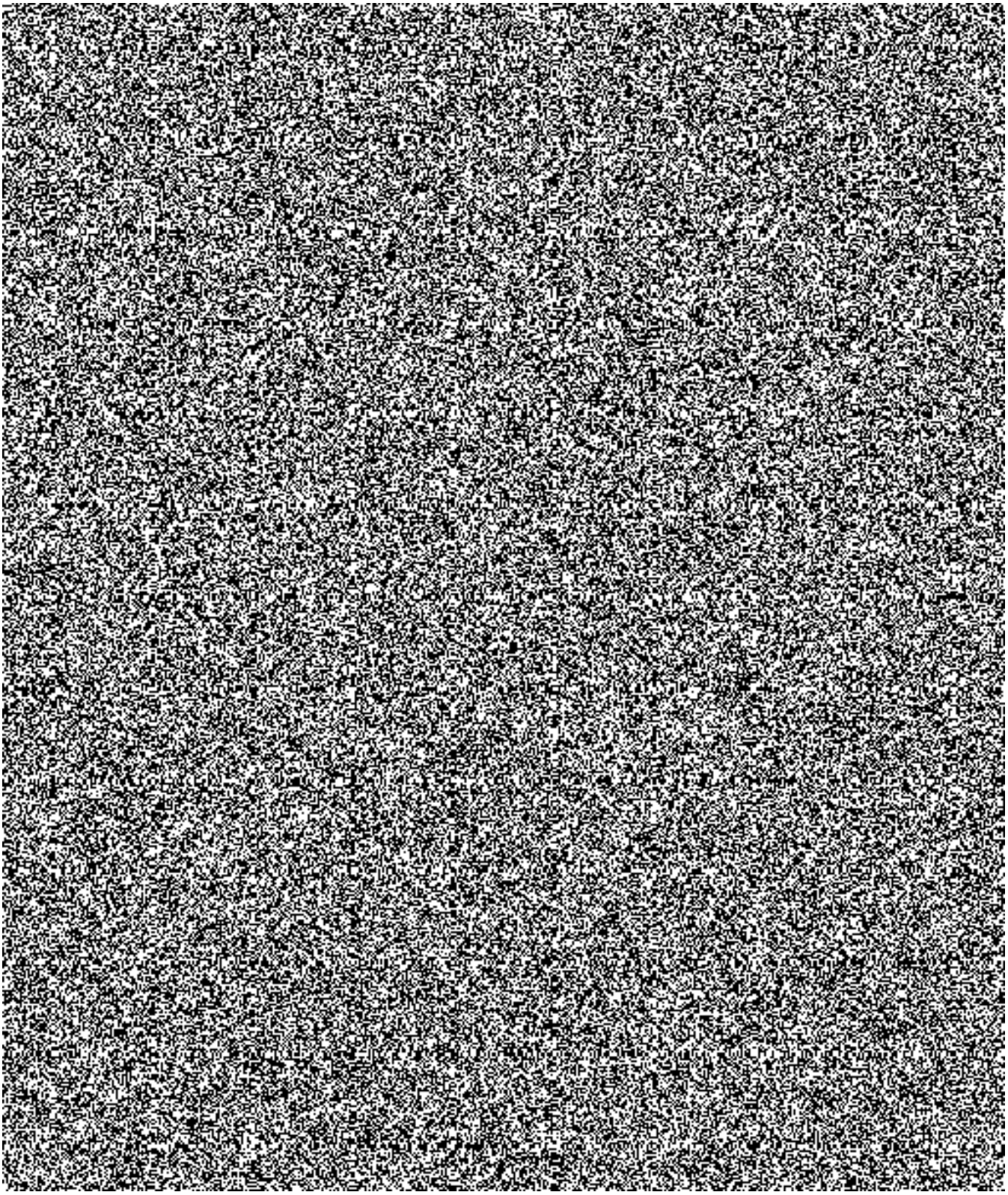


Výše uvedená doménová jména představují odkazy na produkční prostředí. Testovací prostředí bude publikováno na adresách uvozených písmenem „t“ ve třetí úrovni doménového jména (např. tmk.narodnibod.cz).





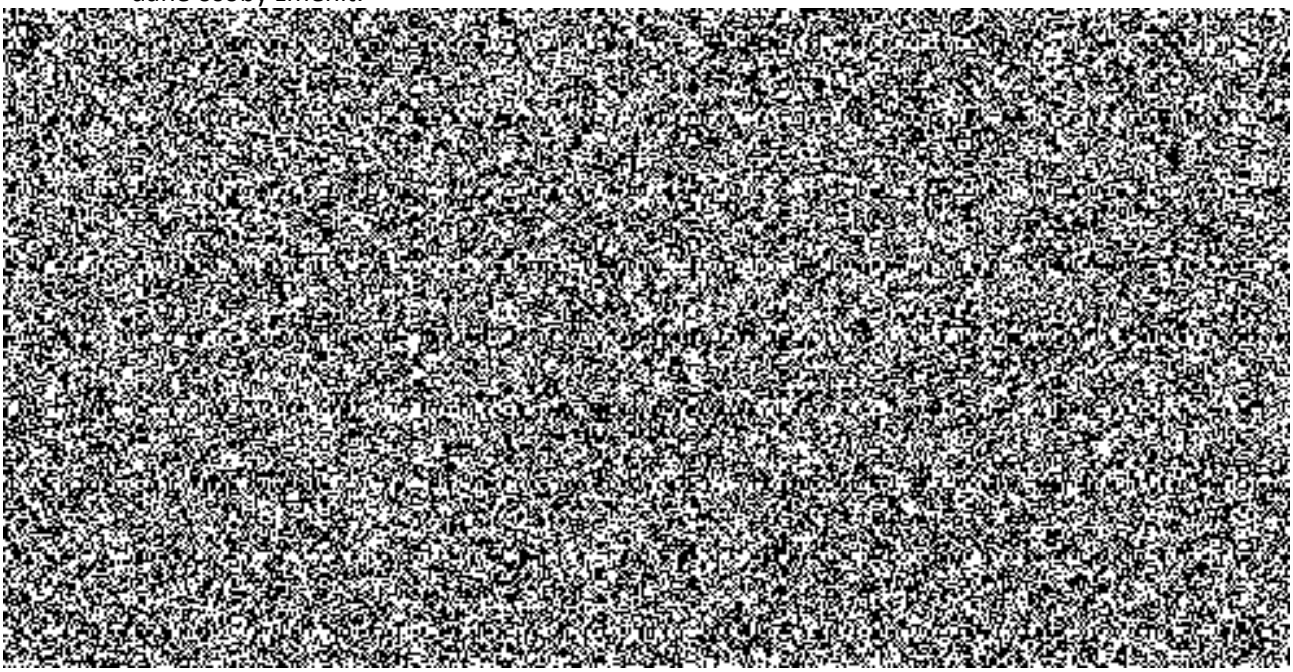




Uživatel na mobilním zařízení se před každou činností s MK musí nejprve do aplikace MK přihlásit. To může udělat dvěma způsoby:

- Heslem - dle volby uživatele buď klasickým textovým heslem, obrázkovým heslem (výběrem sekvence obrázků) nebo číselným PINem. Heslo je k dispozici vždy, uživatel ho nemůže vypnout.

- Biometricky - sejmutím otisku prstu (Android, iOS) nebo potvrzením obličejem (nyní jen iOS - Face ID). Pokud zařízení biometrii umožňuje, uživatel si volí, zda se smí používat, nebo ne. Je tomu tak z toho důvodu, že z některých bezpečnostních hledisek je biometrická autentizace slabší než např. složité heslo, protože používanou charakteristiku (kupř. otisk prstu) nelze u dané osoby změnit.



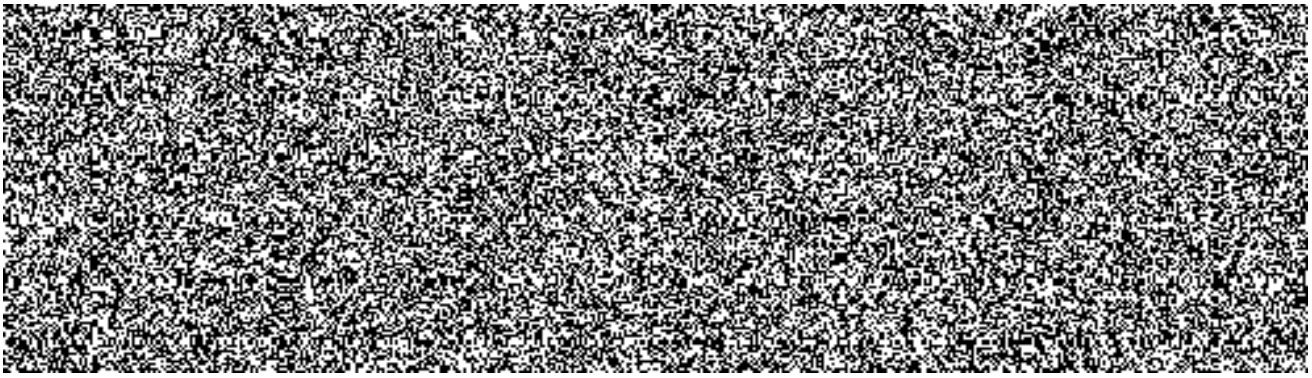
4 Popis komunikace MK (stávající stav)

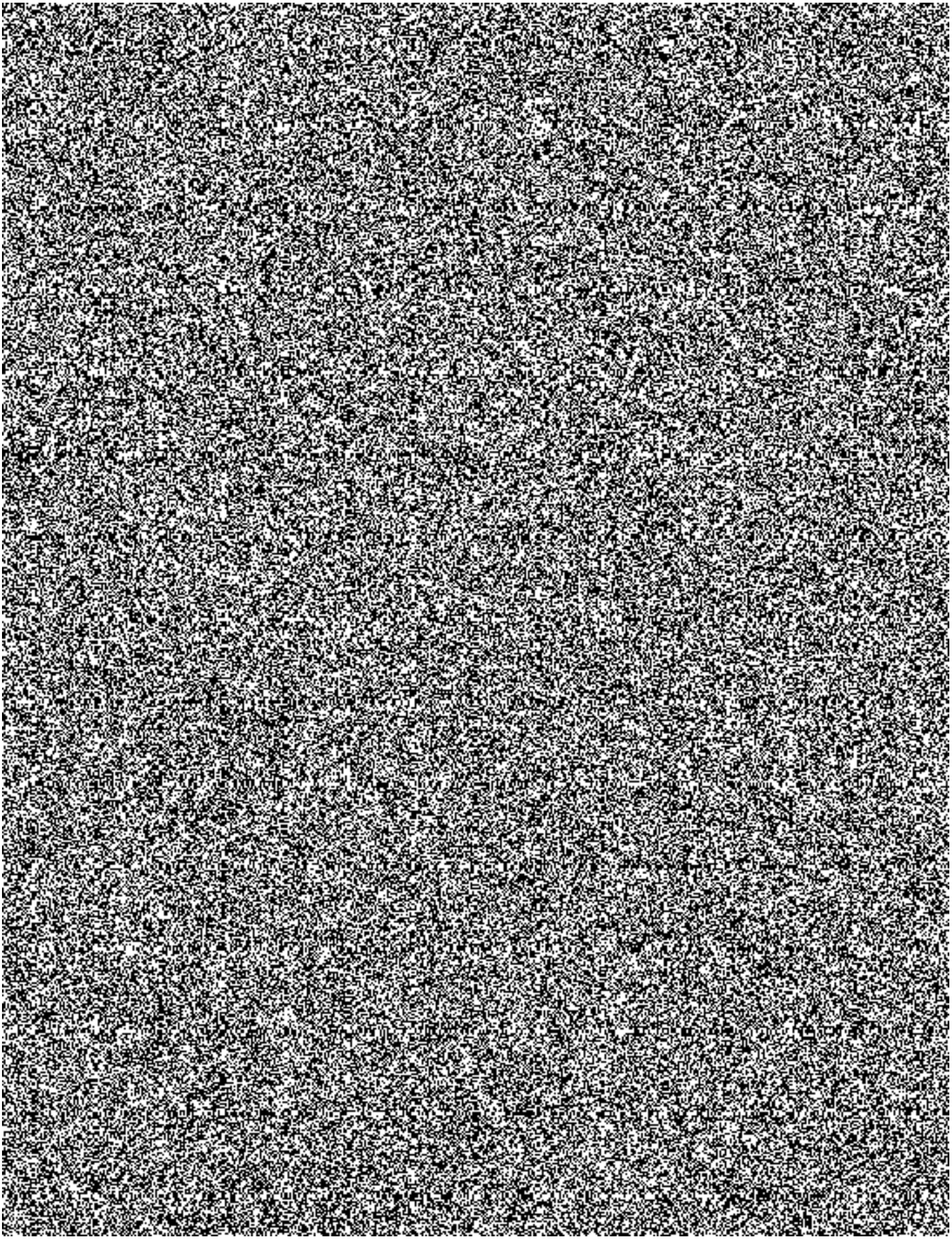
Tato kapitola popisuje aktuální stav komunikace mezi aplikací MK v mobilním zařízení a serverem. Vzhledem k tomu, že některé kroky zpracování jsou odvozené od reprezentace dat na straně serveru, je zde popsána i tato reprezentace.

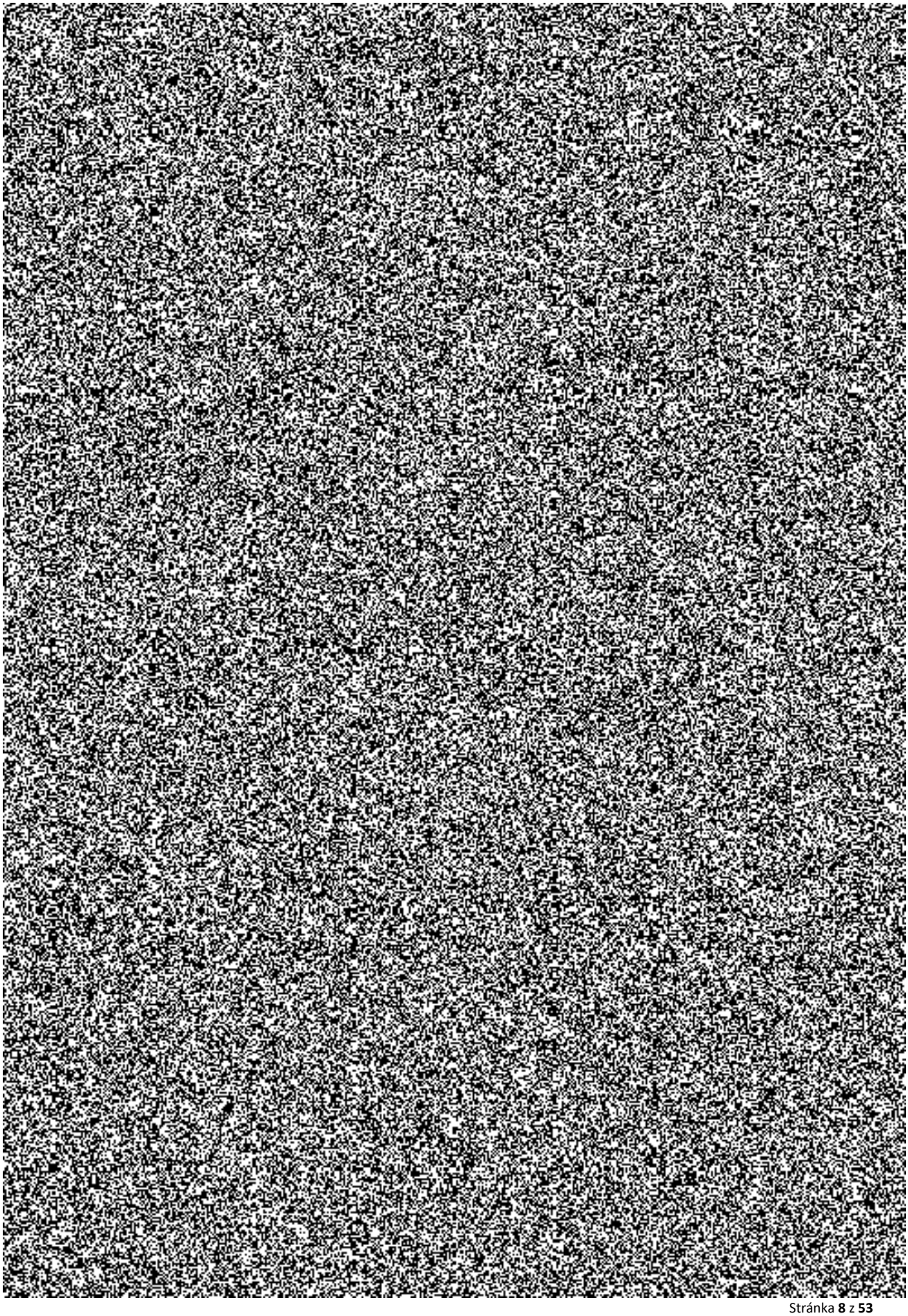
4.1 Popis komunikačních kanálů

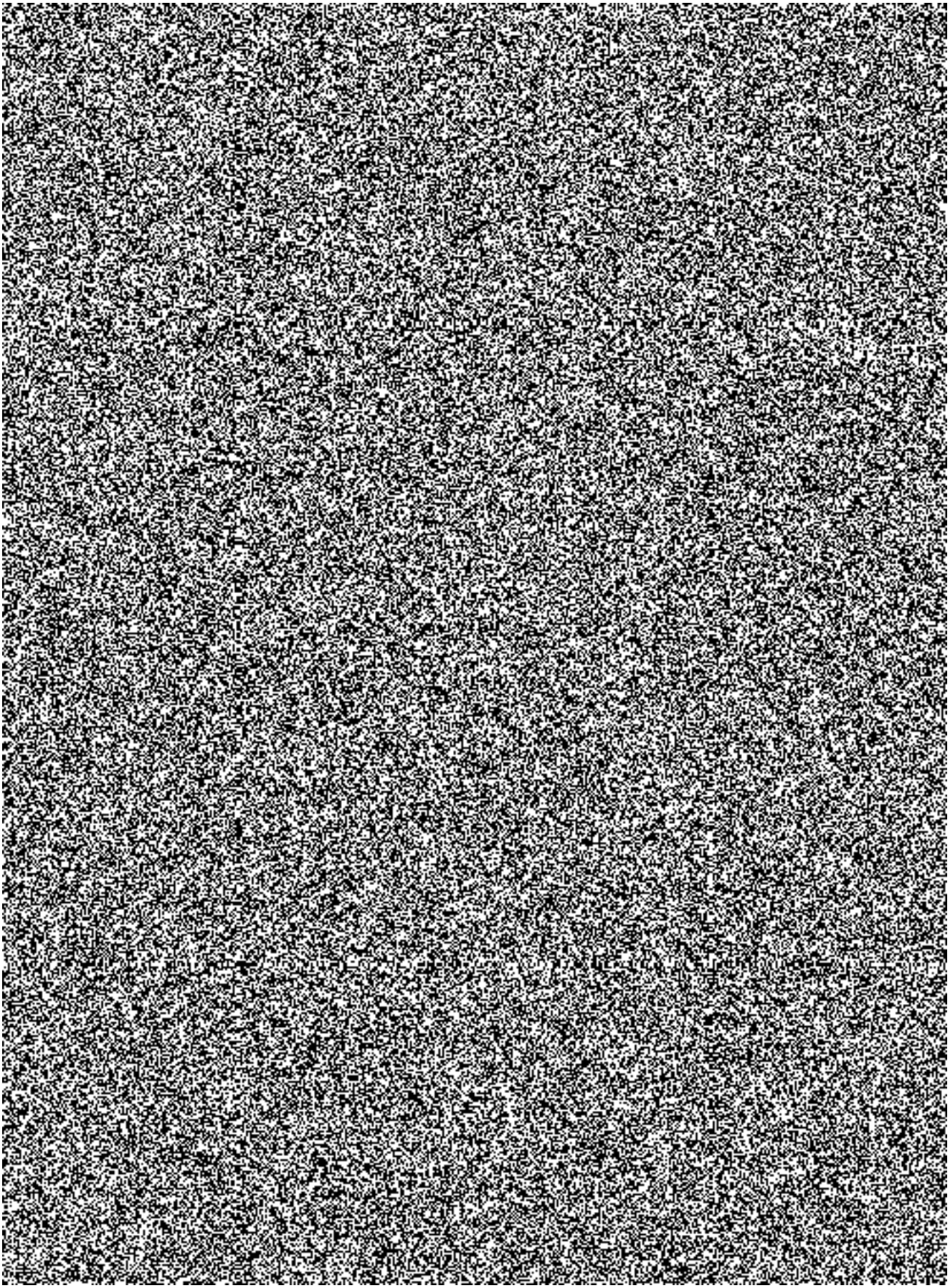
MK má následující komunikační kanály:

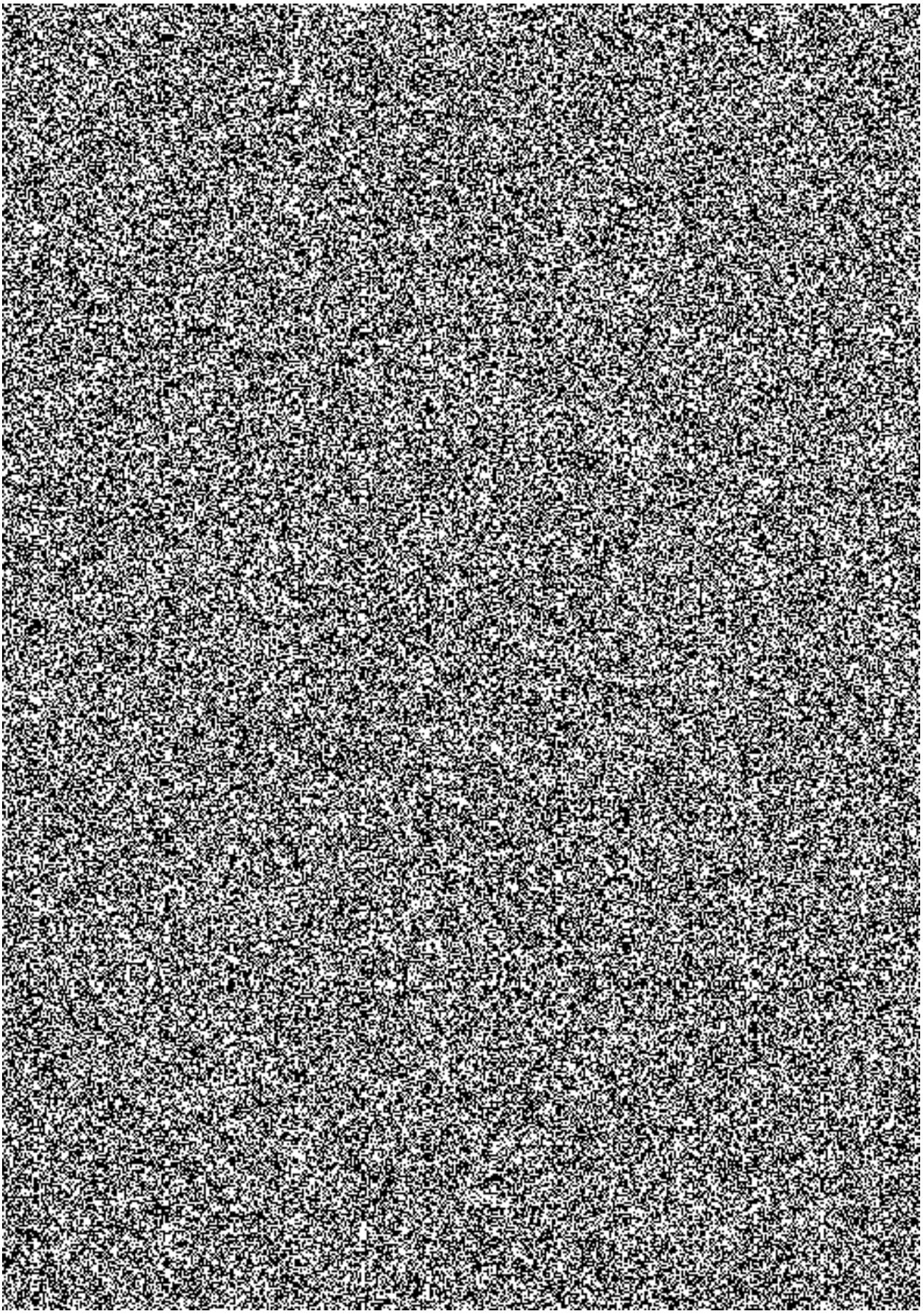
1. Příjem přihlašovacího/párovacího kódu, který má potvrdit - sejmutím QR kódu pomocí fotoaparátu, nebo spuštěním odkazu ve tvaru isds://* na mobilním zařízení. Detailněji: [4.7]
2. Push notifikace zasílané přes Google Firebase Messaging. Push notifikace neobsahuje vlastní payload, ale jen informaci o tom, že si MK má stáhnout notifikace ze serveru. Detailněji: [4.8]
3. HTTPS rozhraní pro komunikaci z MK na server ISDS, pomocí kterého MK předává šifrované požadavky na server a čte šifrované odpovědi. Detailněji: [4.2]

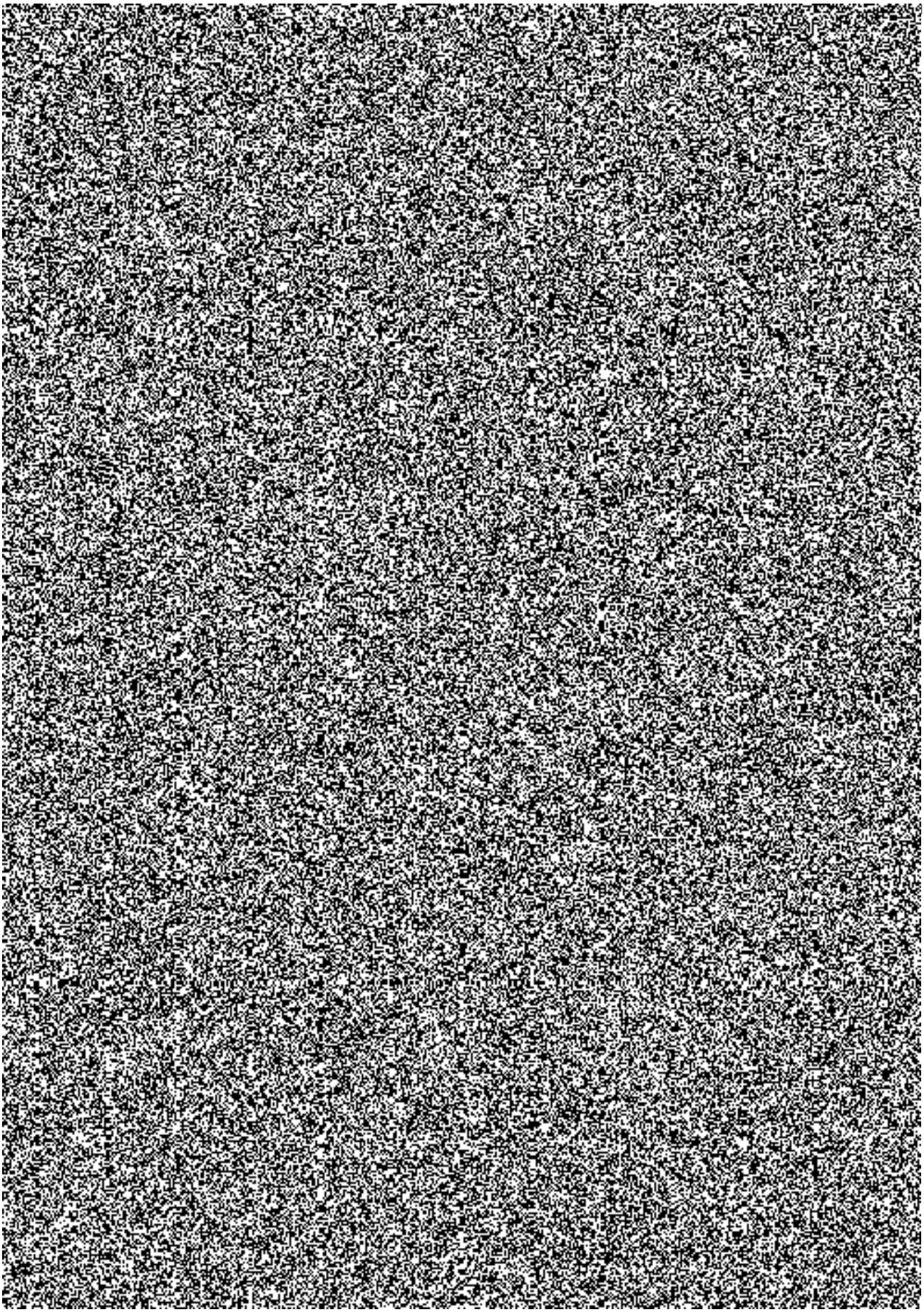


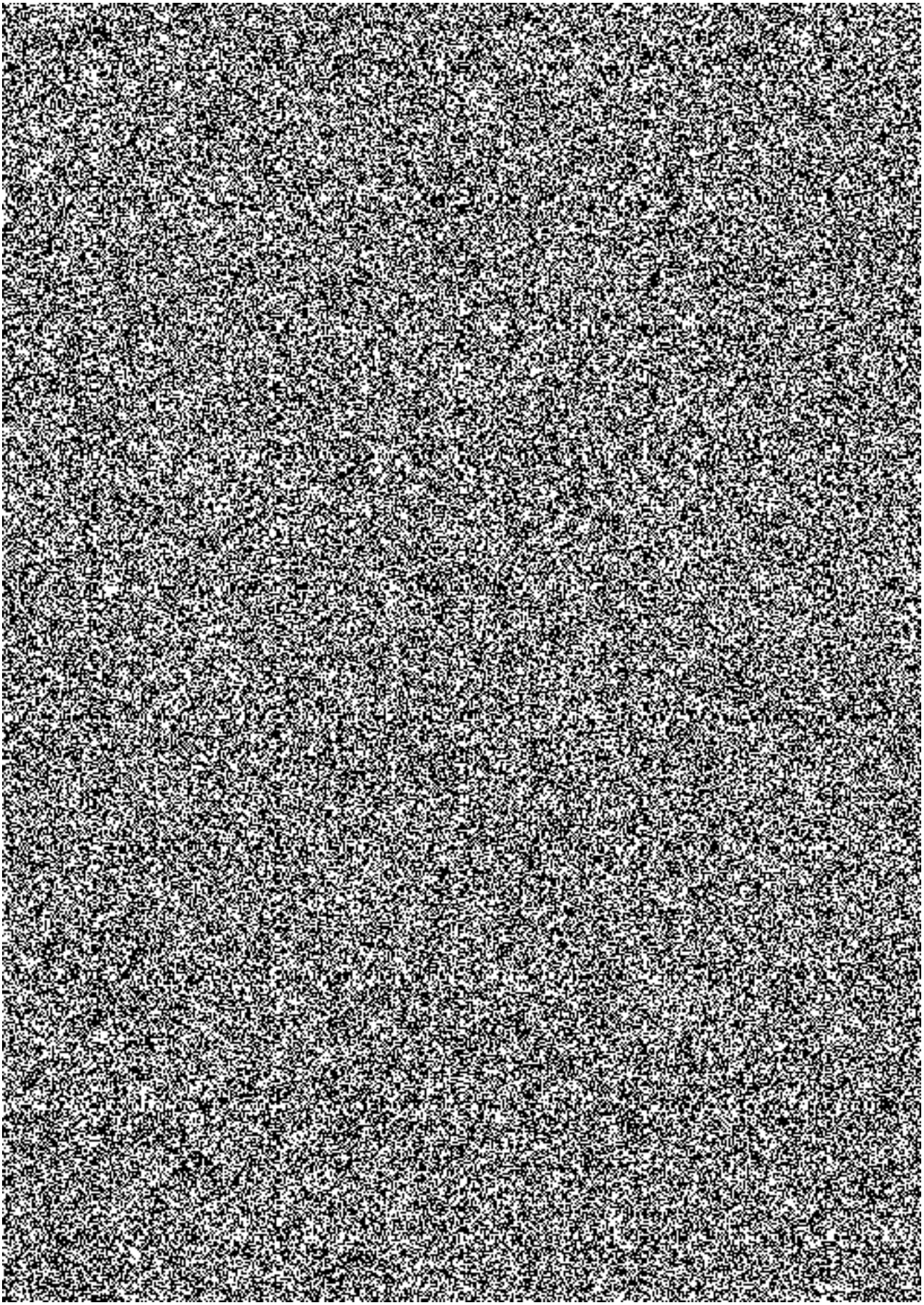


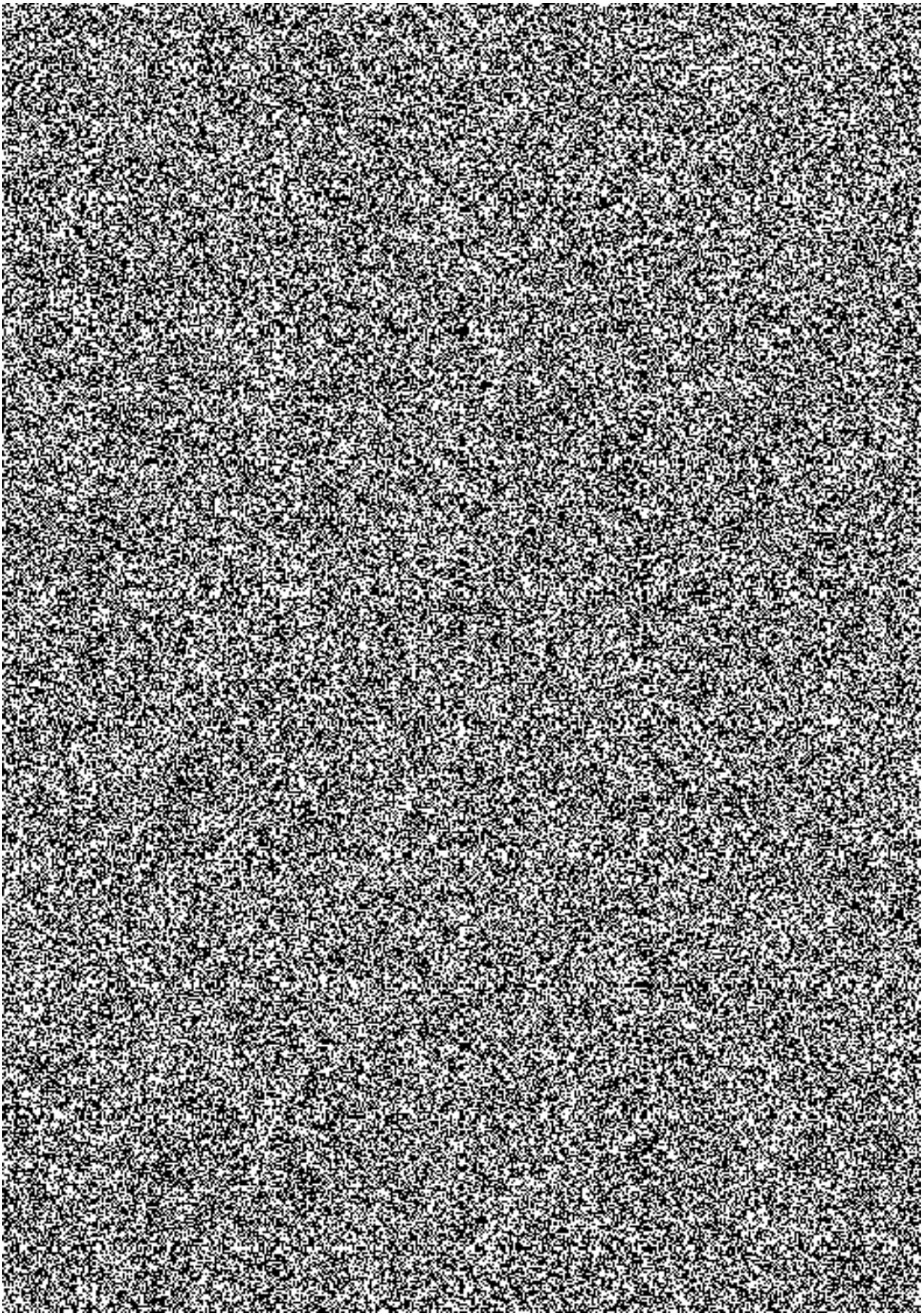


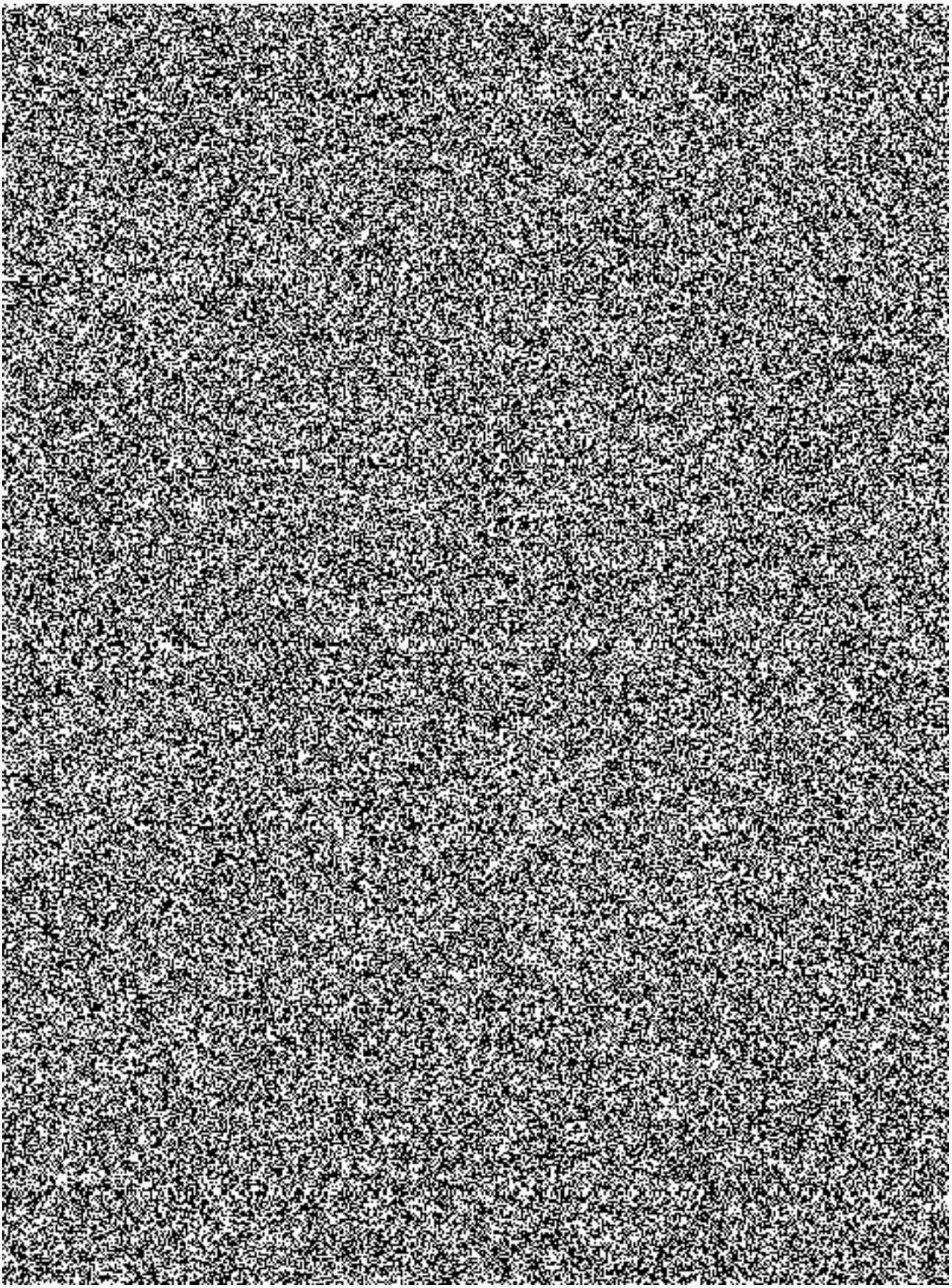


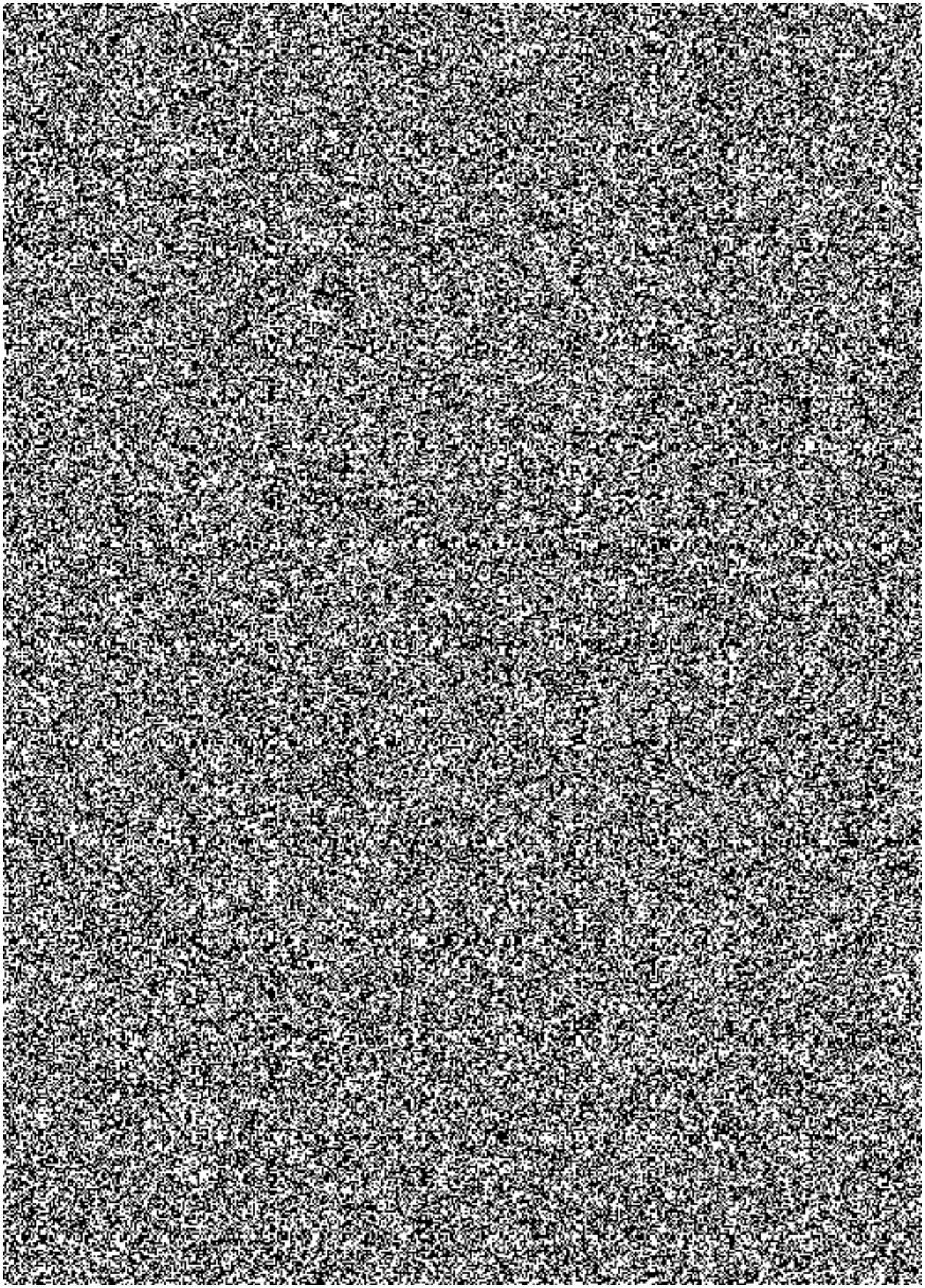


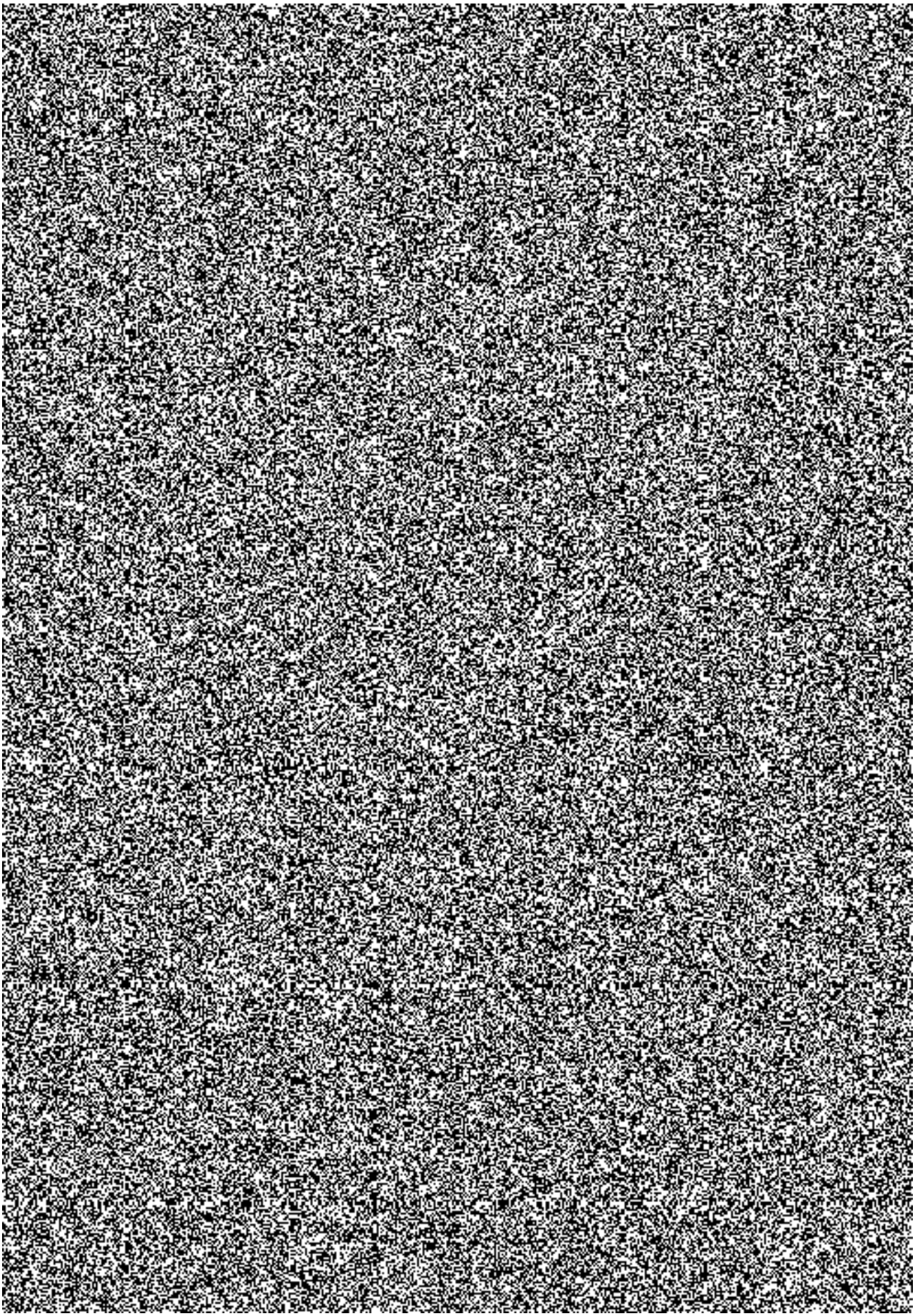


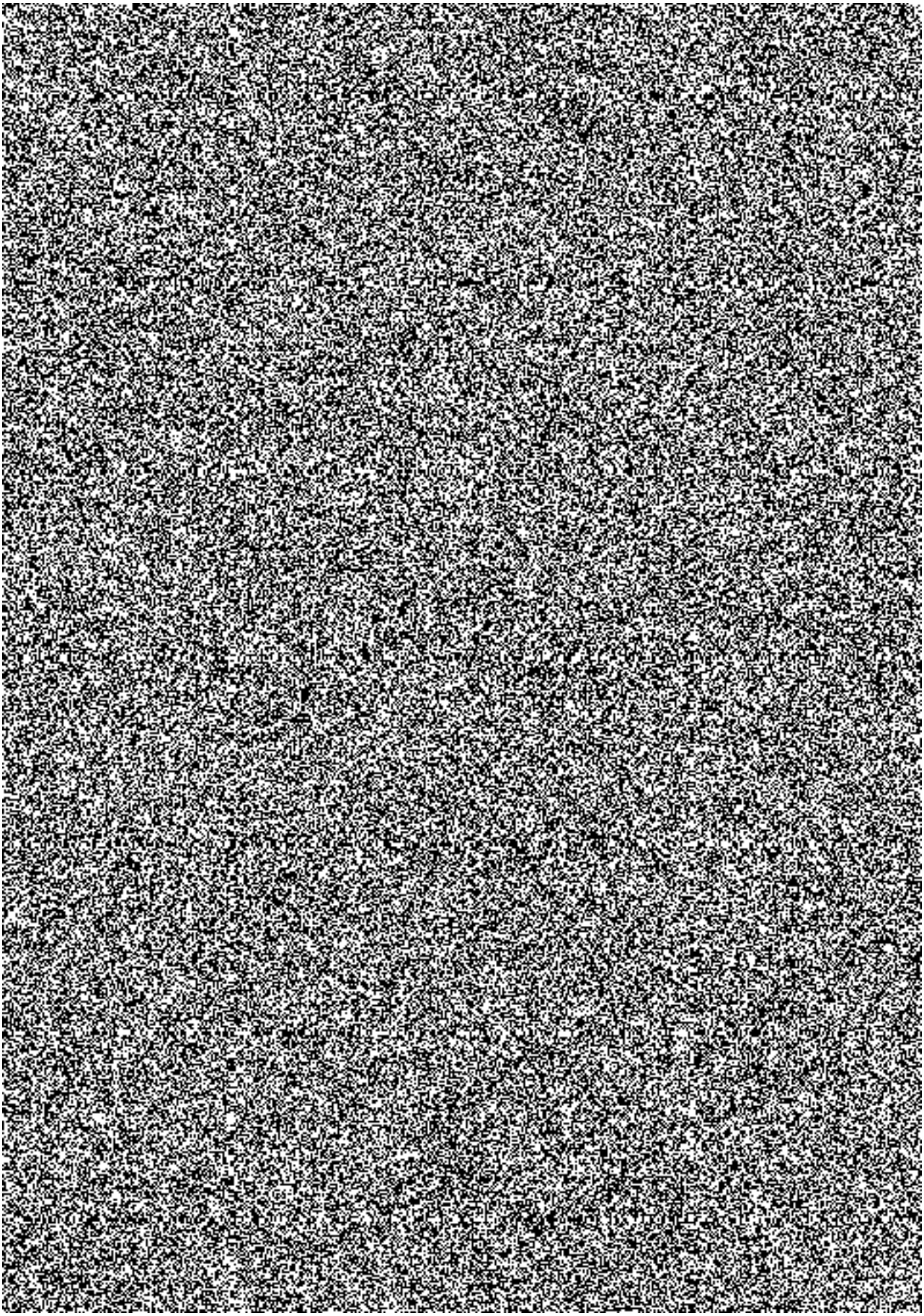


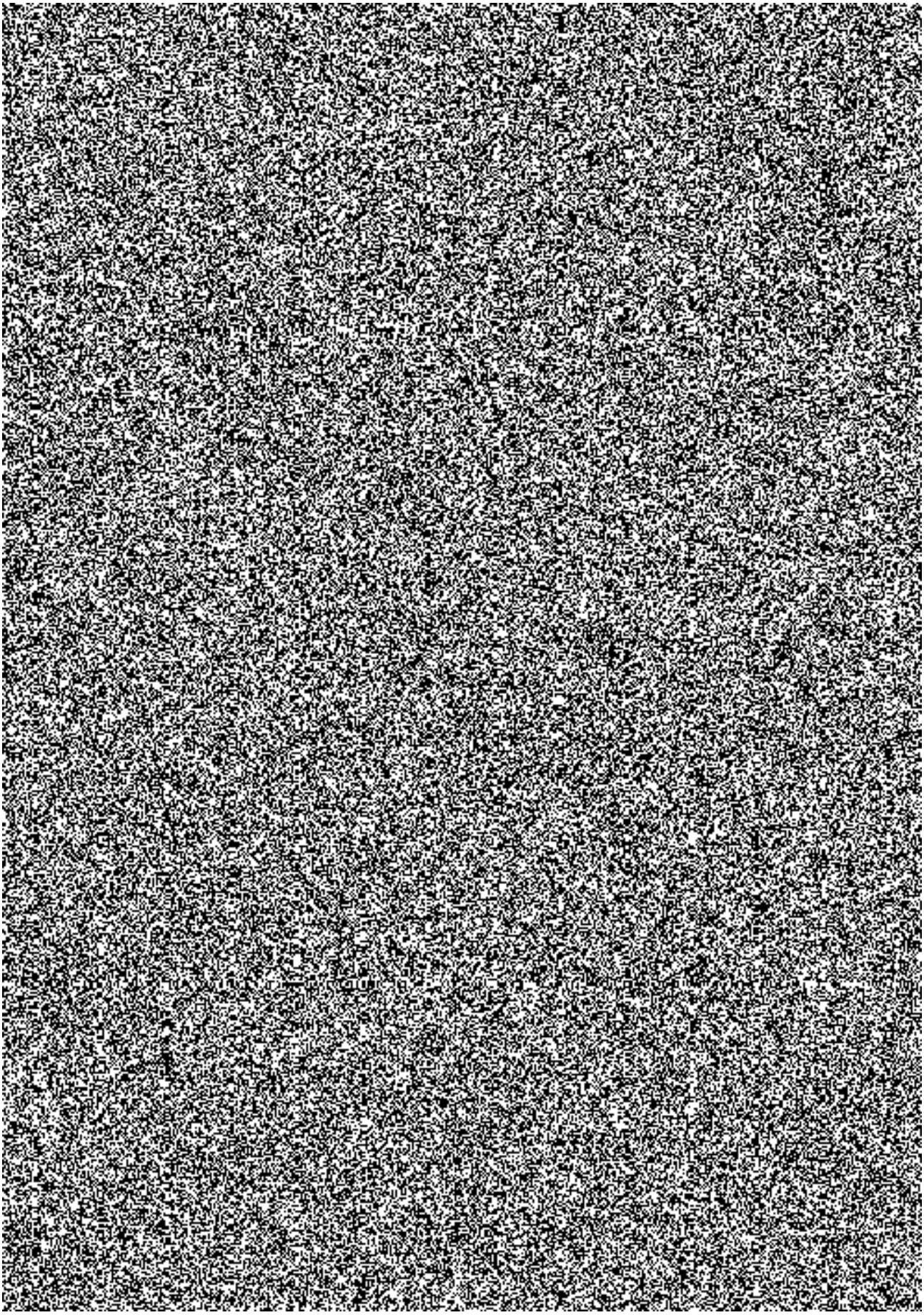


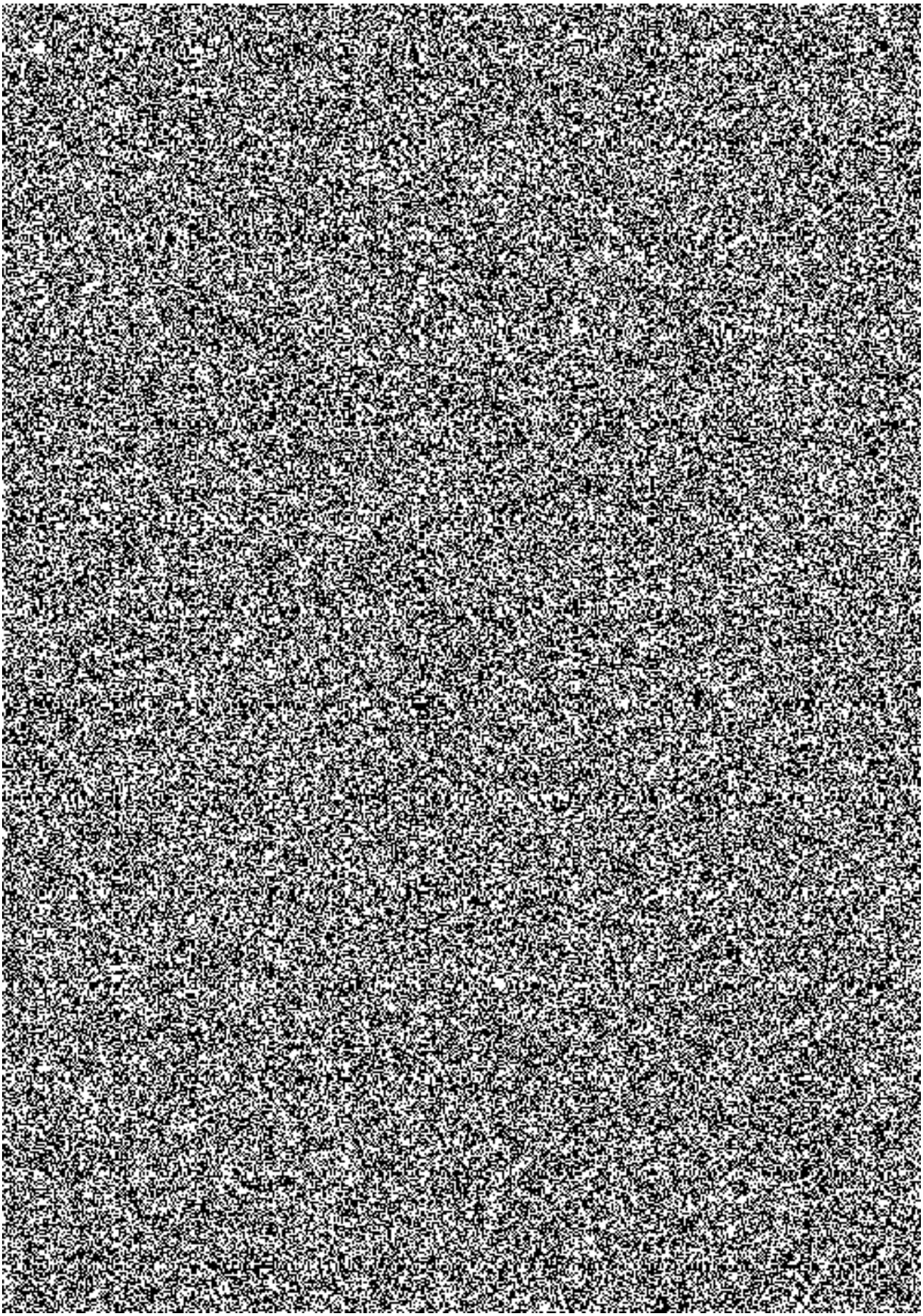


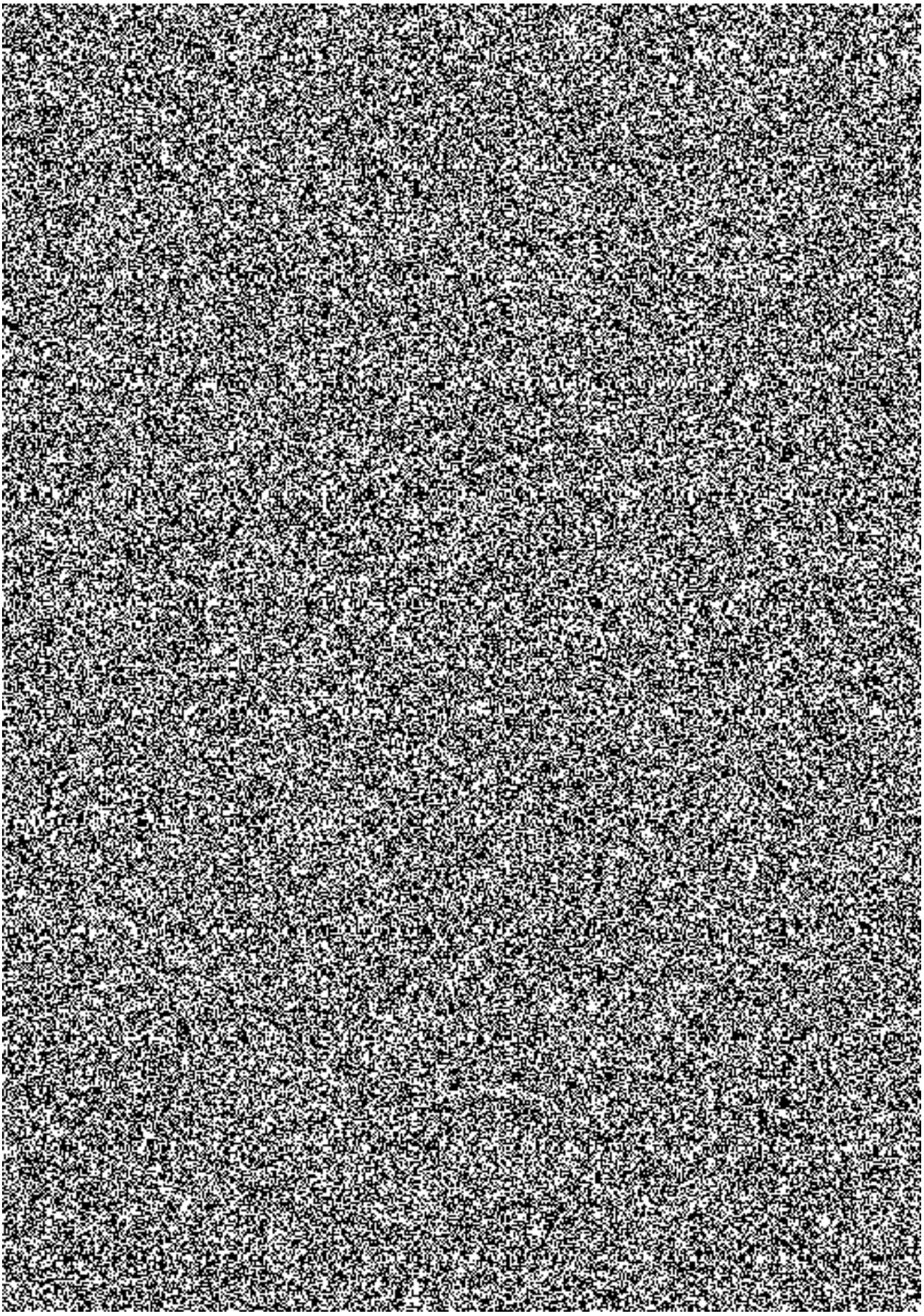


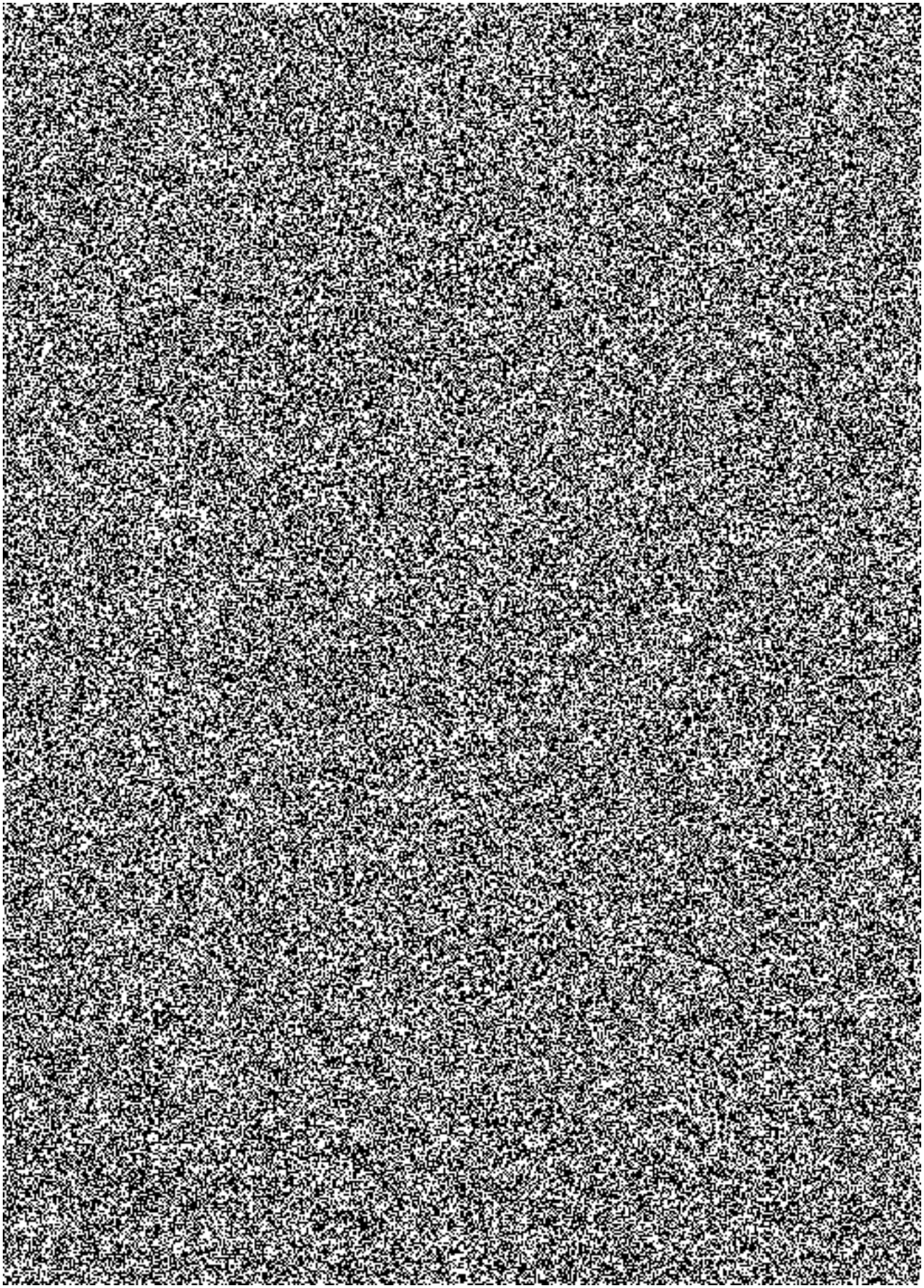


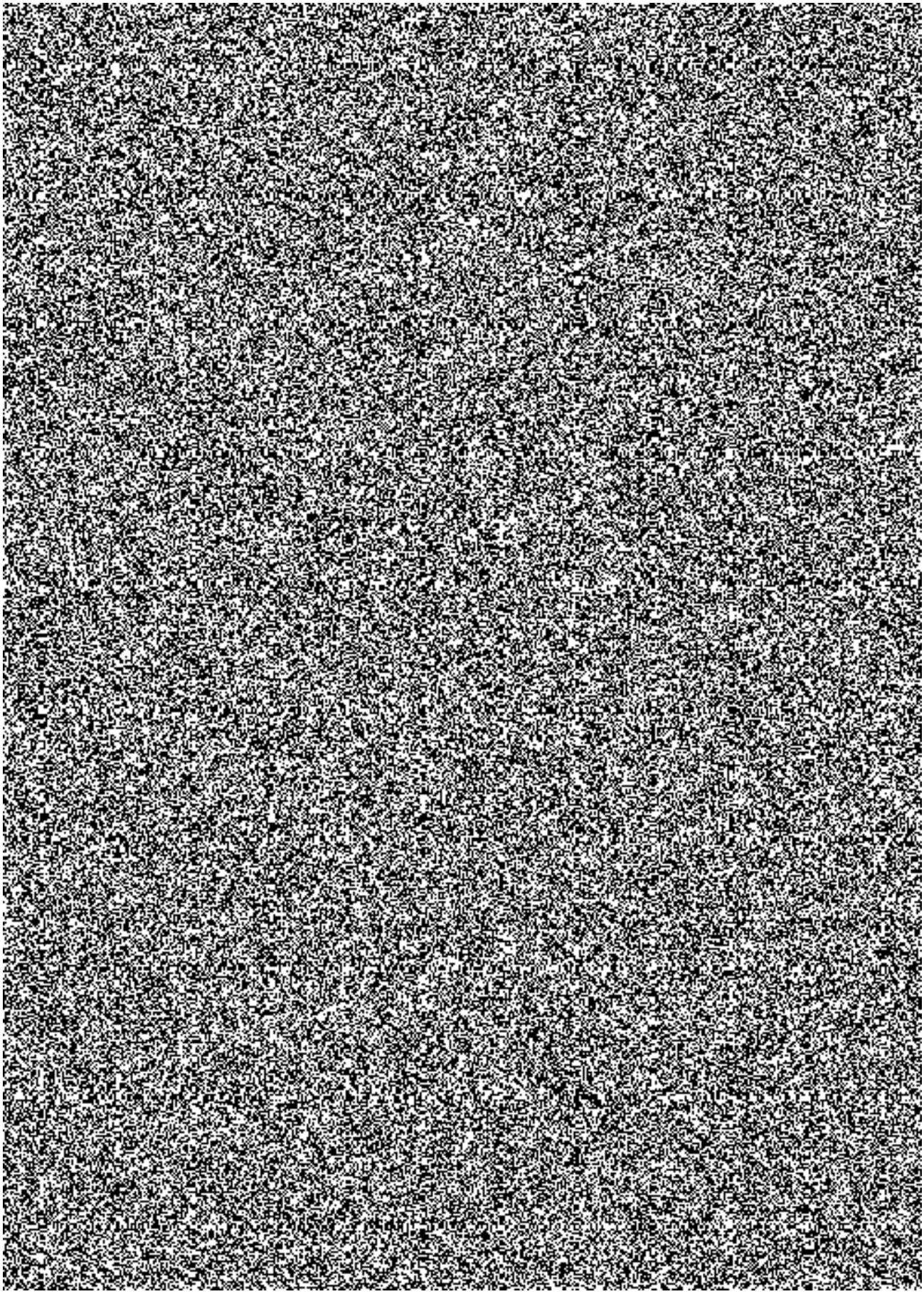


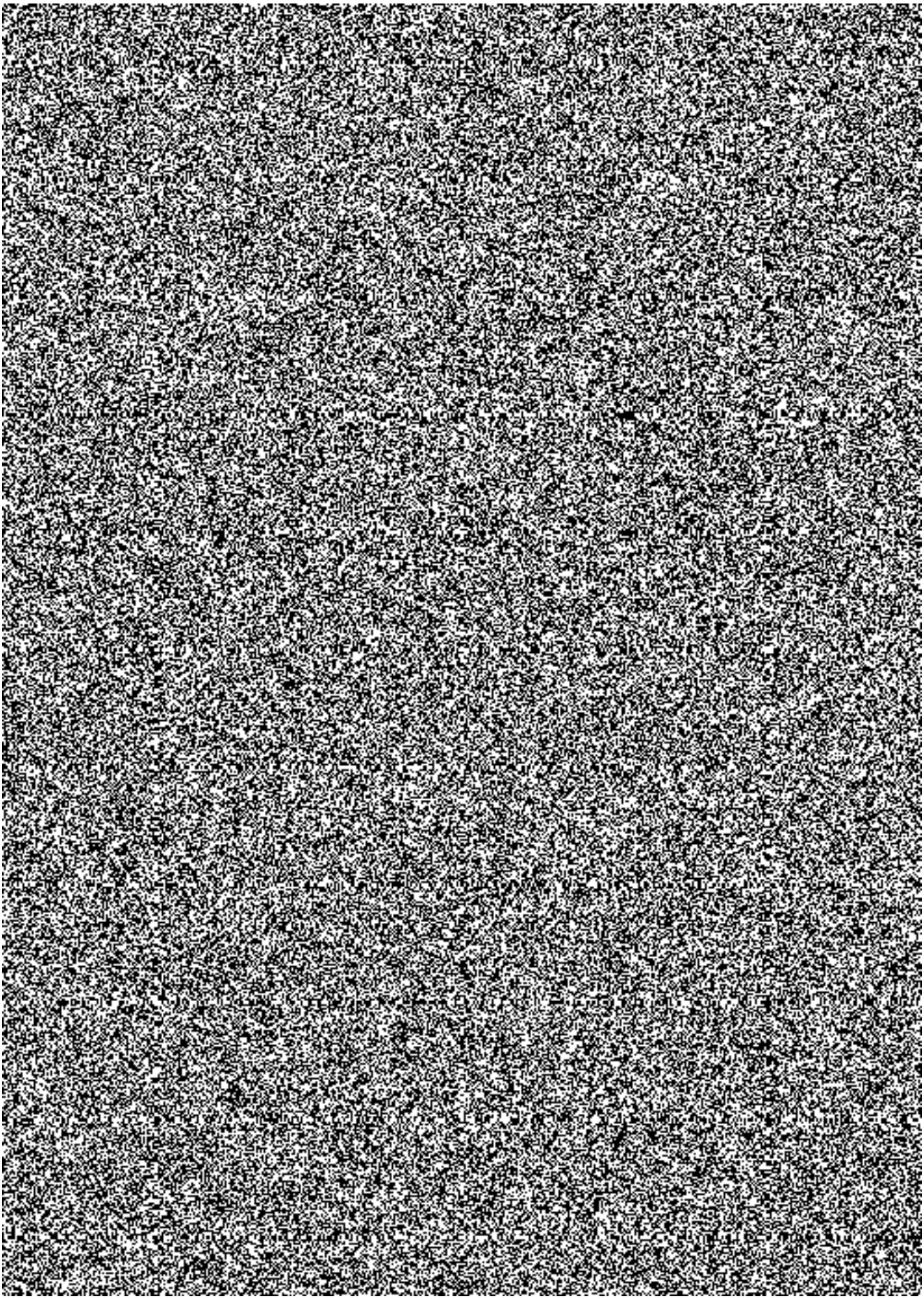


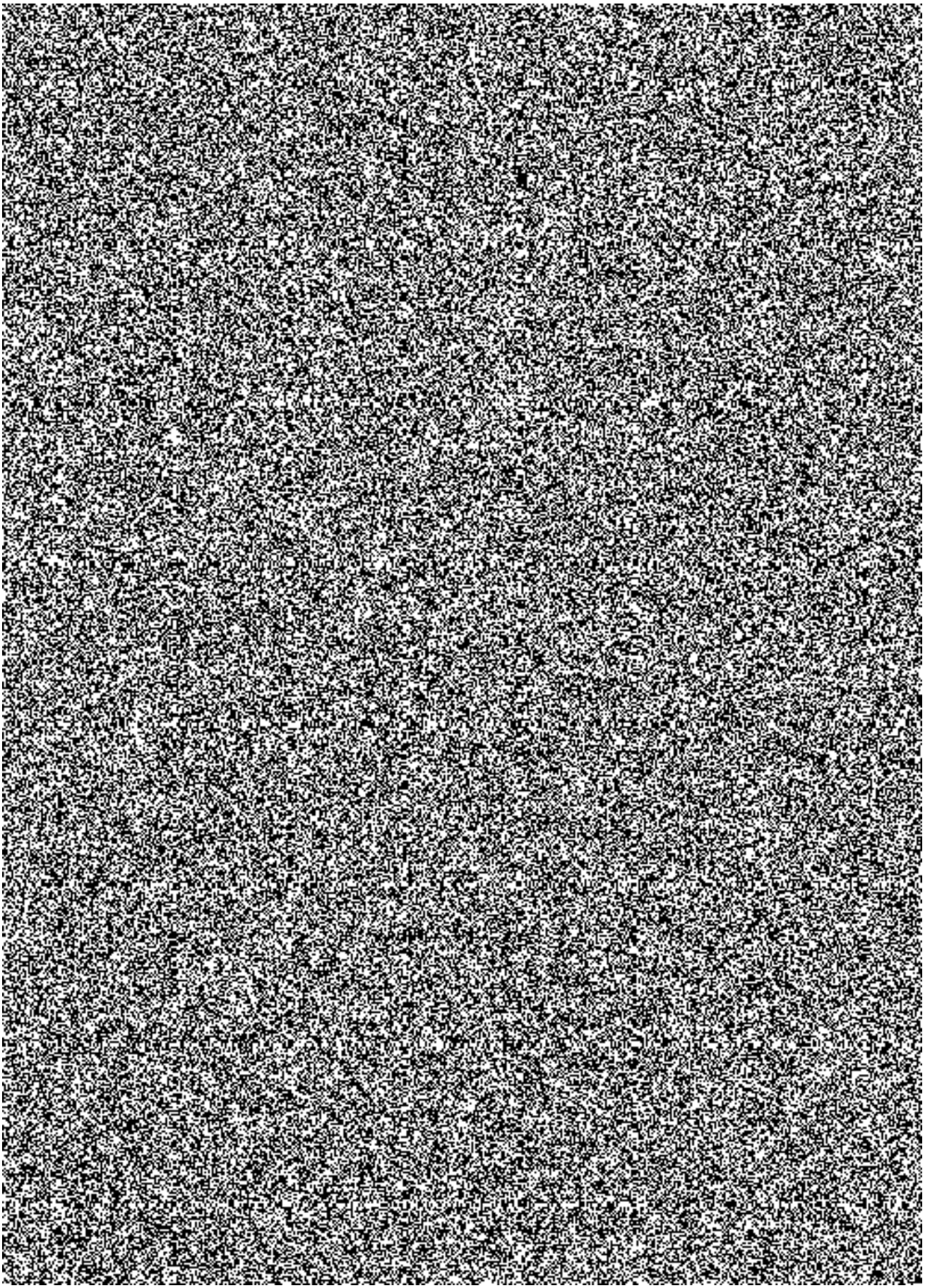


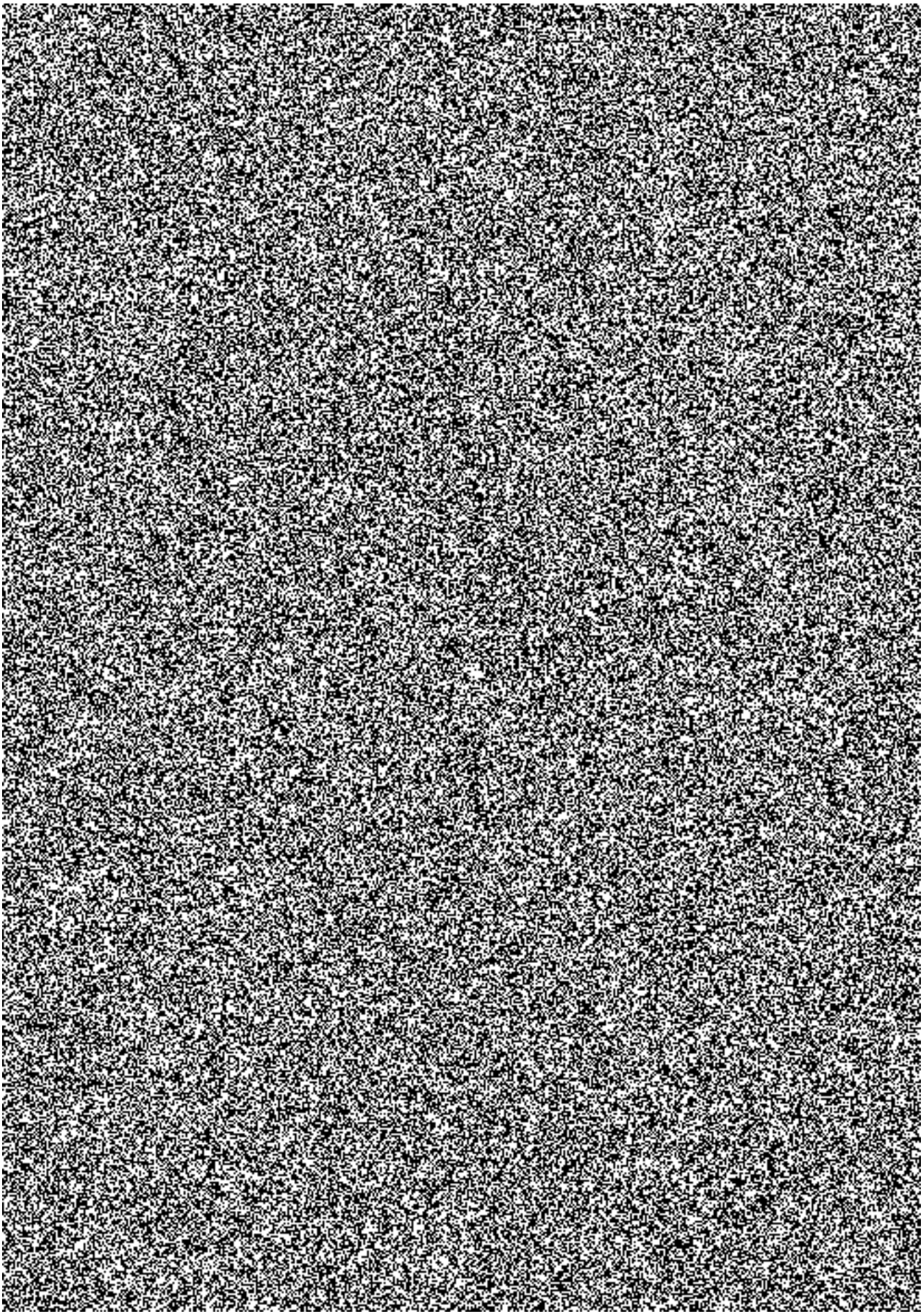


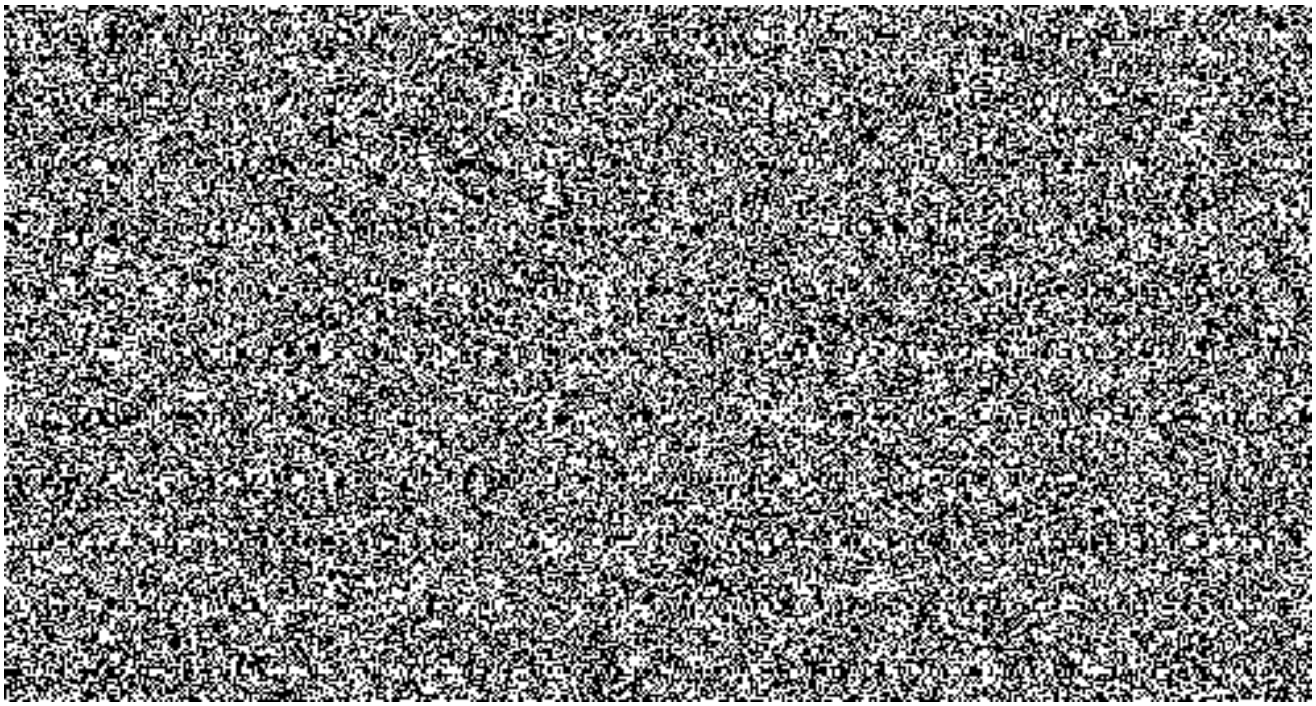












5 Návrh řešení jednotlivých případů užití

5.1 Případ užití 1: Připojení k existující identitě NIA

Zadání: Uživateli, který má již zřízen účet NIA a přihlašuje se do něj některou jinou cestou, umožnit přihlašování Mobilním klíčem.

Scénář použití:

1. Uživatel má identitu NIA a je přihlášen na webový portál NIA.
2. Zvolí připojení Mobilního klíče, je mu zobrazena stránka s informacemi, odkazem ke stažení aplikace a QR kódem pro párování.
3. Uživatel v MK načte párovací kód a provede párování.

5.2 Případ užití 2: Přenos identity z ISDS do NIA

Zadání: Uživatel nemá účet NIA. Má ztotožněný uživatelský účet v ISDS a cílem je umožnit mu jednoduše si založit účet v NIA na základě jeho identity v ISDS, a připojit k tomuto účtu Mobilní klíč.

NIA již v tento okamžik má k dispozici proces pro založení identifikačního prostředku jméno-heslo-SMS, kde po založení prostředku může uživatel ověřit svou identitu buď návštěvou kontaktního místa CzechPOINT, přihlášením jiným identifikačním prostředkem, nebo ověření přihlášením pomocí datové schránky fyzické osoby (Autentizační službou ISDS).

Pro přenos identity uživatele do NIA a založení MK v NIA je navrženo použít velmi podobný proces za použití upravené Autentizační služby ISDS služby (rozšířené dle projektu TS782). Takto upravená autentizační služba vrací AIFO ticket („šatní lístek“) a je tedy možno načíst ztotožnění uživatele ISDS ze základních registrů.

Scénář použití:

1. Pro všechny ztotožněné uživatele ISDS (bez ohledu na to, zda jsou v roli osoby oprávněné, pověřené, administrátora atd.) ve všech typech schránek, vznikne v Nastavení datové schránky

v sekci Informace o schránce nová volba Identita NIA s informacemi a tlačítkem pro založení identity v NIA.

2. Po stisku tlačítka bude uživatel přesměrován na novou stránku NIA pro založení identity MEP z ISDS. Tato stránka jen zaregistruje požadavek na Autentizační službu ISDS a uživatele hned přesměruje na bránu ISDS. Uživatel se nebude muset do Autentizační služby znovu přihlašovat, protože ještě bude platit jeho relace z KP ISDS. Z pohledu uživatele se tedy po stisknutí tlačítka v Nastavení KP ISDS (bod 1) rovnou zobrazí dialog pro potvrzení předání osobních údajů z Datových schránek do NIA.
3. NIA tak získá ztotožnění uživatele a může mu založit identitu. Následně mu zobrazí párovací QR kód pro připojení mobilního klíče nebo možnost založení přihlašovacího prostředku jméno-heslo-SMS. Připojení mobilního klíče probíhá standardní cestou podle případu užití 1.

Poznámky:

- Předání identity nevyžaduje, aby měl uživatel na straně ISDS aktivní MK. Stejně tak nevynucuje aktivaci MK na straně NIA - principiálně si uživatel v NIA může zřídit přihlašovací prostředek jméno-heslo-SMS, pokud mu to NIA nabídne.
- Pro takto navržený proces není nutné vytvářet nová specifická rozhraní mezi ISDS a NIA. NIA využije standardní rozhraní, které ISDS již bude mít (Autentizační služba rozšířená podle TS782 pro použití GFŘ a ČSSZ). Úpravy na straně ISDS se tím omezují na jednu informační stránku v Nastavení s tlačítkem pro přesměrování na portál NIA.

5.3 Případ užití 3: Založení NIA identity a připojení MK

Zadání: Uživatel nemá účet v NIA ani v ISDS. Chce získat identitu v NIA s Mobilním klíčem. Obecně může i existovat stav, kdy uživatel má identitu buď v NIA nebo v ISDS, obecně tomu nejde nijak zabránit, aby si nepřihlášený uživatel požádal o připojení mobilního prostředku bez přihlášení.

MK bude možné založit stejným způsobem, jako je nyní zakládán účet UPS.

Scénář dále předpokládá založení prostředku nově, bez nutnosti „domácí přípravy“.

Uživatel si kdykoli stáhne aplikaci MK na své zařízení. Na tomto zařízení provede aktivaci aplikace, tedy zadání svého kódu do aplikace. Zde zvolí volbu „Vytvoření identity v národním bodu“. MK na pozadí provede komunikaci s národním bodem, vytvoří si komunikační klíče a předá do IdP MEP identitu zařízení (je to podobné jako když si uživatel vytváří prostředek Jméno, Heslo, SMS, pouze nezadává nic přes klávesnici a veškerá komunikace probíhá na pozadí aplikace MK. Výsledkem je neaktivovaný profil, kterým je možné se přihlásit pouze do portálu národního bodu, kde uživatel dostává informace o tom, jak dále pokračovat v aktivaci prostředku. Po aktivaci prostředku je identita zařízení spojena s identitou profilu a identitou v ZR. Profil se tak stává buď aktivním, nebo se prostředek připojí k již existujícímu ztotožněnému identifikačnímu profilu a původní dočasný neaktivní profil je označen ke zrušení.

Protože aplikace komunikuje na otevřeném rozhraní internetu musí být toto rozhraní ochráněno proti přetížení, kdy útoční se snaží nekonečně vytvářet prázdné profily.

5.4 Případ užití 4: Doručení notifikací s obecným textem

Zadání: Uživateli, který má v NIA účet s Mobilním klíčem, doručovat na MK notifikace z centrálního notifikačního systému - např. upozornění na vypršení platnosti jeho dokladů.

Změny aplikace MK:

- Nelze zaslat notifikaci jako obecný text. Nepočítáme s tím ani v dohledné budoucnosti, protože by to bylo spojeno s řadou bezpečnostních slabin, kterým zatím služby platforem dostatečně nečelí. Vždy se zasílá pouze kód typu zprávy a vkládací pole, která se v MK vloží do šablony (aby bylo možno aplikaci volně lokalizovat) - viz 4.5.4.1. Pro účely centrálního notifikačního řešení tak vznikne nový typ notifikace, který nebude obsahovat žádný text v šabloně a bude mít jen jedno vkládací pole - celý text, který bude uživateli zobrazen.
- V nastavení aplikace MK bude přidán odkaz na webové stránky nastavení notifikací v NIA (pokud má uživatel připojenu identitu NIA).
- V Nastavení aplikace MK pro Android vznikne nová volba, zda má být pro tento typ notifikací zobrazováno upozornění v notifikačním centru operačního systému.

5.5 Případ užití 5: Použití MK jako BOK-pad při prezenčním ověřování totožnosti

Zadání: Uživatel, který má účet v NIA s Mobilním klíčem, získá možnost využít Mobilní klíč jako BOK-pad, tj. nástroj pro zadání BOK při prezenčním ověřování totožnosti.

BOK je „bezpečnostní osobní kód“ a občan ČR si ho dle stávajícího zákona 328/1999 o OP definuje při žádosti o občanský průkaz. Není technicky uložen na nosiči OP, je zapsán v základních registrech. Nově je v návrhu nového zákona, který je v říjnu 2019 v meziresortním připomínkovém řízení, předpokládáno, že BOK bude v pozici nepovinného bezpečnostního kódu. Občan si jej bude moci nastavit buď při vyzvednutí OP na ohlašovně (ORP) anebo sám v Portálu občana po elektronické identifikaci (předpokládáme, že s úrovní záruky „vysoká“). BOK bude i nadále uložen ROB a to v jednosměrně zašifrované podobě (solený HASH).

(Poznámka: Mechanismus prvotního zadání BOK za stavu, kdy ještě nebyl zadán, bude upřesněn později.)

BOK je v nejjednodušší variantě definován jako kód, kterým si uživatel bude moci provést nahlášení ztráty OP za účelem jeho jednorázového zneplatnění.

Složitější varianta předpokládá, že občan si bude moci nastavit na Portálu Občana speciální příznak v ROB „chci, aby po mně byl BOK vyžadován v agendách při prezenčním prokazování totožnosti“. Pro tento účel je potřeba BOK-pad ve smyslu zařízení, kam občan bude BOK moci zadávat. Protože úřady nechtějí investovat do drahých HW zařízení typu bankovní terminály, je BOK-pad ve formě aplikace v mobilním telefonu klienta pro MV ekonomicky ideálním východiskem.

Mobilní klíč se tedy stane BOK-padem pouze pro svého, identifikovaného držitele. Nicméně, mezi použitím BOK-pad terminálu versus použitím MK jako náhrady BOK-pad terminálu existuje podstatný bezpečnostní rozdíl. Při zadávání BOK do HW terminálu by úředník ověřující autorizaci uživatele reálně viděl, jak tento s terminálem pracuje (HW terminál by byl zařízením příslušného úřadu) a následně by tentýž úředník obdržel odpověď s výsledkem. V případě, že bude jako BOK-pad použit MK, nebude mít úředník žádnou možnost si ověřit to, že před ním stojící uživatel vůbec MK pro zadání BOKu použil (dokonce by ani ve svém mobilním zařízení MK nemusel mít instalován). Uživatel by např. mohl odeslat SMS a na jejím základě by jiná osoba s jiným mobilním zařízením (ve kterém by byl instalován MK s vhodnou identitou) odeslala platný BOK. Zda v úředních agendách existují procesy, ve kterých by se tyto typy podvodů daly praktikovat (např. s možností popření), k tomu neexistuje žádná procesní ani právní analýza a autoři zde předkládaného dokumentu to bez ní neumějí zhodnotit. Takové hodnocení proto bude na správci ISDS, resp. na NIA jako poskytovateli

takové služby, pro niž MK bude jen prostředkem. Může to v praxi limitovat použitelnost MK jako BOK-padu pro některé agendy.

Uživatel si při připojení MK do NIA bude moci zvolit, zda chce MK používat i jako BOK-pad, tedy nástroj pro zadávání BOK jako druhý faktor při prezenčním ověřování totožnosti v běžných agendách veřejné správy. Jejich výčet bude omezen pravděpodobně katalogem služeb podle zákona o právu na digitální službu a agendy se tedy budou připojovat postupně.

Při použití MK jako BOK-pad nebude BOK v MK ukládán. Pokaždé, když ho uživatel zadá, aplikace pouze v paměti zašifruje zadanou hodnotu a předá ji na BOK server, což je jeden z modulů NIA.

Mobilní klíč nevyhodnocuje, zda je BOK zadán správně nebo ne - toto vyhodnocení provede BOK server a MK dostane pouze odpověď, kterou má zobrazit uživateli.

Případné zablokování BOKu nebo BOK-padu po N opakovaných špatných zadání BOK, pokud tento proces dává bezpečnostní smysl, bude realizovat BOK server/NIA.

Scénář použití:

1) Proces začíná mimo MK a mimo uživatele. Úředník ztotožní uživatele (samotný MK nesmí být použit jako náhrada dokladu totožnosti) ve svém informačním systému a ten dotazem na NIA zjistí, že pro prováděnou agendu je pro daného uživatele vyžadováno potvrzení BOKem. Informační systém pošle do NIA (prostřednictvím ISZR) požadavek na ověření BOKu.
2) NIA zašle na MK push notifikaci. Na mobilním zařízení se v notifikačním centru objeví notifikace, že přišel požadavek na ověření BOKu. Pokud má uživatel v NIA připojeno více MK, notifikace je zaslána na všechny MK. Uživatel může akci provést na kterémkoli z nich.
3) Uživatel na notifikaci klikne, tím spustí MK. Přihlásí se do aplikace.
4) Zobrazí se dialog s textem ve stylu "Pro potvrzení prezenčního ztotožnění agendy <jméno> zadejte prosím svůj BOK", polem pro zadání BOK a tlačítky pro potvrzení a zrušení akce.
5) Uživatel zadá BOK a potvrdí akci.
6) MK pošle standardní potvrzení operace (zpráva 02), jako rozšiřující položku požadavku přidá zašifrovaný BOK. BOK bude zašifrovaný dle požadavku NIA a výsledný šifrovaný blok bude vložen do dále šifrované zprávy 02.
7) NIA převezme potvrzující zprávu z MK, předá data do BOK serveru, ten zpracuje BOK, a ověří, že je zadán správně vůči ZR. Vrátí zpět do MK výsledek operace, což může být jedna z těchto možností:
   a) BOK byl zadán správně;
   b) BOK byl zadán špatně, uživatel to může zkusit znovu ještě N-krát;
   c) BOK byl zadán špatně, byl překročen maximální povolený počet pokusů, nelze to již zkoušet znovu;
   d) Došlo k technické chybě.
8) MK zobrazí výsledek akce; pokud je požadavek na opakované zadání BOK, vrací se k bodu 4.
9) Pokud byl BOK zadán správně, NIA předá výsledek do informačního systému, který si ověření BOK od NIA vyžádal.

Technicky se jedná o rozšíření stávajícího procesu potvrzení popsaného v kapitole 4.5.5 o zadání BOK.

5.6 Případ užití 6: Schválení požadavku na předání osobních údajů – varianta s notifikací

Zadání: Uživatel, který má v NIA účet s Mobilním klíčem, může pomocí MK povolit předání osobních údajů třetí straně. Třetí strana uživatele předem identifikuje - ví tedy, po kom osobní údaje žádá.

Tento případ užití umožňuje uživateli pomocí MK schválit předání osobních údajů třetí straně. Typickým příkladem by mohlo být například schválení předání zdravotnické dokumentace poskytovateli zdravotnických služeb.

Případ užití vychází z toho, že třetí strana má uživatele ztotožněného, tj. dokáže poslat na NIA požadavek na předání osobních údajů konkrétního uživatele.

Scénář použití:

1) Třetí strana chce získat osobní údaje uživatele. Ztotožní uživatele a pošle požadavek na předání osobních údajů do NIA.
2) NIA zašle na MK push notifikaci. Na mobilním zařízení se v notifikačním centru objeví notifikace, že přišel požadavek předání osobních údajů. Pokud má uživatel více MK, notifikace je zaslána na všechny MK. Uživatel může akci provést na kterémkoli z nich.
3) Uživatel na notifikaci klikne, tím spustí MK. Přihlásí se do aplikace.
4) Aplikace zobrazí dialog „Přišel požadavek na povolení předání osobních údajů. Po stisku ZOBRAZIT bude zobrazena stránka autorizačního SP s detailními informacemi a možností potvrzení.“ a tlačítky Zobrazit a Zamítnout.
5) Pokud uživatel zvolí Zobrazit, bude spuštěn webový prohlížeč nasměrovaný na stránku NIA s požadavkem ke schválení. Na stránce NIA bude zobrazeno
   a) komu budou informace předány
   b) jaké údaje (obecně, bez konkrétních hodnot) budou předávány
   c) bude zde tlačítko „Potvrdit Mobilním klíčem“.
   d) Nemusí zde být QR kód, protože stránka byla spuštěna Mobilním klíčem - je jisté, že na zařízení MK je nainstalován.
6) Pokud uživatel stiskne „Potvrdit Mobilním klíčem“, je opět spuštěna aplikace MK. Uživatel se opět přihlásí do MK a tím potvrdí akci.
7) MK odešle standardní potvrzovací zprávu 02 na server NIA.
8) Třetí strana si od NIA vyzvedne odpověď na svůj požadavek zaregistrovaný v bodě 1

5.7 Případ užití 7: Schválení požadavku na předání osobních údajů - varianta načtení QR kódu

Zadání: Uživatel, který má v NIA účet s Mobilním klíčem, může pomocí MK povolit předání osobních údajů třetí straně. Třetí strana předem neví, po kom osobní údaje žádá - vytiskne/zobrazí obecný QR kód k načtení a NIA jí k danému ID požadavku vrátí informace o tom uživateli, který QR kód načetl a povolil předání osobních údajů.

Tento případ užití umožňuje uživateli pomocí MK schválit předání osobních údajů třetí straně, stejně jako předešlý případ užití 6. Rozdíl je v tom, že třetí strana ještě uživatele nemá ztotožněného a součástí scénáře je z pohledu třetí strany i identifikace uživatele, který akci provedl.

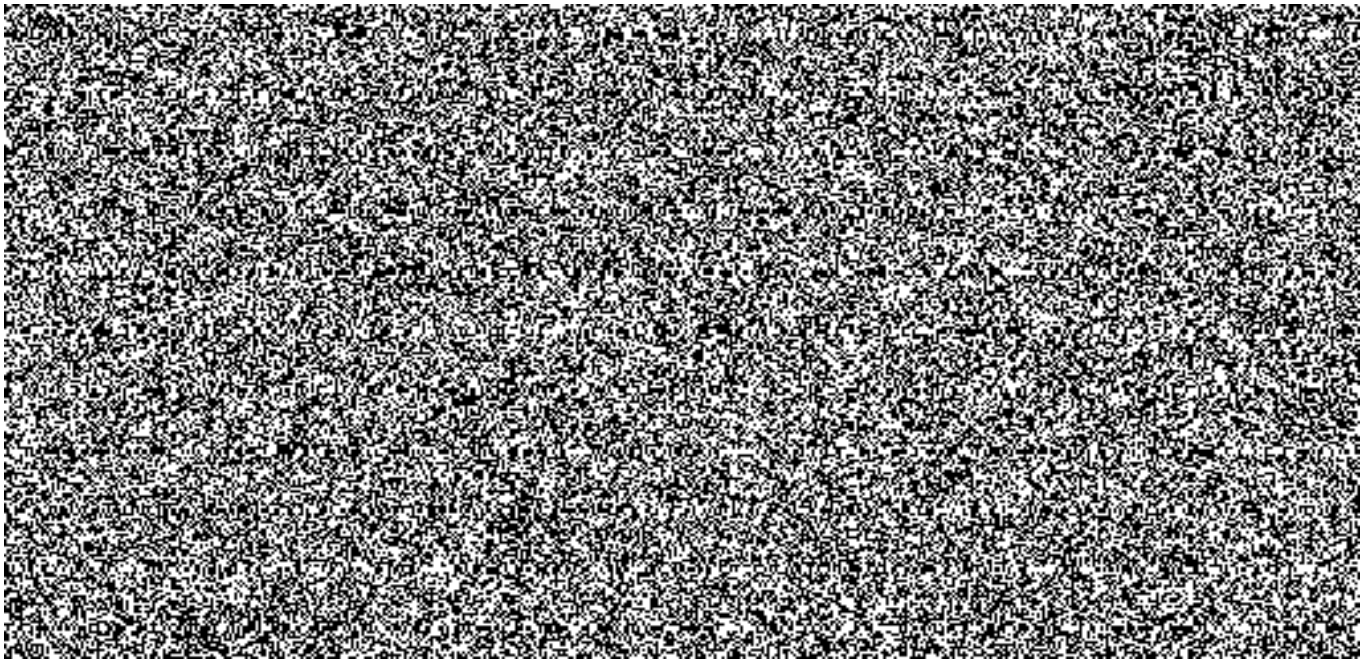
Typický příběh: Uživatel při čekání na poskytnutí zdravotnických služeb dostane pořadový lístek. Na pořadovém lístku je QR kód. Uživatel načte QR kód a potvrdí předání zdravotnické dokumentace. Ve

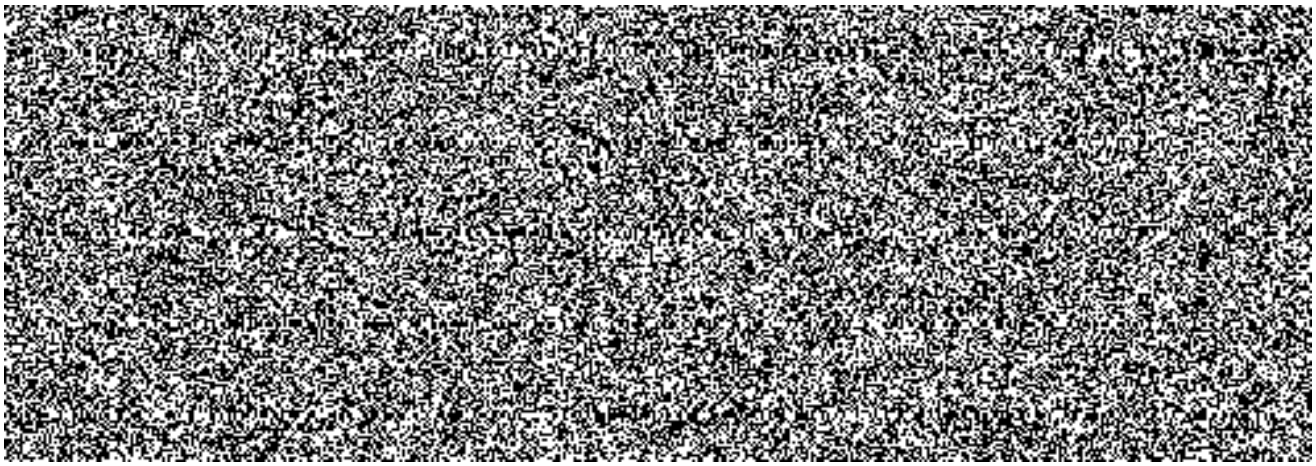
chvíli, kdy přijde na řadu, lékař si do informačního systému opíše číslo pořadového lístku (či také načte QR kód) a okamžitě má k dispozici informace o pacientovi i jeho zdravotnickou dokumentaci; nemusel si nic opisovat z kartičky pojištěnce.

Scénář použití:

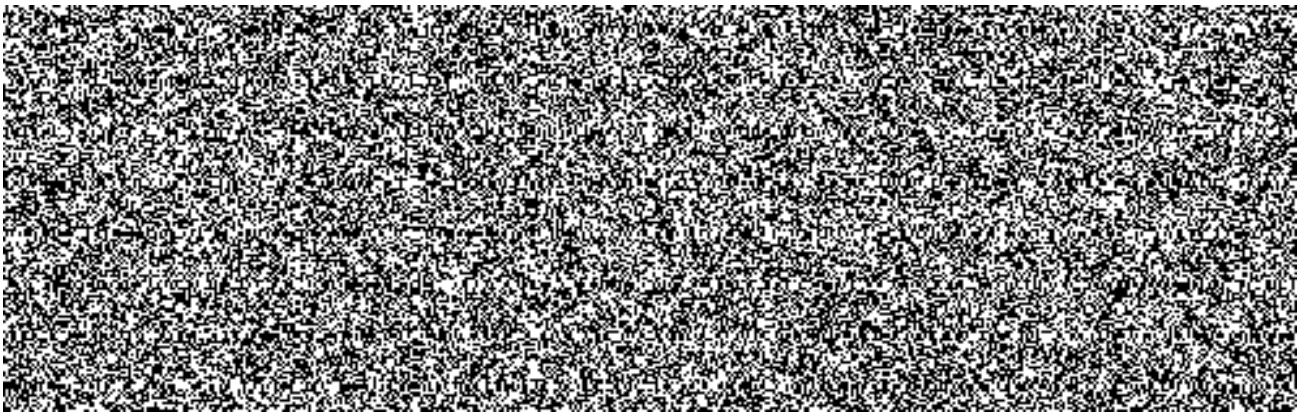
1) Třetí strana chce vytisknout QR kód s požadavkem na přístup k osobním údajům. Zavolá odpovídající službu NIA; zpět dostane číslo požadavku a obsah QR kódu, který má vytisknout.
2) Uživatel spustí aplikaci MK, přihlásí se do ní a načte QR kód.
3) Aplikace zobrazí dialog „Toto je požadavek na povolení předání osobních údajů. Po stisku ZOBRAZIT bude zobrazena stránka NIA s detailními informacemi a možností potvrzení.“ a tlačítky Zobrazit a Zamítnout.
4) Pokud uživatel zvolí Zobrazit, aplikace pošle komunikační zprávu na NIA (aby NIA věděla, kdo bude předání OÚ schvalovat) a v odpovědi dostane odkaz na schvalovací stránku na webu NIA.
5) Aplikace spustí webový prohlížeč nasměrovaný na stránku NIA s požadavkem ke schválení. Na stránce NIA bude zobrazeno
   a) komu budou informace předány
   b) jaké údaje (obecně, bez konkrétních hodnot) budou předávány
   c) bude zde tlačítko „Potvrdit Mobilním klíčem“.
   d) Nemusí zde být QR kód, protože stránka byla spuštěna Mobilním klíčem - je jisté, že na zařízení MK je nainstalován.
6) Pokud uživatel stiskne „Potvrdit Mobilním klíčem“, je opět spuštěna aplikace MK. Uživatel se opět přihlásí do MK a tím potvrdí akci.
7) MK odešle standardní potvrzovací zprávu 02 na server NIA.
8) Třetí strana si od NIA vyzvedne odpověď na svůj požadavek zaregistrovaný v bodě 1. Dostane jak identitu uživatele, který akci schválil, tak vyžádané osobní údaje.

Poznámka: Body 5-8 odpovídají stejným bodům případu užití 6. Oba tyto případy užití se tedy liší v tom, jakým způsobem jsou spuštěny (notifikace pro konkrétního uživatele vs. načtení obecného QR kódu), ale zbytek zpracování je takřka stejný, liší se jen textace.





7 Popis implementace MK



7.1.1 Změny které uvidí uživatel

7.1.1.1 Jméno aplikace a ikona

Aplikace bude přejmenována z „Mobilní klíč ISDS“ na „Mobilní klíč eGovernmentu“.

Ikona aplikace zůstane stejná.

Popiska u ikony na domovské stránce na platformě Apple (kde je méně místa pro popis) bude „Mobilní klíč eG“. Popis na platformě Android bude buď „Mobilní klíč eG“ nebo „Mobilní klíč eGovernmentu“.

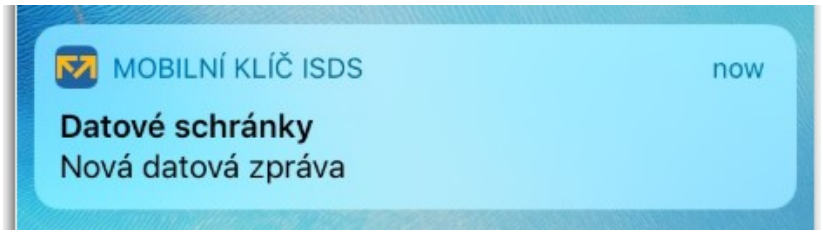
7.1.1.2 Notifikační centrum mobilního zařízení

Notifikace v notifikačním centru mobilního zařízení budou rozlišovat odesilatele.

Notifikace z ISDS budou mít nadpis Datové schránky (stejně jako nyní),

notifikace z NIA budou mít nadpis NIA - eIdentita.

Ikona u notifikace zůstane stejná jako nyní (tj. nebude reagovat na zdroj požadavku); nadpis „Mobilní klíč ISDS“ je jménem aplikace a jako dopad změny jména aplikace (viz 7.1.1.1) se změní na „Mobilní klíč eG“ nebo „Mobilní klíč eGovernmentu“.



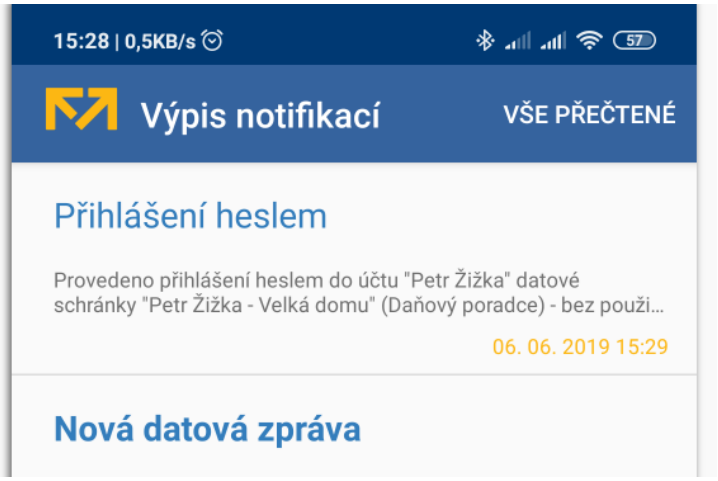
Obrázek 1 - Ukázka stávající notifikace v notifikačním centru zařízení

7.1.1.3 Seznam notifikací v aplikaci

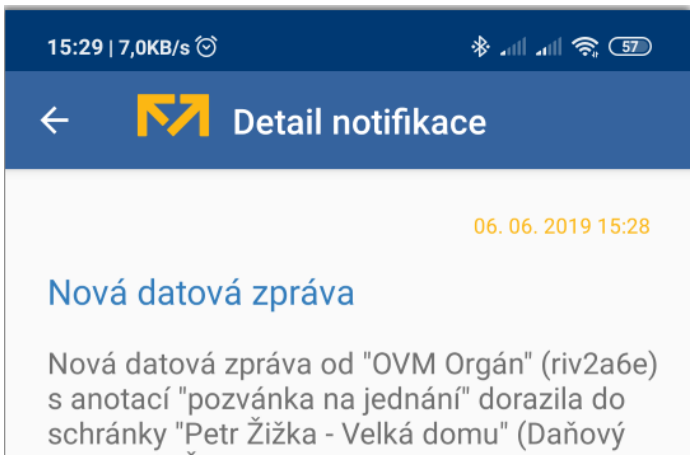
Notifikace z obou systémů (NIA, ISDS) budou v aplikaci v jednom seznamu doručených notifikací.

V seznamu notifikací i v detailu notifikace bude vlevo před typem notifikace („Přihlášení heslem“, „Nová datová zpráva“, ...) ikona, která bude identifikovat, z jakého systému notifikace dorazila.

- pro NIA
- pro ISDS



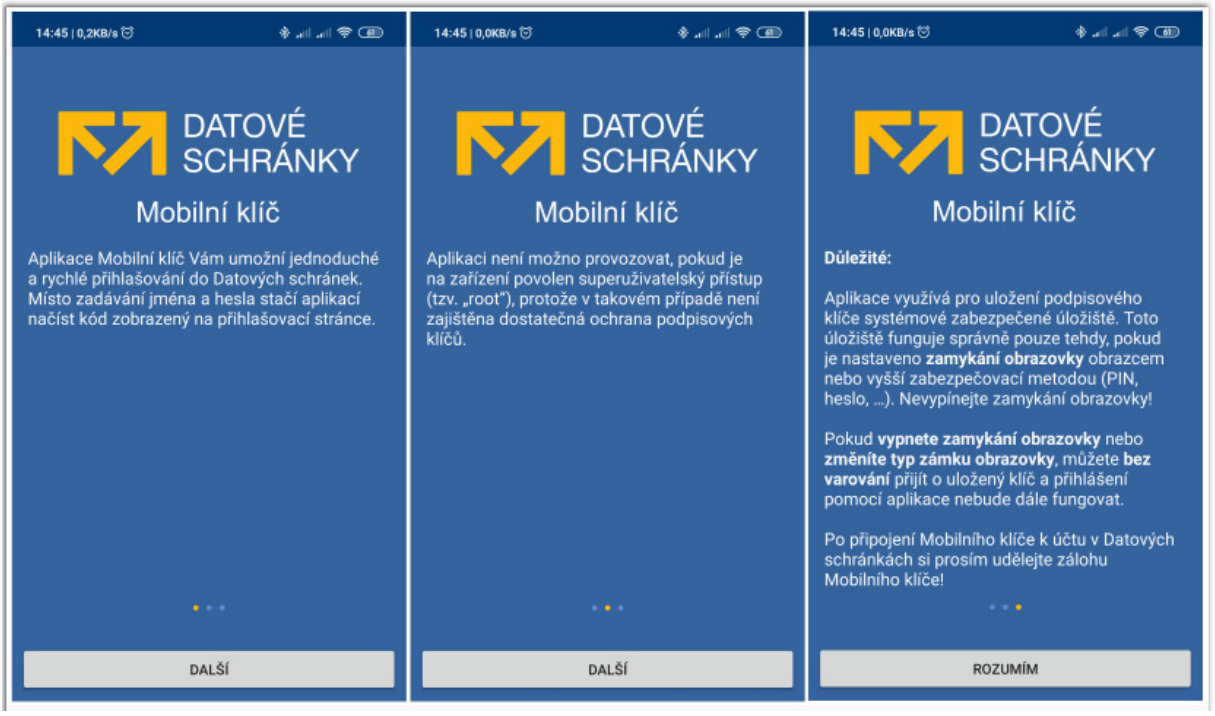
Obrázek 2 - Seznam notifikací - stávající vzhled



Obrázek 3 - Detail notifikace, stávající vzhled

7.1.1.4 Úvodní obrazovky – změny textace

Po prvním spuštění jsou zobrazeny tři úvodní informační obrazovky:



Obrázek 4 - Úvodní informační obrazovky

1. Bude odstraněno logo ISDS s nadpisem „Datové schránky".
2. Nadpis bude změněn na „Mobilní klíč eGovernmentu".
3. Texty budou upraveny.

Text pro Android:

Aplikace Mobilní klíč vám umožní jednoduché a rychlé přihlašování do Datových schránek nebo portálu eIdentity - NIA. Místo zadávání jména a hesla stačí aplikací načíst kód zobrazený na přihlašovací stránce.

[Další]

Aplikaci není možno provozovat, pokud je na zařízení povolen superuživatelský přístup (tzv. „root "), protože v takovém případě není zajištěna dostatečná ochrana podpisových klíčů.

[Další]

Důležité:

Aplikace využívá pro uložení podpisového klíče systémové zabezpečené úložiště. Toto úložiště funguje správně pouze tehdy, pokud je nastaveno zamykání obrazovky obrazcem nebo vyšší zabezpečovací metodou (PIN, heslo, ...). Nevypínejte zamykání obrazovky!

Pokud vypnete zamykání obrazovky nebo změníte typ zámku obrazovky, můžete bez varování přijít o uložený klíč a přihlášení pomocí aplikace nebude dále fungovat.

Po připojení Mobilního klíče k účtu v Datových schránkách nebo NIA si prosím udělejte zálohu mobilního klíče!

[Rozumím]

Text pro iOS:

Aplikace Mobilní klíč vám umožní jednoduché a rychlé přihlašování do Datových schránek nebo portálu eIdentity - NIA. Místo zadávání jména a hesla stačí aplikací načíst kód zobrazený na přihlašovací stránce.

[Další]

Aplikaci není možno provozovat, pokud je na zařízení odemčeno (tzv. „jailbreak“), protože v takovém případě není zajištěna ochrana podpisových klíčů.

[Další]

Po připojení Mobilního klíče k účtu v Datových schránkách nebo NIA si prosím udělejte zálohu mobilního klíče!

[Rozumím]

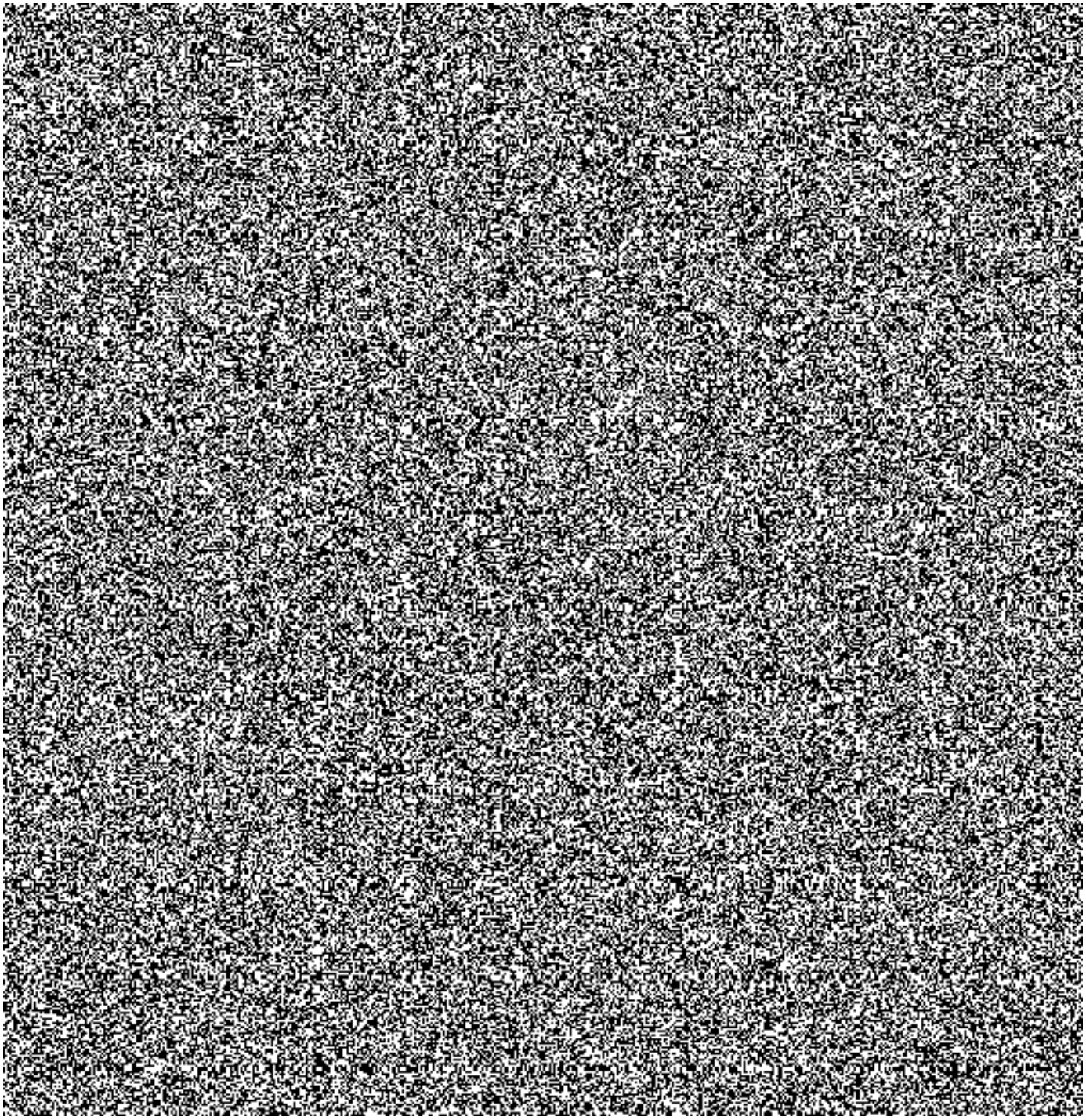
7.1.1.5 Rozcestník pro inicializaci aplikace

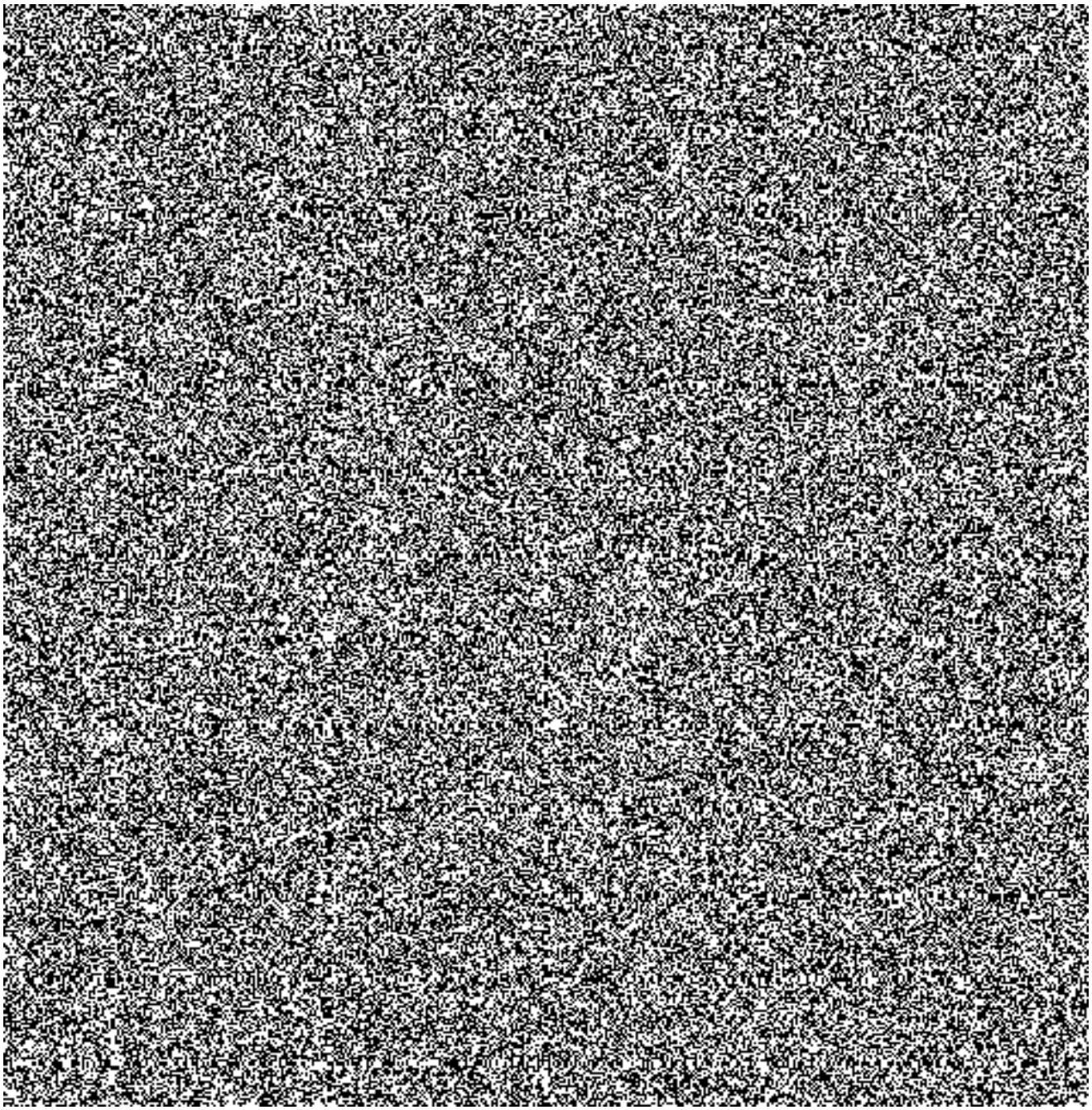
Po úvodním nastavení zabezpečení aplikace je zobrazen rozcestník, kde si uživatel volí, zda chce MK připojit k účtu, nebo obnovit zálohu z předešlého Mobilního klíče.

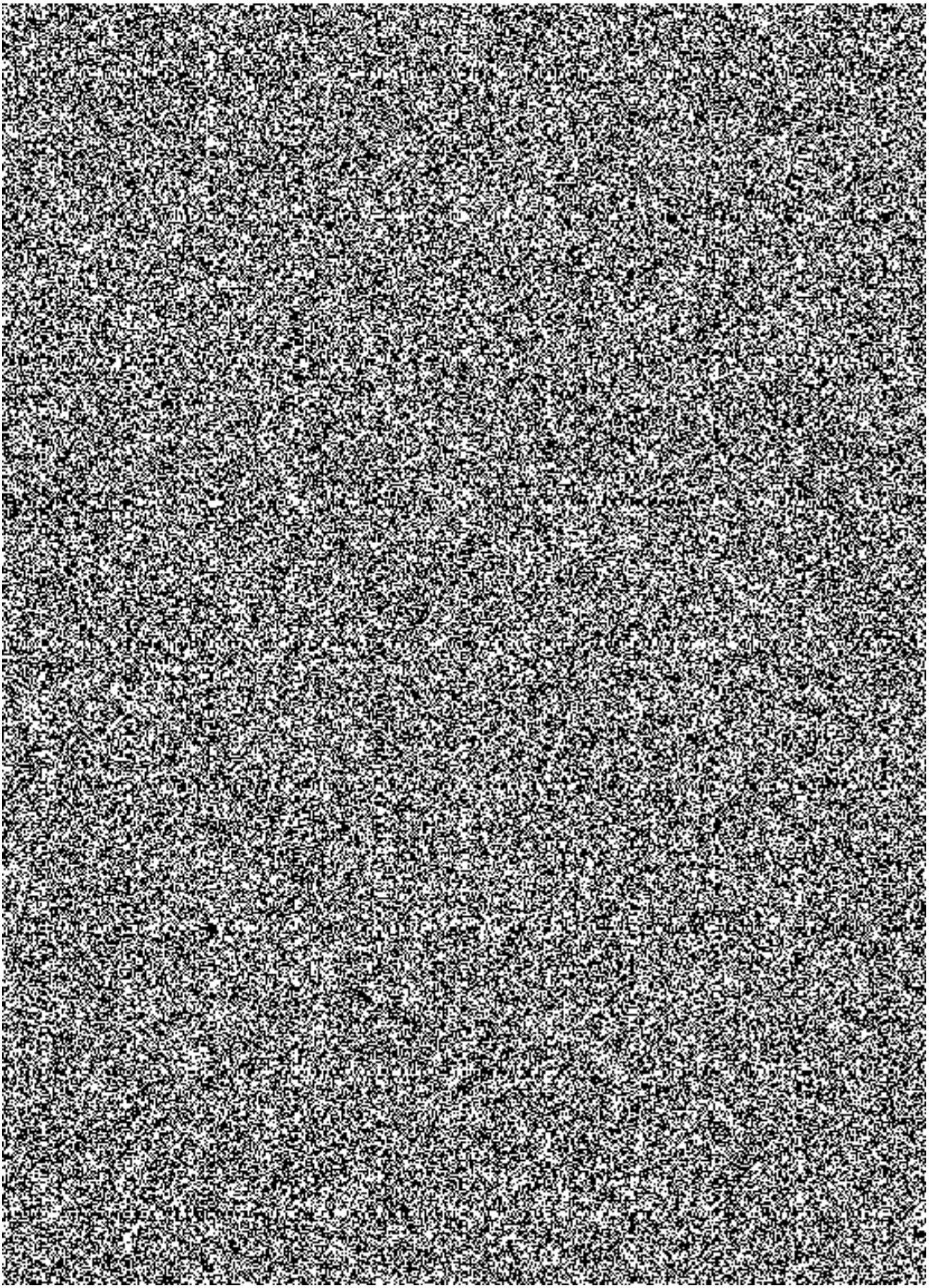
Obrázek 5 - Rozcestník po inicializaci aplikace (stávající stav)

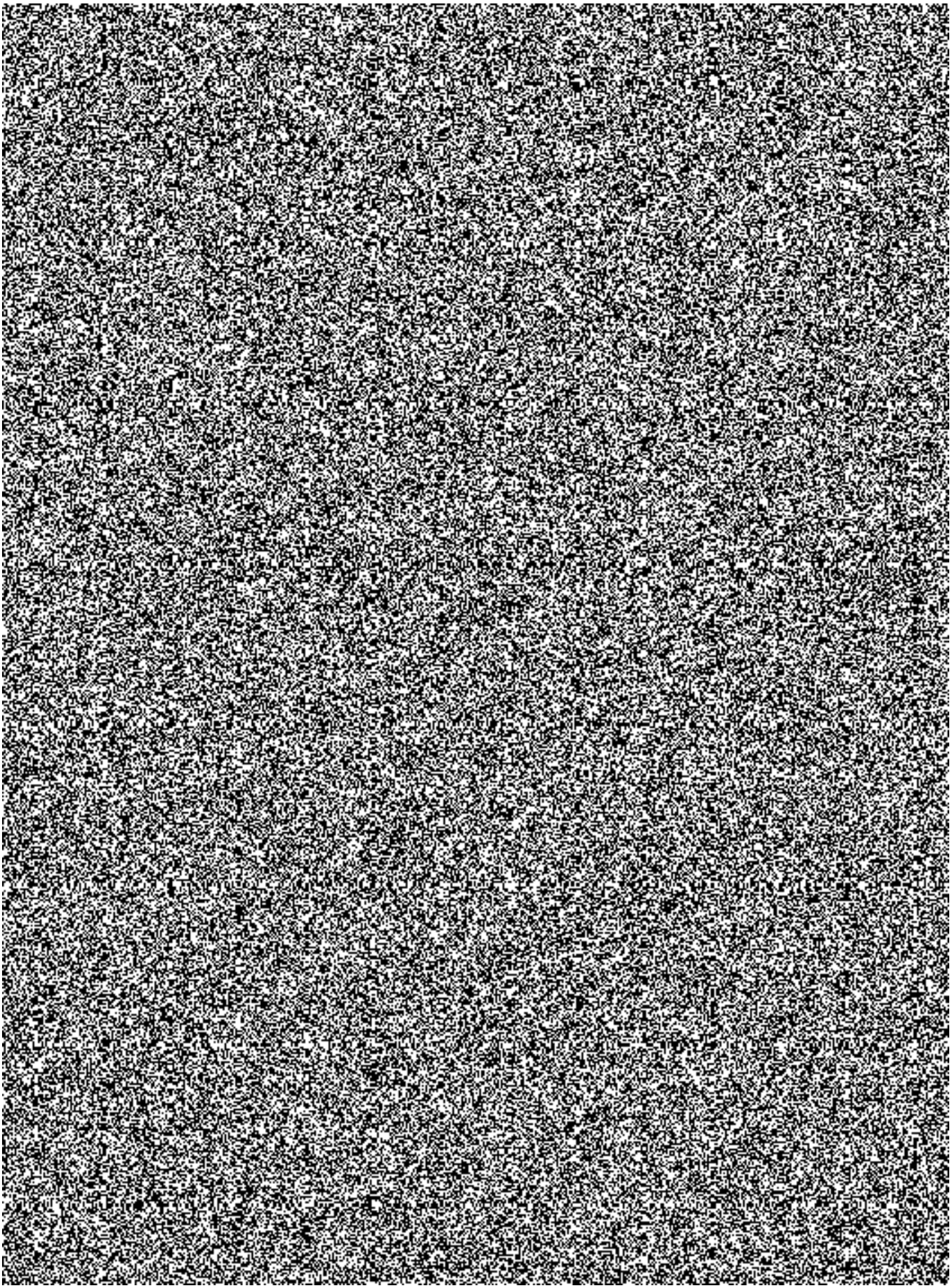
Pokud uživatel zvolí „Připojit k účtu“, je ještě upozorněn, kde najde v klientském portálu ISDS možnost připojení MK k účtu:

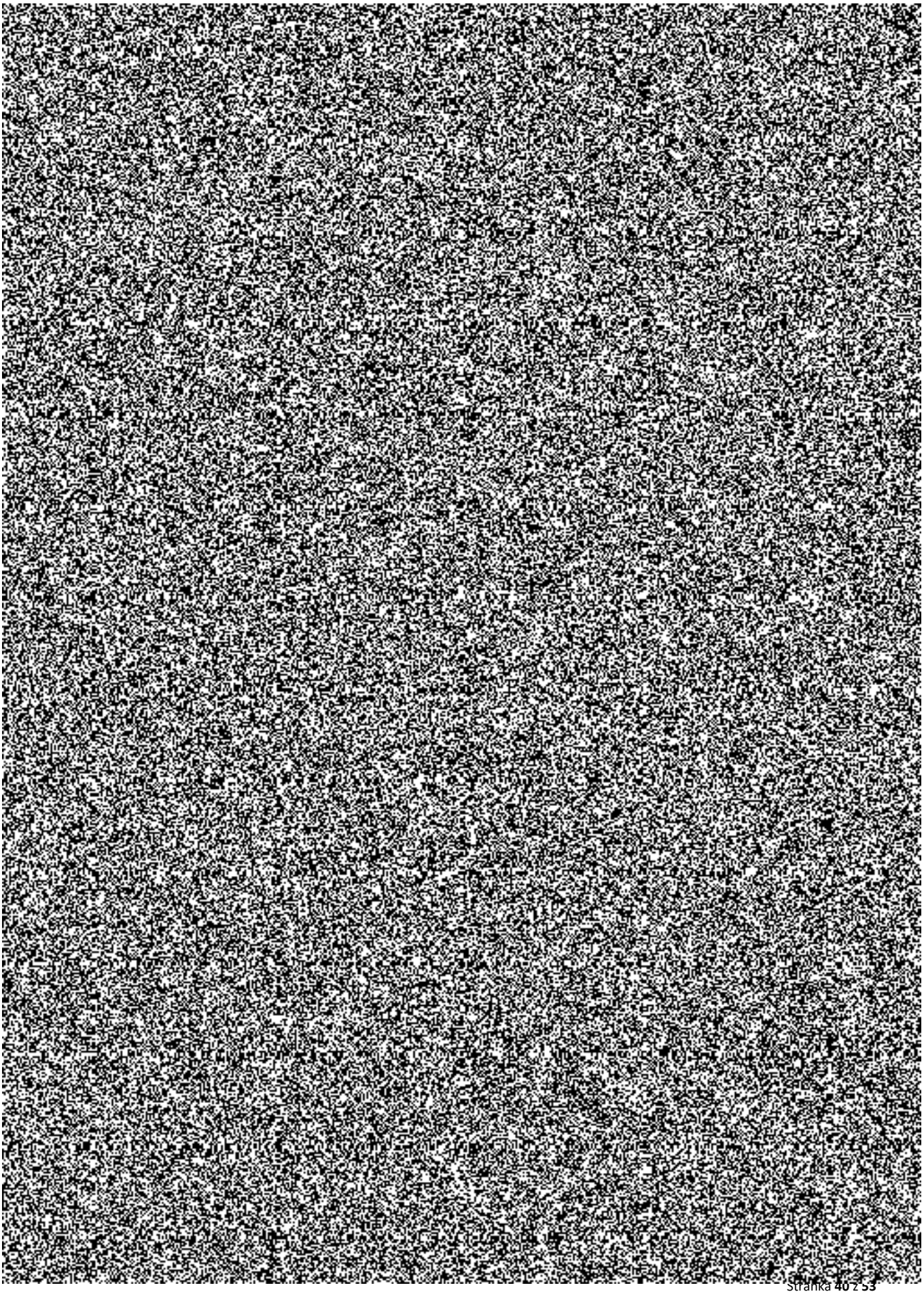
Obrázek 6 - Informace, kde uživatel najde připojení MK (stávající stav)

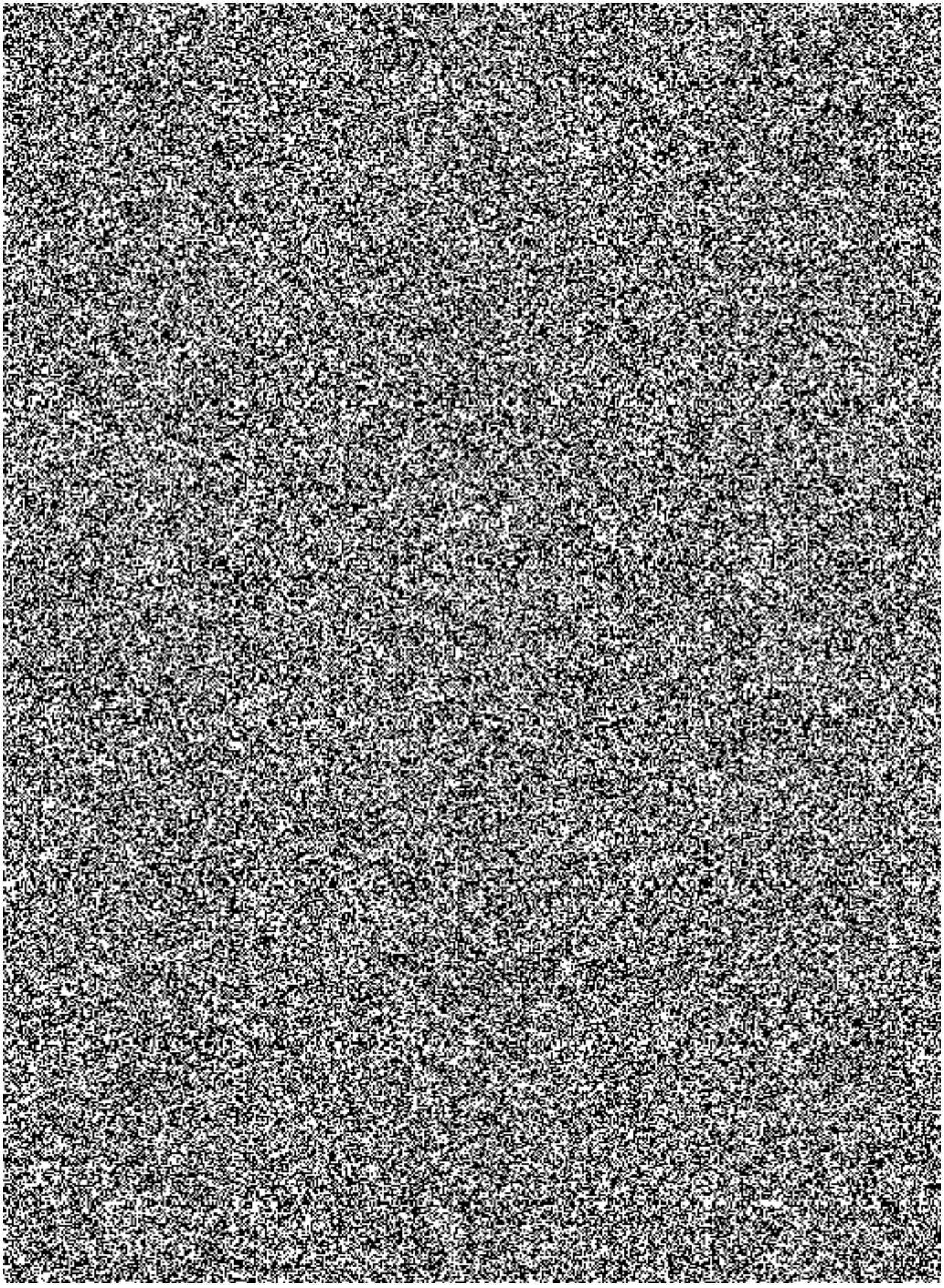


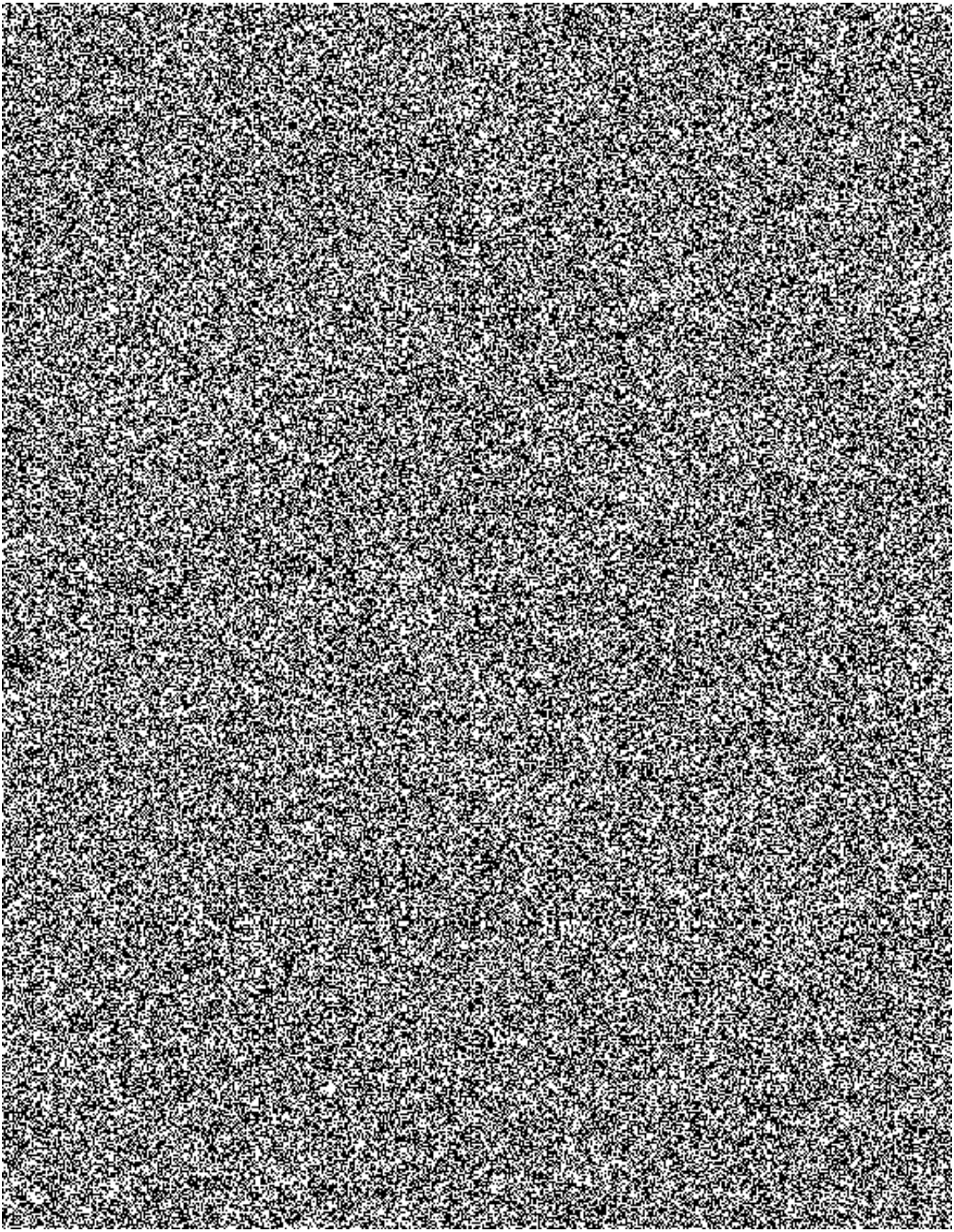


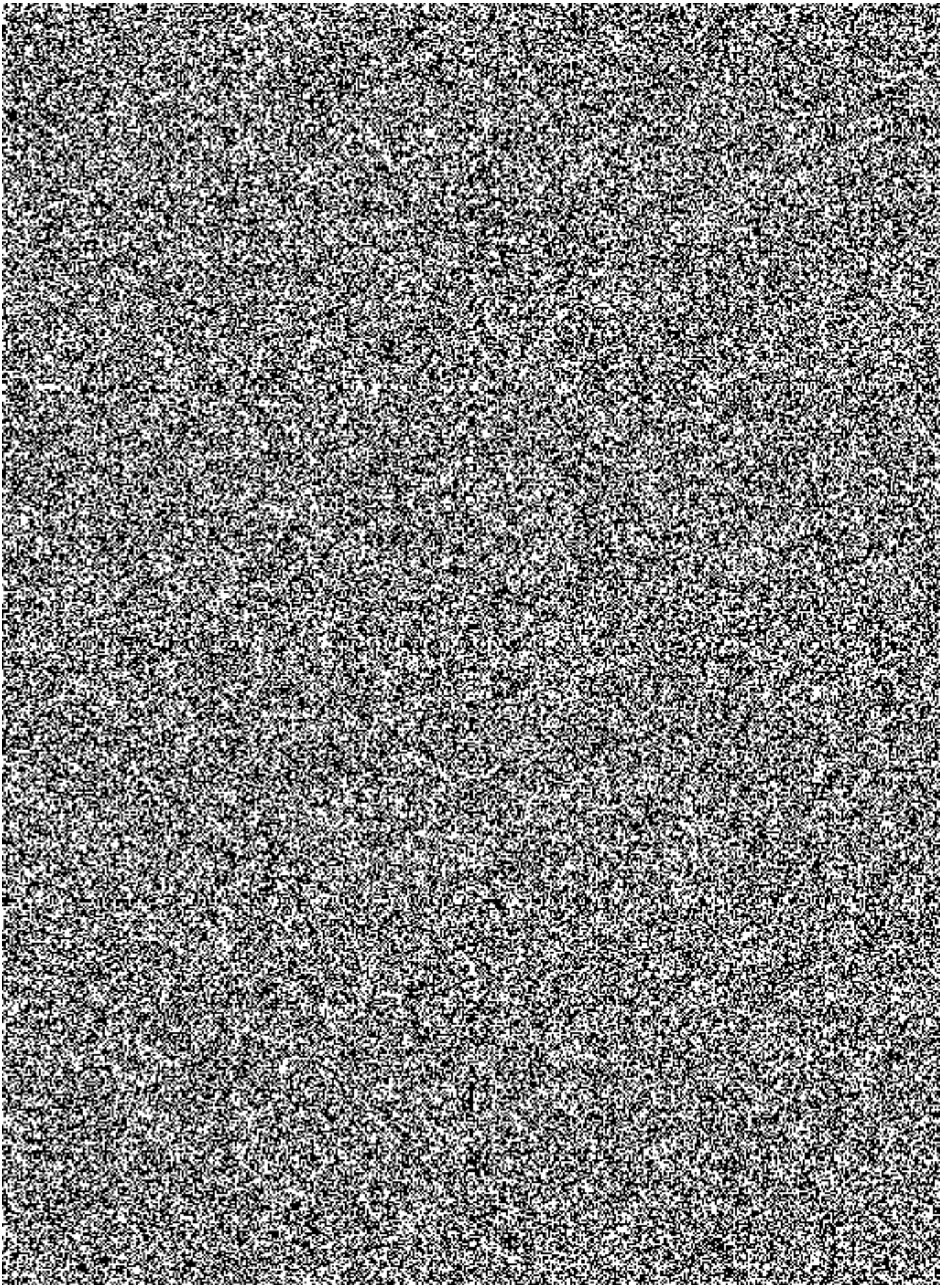


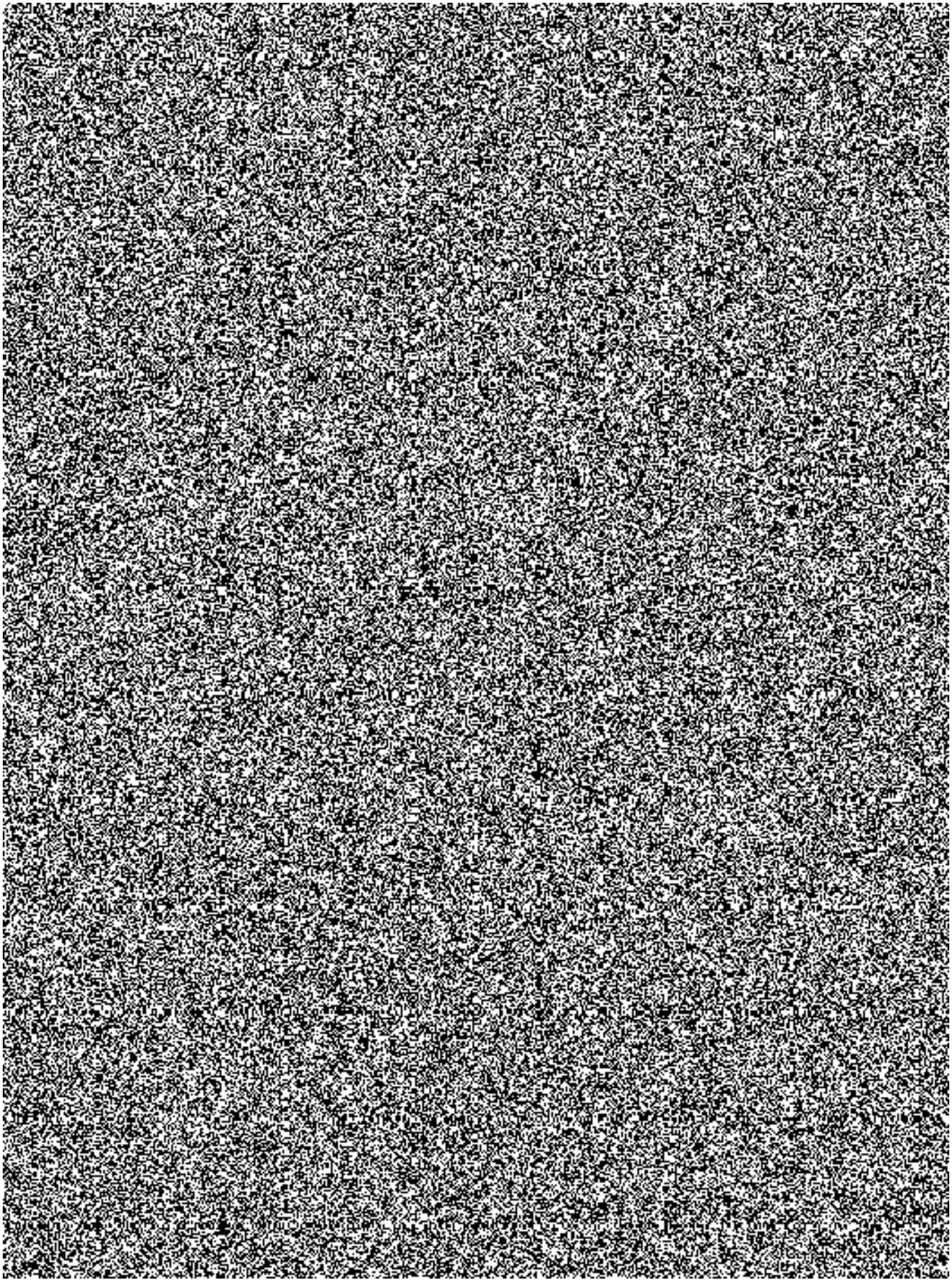


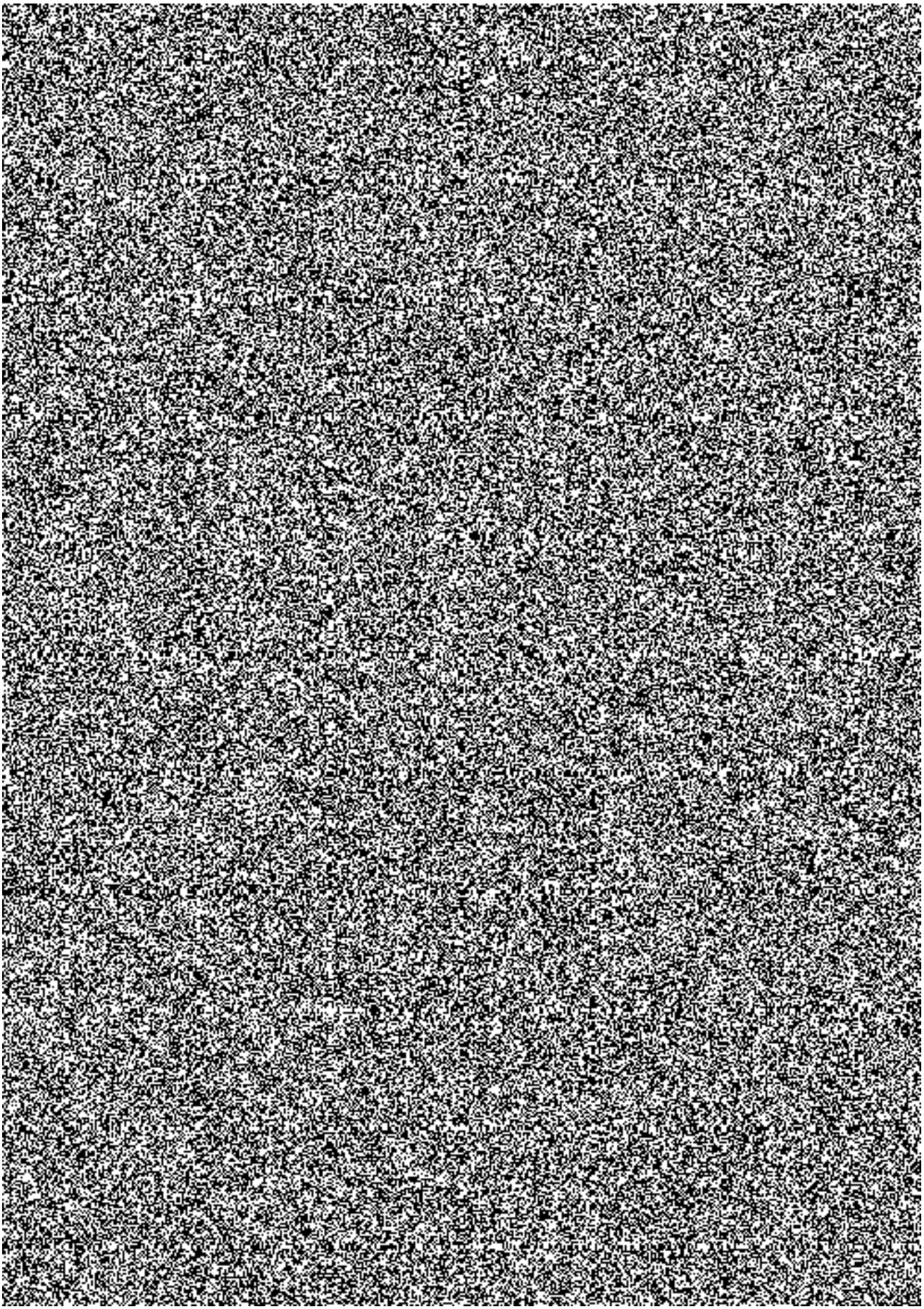


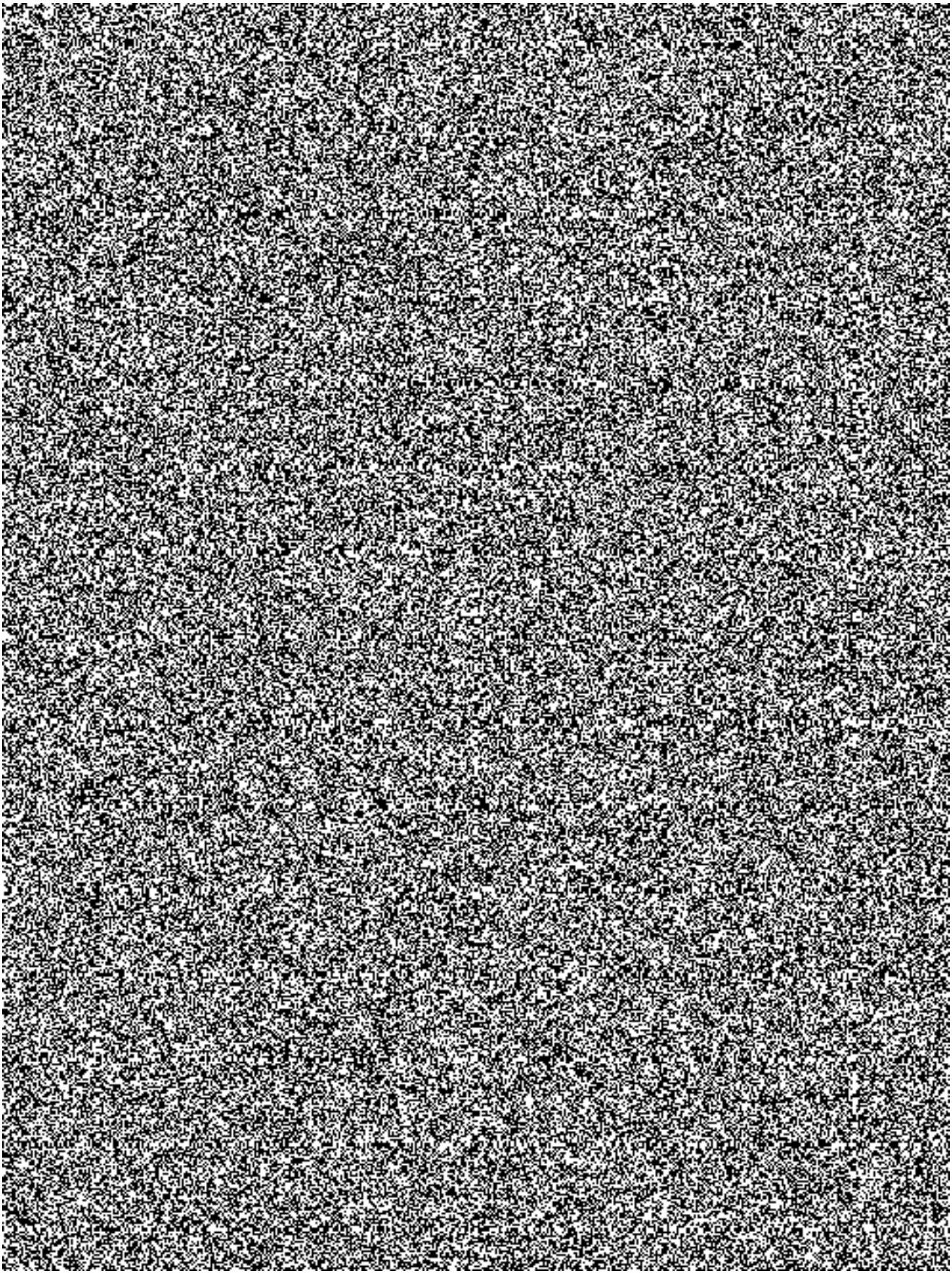




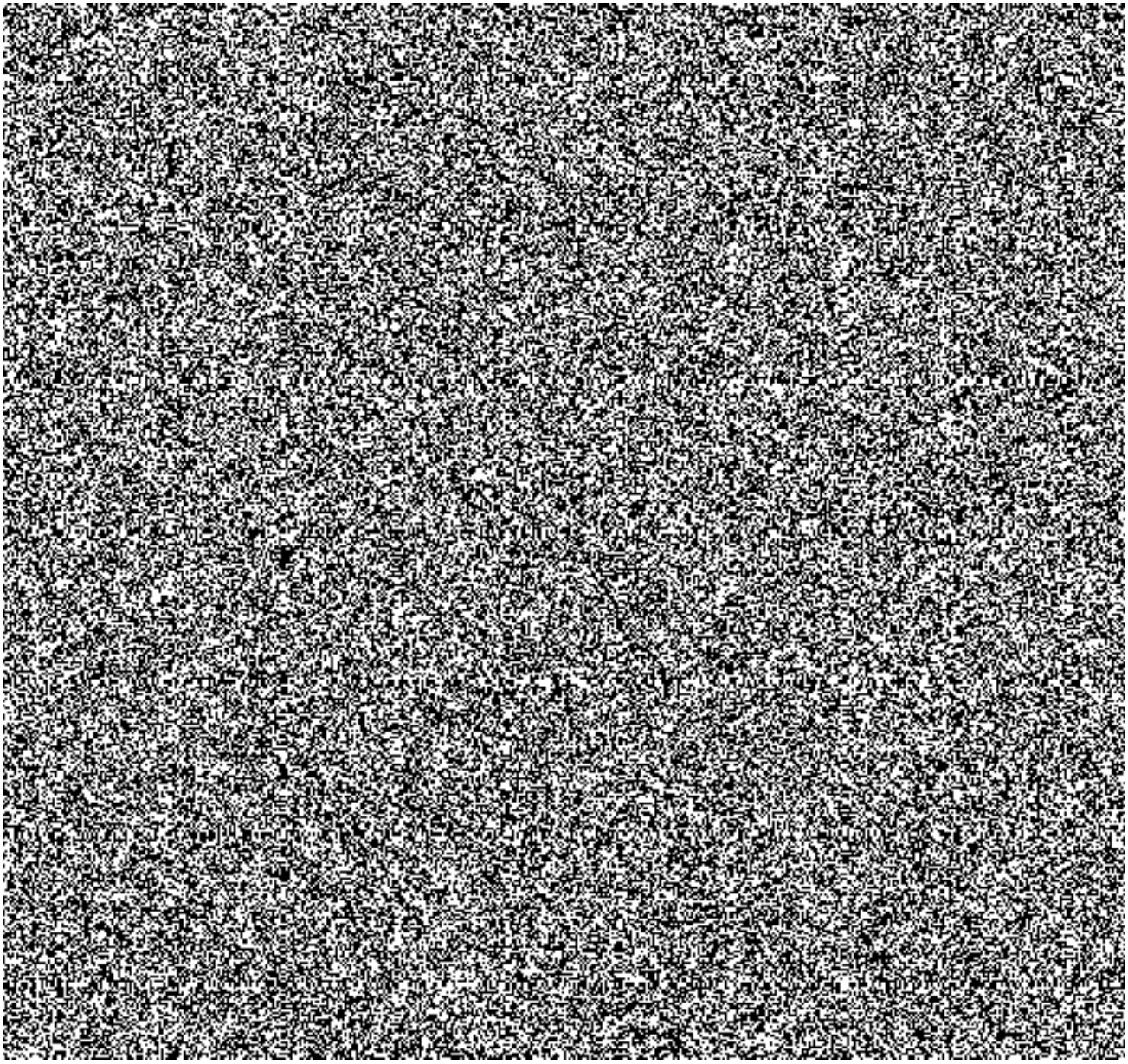








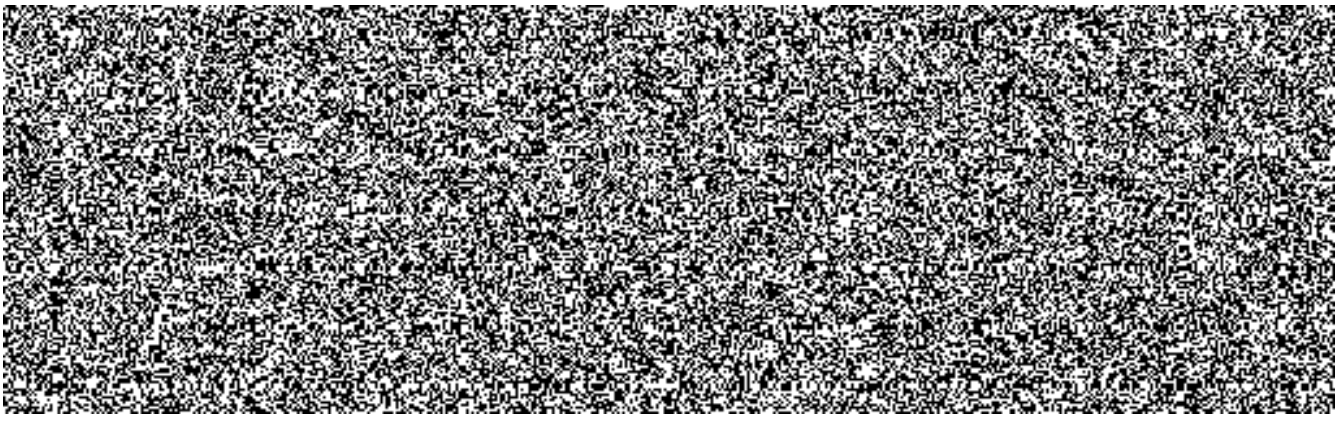
[9] Používá se pro zobrazení v notifikačním centru zařízení.

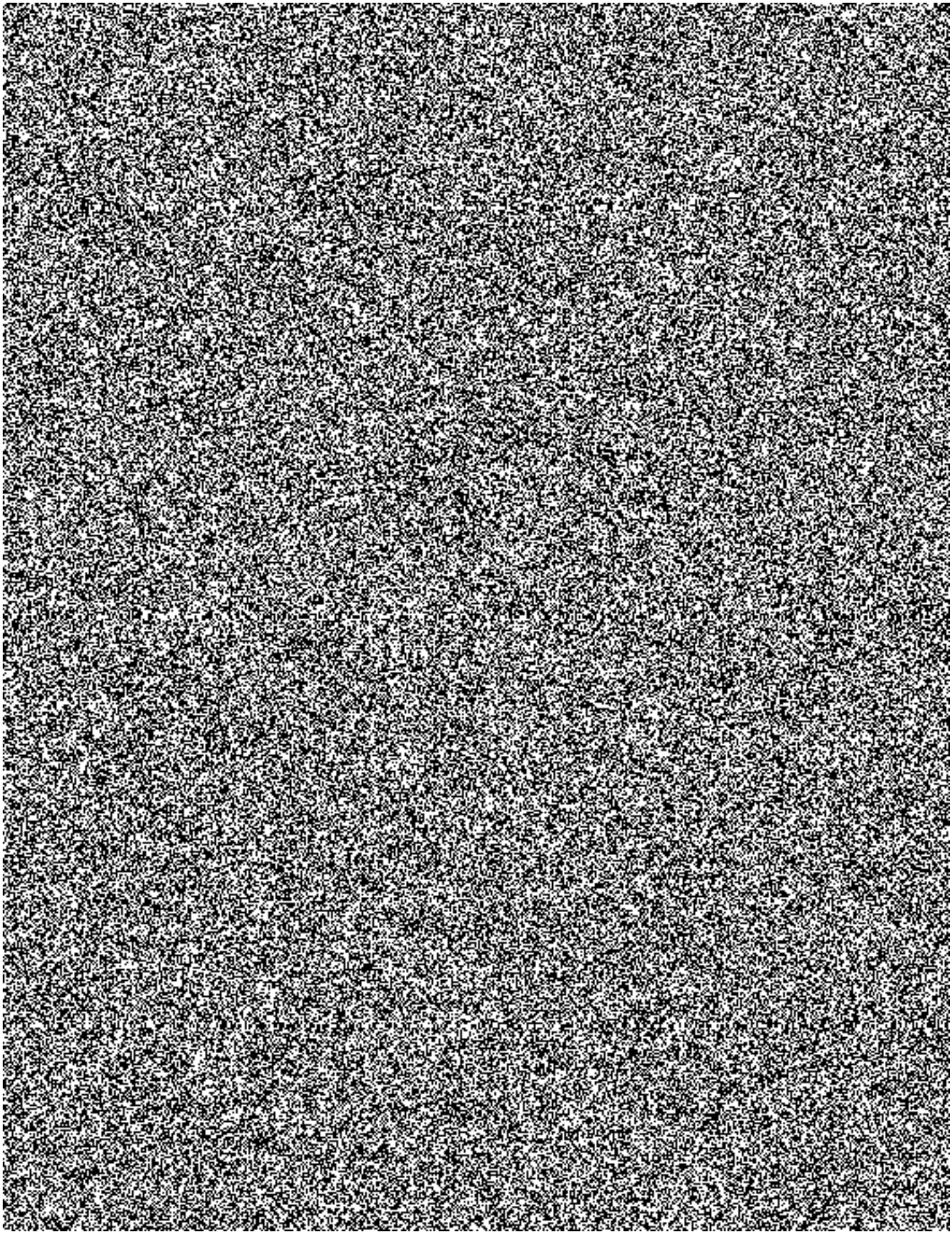


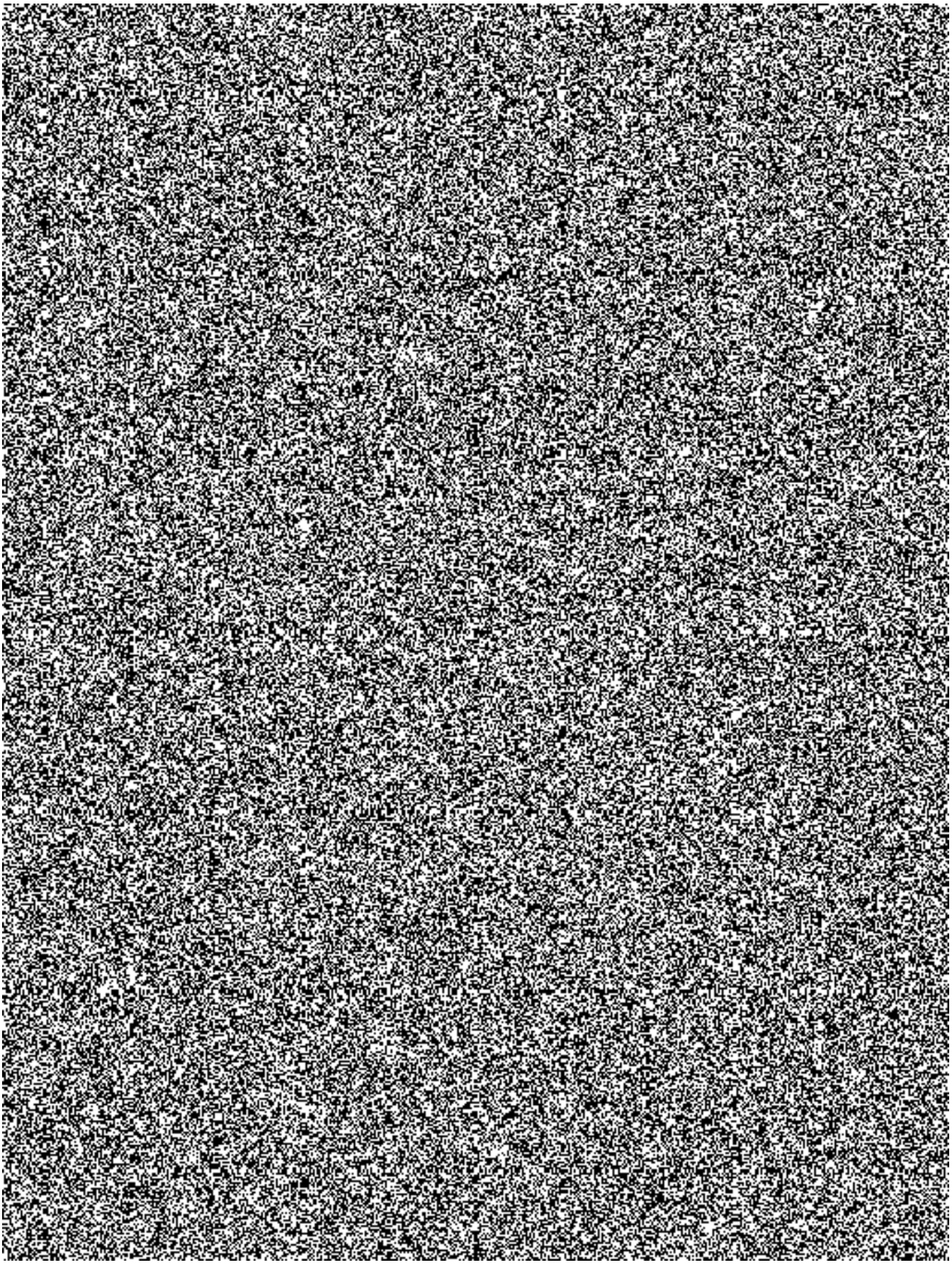
7.3 Změny Klientského portálu ISDS – netýkají se národního bodu

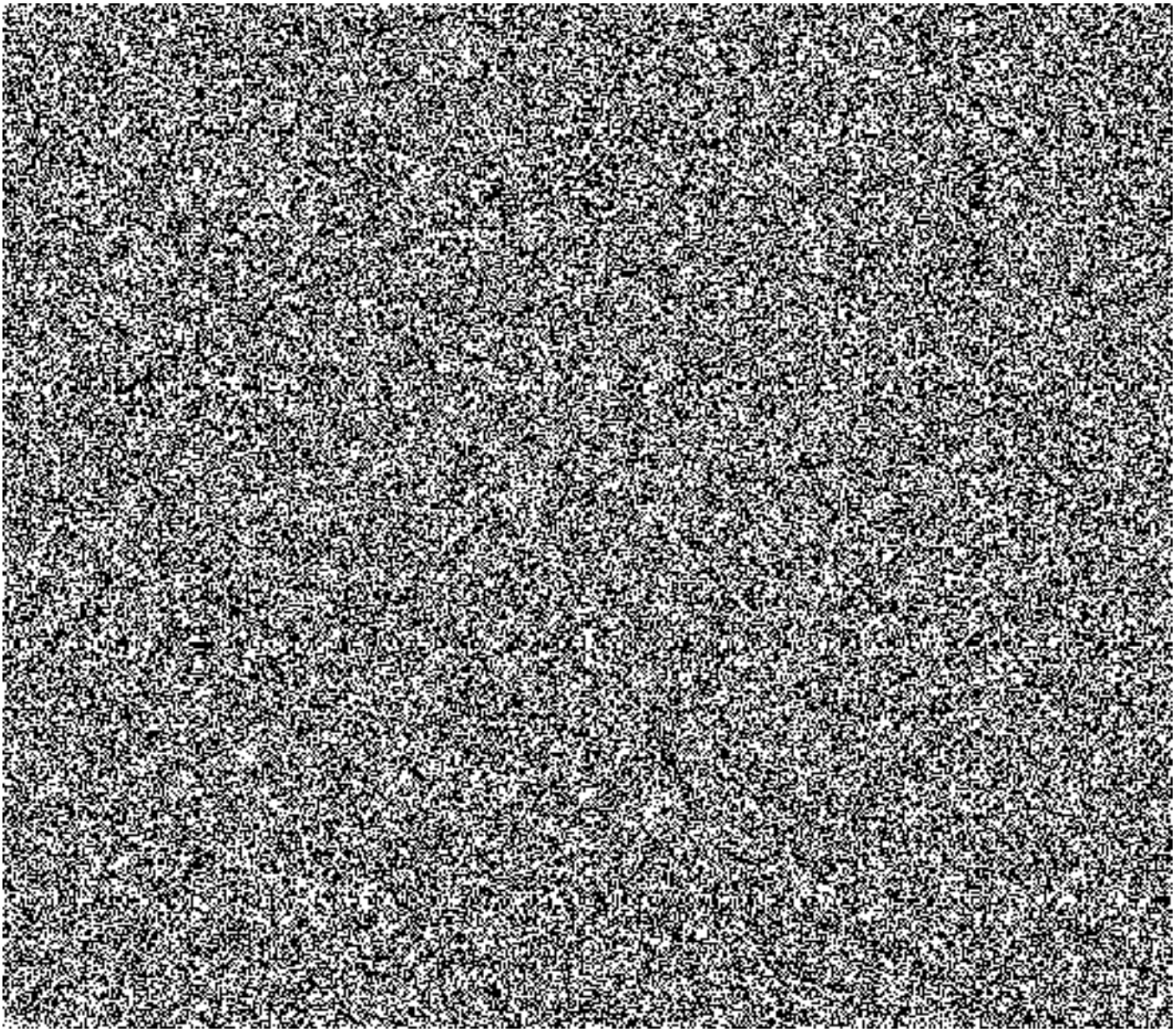
7.4 Změny jádra ISDS – netýkají se národního bodu

7.5 Implementace na straně NIA









Penetrační test

Budou provedeny externí penetrační testy, které budou zaměřeny na vybrané komponenty řešení MORIS dostupné z veřejné sítě Internet. Toto testování bude zaměřeno na ověření funkčnosti aplikačního celku MEP dodávaného NAKIT (tj. bez mobilní aplikace). Cílem penetračního testu bude odhalit co největší množství závažných zranitelností na úrovni konektorů služeb systému, na úrovni referenčních infrastrukturních prvků, ve webovém rozhraní aplikace a prostředí, na kterém aplikace běží, odhalit způsob jejich využití a případnou možnost získání přístupu.
Plán testů – postup a způsob realizace:

- Proběhnou penetrační testy bez znalosti prostředí (black box) a s částečnou znalostí prostředí (grey box – zejm. v případě webových služeb), kdy proběhne simulace počínání útočníků ve výše popsaných rolích / scénářích.
- Externí dodavatel předá zástupcům NAKIT výsledky provedených testů v podobě stručného dokumentu, ve kterém bude uveden soupis nálezů, indikace jejich závažnosti a technické detaily potřebné pro odstranění nálezů. O kritických zjištěních budou zástupci NAKIT informování neprodleně telefonicky.

- Po vypořádání nálezů menšího rozsahu proběhne opětovné otestování (retest) za účelem ověření účinnosti aplikovaných nápravných opatření. Poté bude vyhotoven návrh závěrečné zprávy dle standardů externího dodavatele, které vyhovují požadavkům NAKIT. V závěrečné zprávě budou k jednotlivým zjištěním doplněny výsledky opakovaného testu.

Nasazení (1x nasazení release na produkci)

Kompletní nasazení nových funkcionalit na produkční prostředí. Smoke a regresní testy po nasazení na prostředí, které ověří správnou funkčnost aplikace.

Školení (proškolení SD SZR před nasazením release)

Proškolení SD SZR před nasazením nového release v rozsahu změn, které se v rámci release budou nasazovat, včetně dodání změnové dokumentace ke školení.

Seznam zkratek

AIFO	Agendový identifikátor fyzické osoby
API	Aplikační interface
BOK	Bezpečnostní osobní kód
CzP	Pracoviště CzechPOINT
Google FCM	Google Firebase Cloud Messaging
HASH	Hašovací funkce je matematická funkce (resp. algoritmus) pro převod vstupních dat do (relativně) malého čísla. Výstup hašovací funkce se označuje výtah, miniatura, otisk, fingerprint či hash (česky též někdy jako haš).
HTTPS	Hypertextový transportní protokol zabezpečený prostřednictvím TLS šifrování
IdP	Poskytovatel identity
iOS	Operační systém mobilní platformy společnosti Apple
ISDS	Informační systém datových schránek
ISZR	Informační systém základních registrů
IV	Modul individuálních výdejů
MK	Mobilní klíč
MEP	Mobilní elektronický prostředek
NAKIT	Národní agentura pro komunikační a informační technologie
NB	Národní bod
NIA	Národní identitní autorita
OP	Občanský průkaz
QR	QR kód (anglicky: QR Code, slang. a nepříliš správné označení je také labyrinth, případně bludiště) je prostředek pro automatizovaný sběr dat. Zkratka vychází z anglického „Quick Response“, tedy kódy rychlé reakce. QR kód dokáže zakódovat mnohem větší množství dat než klasický EAN čárový kód. Specifikace QR kódů je od června 2000 standardem ISO 18004.
ROB	Registr obyvatel
SD	Service Desk

SDÚ	Modul Subjektem definovaných údajů národního bodu
SP	Poskytovatel služby
SZR	Správa základních registrů
UPS	IDP jméno heslo, SMS

Seznam obrázků