MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

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

č.j.: 2018/295 NAKIT
č.j.: MV-

DÍLČÍ SMLOUVA Č. 8
O DÍLO

k Rámcové smlouvě na Vybudování Dohledového centra eGovernmentu
č. j. MV-159071-28/OKB-2015, č. j. 2016/010 NAKIT

Národní agentura pro komunikační a informační technologie, s.p.
se sídlem: Kodaňská 1441/46, Vršovice, 101 00 Praha 10
IČO: 04767543
DIČ: CZ04767543
zastoupen: [redacted]

zapsán v obchodním rejstříku: Městského soudu v Praze, oddíl A, vložka 77322
bankovní spojení: [redacted]

na straně jedné (dále jen **„Zhotovitel“**)

a

Česká republika – Ministerstvo vnitra

se sídlem: Nad Štolou 936/3, 170 34 Praha 7
IČO: 00007064
DIČ: CZ00007064
zastoupen: Ing. Miroslavem Tůmou, PhD., [redacted]

bankovní spojení: Česká národní banka,
č. ú.: 3605881/0710

na straně druhé (dále jen **„Objednatel“**)

(Zhotovitel a Objednatel společně jako „**Smluvní strany**“ anebo jednotlivě též jako „**Smluvní strana**“)

uzavírají níže uvedeného dne, měsíce a roku v souladu s ustanovením § 2586 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**Občanský zákoník**“), tuto Dílčí smlouvu č. 8 (dále jen „**Smlouva**“) k Rámcové smlouvě na Vybudování Dohledového centra eGovernmentu ze dne 8. srpna 2016 (dále jen „**Rámcová smlouva**“), a to takto:

Článek 1
Předmět a účel Smlouvy

1.1 Předmětem této Smlouvy je rozšíření a optimalizace samostatné domény dcegov.local (Active Directory) určené pro servery a jejich služby, stanice a uživatele dohledu a pro řízení přístupu k nástrojům a službám bezpečnostního dohledu zhotovené pro Objednatele na základě dílčí smlouvy č. 4B č.j. MV-159071-337/OPR-2015, 2017/196 NAKIT, a to dle specifikace uvedené v Příloze č. 1 této Smlouvy (dále jen „**Dílo**“).

1.2 Účelem této Smlouvy je provedení Díla, jehož funkčnost spočívá v rozšíření a optimalizaci Díla s ohledem na zvýšení bezpečnosti a flexibility samotné správy ICT infrastruktury Objednatele.

1.3 Předmětem této Smlouvy je závazek Zhotovitele provést pro Objednatel Dílo závazek Objednatele zaplatit za Dílo provedené v souladu s touto Smlouvou sjednanou cenu.

Článek 2
Práva a povinnosti Smluvních stran při plnění Smlouvy

A. Místo, termín a způsob plnění

2.1 Zhotovitel se zavazuje Dílo provést, dokončit a předat Objednateli nejpozději do 7.11.2018. Akceptaci Díla dle čl. 1 odst. 1.1 Smlouvy stvrdí obě Smluvní strany Akceptačním protokolem podepsaným odpovědnými osobami obou Smluvních stran. Vzor Akceptačního protokolu tvoří Přílohu č. 2 této Smlouvy. Podpisu Akceptačního protokolu bude předcházet akceptační řízení definované v čl. 2 odst. 2.3 až 2.7 Smlouvy.

2.2 Místem předání Díla je adresa [redacted]

B. Předání, převzetí a akceptace Díla

2.3 Akceptační řízení zahrnuje ověření funkčnosti Díla porovnáním skutečných vlastností Díla s jeho podrobnou specifikací dle Přílohy č. 1 Smlouvy a prověřením, že Dílo je způsobilé sloužit svému účelu definovaném v čl. 1 odst. 1.2 Smlouvy. Finální technická podoba Díla podléhá odsouhlasení ze strany technického garanta Objednatele, a to na základě akceptace řešení Díla v souladu s akceptovanou dokumentací skutečného provedení. Tato dokumentace skutečného provedení provádí specifikaci dle Přílohy č. 1 Smlouvy.

2.4 Akceptační řízení je zahájeno dnem jeho předání Objednateli k Akceptačnímu řízení na základě Předávacího protokolu podepsaného oběma Smluvními stranami a je ukončeno podpisem Akceptačního protokolu oběma Smluvními stranami. Splňuje-li Dílo technické podmínky a vlastnosti stanovené touto Smlouvou a jejími přílohami a je-li Dílo funkční potvrdí Objednatel uvedené skutečnosti v Akceptačním protokolu, jehož vzor tvoří Přílohu č. 2 Smlouvy. Vzor Předávacího protokolu tvoří Přílohu č. 3 Smlouvy.

2.5 V případě výskytu ojedinělých drobných vad a nedodělků v termínu jeho předání a převzetí, které nebrání Objednateli v užívání Díla a jeho funkčnosti a dále ani jeho užívání podstatným způsobem definovaným v Příloze č. 4 této Smlouvy neomezují, převezme Objednatel plnění, přestože jeho určitá část nesplňuje všechna akceptační kritéria (převzetí s výhradou). Smluvní strany si zároveň dohodnou lhůtu, do kdy Zhotovitel odstraní zbývající vady části plnění tak, aby byla splněna všechna akceptační kritéria. Pro vyloučení všech pochybností se Smluvní strany dohodly, že nebude-li mezi Smluvními stranami dosaženo dohody o lhůtě, ve které Zhotovitel odstraní vady plnění dle předchozí věty tohoto ustanovení Smlouvy, bude tato lhůta stanovena Objednatelem, kdy délka takto stanovené lhůty nesmí být kratší než 20 pracovních dnů. Tyto skutečnosti budou zaznamenány v Akceptačním protokolu vyhotoveném při akceptaci plnění s výhradou. Po odstranění takových vad sepíší Smluvní strany zápis stvrzující odstranění vad, pro které bylo částečné plnění Díla akceptováno s výhradou. Klasifikace vad a nedodělků je specifikována v Příloze č. 4.

2.6 Akceptační kritéria jsou specifikována v bodě 15 Přílohy č. 1 Smlouvy – Specifikace Díla.

C. Cena a platební podmínky

2.7 Smluvní strany sjednávají, že cena za Dílo dle odst. 1.1 Smlouvy činí maximálně 1 750 000,00Kč (slovy: jeden milion sedm set padesát tisíc korun českých) bez DPH, k níž se v souladu s daňovými předpisy přičítá příslušná sazba DPH v zákonem stanovené výši (celkem 367 500,00 Kč), tzn. cena za provedení Díla činí maximálně 2 117 500,00 Kč (slovy: dva miliony sto sedmnáct tisíc pět set korun českých) včetně DPH.

2.8 Cena za Dílo bude specifikována dodatkem ke Smlouvě dle znaleckého posudku. Objednatel je povinen znalecký posudek předložit Zhotoviteli k vyjádření. Nevyjádří-li se Zhotovitel k závěrům znaleckého posudku do 10 pracovních dnů od jeho předložení, platí, že jako výsledná cena Díla bude fakturována cena v rozsahu a ve výši uvedené ve znaleckém posudku. V případě, že Zhotovitel bude mít vůči závěrům znaleckého posudku odůvodněné a podložené připomínky, písemně vyzve Objednatele k ústnímu jednání za účelem jejich projednání.

2.9 Výsledná cena za provedení Díla bude stanovena dohodou Smluvních stran s přihlédnutím ke znaleckému posudku a následně stvrzena dodatkem k této Smlouvě.

2.10 Právo na vystavení faktury – daňového dokladu a na zaplacení ceny za provedené Dílo vzniká Zhotoviteli dnem podpisu dodatku k této Smlouvě v souladu s odst. 2.9 Smlouvy. Za den uskutečnění zdanitelného plnění je považováno datum podpisu dodatku ke Smlouvě dle odst. 2.9.

2.11 Ostatní podmínky pro daňový doklad se řídí podmínkami Rámcové smlouvy.

D. Vlastnická práva a práva duševního vlastnictví

2.12 Vlastnictví k hmotným nosičům dat, na nichž je Dílo zaznamenáno, a k ostatním

případným materiálům přechází na Objednatele okamžikem podpisu Předávacího protokolu. Cena hmotných nosičů dat je již zahrnuta v ceně dle článku 2. odst. 2.10 této Smlouvy. Nebezpečí škody na hmotných složkách Díla přechází na Objednatele okamžikem jejich převzetí.

2.13 Zhotovitel dnem podpisu Akceptačního protokolu poskytuje Objednateli na neomezenou dobu pro území celého světa výhradní licenci, tj. oprávnění k výkonu práva užit Dílo všemi způsoby v neomezeném rozsahu. Právo užití v neomezeném rozsahu dle předchozí věty v sobě zahrnuje rovněž právo Objednatele takové dílo doplňovat, upravovat, rozdělovat, učinit dílo nebo jeho část součástí jiného díla, jakož i přenechat dílo do užívání ve stejném rozsahu třetí osobě dle uvážení Objednatele. Smluvní strany vylučují aplikaci § 2370 Občanského zákoníku.

2.14 Zhotovitel prohlašuje, že Dílo ani jeho část nemá žádné právní vady, že není zatíženo právy třetích osob týkajících se zejména vlastnického práva a práv duševního vlastnictví a že Zhotovitel je zcela oprávněn disponovat bez jakéhokoli omezení veškerými majetkovými právy k Dílu a jeho částem a uzavřít s Objednatelem tuto Smlouvu na celý rozsah předmětu plnění. V případě, že se uvedené prohlášení Zhotovitele nezakládá na pravdě, Zhotovitel odpovídá Objednateli za vyplývající důsledky v plném rozsahu včetně odpovědnosti za skutečnou škodu a ušlý zisk.

2.15 Bude-li výsledkem nebo součástí poskytovaného plnění i zaměstnanecké či kolektivní dílo, které je předmětem autorských práv, práv souvisejících s právem autorským či práv pořizovatele k jím pořízené databázi, mohou se smluvní strany v konkrétním případě dohodnout, že Zhotovitel jako zaměstnavatel či osoba, z jejíhož podnětu a pod jejímž vedením je dílo vytvářeno a pod jejímž jménem je dílo uváděno na veřejnost, postupuje ke dni předání takovéhoto díla právo výkonu majetkových práv autora k dílu na Objednatele, přičemž výše odměny za postoupení je již zahrnuta v ceně poskytovaného plnění.

2.16 Zhotovitel výslovně prohlašuje, že je plně oprávněn disponovat právy k duševnímu vlastnictví včetně výše uvedených autorských práv, a zavazuje se za tímto účelem zajistit řádné a nerušené užívání díla Objednatelem, včetně případného zajištění dalších souhlasů a licencí od autorů děl v souladu s autorským zákonem, popř. od vlastníků jiných práv duševního vlastnictví v souladu s právními předpisy. Zhotovitel se zavazuje, že Objednateli uhradí veškeré náklady, výdaje, škody a majetkovou i nemajetkovou újmu, které Objednateli vzniknou v důsledku toho, že Objednatel nemohl dílo užívat řádně a nerušeně.

2.17 Smluvní strany tímto výslovně prohlašují, že veškerá finanční vyrovnání za užívání Díla jsou zahrnuta v ceně dle článku 2. odst. 2.10 této Smlouvy.

E. Záruka za jakost

2.18 Zhotovitel se zaručuje, že Dílo bude po dobu záruky způsobilé a funkční pro použití k ujednanému účelu a že si podrží ujednané vlastnosti ke dni podpisu Akceptačního protokolu Objednatelem. Zhotovitel odpovídá za to, že to, že jím dodané Dílo bude v jakosti a provedení vyhovujícím v plném rozsahu zákonům, předpisům a normám platným pro Českou republiku.

2.19 Zhotovitel odpovídá za to, že Dílo bude ke dni podpisu Akceptačního protokolu fungovat v souladu s požadavky Objednatele uvedenými ve Smlouvě a jejích přílohách.

2.20 Zhotovitel garantuje Objednateli záruku za jakost po dobu jednoho (1) roku ode dne provedení Díla, tj. ode dne podpisu Akceptačního protokolu, a že nahradí nebo obnoví funkčnost jakékoliv části vykazující vadu.

2.21 Záruka dle odst. 2.20. této Smlouvy poskytovaná Zhotovitelem se vztahuje na funkčnost Díla, jakož i na jeho vlastnosti požadované Objednatelem. Záruční doba se prodlužuje o dobu, po kterou mělo Dílo vadu bránící jeho řádnému užívání Objednatelem. Záruka se nevztahuje na vady, které na Díle vznikly bez vědomí Zhotovitele, zásahem Objednatele nebo jím pověřených třetích osob.

2.22 Veškeré zjištěné nedostatky, nedodělky a vady Díla (dále jen „**Vady**“), které se vyskytnou v záruční době a budou Zhotoviteli Objednatelem řádně písemně oznámeny, se Zhotovitel zavazuje odstranit ve lhůtě poskytnuté Objednatelem v písemném oznámení prostřednictvím kontaktních osob uvedených v čl. 3. odst. 3.21, která však nesmí být kratší než 5 pracovních dní.

Článek 3
Obecná ustanovení

A. Mlčenlivost

3.1 Smluvní strany se zavazují zachovat mlčenlivost o uvedených skutečnostech a informacích, které označí jako důvěrné dle § 1730 Občanského zákoníku, a to až do doby, kdy se informace této povahy stanou obecně známými za předpokladu, že se tak nestane porušením povinnosti mlčenlivosti (dále společně jako „**Důvěrné informace**“).

3.2 Smluvní strany se zavazují, že Důvěrné informace druhé smluvní strany jiným subjektům nesdělí, nezpřístupní, ani nevyužijí pro sebe nebo pro jinou osobu bez předchozího písemného souhlasu. Zavazují se zachovat je v přísné tajnosti a sdělit je výlučně těm svým zaměstnancům nebo poddodavatelům, kteří jsou pověřeni plněním Smlouvy a za tímto účelem jsou oprávněni se s těmito informacemi v nezbytném rozsahu seznámit. Smluvní strany se zavazují zabezpečit, aby i tyto osoby považovaly uvedené informace za důvěrné a zachovávaly o nich mlčenlivost. To neplatí, pokud mají být Důvěrné informace zpřístupněné pouze za účelem plnění Smlouvy, na základě obecného závazného předpisu, a to vždy jen v rozsahu zcela nezbytně nutném pro řádné plnění

Smlouvy či naplnění jejího účelu.

3.3 Smluvní strany budou za Důvěrné informace považovat též veškeré informace vzájemně poskytnuté v jakékoliv objektivně vnímatelné formě, ať již v ústní, písemné, grafické, elektronické či jiné formě, které se smluvní strany dozvěděly v souvislosti s touto Smlouvou, a to bez ohledu, zda jsou nebo nejsou označené za Důvěrné informace.

3.4 V případě porušení obchodního tajemství třetí stranou ve smyslu § 2985 Občanského zákoníku, použijí Smluvní strany prostředky právní ochrany proti nekalé soutěži.

3.5 Povinnost plnit ustanovení tohoto článku této Smlouvy se nevztahuje na informace, které: byly písemným souhlasem obou Smluvních stran zproštěny těchto omezení;

a) jsou známé nebo byly zveřejněny jinak, než následkem zanedbání povinnosti jedné ze Smluvních stran;
b) příjemce je zná dříve, než je sdělí Smluvní strana;
c) jsou vyžádány soudem, státním zastupitelstvím nebo příslušným správním orgánem na základě zákona;
d) Smluvní strana sdělí osobě vázané zákonnou povinností mlčenlivosti (např. advokátovi nebo daňovému poradci) za účelem uplatňování svých práv nebo plnění povinností stanovených právními předpisy.

3.6 Povinnost mlčenlivosti dle ustanovení tohoto článku této Smlouvy trvá bez ohledu na ukončení platnosti této Smlouvy.

3.7 V případě, že se kterákoliv Smluvní strana hodnověrným způsobem dozví, popř. bude mít důvodné podezření, že došlo ke zpřístupnění Důvěrných informací neoprávněné osobě, je povinna o tom bez zbytečného odkladu písemně informovat druhou Smluvní stranu.

3.8 Smluvní strany se zavazují, že budou-li Důvěrné informace, které jsou nezbytné pro plnění povinností dle této Smlouvy, obsahovat data podléhající režimu zvláštní ochrany dle zák. č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů, důsledně dodržovat důvěrnost a tajnost těchto dat.

3.9 Pokud bude druhé smluvní straně uděleno předchozí písemné svolení ke zpřístupnění Důvěrných informací, zajistí smluvně ochranu Důvěrných informací tak, aby byla minimálně na stejné úrovni, jakou sama poskytuje.

B. Sankce

3.10 V případě nedodání Díla v termínu podle čl. 2 odst. 2.1 Smlouvy, má Objednatel vůči Zhotoviteli právo na smluvní pokutu ve výši 0,05 % z ceny Díla bez DPH, a to za každý, byť jen započatý den prodlení, maximálně však do výše ceny Plnění bez DPH.

3.11 Za prodlení Objednatele s úhradou faktury má Zhotovitel vůči Objednateli právo na smluvní pokutu ve výši 0,05 % z dlužné fakturované částky bez DPH za každý, byť jen započatý den prodlení po termínu splatnosti, maximálně však do výše hodnoty dlužné fakturované částky bez DPH, s jejíž úhradou je Objednatel v prodlení.

3.12 V případě porušení kterékoli povinnosti podle čl. 3.1, 3.2, 3.3 a 3.8 této Smlouvy je Smluvní strana, která povinnost porušila, povinna zaplatit druhé Smluvní straně smluvní pokutu ve výši 100 000,- Kč za každé jednotlivé prokázané porušení povinnosti.

3.13 Vznikem povinnosti platit smluvní pokutu ani jejím skutečným zaplacením nezaniká povinnost Smluvních stran splnit povinnost, jejíž plnění bylo zajištěno smluvní pokutou.

3.14 Smluvní pokuty jsou splatné do 30 kalendářních dnů po obdržení vyúčtování smluvní pokuty na základě samostatné faktury.

C. Součinnost, další práva a povinnosti a kontaktní osoby

3.15 Smluvní strany se zavazují vzájemně spolupracovat a poskytovat si součinnost nezbytnou pro řádné naplnění předmětu této Smlouvy. Smluvní strany jsou povinny informovat bezodkladně druhou Smluvní stranu o veškerých skutečnostech, které jsou nebo mohou být důležité pro řádné plnění dle této Smlouvy.

Součástí nezbytné součinnosti ze strany Objednatele je zajištění licencí uvedených v Příloze č. 5 této Smlouvy. V případě neposkytnutí součinnosti není Zhotovitel v prodlení.

3.16 V rámci řádného plnění předmětu Smlouvy mají obě Smluvní strany zejména následující práva a povinnosti:

3.16.1 vzájemně spolupracovat a poskytovat si veškeré informace potřebné pro řádné plnění svých závazků vyplývajících z této Smlouvy;

3.16.2 neprodleně informovat druhou Smluvní stranu o vzniku nebo hrozícím vzniku překážky mající významný vliv na řádné a včasné plnění dle této Smlouvy;

3.16.3 poskytovat druhé Smluvní straně úplné, pravdivé a včasné informace o veškerých skutečnostech, které jsou nebo mohou být důležité pro řádné plnění dle této Smlouvy;

3.16.4 plnit své závazky vyplývající z této Smlouvy tak, aby nedocházelo k prodlení s plněním a splatností jednotlivých peněžních závazků;

3.17 V souvislosti s prováděním Díla má Objednatel zejména následující práva a povinnosti:

3.17.1 vytvářet předpoklady pro plnění závazků vyplývajících z této Smlouvy tak, aby mohly být splněn termín realizace Díla a je povinen po celou dobu

účinnosti Smlouvy udržovat v platnosti licence, souhlasy, povolení a další oprávnění Poskytnuté Objednatelem Zhotoviteli za účelem realizace Díla a v souvislosti s ní;

3.17.2 poskytovat požadované podklady a informace nezbytné pro realizaci Díla Zhotoviteli, průběžně zajišťovat řádnou a včasnou spolupráci a součinnost třetích stran, např. další dotčené subjekty, a to zejména koncoví uživatelé

3.17.3 řádné a včasné předávání potřebných nebo Zhotovitelem vyžádaných dokumentů, předpisů, informací, rozhodnutí, specifikací požadavků a dalších podkladů souvisejících s realizací Díla a nezbytných pro realizaci Díla;

3.17.4 písemně se řádně a včas vyjadřovat k předkládaným materiálům;

3.17.5 poskytovat řádnou a včasnou součinnost při předávání Díla, včetně písemného oznamování vad a nedodělků Díla bránících převzetí Díla;

3.17.6 poskytovat konzultace současného stavu, upřesňovat požadavky a zadání v průběhu realizace Díla.

3.16.5 zajistit přístup ke stávajícímu hardware a software prostředí, které není předmětem Díla dle této Smlouvy, avšak je nezbytné pro realizaci plnění, pokud této povinnosti nebudou bránit smluvní vztahy uzavřené Objednatelem s třetí stranou, přičemž se v tomto případě zavazuje k maximální součinnosti směřující k zajištění tohoto přístupu.

3.16.6 umožnit Zhotoviteli přístup do objektů, k zařízení, k programovému vybavení, databázím a informačním systémům Objednatele v rozsahu nezbytném pro řádné provedení Díla dle této Smlouvy dle vzájemně schválených postupů.

3.16.7 Objednatel je oprávněn kontrolovat způsob provádění Díla za účelem ověření souladu s podmínkami stanovenými Smlouvou.

3.18 V souvislosti s plněním předmětu Smlouvy má Zhotovitel zejména následující práva a povinnosti:

3.18.1 postupovat při plnění Smlouvy řádně tak, aby bylo dosaženo účelu Smlouvy;

3.18.2 zajistit dostatečnou kapacitu svých pracovníků s odpovídající kvalifikací;

3.18.3 poskytovat bezplatnou záruku za jakost na Objednatelem reklamované závady po dobu trvání záruční lhůty;

3.19 Zhotovitel je povinen plnit zadání a/nebo příkazy Objednatele, přitom je však povinen písemně upozornit Objednatele na nevhodnost jím udělených zadání a/nebo příkazů, jestliže tuto nevhodnost je schopen zjistit při vynaložení veškeré potřebné péče. Zhotovitel v písemném upozornění stanoví Objednateli přiměřenou lhůtu, která nesmí být kratší než 10 pracovních dní, ve které je Objednatel povinen Zhotoviteli sdělit, zda na svém zadání a/nebo příkazu trvá.

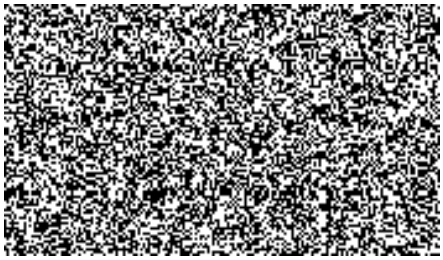
Uplynutím této lhůty se má za to, že Objednatel na svém zadání a/nebo příkazu trvá; v takovém případě je Zhotovitel oprávněn od Smlouvy odstoupit.

3.20 V případě prokazatelného prodlení povinné Smluvní strany s poskytnutím součinnosti není oprávněná Smluvní strana v prodlení s plněním svých závazků podle Smlouvy a veškeré lhůty se o prokazatelné prodlení povinné Smluvní strany prodlužují; to neplatí v případech, kdy prodlení v poskytnutí součinnosti ze strany povinné Smluvní strany bylo vyvoláno v přímé příčinné souvislosti s prokazatelným neposkytnutím součinnosti nebo prodlením ze strany oprávněné. Objednatel je v prodlení, jestliže v rozporu se svými povinnostmi vyplývajícími ze smluvního vztahu, nepřevezme řádně nabídnuté plnění nebo neposkytne součinnost nutnou k tomu, aby Zhotovitel mohl splnit svůj závazek. Zhotovitel je v prodlení, jestliže v rozporu se svými povinnostmi vyplývajícími ze smluvního vztahu, nepředá řádné a bezvadné plnění nebo neposkytne součinnost nutnou k tomu, aby Objednatel mohl splnit svůj závazek.

3.21 Kontaktními osobami jsou:

Za Zhotovitele:
Mail:
Tel:

Za Objednatele:
Mail:
Tel:



D. Odpovědnost za škodu

3.22 Škody, které prokazatelně vzniknou v příčinné souvislosti s činností Zhotovitele či Objednatele dle této Smlouvy, se Smluvní strany zavazují zaplatit druhé Smluvní straně na základě samostatné faktury mající náležitosti daňového dokladu. Podmínky pro uplatnění nároku na náhradu škody a vystavení příslušného daňového dokladu se řídí příslušnými ustanoveními Rámcové smlouvy.

3.23 Zhotovitel je oprávněn provést Dílo samostatně nebo i prostřednictvím poddodavatele, přičemž takto zhotovené Dílo se posuzuje jako by jej Zhotovitel provedl sám. Zhotovitel odpovídá za způsobenou škodu rovněž v případě, že část Díla bude provedena prostřednictvím poddodavatele.

3.24 Žádná Smluvní strana není povinna k náhradě škody, prokáže-li, že jí ve splnění povinnosti z této Smlouvy nebo Rámcové smlouvy dočasně nebo trvale zabránila mimořádná nepředvídatelná a nepřekonatelná překážka vzniklá nezávisle na její vůli ve smyslu ustanovení § 2913 odst. 2 Občanského zákoníku. Smluvní strany se zavazují k vyvinutí maximálního úsilí k odvrácení a překonání výše uvedených překážek.

3.25 Brání-li některé ze Smluvních stran v plnění povinností mimořádná nepředvídatelná a nepřekonatelná překážka vzniklá nezávisle na její vůli ve smyslu ustanovení § 2913 odst. 2 Občanského zákoníku, je Smluvní strana povinna o vzniku, důsledcích, povaze a zániku takové překážky druhou Smluvní stranu neprodleně informovat. Zpráva musí být podána písemně, neprodleně

poté, kdy se povinná Smluvní strana o překážce dozvěděla, nebo při náležité péči mohla dozvědět. Bezprostředně po zániku takové překážky povinná Smluvní strana obnoví plnění svých závazků vůči druhé Smluvní straně a učiní vše, co je v jejích silách, ke kompenzaci doby, která uplynula v důsledku takového prodlení. Pokud překážka nepomine do 3 pracovních dnů od doby svého vzniku, oprávnění zástupci obou Smluvních stran se sejdou za účelem projednání dalšího postupu při plnění závazků vyplývajících ze Smlouvy.

3.26 Smluvní strany se zavazují, že vždy před uplatněním nároku na náhradu škody písemně vyzvou povinnou Smluvní stranu k jednání o způsobu stanovení výše škody, a to bez zbytečného odkladu poté, kdy se oprávněná Smluvní strana prokazatelně dozví o vzniku škodní události.

3.27 Smluvní strany se dohodly, že povinnost Zhotovitele k náhradě škody (újmy) je limitována výší pojistky sjednané na základě Smlouvy č. 899-24250-13 o pojištění majetku podnikatelů (pojištění živelní, pojištění odcizení) o pojištění odpovědnosti ze dne 4. 1. 2017 Toto omezení se neuplatní u těch nároků, u nichž § 2898 Občanského zákoníku limitaci výše škody (újmy) neumožňuje.

Článek 4
Závěrečná ustanovení

4.1 Veškerá ujednání této Smlouvy navazují na Rámcovou smlouvu a Rámcovou smlouvou se řídí, tj. práva, povinnosti či skutečnosti neupravené v této Smlouvě se řídí ustanoveními Rámcové smlouvy. V případě, že ujednání obsažené v této Smlouvě se bude odchylovat od ustanovení obsaženého v Rámcové smlouvě, má ujednání obsažené v této Smlouvě přednost před ustanovením obsaženým v Rámcové smlouvě, ovšem pouze ohledně plnění sjednaného touto Smlouvou. V otázkách touto Smlouvou neupravených se použijí ustanovení Rámcové smlouvy.

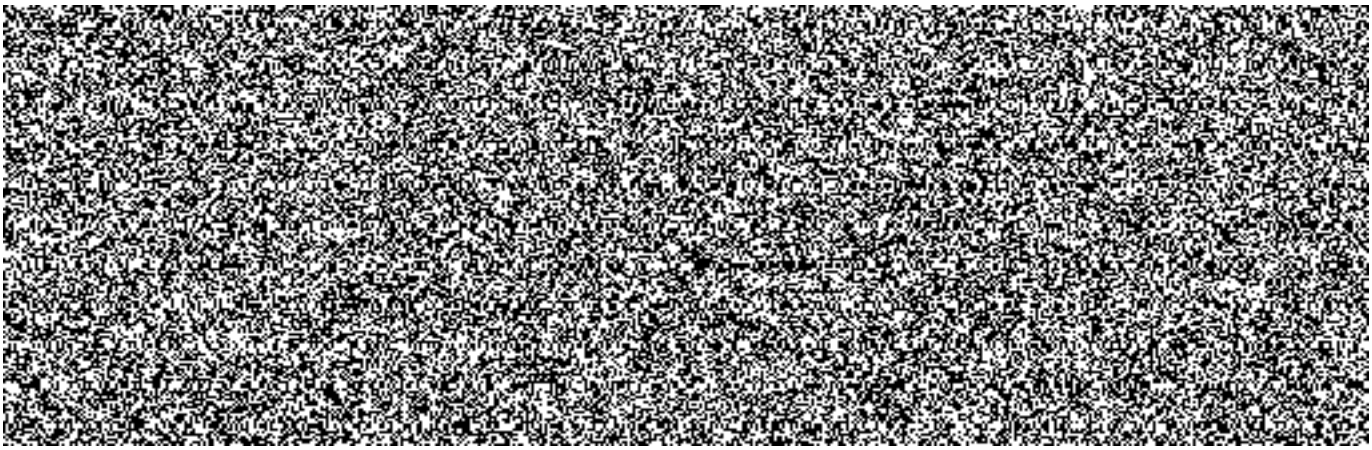
4.2 Smluvní strany prohlašují, že tato Smlouva ve spojení s Rámcovou smlouvou a jejími přílohami vyjadřuje jejich úplné a výlučné vzájemné ujednání týkající se daného předmětu této Smlouvy. Smluvní strany po přečtení této Smlouvy prohlašují, že byla uzavřena po vzájemném projednání, určitě a srozumitelně, na základě jejich pravé, vážně míněné a svobodné vůle. Na důkaz uvedených skutečností připojují podpisy svých oprávněných osob či zástupců.

4.3 Tato Smlouva vstupuje v platnost dnem podpisu oběma Smluvními stranami a účinnost dnem zveřejnění v registru smluv v souladu se zák. č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv) ve znění pozdějších předpisů.

4.4 Tato Smlouva je vyhotovena ve čtyřech stejnopisech, z nichž dvě vyhotovení obdrží Objednatel a dvě Zhotovitel.

4.5 Nedílnou součástí této Smlouvy jsou přílohy:
a) Příloha č. 1 – Specifikace Díla
b) Příloha č. 2 – Akceptační protokol
c) Příloha č. 3 – Předávací protokol
d) Příloha č. 4 - Klasifikace vad a nedodělků

e) Příloha č. 5 - Specifikace licencí dodaných MV



Příloha č. 1 – Specifikace Díla

1. Úvod

Informační systém „Dohledové centrum eGovernmentu (dále jen DCeGOV)“ je určen jako součást kritické informační infrastruktury státu, jako informační systém kritické informační infrastruktury podle §2 odst b), zákona 181/2014 Sb.

Pro jeho správce a provozovatele vyplývají povinnosti, dané platnou legislativou v oblasti kybernetické bezpečnosti, především podle zákona 181/2014 Sb., o kybernetické bezpečnosti (dále jen ZoKB) a vyhlášky 82/2018 Sb., o kybernetické bezpečnosti.

Především vyhláška o kybernetické bezpečnosti určuje, jaká bezpečnostní opatření musí být zavedena.

2. 802.1x ověření do sítě

Pro připojení pracovních stanic na [redacted] jsou nyní použity 3 kusy přepínačů [redacted] Porty těchto přepínačů jsou rozvedeny strukturovanou kabeláží do jednotlivých kanceláří [redacted] Pro zabránění neautorizovaného přístupu do sítě LAN bude implementována autentizace do sítě standardem 802.1x. Autentizace standardem 802.1x se skládá z následujících základních komponent:

1) Autentizační server – RADIUS server v doméně DCeGOV
2) Authenticator – Přepínače [redacted]
3) Supplicant – Součástí Windows 10 na připojovaných pracovních stanicích

Mimo výše uvedených komponent nutných pro zprovoznění autentizace do sítě standardem 802.1x, je nutné definovat způsob ověřování uživatelů, způsob ověřování pracovních stanic, na kterých není uživatel přihlášen, mapování jednotlivých uživatelů do LAN sítí a způsob připojení do sítě pro zařízení, která neumožňují autentizaci do sítě standardem 802.1x.

V rámci LAN sítí v [redacted] existuje následující rozdělení:

Celkový přidělený rozsah IP [redacted]

Číslo VLAN	Označení	IP adresace	Poznámka
[redacted]			Instalační a startovací síť. Pracovní stanice bez přihlášeného uživatele.
			Síťový management. Nemá fyzický port, 802.1x není použito.
			Síť podpůrných služeb - Tiskárny MAC auth bypass
			Náhledové nástroje – Autentizace pracovní stanice **only**
			HelpDesk + Produkční dohled – Nutná autentizace klienta
			Bezpečnostní dohled – Nutná autentizace klienta
			Hlasové služby – Port Security na MAC adresu telefonu
			Krizové pracoviště SPCSS – Nutná autentizace klienta
			VLAN pro stanice, které neprošli autentizací.

Z jednotlivých sítí jsou definovány prostupy na Firewallu do ostatních sítí. Soupis dostupných zdrojů, z jednotlivých VLAN, jsou specifikovány v kapitole 2. Uživatelé, pracovní stanice a ostatní zařízení budou vždy autentizovány do jedné z výše uvedených LAN sítí. Politika přiřazení uživatele do VLAN bude definována na Microsoft NAP serveru (RADIUS), který je součástí domény DCeGOV.

Na Active Directory serverech domény DCeGOV je nutné vydefinovat security skupiny, které budou obsahovat uživatele dle jejich oprávnění.

2.1. Autentizace do sítě

Jednotlivé LAN sítě v 7. patře Olšanské 4 jsou zapojeny různá zařízení a každé zařízení nabízí rozdílné možnosti autentizace do datové sítě, případně neumožňují autentizaci do datové sítě. Pro korektní fungování autentizace standardem 802.1x musí být na zařízení takzvaný „supplicant“, který zabezpečuje autentizaci.

1) Pracovní stanice (PC, notebooky nebo servery s operačním systémem a supplicantem)
    a. Autentizace stanice (na stanici není přihlášen uživatel)
    b. Autentizace uživatele (po přihlášení do stanice)
2) IP telefony
    a. VoIP VLAN
3) Tiskárny a další zařízení bez 802.1x supplicanta
    a. MAC-Auth-bypass

Pro autentizaci do sítě se bude primárně používán protokol PEAP s MS-CHAPv2. Pro použití protokolu PEAP je nutné na NPS server nainstalovat certifikát, kterým se bude NPS server prokazovat klientům. Certifikát pro NPS server bude podepsán Certifikační autoritou CMS a je nutné zabezpečit důvěryhodnost CMS CA na stanicích připojených do domény DCeGOV. PEAP protokol zabezpečí bezpečný šifrovaný tunel, mezi klientem a NPS serverem, přes který jsou zaslány autentizační údaje (uživatelské jméno a heslo).

Pro zařízení, která nepodporují 802.1x (nemají supplicant) je nutné zavést MAC-Authentication bypass, který zabezpečí, že zařízení bude do sítě autentizováno svojí MAC adresou. Tyto zařízení je proto nutné zavést do AD, jako uživatele bez oprávnění. Při použití MAC authentication bypass je jako uživatelské jméno a heslo použita MAC adresa zařízení, která je odeslána na NPS server protokolem PAP.

Výchozí nastavení portů na přepínačích

Ve výchozím nastavení bude mít přepínač všechny porty nastaveny do Guest VLAN. Guest VLAN je slepá síť, z které není možné se kamkoli dostat.

Autentizace pracovní stanice nebo uživatele

Po připojení pracovní stanice do přepínače [redacted] je z přepínače (Authenticator) vyžádána autentizace. Pokud na pracovní stanici není připojen uživatel, bude se pracovní stanice prokazovat účtem stanice, který je přidělen stanici z ActiveDirectory (computer authentication). Po přihlášení uživatele proběhne re-autentizace s uživatelským jménem a heslem uživatele. Uživatel nemusí zadávat své přístupové údaje explicitně pro přihlášení do sítě, neboť OS Windows 10 předloží jeho přihlašovací údaje použité pro přihlášení na pracovní stanici (Single-Sign-On).

Po úspěšné autentizaci, uživatele nebo stanice, je port na přepínači přiřazen do VLAN, kterou vrátí RADIUS server v odpovědi s informací, zda je uživatel/stanice autentizována nebo zamítnuta. V případě zamítnutí přístupu do sítě bude stanice/port zařazena to Guest VLAN.

Autentizace IP telefonu

[redacted] je implementována IP telefonie s telefony [redacted] Telefony mají Ethernet přepínač, který umožňuje 802.1x pass-through. Stanice připojená za IP telefon je možné stále autentizovat do sítě protokolem PEAP s MS-CHAPv2 jako standartní pracovní stanici/uživatele. V případě zamítnutí přístupu do sítě bude zařízení, připojené za IP telefonem, zařazeno to Guest VLAN.

Autentizace zařízení bez podpory 802.1x

Pro zařízení, která nepodporují 802.1x autentizaci bude použita metoda MAC-Authentication bypass. V případě, kdy zařízení připojené do sítě neodpovídá na výzvy k autentizaci, vyplní přepínač (Authenticator) jako uživatelské jméno a heslo MAC adresu připojeného zařízení. Po úspěšné autentizaci zařízení je port na přepínači přiřazen do VLAN, kterou vrátí RADIUS server v odpovědi s informací, zda je zařízení autentizováno nebo zamítnuto. V případě zamítnutí přístupu do sítě bude zařízení zařazeno to Guest VLAN.

2.2. Autentizační server

Pro autentizaci uživatelů bude použitý MS NAP server, který je součástí domény DCeGOV. Pro komunikaci mezi přepínači (Authenticator) a NAP serverem bude použitý AAA protokol RADIUS.

Parametry pro připojení k NPS serverům DCeGOV:

IP adresa MS NPS server DC1: [redacted]
IP adresa MS NPS server DC2:
Port pro autentizaci: UDP 1812
Port pro autorizaci: UDP 1813

Pro zabezpečenou komunikaci mezi NPS serverem a přepínačem ověřujícím uživatele je nutné na NPS servery (RADIUS) přidat každý přepínač jako klienta a nastavit „pre-shared-key“.

Po přidání RADIUS klientů je nutné na NPS serveru nastavit „network policies“. Pro každou uživatelskou skupinu, je nutné nastavit samostatnou network policy. Pro každou policy bude na straně AD vytvořena skupina ve formátu ACL_NET_XXX (tedy ACL_NET_CON, ACL_NET_SRV, atd.)

Network policy name	AD Group	Athentication methods	Tunnel-Pvt-Group-ID
[redacted]	[redacted]	PEAP s MS-CHAPv2	[redacted]
		PAP (MAC-Authentication Bypass)	
		PEAP s MS-CHAPv2	
		PEAP s MS-CHAPv2	
		PEAP s MS-CHAPv2	

[illegible]	PEAP s MS-CHAPv2	[illegible]
	PEAP s MS-CHAPv2	

Další RADIUS atributy stejné pro všechny policy:

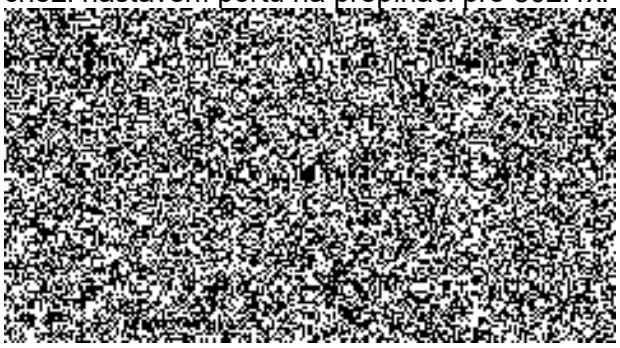
Tunnel-Medium-Type = 802 (Includes all 802 media plus Ethernet canonical format)
Tunnel-Type = Virtual LANs (VLAN)

2.3. Přístupový přepínač

Přístupový přepínač funguje v 802.1x autentizaci jako Authenticator, který vyzívá připojená zařízení k autentizaci a povoluje nebo omezuje přístup do sítě. Přístupový přepínač je klientem NPS (RADIUS) serveru. Komunikace s NPS servery bude probíhat po standardních portech určených pro RADIUS komunikaci UDP 1812/1813.

IP adresa přepínače: 10.71.126.36

Výchozí nastavení portů na přepínači pro 802.1x:



Mimo nastavení autentizace bude na portu přepínače nastavena port security dle popisu v dokumentu „Implementace síťového nastavení pro doménu DCeGOV“.

3. Active Directory

3.1. Admin Rights Assignment

Oprávnění bude rozdělené na níže uvedené skupiny, které budou mít rozdílná oprávnění s rozdílnou delegací.

- Domain Admins

  Tato skupina Administrátorů bude vlastnit oprávnění „Domain Admins“ a bude sloužit pro správu Active Directory (dále jen „AD“). Tato skupina bude defaultně distribuována na všechna doménová zařízení s oprávněním lokálních Administrátorů.

- Enterprise Admins

  Tato skupina Administrátorů bude sloužit pro správu AD forestu a jeho trustů. Defaultně je tato skupina prázdná, toto oprávnění „Enterprise Admins“ bude přiděleno jen v případě konfigurací toto oprávnění vyžadujících, po ukončení konfigurací bude oprávnění opět odebráno. Oprávnění bude přidělováno procesem Change managementu po odsouhlasení změnovou komisí a vlastníkem systému.

- Schema Admins

  Tato skupina Administrátorů bude sloužit pro správu AD schématu. Defaultně je tato skupina prázdná, toto oprávnění „Schema Admins“ bude přiděleno jen v případě konfigurací toto oprávnění vyžadujících, po ukončení konfigurací bude oprávnění opět odebráno. Oprávnění bude přidělováno procesem Change managementu po odsouhlasení změnovou komisí a vlastníkem systému.

- Server Admins

  Tato skupina bude delegovat oprávnění správcům serverů v AD vyjma doménových kontrolerů. Všichni správci serverů v AD budou mít oprávnění lokálních Administrátorů. Zároveň budou moci připojovat / registrovat a odebírat servery do a z AD domény. Server Administrátoři se nebudou moci hlásit na počítače.

- Workstation Admins

  Tato skupina bude delegovat oprávnění správcům počítačů v AD. Všichni správci počítačů v AD budou mít oprávnění lokálních Administrátorů na doménových počítačích. Zároveň budou moci připojovat / registrovat a odebírat pracovní stanice do a z AD domény. Workstation Administrátoři se nebudou moci hlásit na servery.

- SQL Admins

  Tato skupina bude delegovat oprávnění správcům SQL v AD. Všichni správci SQL v AD budou mít oprávnění lokálních Administrátorů na serverech hostujících SQL Server. Zároveň budou mít sysadmin oprávnění na všech SQL instancích.

- SCOM Admins

  Tato skupina bude delegovat oprávnění správcům SCOM. Všichni správci SCOM budou mít oprávnění lokálních Administrátorů na management serverech. Zároveň budou mít oprávnění nad SCOM aplikací.

- SCCM Admins

Tato skupina bude delegovat oprávnění správcům SCCM. Všichni správci SCCM budou mít oprávnění lokálních Administrátorů na site serverech. Zároveň budou mít oprávnění nad SCCM aplikací.

- Network Admins

Tato skupina bude delegovat oprávnění správcům síťových prvků ověřovaných přes RADIUS v AD. Všichni správci síťových prvků budou mít oprávnění provádět konfigurace na těchto prvcích.

U klíčových skupin administrátorů budou vytvořeny recovery účty, tyto účty budou mít nastaveno silné heslo a přihlašovací údaje budou bezpečně uloženy a vydávány oproti podpisu na základě oprávněného požadavku. Na straně MV budou přihlašovací údaje uloženy v trezoru u manažera kybernetické bezpečnosti a na straně NAKIT v trezoru odboru Informační bezpečnost a BCM. Expirace hesla a jejich obtížnost u těchto účtů bude nastavena dle kapitoly politiky hesel.

3.2. Návrh skupin správců

Níže uvedená tabulka specifikuje základní AD skupiny, které rozdělují oprávnění dle výše uvedených bodů.

AD Group Name	Descriptions
Domain Admins	Správci AD domény
Enterprise Admins	Správci AD forestu
Schema Admins	Správci AD schématu
Server Admins	Správci Serverů
Workstation Admins	Správci počítačů
SQL Admins	Správci SQL serverů
SCOM Admins	Správci SCOM
SCCM Admins	Správci SCCM
Network Admins	Správci sítí

Tabulka 1 - Návrh skupin správců

3.3. Návrh správců

Níže uvedená tabulka specifikuje konkrétní AD účty.

SamAccountname	Display Name	Members	Recovery účty	Status
da_ %SamAccountName%	%LastName% %FirstName% DA	Domain Admins	NE	Enabled

srv_ %SamAccountName%	%LastName% %FirstName% SRV	Domain Users Server Admins Local Administrators (na Serverech vyjma DC)	NE	Enabled
adm_ %SamAccountName%	%LastName% %FirstName% ADM	Domain Users Workstation Admins Local Administrators (na Počítačích)	NE	Enabled
net_ %SamAccountName%	%LastName% %FirstName% NET	Domain Users Network Admins	NE	Enabled
[redacted]	[redacted]	Domain Admins	ANO	Enabled
		Domain Admins	ANO	Enabled

Tabulka 2 - Návrh konkrétních AD účtů

3.4. Politika hesel

Politika hesel bude určená všem správcům a uživatelům AD, přičemž s ohledem na bezpečnost domény vymezuje, jakým způsobem se budou hesla vytvářet a využívat.

Bezpečnostní požadavky na hesla musí být mimo jiné, v souladu s požadavky § 19, Správa a ověřování identit, vyhlášky 82/2018 Sb., o kybernetické bezpečnosti.

Pro ověřování identity uživatelů administrátorů a aplikací je vyžadován více faktorový autentizační mechanizmus s minimálně dvěma různými typy faktorů. Dočasně bude používána autentizace pomocí login a heslo s vynuceným pravidlem síly hesla, která je uvedena dále.

Součástí politiky hesel jsou níže definovaná pravidla, která zajistí základní ochranu proti útokům typu „Brute force“.

3.4.1 Enforce Password history

Tato politika zajišťuje historii zvolených hesel a tím pádem je schopná zabránit jejich opakování.

Tato politika bude nastavená na hodnotu [redacted] hesel.

3.4.2 Maximum Password age

Tato politika nastavuje maximální stáří hesla.

Expirace hesla bude nastavená na [redacted] U recovery účtů nebude nastavena expirace

3.4.3 Minimum Password age

Tato politika nastavuje minimální stáří hesla, tedy minimální možnou dobu, po které bude možné provést změnu hesla.

Tato politika bude nastavená na hodnotu jednoho dne.

3.4.4 Minimum Password length

Tato politika nastavuje délku hesla.

Tato politika bude nastavená na hodnotu minimálně [redacted] u uživatelů a minimálně [redacted] u administrátorů a aplikací. U recovery účtů bude délka minimálně [redacted]

3.4.5 Passwords must meet Complexity Requirements

Tato politika vynucuje složitost hesla. Během zadávání hesla budou vyžadované níže uvedené prerekvizity.

[redacted]

3.4.6 Account Lockout treshold

V případě, že dojde k překročení povolených chyb, bude uživatelský účet zamčen. Hodna bude nastavená na pět možných chyb.

3.4.7 Account Lockout duration

V případě, že dojde k překročení povolených chyb během přihlášení, politika zajistí zakázaní uživatelského účtu na [redacted]

3.4.8 Reset Account Lockout counter after

Tato politika udává dobu, ve které se resetuje počítadlo neúspěšných hesel. S ohledem na „best practices“ společnosti Microsoft, bude tato politika nastavená na stejnou hodnotu, jako politika „Account Lockout Duration“, tedy na hodnotu [redacted]

3.5. Napojení resortu na doménu DCeGOV

V rámci propojení domén bude realizován jednostranný trust s [redacted] Zajištění ověřování uživatelů z ostatních domén resortu MV a domény DCeGOV bude nutné řešit individuálně.

3.6. 802.1x

Pro potřeby ověřování přístupu zařízení a uživatelů do sítí DCeGOV v lokalitě [redacted] je nutné provést úpravy v rámci Active Directory.

3.6.1 Přístupové skupiny

V následujícím umístění [redacted] budou vytvořené skupiny ACL_NET_XXX, kde XXX je zkratka z označení VLANy. Tyto skupiny budou rozlišovat přístupová oprávnění uživatelů. Každý uživatel smí být členem pouze jedné z těchto skupin, aby byl mechanismus funkční. Další podrobnosti jsou uvedeny v kapitole 2. zaobírající se problematikou 802.1x

3.6.2 Skupinová politika

V doméně bude doplněna politika pro aktivaci podpory 802.1x na stanicích a nastavení potřebné pro správný chod této technologie. Tato politika bude aplikovaná na [redacted] kde se nacházejí všechny uživatelské pracovní stanice.

3.6.3 Nedoménová zařízení

Všechna zařízení používaná v rámci DCeGOV nepodporují technologii autentizace 802.1x z tohoto důvodu bude použita metoda MAC-Authentication bypass, jak je uvedeno v kapitole 2. Z tohoto důvodu budou v AD vytvořeny objekty těchto zařízení v následujícím

umístění  Objekt bude obsahovat informace o typu zařízení, výrobním čísle a pro potřeby metody MAC-Authentication bypass bude v atributu networkAddress evidována MAC adresa zařízení.

3.7. Audit policy

Servery budou mít nastaveno audit policy dle požadavků na KIS/VIS

4. Dohledová síť a prostupy do ostatních sítí

[redacted]
Je počítáno s minimálně [redacted] rozsahem síťového segmentu.
Jako firewall budeme využívat [redacted] který zajistí prostupy do ostatních sítí (tabulky níže s jednotlivými IP).

4.1. Aktuální stav

Rozsah [redacted] síti [redacted]
NAT do produkční sítě je prováděn 1:1 na [redacted]

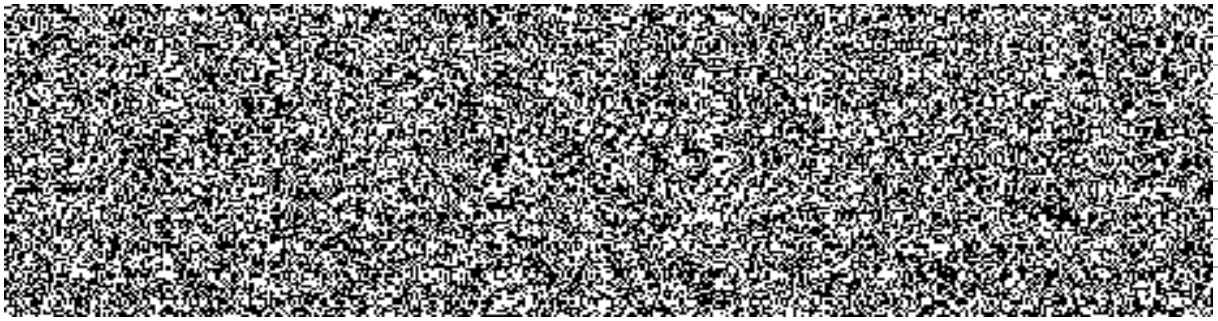
4.1.1 LAN a VPN

4.1.1.1. Funkční přístupy do provozního prostředí z LAN:

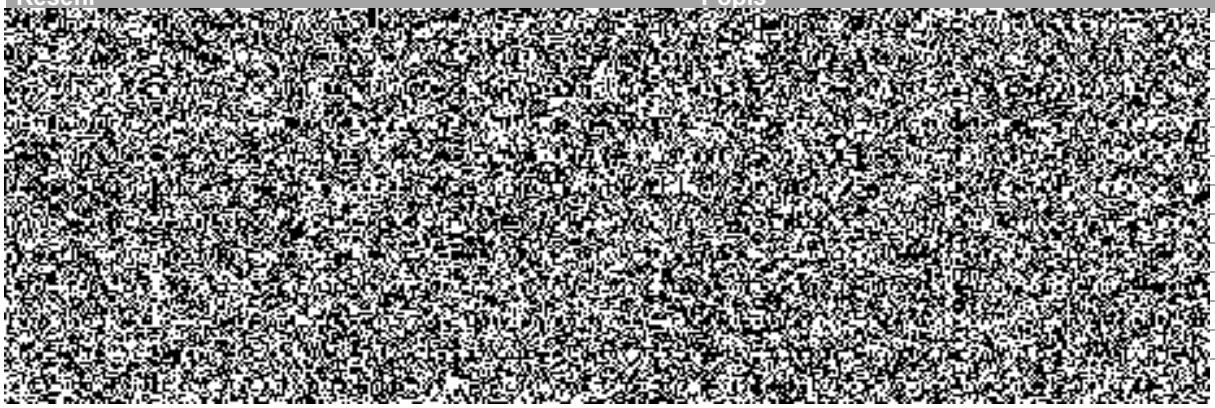
Řešení	Popis
[redacted]	

4.1.1.2. Funkční přístupy do provozního prostředí z VPN:

Řešení	Popis
[redacted]	



4.1.1.3. Funkční přístupy do OOB (pouze weby http(s)):

Řešení	Popis
	

4.2. Cílové nastavení sítí

4.2.1 Testovací LAN síť

V rámci přípravy a budování nové AD domény a její sítě, je v rámci projektu nutné vytvořit novou síť a novou síť propojit na Firewall dohledové sítě. Nová síť bude VLAN na aktuálně užívaném zařízení pro potřeby dohledového centra (3x zapojené ve stacku, která je nyní připojena do. Jako firewall nové sítě bude použit dosavadní firewall dohledové sítě. Po plném zprovoznění nové sítě (VLAN a propojení na Firewall) a jejím otestování budou přepínače, užívané pro potřeby dohledového centra, odpojeny od a plně nastaveny pro provoz v rámci nové sítě, která bude součástí dohledové sítě na.

4.2.2 Fyzické připojení na Firewall dohledových sítí

K přepínači je připojen Firewall který bude využitý jako výchozí brána pro všechny VLAN sítě v Firewall budou současně zajišťovat bezpečnost nových sítí proti přístupu z externích lokalit.

Pro zapojení osobních počítaču a dalších nástrojů bude v využito tří přepínačů, které jsou zapojené ve stacku a jmenují se. Pro připojení na Firewall je nutné vytvořit nové fyzické propojení mezi přepínači a přepínači dohledové sítě.

Propojení bude realizováno dvěma spoji o rychlosti 1Gbps, které budou zapojené do link agregace. 1GE SFP Multimode dodá oddělení „přenosové technologie“.

	DC3SWM02	SQLS09
		

Přepinač [redacted] je nyní zapojen v [redacted] a po kompletním přepojení všech stanic a nástrojů do nových sítí bude přepínač [redacted] odpojen z [redacted] a bude spravován v management síti [redacted]

4.2.3 Použité VLAN

Pro sítě v [redacted] budou použity [redacted] Tyto VLAN ID nejsou v [redacted] používány, takže je možné nastavit tyto VLAN na řepínači [redacted] bez ovlivnění [redacted]

4.2.4 Výchozí nastavení VLAN na přepínači

V rámci testování bude využita [redacted] Testovací VLAN. V této VLAN budou prvotně otestovány všechny prostupy a následně po jejich odladění dojde k vytvoření/využití dalších VLAN. Jednotlivá PC pak budou rozdělena do VLAN dle oprávnění jednotlivých uživatelů. Testovací VLAN bude vytažena na porty switche [redacted]

Při zavedení 802.1x dojde k úprave nastavení tak, že všechny porty přepínače budou nastaveny do výchozí VLAN sítě [redacted] Přepojeni uživatele do definované VLAN dojde až na základě úspěšné autentizace.

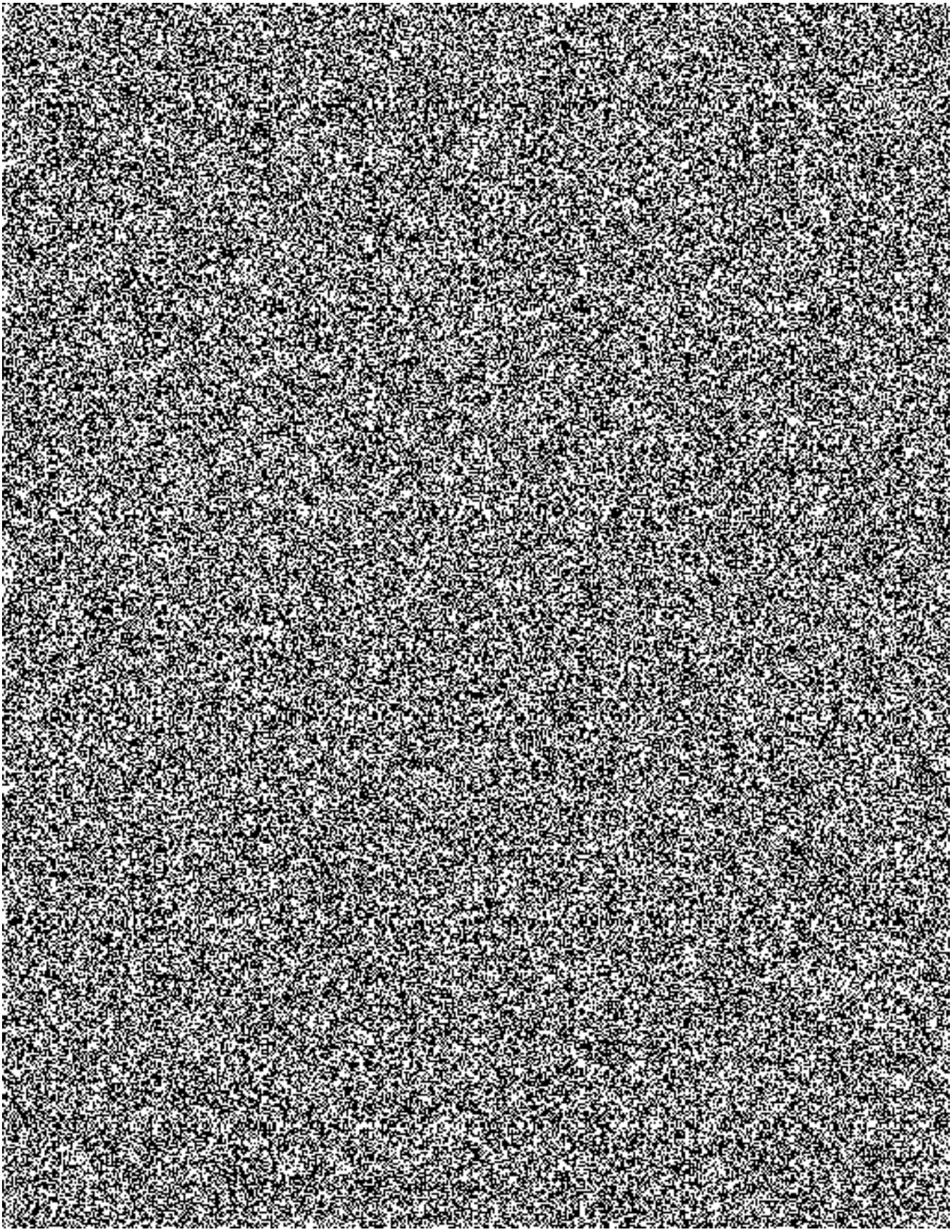
4.2.5 Výsledné rozdělení VLAN dohledové centrum

IP rozsah pro novou LAN je [redacted]

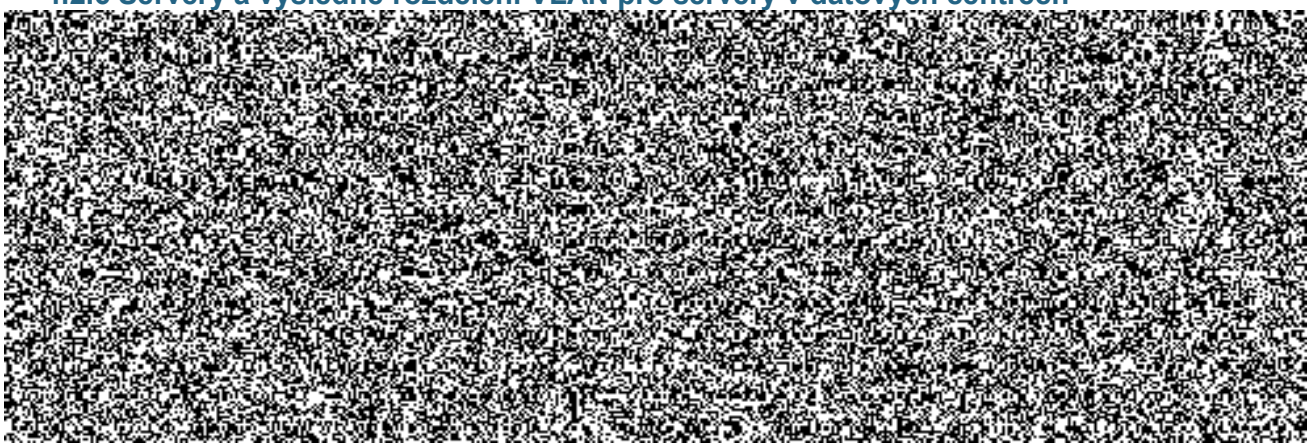
Číslo VLAN	Označení	IP adresace	Poznámka
[redacted]			Instalační a startovací síť
			Síťový management
			Síť podpůrných služeb
			Náhledové nástroje
			HelpDesk + Produkční dohled
			Bezpečnostní dohled
			Hlasové služby
			Krizové pracoviště SPCSS
			VLAN pro stanice, které neprošly autentizací.

Všechny sítě budou zakončeny na firewallu, níže jsou uvedeny jednotlivé vazby:

[redacted]

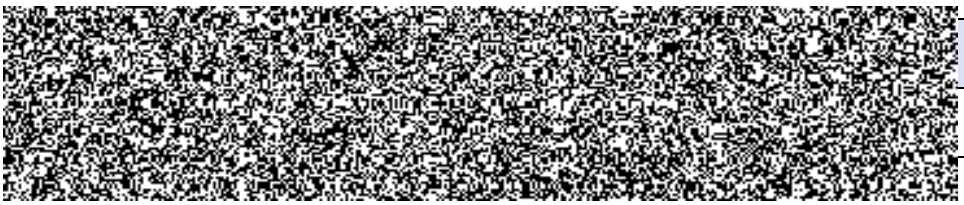


4.2.6 Servery a výsledné rozdělení VLAN pro servery v datových centrech



4.2.6.1. Rozdělení serverů do jednotlivých VLAN

Server	VLAN name	VLAN	Poznámka
			Hyper-v host
			Hyper-v host
			Hyper-v host
			Hyper-v host
			Terminal server
			Terminal server
			SQL
			SQL
			File server
			File server
			System Center Operation Manager
			System Center Operation Manager
			Domain controler, DNS, NTP
			Domain controler, DNS, NTP
			DHCP
			DHCP
			Radius server
			Radius server
			System Center Configuration Manager, WSUS, SCEP (endpoint protection)
			System Center Configuration Manager, WSUS, SCEP (endpoint protection)



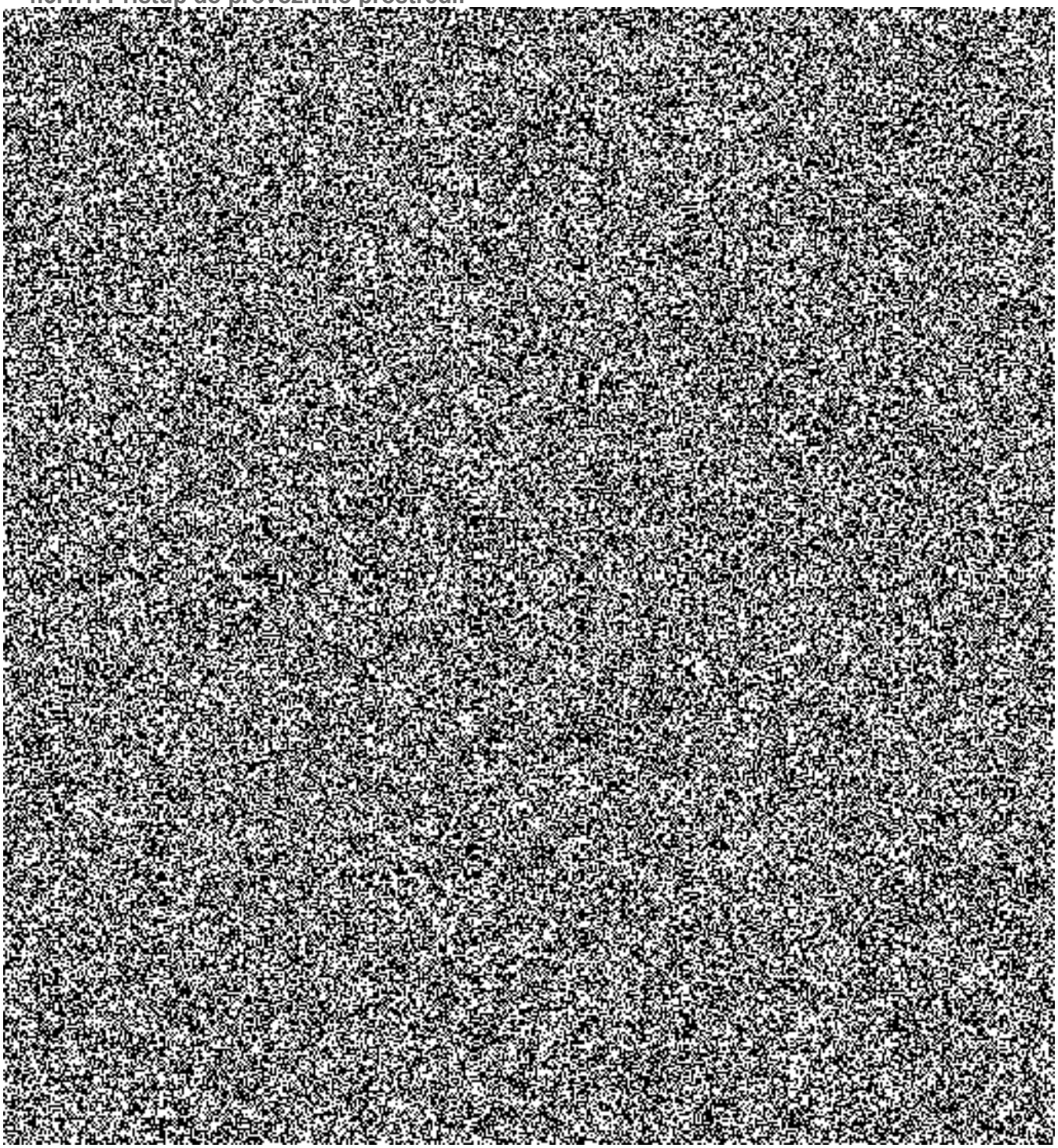
Key Management Service, licenční služba pro TS
Key Management Service, licenční služba pro TS

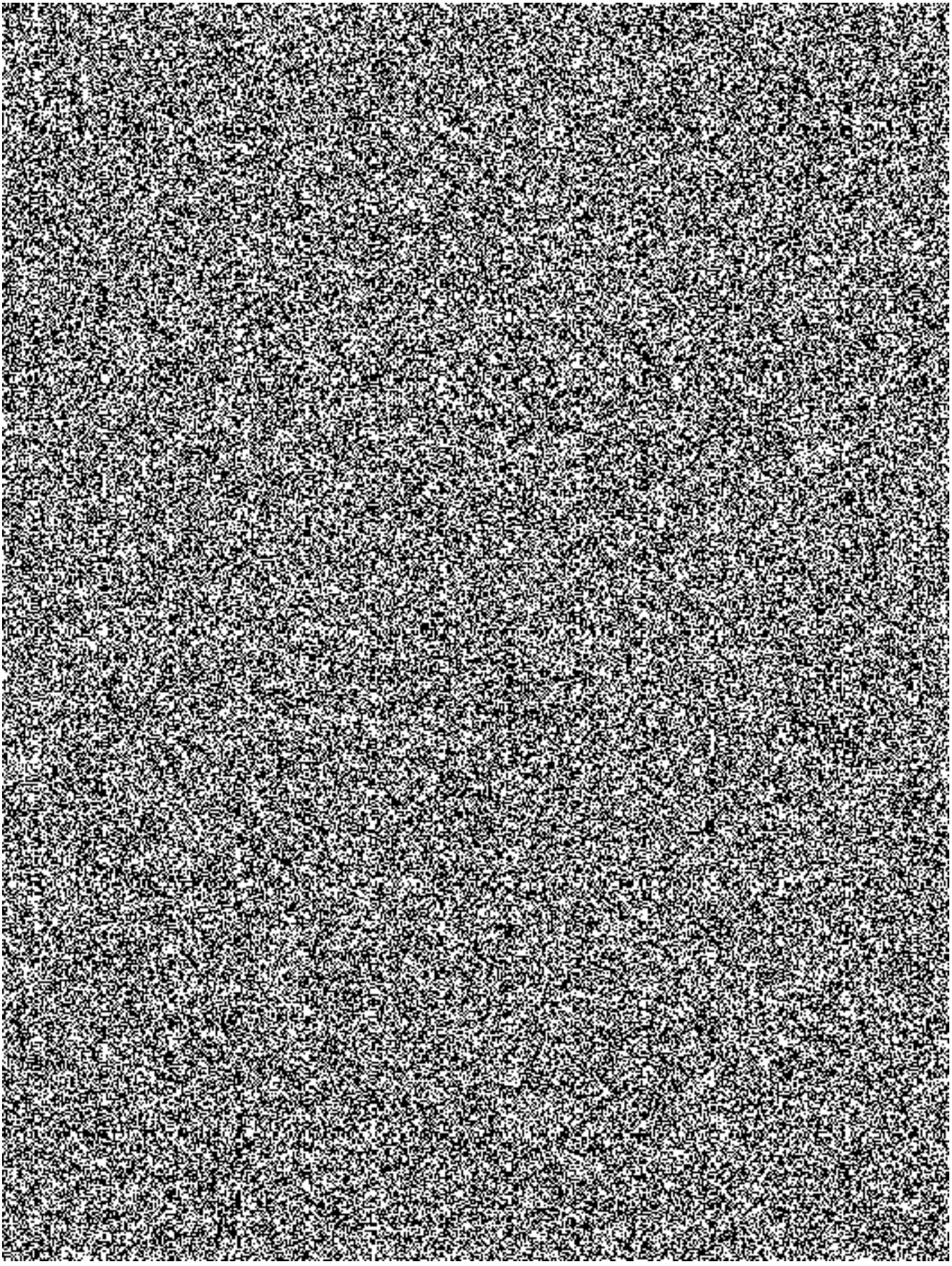
4.3. Prostupy z jednotlivých VLAN

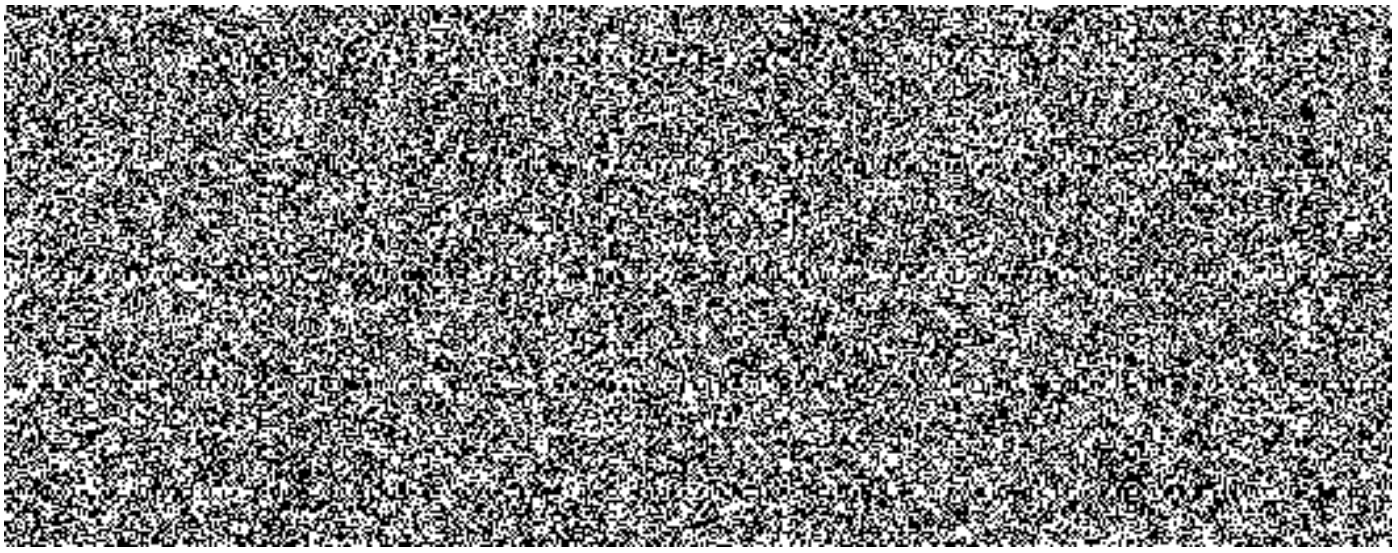
Detailní rozpis prostupů bude na základě informací získaných v průběhu instalace a testování (včetně dosud nepřidělených rozsahů)

4.3.1 Prostředí LAN

4.3.1.1. Přístup do provozního prostředí:



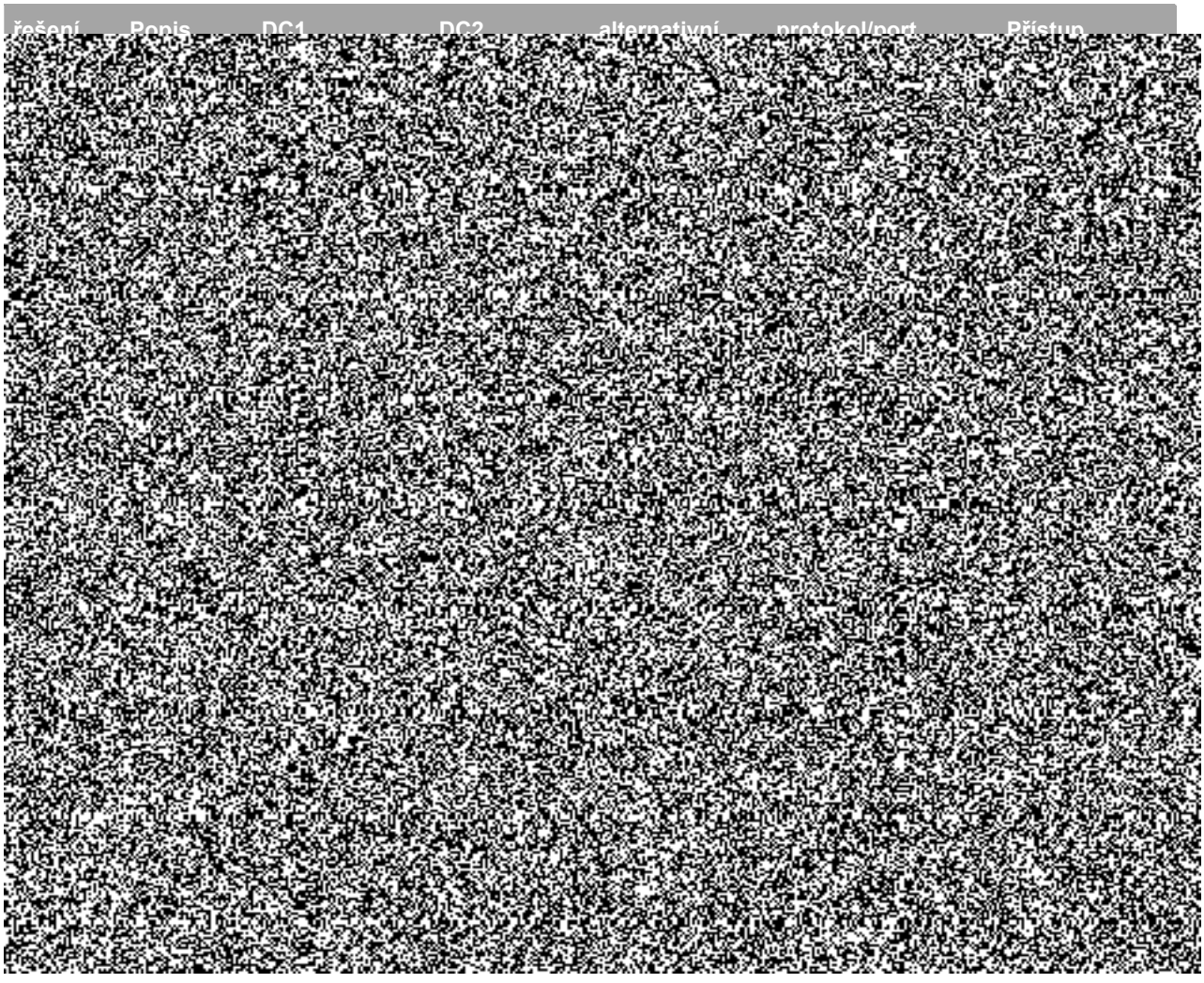


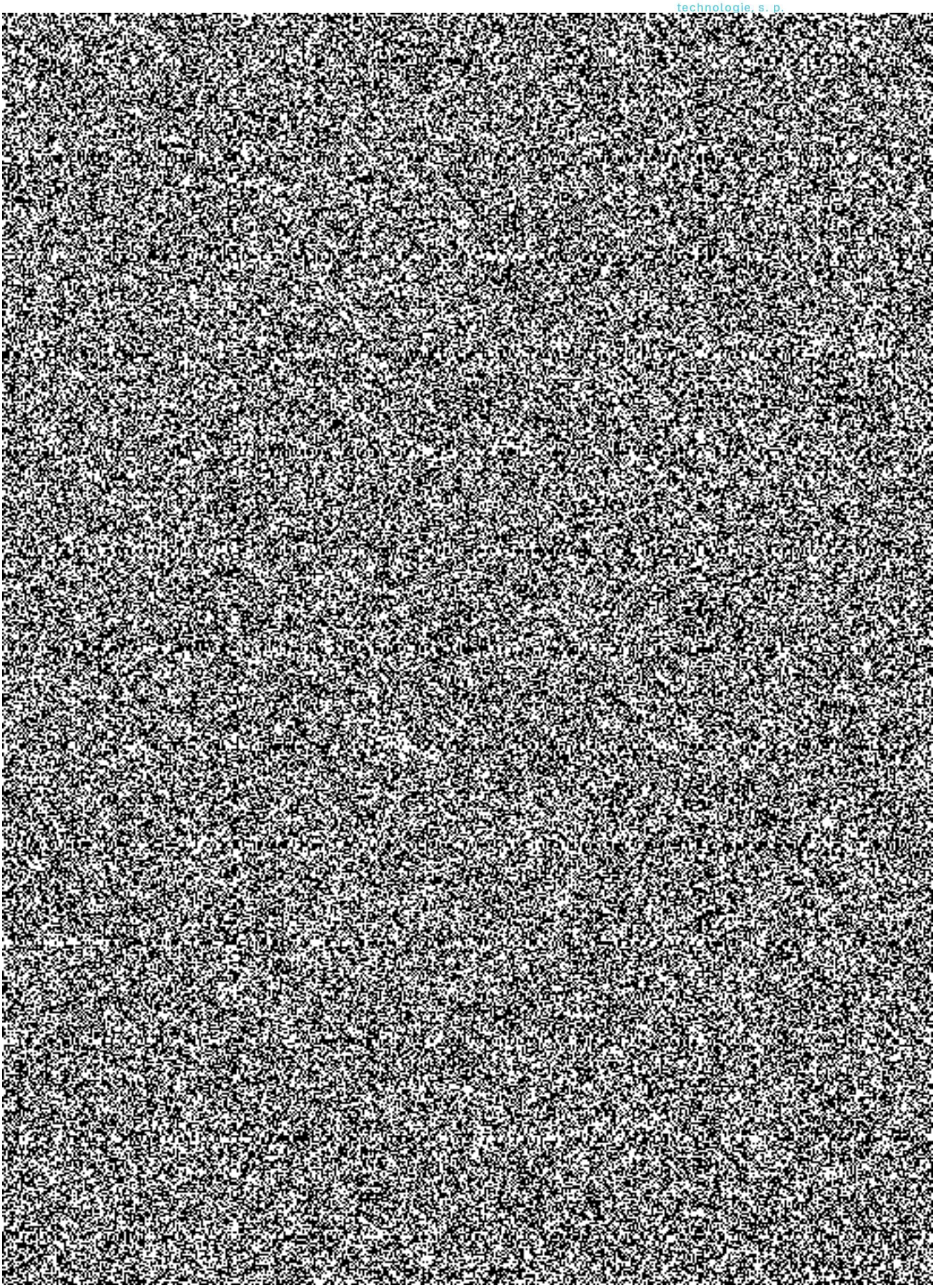


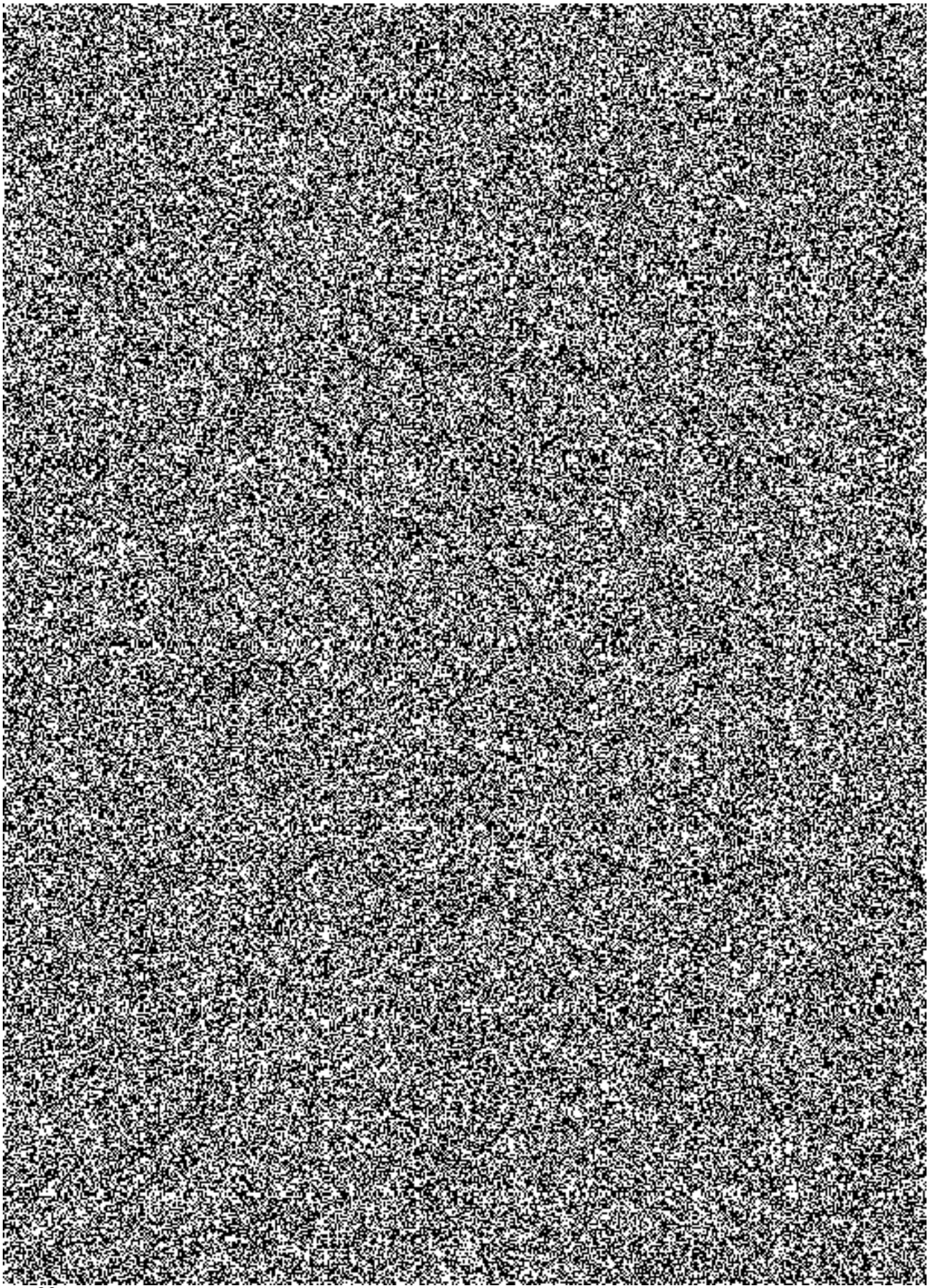
Část prostupů byla ověřována během akceptaci první etapy 2017. Po zprovoznění 802.1x budou všechny prostupy znovu otestovány a výstup předán k akceptaci.

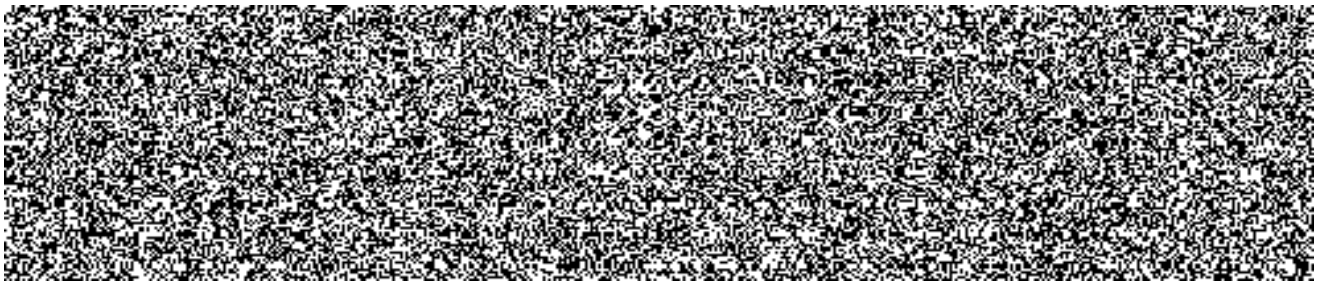
4.3.2 Terminálové servery

4.3.2.1. Přístup do provozního prostředí:









5. Bezpečná síťová komunikace

5.1. Pravidla komunikace Active Directory

Řadiče AD budou využívat pro synchronizaci času NTP servery z prostředí [redacted] DNS těchto řadičů bude přesměrovávat DNS dotazy, které se netýkají domény [redacted] na DNS servery z prostředí [redacted]

5.2. Pravidla komunikace s Windows Update

Se službou Windows update bude komunikovat pouze služba WSUS a to s přihlédnutím k zabezpečení její stability prostřednictvím protokolů HTTP/HTTPS skrze přímé připojení k internetu s omezením výlučně na cílové adresy této služby. Seznam cílových IP adres je součást technické specifikace žádosti o službu v [redacted]

5.3. Pravidla komunikace pro terminálové servery

Na TS bude možné přistupovat RDP protokolem z vnitřní sítě dohledového centra nebo ze vzdáleného pracoviště skrze VPN, kterou poskytuje prostředí [redacted] v DC1 a DC2 [redacted]

6. Terminálové servery

6.1. Základní popis řešení

Smyslem řešení terminálových serverů v projektu DCEGOV je zajištění bezpečného přístupu na systémy dohledového centra ze vzdálených pracovišť. Terminálové servery představují pro takové řešení nejlepší podmínky, neboť je lze velmi dobře centrálně konfigurovat a zároveň omezovat.

6.2. Zabezpečení terminálových serverů

Na terminálových serverech bude nasazena politika zabezpečující snížení rizika ovlivnění chodu systému uživatelem a to formou omezení práv uživatelů. Spouštění dostupných aplikací bude řízené prostřednictvím služby AppLocker. S ohledem na zajištění bezpečnosti poskytovaných dat nebude povolena funkce „drive redirection“, tím pádem se lokální či flash disky nebudou přesměrovávat do terminálové relace.

V každém datovém centru je instalován jeden terminálový server, na těchto serverech jsou dostupné všechny konzole a nástroje používané [redacted] a bezpečnostním dohledem. Pro správný chod budou instalovány licenční služby umožňující uživatelský přístup v požadovaném počtu uživatelů.

7. Autentifikace uživatelů v nástrojích [redacted]

V současné době jsou uživatelé autentifikování v nástrojích [redacted] pomocí lokálních účtů v těchto nástrojích.

Ověřování uživatelů vůči doméně bude implementováno pouze pro aplikace [redacted]

Napojení DCeGOV na dohledové centrum bude řešeno v rámci jiného předmětu plnění.

Přiřazování uživatelů do rolí bude řízeno AD.

7.1. Popis řešení

Autentifikace uživatelů nástrojů ArcSight bude probíhat přímo z řadičů domény prostřednictvím protokolu LDAP a LDAPS (LDAP over SSL/TLS).

Certifikát pro LDAPS bude vygenerovaný certifikační autoritou v [redacted]

Za předpokladu, že současné verze dohledových nástrojů podporují LDAPS, doporučujeme LDAP nepoužívat a upřednostňovat výhradně LDAPS.

7.2. [redacted] - Ověřování uživatelů vůči MS Active Directory

Veškeré majoritní komponenty SIEM [redacted] podporují ověřování uživatelů vůči MS Active Directory. To znamená, že uživatel využívá svoje doménové přihlašovací údaje pro autentizaci do jakékoliv z výše uvedených komponent.

7.2.1 Výhody:

- Není zde nutnost si využívat další lokální účet.
- Veškerá politika hesel, které je vynucená na doméně, se aplikuje i zde.
- Jakmile je někomu zrušen účet v AD, nepřihlásí se ani do jedné z komponent.
- Seznam lidí, kteří se mohou připojit, lze omezit na členství v určitě skupině.

7.2.2 Konfigurace:

Pro úspěšné nastavení ověřování oproti AD, bude potřeba následující:

- seznam doménovýchřadičů (hostname, IP)
- Informace o zabezpečení komunikačního protokolu,
- Komunikační certifikáty
- Search base pro vyhledávání uživatelů
- Servisní účet v AD
- Volitelně seznam skupin v AD, jejichž členové budou mít přístup (není nutné omezovat).

7.2.3 Úpravy na straně [redacted]

- Konfigurace uživatelských skupin a jejich oprávnění pro [redacted]
- Konfigurace autentizace vůči AD pro všechny [redacted]

7.2.4 Používání:

Uživatelé nebudou mít implicitně po konfiguraci přístup do jednotlivých komponent – je nutné jim vždy v [redacted] vytvořit účet a spárovat ho s příslušným uživatelským účtem v AD.

8. Bezpečný internet 

Bezpečný internet  bude použit pro koncové stanice dohledového centra (včetně uživatelského prostředí terminálových serverů) a všechny ostatní pracovní stanice připojené do domény DCeGOV.

9. Počítače, System Center

Pro zajištění efektivní správy desktopového prostředí, budou všechny počítače napojené do domény [redacted] a zároveň připojené k systémům dohledů a správy. Dohled a správu desktopového prostředí zajistí nástroje „System Center“, které jsou již nainstalované, a to s ohledem na možnosti deploymentu a na validaci vyhovujícího stavu aktualizací Windows a antivirů. Pro zmiňované funkcionality proběhne další konfigurace „System Center” prostředí. Na stanice bude nasazen OS Windows 10 [redacted]

10. Aktualizace operačních systémů Windows

O aktualizace operačních systémů Windows se bude starat nástroj „System Center Configuration Manager" (dále jen „SCCM"), který je již nainstalovaný. Řešení SCCM v sobě zahrnuje implementaci tzv. Software Update Point (dále jen „SUP"), který se spojí s WSUS serverem, a od kterého si bude bezpečně stahovat aktualizace. SUP bude instalovat předem schválené aktualizace a balíčky na počítače/servery prostřednictvím SCCM agenta.

Systém bude předán do provozu s nainstalovaným kumulativním updatem 

11. Antivirové řešení

Antivirové řešení v současné době již zajišťují dvě technologie, jejichž specifikace je popisovaná níže.

[redacted] bude instalován výhradně na desktopy. Jeho deployment, řízení politik a dohled nad jeho stavem, bude zajišťovat již nainstalovaný nástroj [redacted]

[redacted] bude instalován výhradně na servery TS a FS. Jeho deployment a dohled nad jeho stavem, bude zajišťovat již nainstalovaný nástroj [redacted]

12. Zakázání USB Flash disků

S ohledem na nejvyšší bezpečnost poskytovaných dat budou USB flash disky zakázané na všech počítačích. Na terminálových serverech nebude povolená funkce přesměrování USB flash disků a lokálních disků klienta.

V případě pracovních stanic, je možné udělit výjimku na základě zjištěných potřeb. Výjimku může udělit vedoucí bezpečnostního dohledu.

13. Zálohování

Celé řešení zálohování bude postavené na technologii HPE Data Protector.

Bude využito zálohovací řešení, které je vybudované v rámci prostředí CMS, do kterého projekt DCeGOV poskytl zálohovací licence.

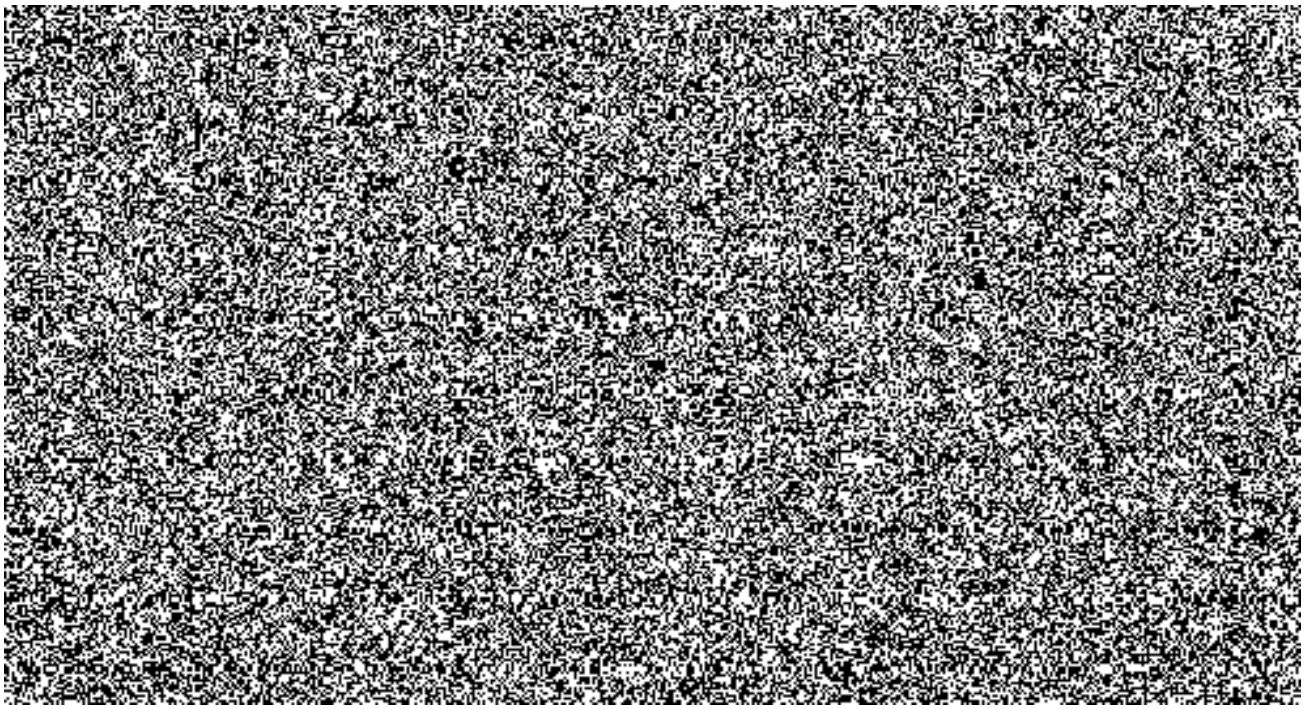
13.1. Úprava sítě

Pro zálohování bude vytvořena Backup síť. Pro Backup síť bude vytvořená Backup VRF, která zajistí routing směrem k zálohovaným serverům (terminálové servery, virtualizačním hostům, či virtuálním serververům).

13.2. Způsob uložení dat

Způsob uložení dat je koncipováno tzv. [redacted] to znamená, že každá záloha je přímo ukládádna do [redacted] v dané lokalitě a posléze zreplikována do druhé lokality. Tento způsob zajišťuje nejen rychlý přístup k uloženým zálohám, ale zároveň zajišťuje i vysokou bezpečnost uložených záloh.

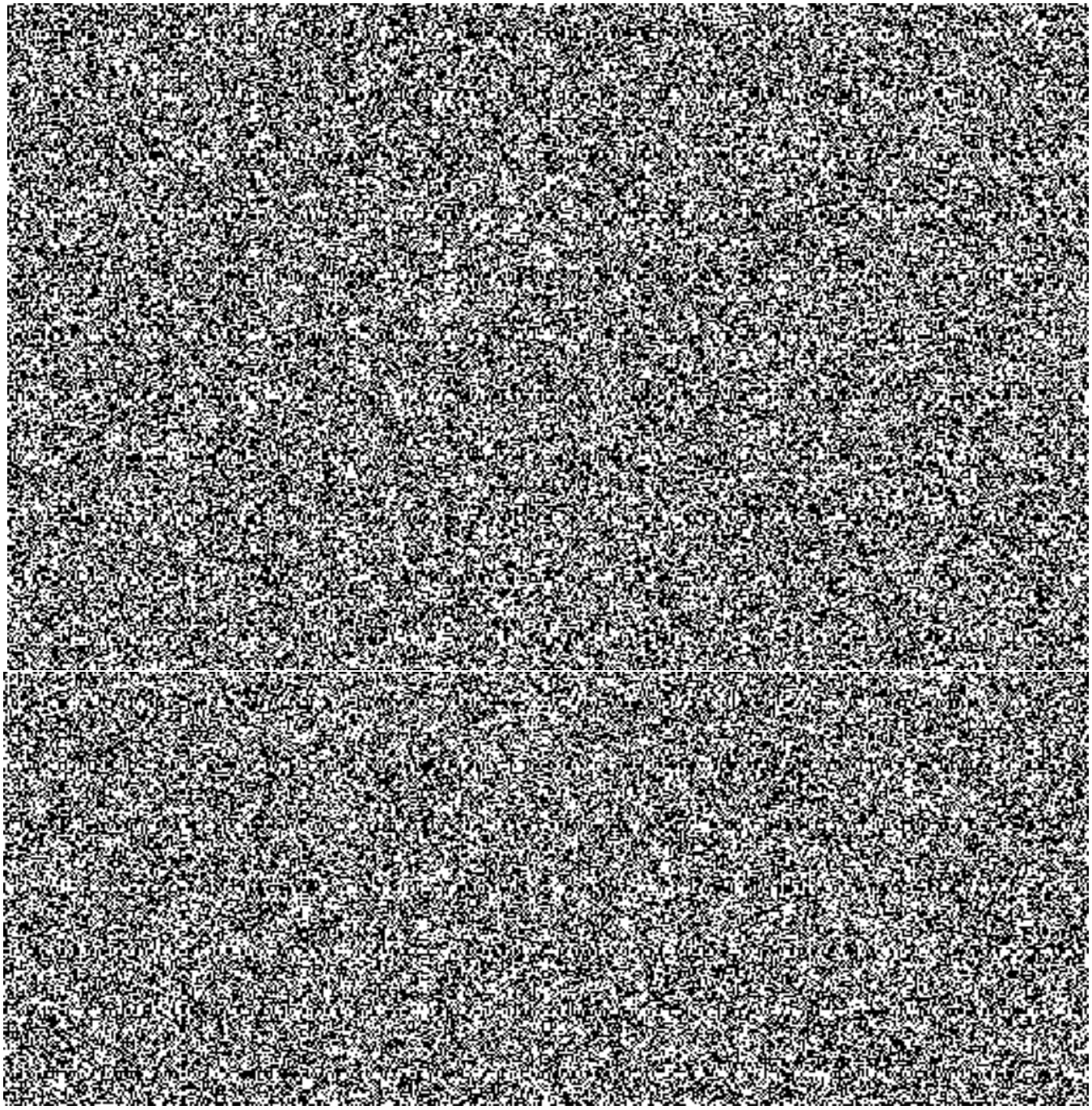
Všechna zálohovaná dat jsou vždy uložena v obou datacentrech DCeGOV v několika úrovních:



13.3. Způsob zálohování

Způsob zálohování byl primárně koncipováno tak, aby nedošlo ke ztrátě dat větší než [redacted] s ohledem ná různé Kategorie (typy) dat:

Kategorie dat	Popis	Zálohování



13.4. Předpoklad

Před konfigurací a otestováním zálohovacího řešení je nutný upgrade [redacted] pro podporu Windows server 2016.

14. Microsoft SQL Server

14.1. Datová síť

S ohledem na bezpečnost bude pro MS SQL Cluster vyhrazena dedikovaná datová síť, na kterou bude řešení [redacted] availbility groups přesunuté.

15. Připojení DCeGOV na systémy pro správu a dohled

DCeGOV bude připojen na níže uvedené systémy pro správu.

15.1. System Center Configuration Manager

System Center Configuration Manager (dále jen „SCCM“) bude sloužit výhradně pro správu desktopového prostředí a prostředí windows serverů. SCCM bude mít na starosti níže uvedené role.

- Operating System Deployment – desktopy
- Application Deployment – určeno pro desktopy a terminálové farmy
    - Compliance check
- Windows Update (Software Update Point)
- SC Endpoint Protection Management (definuje politiky antiviru, zajišťuje instalaci, aktualizaci a dohled nad stavem)

15.2. System Center Operations Manager

System Center Operations Manager (dále jen „SCOM“) bude sloužit pro monitoring serverového prostředí.

Management packs:

- Windows Server 2016 a vyšší
- MS SQL 2016 a vyšší

Pokud se událost ve SCOM vyhodnotí jako incident, bude založen ticket v 

15.3. 

Pro připojení řešení  do Domeny DCeGOV je třeba realizovat úpravy prostředí. Předmětem úprav je instalace a konfigurace dočasných  a Relay na nový HW z důvodu přetrvávajících výkonnostních problémů.

16. Akceptační kritéria

16.1. Sítě

- Existuje vytvořený síťový plán.
- Existuje vytvořená komunikační matice, která zajistí správnou konfiguraci komunikačních pravidel na straně firewallu.
- Existuje vytvořený „Low Level Desing (dále jen „LLD“)“, který bude stanovovat architekturu sítě.

16.2.

- Existují nainstalované nové sítě, které stanovil LLD.
- Existují nastavená komunikační pravidla na firewallu.

16.3.

- Uživatelské účty byly vytvořeny, případně omezeny na základě doporučení „Admin Rights Assignment“
- Zároveň byla zajištěná výchozí expirace doménových uživatelů (nikoli správců). Platnost 1 rok. Nebudou tohoto součástí servisní účty a recovery účty z obálek.
- Byla zajištěná politika hesel na základě doporučení, které stanovuje ZoKB.
- Existuje úspěšné vytvoření trustů s doménou resortmv.cz – pokud nebude dodána součinnost s MV, nebude v rámci akceptačních kritéirí
    - Je možné ověřit uživatele vůči AD na [redacted]Loggeru.

16.4.

- Všem klientským zařízením byla zřízená služba 802.1x.

16.5.

- Existuje funkční licenční server, včetně poskytovaných licencí.
- Existuje bezpečnostní omezení na straně terminálových serverů (zákazné přesměrování flashdisků, omezení aplikací a omezení veškerého provozu na plochu, dokumenty a uživatelské složky). Řízeno pro uživatelské skupiny, které mají mít zakázaný přistup k výměnným devicům. Posoudit, zda i pro jiné skupiny.
- Existuje úspěšně dokončené nasazení počítačových stanic , včetně nainstalovaných aplikací, hotových přístupů a omezení flashdisků.
- Existují nainstalované antivirové aplikace jak na servery (týká se pouze serverů, kde je přímý přístup uživatelů – FS/TS), tak na počítačové stanice.

16.6.

- Existují funkční pravidla pro zálohování.
- Existuje funkční zálohování v obou datových center.

16.7.

- Servery a počítačové stanice jsou připojené do managementu SCCM.
- SCOM má funkční pravidla „health check“ pro servery.

16.8.

- Existuje úspěšně dokončená a odsouhlasená Dokumentace skutečného provedení díla

- Řešení Díla je v souladu s Dokumentací skutečného provedení.

Příloha č. 2 – Akceptační protokol

Zhotovitel	*Národní agentura pro informační a komunikační technologie, s.p.*
Objednatel	*Česká republika – Ministerstvo vnitra*
Rámcová smlouva	*Číslo platné Rámcové smlouvy*
Dílčí smlouva	*Číslo platné Dílčí smlouvy*
Název Projektu	*Dohledové centrum eGovernmentu*
Datum předání	*Datum*

Předmět akceptace

Číslo	Popis	Akceptováno	Akceptováno s výhradou	Neakceptováno
01				

Výhrady

Číslo	Popis výhrady	Kategorie vady	Termín pro vypořádání vady
01			

Seznam příloh

Závěrečná ustanovení

Zhotovitel a Objednatel svým podpisem stvrzují akceptaci Díla dle výše specifikované Dílčí smlouvy a Rámcové smlouvy.

	Jméno a příjmení	Datum	Podpis
Akceptoval za Zhotovitele			
Akceptoval za Objednatele			

Příloha č. 3 – Předávací protokol

Zhotovitel	*Národní agentura pro informační a komunikační technologie, s.p.*
Objednatel	*Česká republika – Ministerstvo vnitra*
Rámcová smlouva	*Číslo platné Rámcové smlouvy*
Dílčí smlouva	*Číslo platné Dílčí smlouvy*
Název Projektu	*Dohledové centrum eGovernmentu*
Datum předání	*Datum*

Předmět předání

Číslo	Popis
01	*Popis Díla*

Výhrady k předanému Dílu

Číslo	Popis
01	*Popis výhrady*
02	*Popis výhrady*

Zhotovitel a Objednatel svým podpisem stvrzují předání a převzetí Díla dle výše specifikované Dílčí smlouvy a Rámcové smlouvy.

V Praze dne *xx.xx.xxxx*

Společnost	Jméno	Podpis
Předal za Zhotovitele		
Převzal za Objednatele		

Příloha č. 4 - Klasifikace vad a nedodělků

Kategorie	*Vada*	*Popis*
A	*Kritická*	*Z důvodu vady Díla některé nebo všechny dodané systémy podporující hlavní procesy selhaly, jsou zcela nefunkční nebo je jejich funkčnost omezena podstatným způsobem, tedy tak, že je kriticky ovlivněna činnost Objednatele.*
B	*Vážná*	*Z důvodu vady Díla je činnost Objednatele podstatným způsobem ovlivněna z důvodu selhání nebo omezení některé ze systémových funkcí podporujících důležité procesy.* *Vada znemožňuje nebo výrazně komplikuje využívání dodaných systémů.*
C	*Drobná*	*Z důvodu vady Díla některé funkce dodaných systémů sice selhaly, ale nejsou v daný moment využívány a nemají žádný vliv na řádný chod systému.* *Vada má zanedbatelný vliv na činnost Objednatele.* *Vada se vyskytuje v izolované části dodaných systémů, jejich využívání je ztíženo a vada nemá vliv na ostatní funkce dodaných systémů.*
D	*Kosmetická*	*Vada Díla je pouze kosmetického charakteru.* *Vada nemá vliv na činnost Objednatele.* *Vada nekomplikuje využívání dodaných systémů. Jedná se například o vady v grafice či vady, které neomezují používání dodaných systémů.*

Definice výsledků akceptačního řízení

Akceptováno - Pro výrok a formulaci akceptačního rozhodnutí Akceptováno je podmínkou úspěšné ukončení akceptačního řízení. Musí být odstraněny veškeré vady kategorie A, B i C. Vad kategorie D může zůstat neodstraněných maximálně 15. K těm navrhne Zhotovitel termín a harmonogram odstranění.

Akceptováno s výhradou - Pro výrok a formulaci akceptačního rozhodnutí Akceptováno s výhradou musí být odstraněny veškeré vady kategorie A, může zůstat maximálně 5 vad kategorie B, maximálně 10 vad kategorie C a maximálně 15 vad kategorie D. K těm navrhne Zhotovitel termín a harmonogram odstranění.

Neakceptováno - Pro výrok a formulaci akceptačního rozhodnutí Neakceptováno je podmínkou neúspěšné ukončení (nedokončení) akceptačního řízení a/nebo neodstranění jakékoliv vady kategorie A a/nebo existence více jak 5 vad kategorie B a/nebo existence více než 10 vad kategorie C a/nebo více jak 15 vad kategorie D.

Příloha č. 5 - Specifikace licencí dodaných MV

Part Number	Item Name	License Agreement Type	Program	Level	Purchase Unit	Purchase Period	Pool	Product Type
[illegible]								

[illegible]