ZATWIERDZAM

KOMENDANT GŁÓWNY POLICJI
z upoważnienia
PIERWSZY ZASTĘPCA
KOMENDANTA GŁÓWNEGO POLICJI
nadinsp. Dariusz AUGUSTYNIAK
2020 -03- 06

4 - 1104 / 20

WYMAGANIA
DOTYCZĄCE STANDARDÓW TECHNICZNYCH,
UŻYTKOWYCH ORAZ BEZPIECZEŃSTWA, STOSOWANYCH W POLICJI,
W ZAKRESIE INFORMATYKI I ŁĄCZNOŚCI

STYCZEŃ 2020

Matryca odpowiedzialności:

	Jednostka organizacyjna Policji	Komórka organizacyjna KGP	Biuro Łączności i Informatyki KGP	Komendant Główny Policji
Odpowiedzialny za dokument (R)			X	
Zatwierdzający dokument (A)				X
Merytorycznie Konsultowany (C)	X			
Informowany (I)	X	X		

Opis dokumentu

Nazwa dokumentu	Wymagania dotyczące standardów technicznych, użytkowych oraz bezpieczeństwa, stosowanych w Policji w zakresie informatyki i łączności
Wersja	1
Data ostatniej modyfikacji	2020-01-09
Autor dokumentu	Biuro Łączności i Informatyki Komendy Głównej Policji
Status dokumentu (projekt, zatwierdzony)	Zatwierdzony
Liczba stron	96

Wymagane podpisy:

Imię i nazwisko	Rola/stanowisko	Podpis	Data
insp. Przemysław Więcław	Dyrektor Biura Łączności i Informatyki KGP	insp. Przemysław WIĘCŁAW	10.1.2020
nadkom. Marcin Mieńkowski	Naczelnik Wydziału Zarządzania Projektami BŁiI KGP		2020 -01- 22
nadkom. Adam Bogucki	Naczelnik Wydziału Ochrony Systemów Informatycznych BŁiI KGP		2020 -01- 10
Paweł Janowski	Zastępca Naczelnika Wydziału Utrzymania Systemów Informatycznych Policyjnych i Krajowych BŁiI KGP		22.01.2020
kom. Wojciech Rafalo	Naczelnik Wydziału Utrzymania Systemów Informatycznych Międzynarodowych BŁiI KGP		31.01.20
podkom. Arkadiusz Żołądek	Naczelnik Wydziału Utrzymania Systemów Telekomunikacyjnych BŁiI KGP		03.02.2020
ml. insp. Wojciech Dąbrowski	Naczelnik Wydziału Technicznego Wsparcia Systemu Powiadamiania Ratunkowego BŁiI KGP		03.02.20
podkom. Piotr Wasilewski	Naczelnik Wydziału Radiokomunikacji BŁiI KGP	w.z.	2020 -01- 21
nadkom. Andrzej Dziwiszek	Naczelnik Wydziału Obsługi Wsparcia Końcowego Użytkownika BŁiI KGP		21.01.2020
ml. insp. Grażyna Ryszkowska	Naczelnik Wydziału Programistycznego		10.01.20

ZASTĘPCA DYREKTORA
BIURA ŁĄCZNOŚCI I INFORMATYKI
KOMENDY GŁÓWNEJ POLICJI
insp. Sławomir RYSAK

Załącznik nr 3

Rozdział 1 Postanowienia wstępne

1.1 Cele i zakres dokumentu

Niniejszy dokument ustanawia wymagania w zakresie planowania, projektowania, wdrażania, użytkowania oraz bezpieczeństwa systemów łączności i informatyki w Policji. Wymagania te winny być stosowane w jednostkach organizacyjnych Policji, w celu stworzenia warunków do zapewnienia interoperacyjności, spójności, integralności oraz efektywności rozwiązań w obszarach łączności i informatyki.

W przypadku, gdy obecnie użytkowane komponenty systemów łączności i informatyki nie spełniają wymagań określonych w niniejszym dokumencie, należy zaplanować i podjąć działania prowadzące do zapewnienia zgodności. Tempo tych działań należy dostosować do możliwości finansowych i organizacyjnych jednostek Policji.

Za wdrożenie i przestrzeganie wymagań określonych w niniejszym dokumencie odpowiadają kierownicy jednostek organizacyjnych Policji.

1.2 Akty prawne obowiązujące w zakresie przedmiotowym objętym dokumentem

Wszelkie działania w zakresie objętym niniejszym dokumentem, muszą być zgodne z obowiązującymi regulacjami prawnymi, zawartymi w ustawach i aktach wykonawczych.

1.3 Terminologia przyjęta w dokumencie

1)	**AAA** (*Authentication, Authorization and Accounting*)	Uwierzytelnianie, Autoryzacja, Rozliczalność.
2)	**Administrator**	Policjant albo pracownik Policji, któremu powierzono obowiązki w zakresie eksploatacji systemu teleinformatycznego, sieci lub ich wyodrębnionych komponentów. Administratorów wyznaczają właściwi przełożeni. Osobom wyznaczanym do pełnienia roli administratora można uzupełnić nazwę funkcji o określenie wskazujące na specyfikę wykonywanych zadań, przez te osoby lub o ograniczoną właściwość terytorialną, np. administrator urządzeń sieciowych, administrator materiałów kryptograficznych, administrator baz danych, administrator lokalny, administrator kopii zapasowych itp. W systemach teleinformatycznych, w których przetwarzane są informacje niejawne, sposób powoływania oraz zadania administratorów systemu określa dokumentacja bezpieczeństwa tworzona na podstawie przepisów o ochronie informacji niejawnych.

3)	**Administrator Lokalny**	Policjant albo pracownik Policji wyznaczony przez właściwego przełożonego, który odpowiada za prawidłowe funkcjonowanie, eksploatację i zabezpieczenie, użytkowanych w tej jednostce lub komórce organizacyjnej Policji, komponentów systemów łączności oraz informatyki, wymagających działań administracyjnych i eksploatacyjnych.
4)	**AGA** (*Air-Ground-Air*)	łączność radiowa z obiektami latającymi w relacji ziemia-powietrze i powietrze-ziemia.
5)	**Akredytacja**	formalne potwierdzenie przez uprawniony podmiot spełnienia ustalonych wymagań i kryteriów jakości.
6)	**Algorytm Szyfrowania Danych**	sposób szyfrowania informacji przetwarzanych w systemach teleinformatycznych. Przykładami takich algorytmów są DES (Data Encryption Standard), 3DES, AES (Advanced Encryption Standard) i inne.
7)	**API** (*Application Programming Interface*)	interfejs programistyczny aplikacji, rozumiany jako zestaw reguł i opisów wzajemnej komunikacji oprogramowania.
8)	**APN** (*Access Point Name*)	dedykowany punkt dostępu do sieci operatora GSM, umożliwiający transmisję danych.
9)	**Atak typu DoS** (*Denial of Service*)	atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania poprzez zajęcie wszystkich lub części wolnych zasobów, przeprowadzany równocześnie z wielu komputerów.
10)	**Autoryzacja**	proces, w którym sprawdzane jest czy dany podmiot (o ustalonej właśnie tożsamości) ma prawo dostępu do żądanych zasobów.
11)	**Bezpieczeństwo danych**	zbiór zagadnień z dziedziny teleinformatyki związany z szacowaniem i kontrolą ryzyka wynikającego z korzystania z komputerów i sieci teleinformatycznych, rozpatrywany z perspektywy poufności, integralności, rozliczalności i dostępności danych.
12)	**Bezpieczeństwo TI** *(teleinformatyczne)*	wykorzystanie sprzętowych i programowych środków w celu ochrony przetwarzanych, przechowywanych oraz przekazywanych danych w Systemach TI w sposób zapewniający poufność, rozliczalność, integralność i dostępność.

36)	**MTN**	Mobilny Terminal Noszony – komputer przenośny komunikujący się z systemami teleinformatycznymi dostępnymi poprzez sieć PSTD z wykorzystaniem bezprzewodowej transmisji danych.
37)	**MTP**	Mobilny Terminal Przewoźny – komputer zainstalowany w pojeździe, komunikujący się z systemami teleinformatycznymi dostępnymi poprzez sieć PSTD z wykorzystaniem bezprzewodowej transmisji danych.
38)	**NAC** (*Network Access Control*)	kontrola dostępu do sieci.
39)	**Napięcie gwarantowane**	napięcie zasilające gwarantujące parametry zgodnie z normami/zaleceniami dla sprzętu teleinformatycznego.
40)	**OST 112**	Ogólnopolska platforma komunikacyjna służąca do obsługi wywołań na numer alarmowy 112 i inne numery alarmowe oraz komunikacji pomiędzy służbami odpowiedzialnymi za ratownictwo i bezpieczeństwo publiczne.
41)	**OTAR** *(Over the Air Rekeying)*	usługa zdalnej aktualizacji kluczy maskujących poprzez interfejs radiowy w systemie TETRA.
42)	**PEL**	Punkt Elektryczno-Logiczny min. 4xRJ45 i min. 4x230V.
43)	**Poczta Elektroniczna**	Usługa realizowana w oparciu o infrastrukturę teleinformatyczną Policji, z wykorzystaniem protokołów komunikacyjnych SMTP, POP3/IMAP i innych, umożliwiających wymianę wiadomości tekstowych i multimedialnych w formie elektronicznej.
44)	**Polifax–A i Polifax–Z**	podsieci przeznaczone do transmisji telekopiowej jawnej.
45)	**Poufność**	właściwość określająca, że informacja nie jest ujawniania podmiotom do tego nieuprawnionym.
46)	**PPU**	Policyjna Platforma Usługowa - narzędzie wymiany danych pomiędzy systemami za pośrednictwem usług sieciowych (ang. web services).
47)	**PSTD** *(Policyjna Sieć Transmisji Danych)*	wirtualna sieć prywatna VPN, działająca na bazie wydzielonej sieci szkieletowej OST 112 w technologii IP MPLS z zaimplementowaną kryptografią, umożliwiająca łączenie sieci LAN na obszarze całego

		kraju w jedną sieć korporacyjną i zapewniająca użytkownikom policyjnym bezpieczny dostęp do centralnych systemów informatycznych Policji.
48)	**PSTN** *(Public Switched Telephone Network)*	publiczna komutowana sieć telefoniczna.
49)	**RADIUS** *(Remote Authentication Dial In User Service)*	protokół opisany w RFC2865 dotyczący uwierzytelniania, autoryzacji oraz informacji o jego konfiguracji.
50)	**RFC** (*Request For Comments*)	dokumenty opisujące protokoły (standardy) internetowe stanowiące propozycję rozwiązań przedstawione przez projektantów i naukowców do akceptacji przez odpowiednie organizacje opiniujące i zatwierdzające standardy telekomunikacyjne (np. ANSI, ITU itp.).
51)	**Router CE** *(Customer Edge)*	router kliencki sieci operatorskiej MPLS.
52)	**Router PE** *(Provider Edge)*	router brzegowy w sieci operatorskiej MPLS.
53)	**Rozliczalność**	właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
54)	**SDS** *(Short Data Service)*	usługa krótkich wiadomości tekstowych.
55)	**Sieć TI** *(teleinformatyczna)*	element składowy Systemu TI Policji zapewniający transport danych w sposób automatyczny.
56)	**SMDB**	System Mobilnego Dostępu do Baz Danych.
57)	**SSR**	Samodzielne Stanowisko Robocze – stanowisko komputerowe, które nie jest Stanowiskiem Dostępowym (komputer stacjonarny/komputer przenośny).
58)	**Stanowisko Dostępowe**	stanowisko komputerowe, podłączone do sieci TI w celu dostępu do centralnych zasobów informatycznych Systemów TI BŁiI.
59)	**SUŁTelP**	System Utajnionej Łączności Telekopiowej Policji funkcjonujący w oparciu o podsieć komutowaną przeznaczony do szyfrowanej transmisji telekopiowej.
60)	**SwMI** *(Switching and Management Infrastructure)*	elementy infrastruktury systemu TETRA odpowiedzialne za zarządzanie i komutację.
61)	**SWWN**	System Wykrywania Włamań i Napadów.

i kompatybilności wdrażanych rozwiązań z rozwiązaniami już funkcjonującymi bądź planowanymi do realizacji.

Policyjne systemy TI muszą zapewniać bezpieczeństwo informacjom w nich przetwarzanych, w stopniu adekwatnym do oszacowanego poziomu ryzyka. Realizacji powyższego mają służyć następujące działania i zasady:

1) Jednostki organizacyjne Policji powinny ustanowić, wdrożyć, eksploatować, monitorować, przeglądać, utrzymywać i stale doskonalić udokumentowany System Zarządzania Bezpieczeństwem Informacji (SZBI) w kontekście prowadzonej działalności i występującego ryzyka. W celu realizacji powyższego należy stosować Polskie Normy, w tym normy ISO serii 27001.

2) SZBI obejmować musi normy, zasady i wszystkie przedsięwzięcia realizowane przez użytkowników systemów TI, zmierzające do utrzymania odpowiedniego poziomu bezpieczeństwa informacji, zapewniającego ich poufność, dostępność i integralność. Założenia SZBI muszą być zatwierdzone przez kierownika jednostki organizacyjnej Policji.

3) Systemy teleinformatyczne przetwarzające informacje niejawne o klauzuli „poufne" lub wyższej, podlegają procesowi akredytacji w Departamencie Bezpieczeństwa Teleinformatycznego ABW. Komendant Główny Policji udziela akredytacji bezpieczeństwa teleinformatycznego dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli „zastrzeżone", przez zatwierdzenie dokumentacji bezpieczeństwa systemu teleinformatycznego.

4) Zbiory danych osobowych muszą być przetwarzane w systemach informatycznych, zgodnie z obowiązującymi w tym zakresie regulacjami prawnymi. Dla systemów informatycznych przetwarzających dane osobowe, musi być opracowana polityka bezpieczeństwa oraz instrukcja zarządzania systemem, a także winni być wyznaczeni przeszkoleni administratorzy, ponoszący odpowiedzialność za utrzymanie danego systemu.

2.1 Normy i międzynarodowe standardy

Jednolite kryteria oceny bezpieczeństwa Systemów TI zapewnia stosowanie międzynarodowych standardów. Do najważniejszych dokumentów o znaczeniu międzynarodowym należą[2]:

2.1.1 w zakresie technologii informatycznych oraz kompatybilności elektromagnetycznej:

1) **PN-ISO/IEC 15408: 2016-10** - Technika informatyczna – Techniki zabezpieczeń – Kryteria oceny zabezpieczeń informatycznych:

Część 1 - Wprowadzenie i model ogólny,

[2] W dokumencie przywołano normy i standardy oraz ich wersje, dostępne w dniu wprowadzenia niniejszych wytycznych w życie. W dłuższej perspektywie czasowej należy uwzględniać aktualne wersje norm i standardów oraz pojawiające się nowe normy i standardy, w obszarach objętych wymaganiami.

Część 2 – Komponenty funkcjonalne zabezpieczeń,

Część 3 - Wymagania uzasadnienia zaufania do zabezpieczeń.

2) **dyrektywa Parlamentu Europejskiego i Rady** 2014/30/UE z dnia 26 lutego 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich odnoszących się do kompatybilności elektromagnetycznej (wersja przekształcona) *(Dz. Urz. UE L 96/77 z 29.3.2014).*

3) **dyrektywa Parlamentu Europejskiego i Rady** 2014/53/UE z dnia 16 kwietnia 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich dotyczących udostępniania na rynku urządzeń radiowych i uchylająca dyrektywę 1999/5/WE *(Dz. Urz. UE L 153/62 z 22.5.2014).*

4) **rozporządzenie Parlamentu Europejskiego i Rady (WE)** 174/2013 z dnia 5 lutego 2013 r. zmieniające rozporządzenie (WE) nr 106/2008 w sprawie wspólnotowego programu znakowania efektywności energetycznej urządzeń biurowych (*Dz. Urz. UE L 63/1 z 6.3.2013).*

2.1.2 w zakresie technologii telekomunikacyjnych przepisy międzynarodowe wyszczególnione w Prawie telekomunikacyjnym, a w szczególności:

1) Rekomendacje Sektora Standaryzacji Międzynarodowej Unii Telekomunikacyjnej (ITU-T).

2) Standardy/normy Europejskiego Instytutu Standardów Telekomunikacyjnych (ETSI), w tym:

- **PN-ETSI EN 300 247 V1.2.1:2002U** Dostęp i urządzenia końcowe (AT) - Cyfrowe łącze dzierżawione o przepływności 2.048 kbit/s pracujące w trybie nieramkowym (D2048U) - Parametry połączenia;
- **PN-ETSI EN 300 452 V1.2.1:2002U** Dostęp i urządzenia końcowe (AT) - Analogowe czteroprzewodowe łącze dzierżawione specjalnej jakości, wykorzystujące pasmo mowy (A2S) - Parametry połączenia i prezentacja interfejsu sieciowego;
- **PN-ETSI EN 300 289 V1.2.1:2002U** Dostęp i urządzenia końcowe (AT) - Cyfrowe łącza dzierżawione o przepływności 64 kbit/s bez ograniczeń z integralnością oktetową (D64U) - Parametry połączenia;
- **PN-ETSI EN 300 418 V1.2.1:2002U** Dostęp i urządzenia końcowe (AT) - Cyfrowe łącza dzierżawione o przepływności 2.048 kbit/s pracujące w trybie nieramkowym i ramkowym (D2048U i D2048S) - Prezentacja interfejsu sieciowego;

4) **PN-T-83103:1996** – Urządzenia zasilające w telekomunikacji – zespoły prostownikowe. Wymagania i badania.

5) **PN-T-83104:1996** – Urządzenia zasilające w telekomunikacji – przetwornice półprzewodnikowe. Wymagania i badania.

6) **PN-EN 55022:2006** – Kompatybilność elektromagnetyczna (EMC) – Urządzenia informatyczne, Charakterystyki zaburzeń radioelektrycznych, poziomy dopuszczalne i metody pomiaru, Kompatybilność elektromagnetyczna (EMC), Urządzenia informatyczne, Charakterystyki zaburzeń radioelektrycznych, Poziomy dopuszczalne i metody pomiaru.

7) **PN-S-76020:1997** - Pojazdy drogowe - Urządzenia elektroniczne pojazdów samochodowych - Ogólne wymagania i metody badań.

8) **PN-ETS 300 683:2000** - Systemy i urządzenia radiowe (RES) - Kompatybilność elektromagnetyczna (EMC) urządzeń małego zasięgu (SRD) pracujących na częstotliwościach pomiędzy 9 kHz i 25 GHz.

9) **PN-ETSI EN 301 489-1 V1.8.1:2008** - Kompatybilność elektromagnetyczna i zagadnienia widma radiowego (ERM) - Norma kompatybilności elektromagnetycznej (EMC) dotycząca urządzeń i systemów radiowych - Część 1: Ogólne wymagania techniczne.

10) **PN-ETSI EN 301 489-5 V1.3.1:2003** - Kompatybilność elektromagnetyczna i zagadnienia widma radiowego (ERM) - Norma kompatybilności elektromagnetycznej (EMC) dotycząca urządzeń i systemów radiowych - Część 5: Wymagania szczegółowe dla urządzeń lądowej radiokomunikacji ruchomej typu dyspozytorskiego (PMR) i wyposażenia pomocniczego (do transmisji sygnałów mowy i innych).

Rozdział 3 Wymagania dotyczące bezpieczeństwa

3.1 Wymagania w zakresie wyposażenia Centrów Przetwarzania Danych (PCPD – Podstawowego Centrum Przetwarzania Danych, ZCPD – Zapasowego Centrum Przetwarzania Danych oraz RCPD – Regionalnych Centrów Przetwarzania Danych)

a) Współczynnik niezawodności na poziomie 99,99%;
b) System monitoringu, kontroli dostępu, SWWN;
c) Zasilanie podstawowe i rezerwowe (rozwiązania w zakresie zasilania powinny umożliwiać osiągnięcie parametrów napięcia gwarantowanego bez względu na jakiekolwiek problemy z zasilaniem podstawowym – tzw. zasilanie bezprzerwowe);
d) System PPOŻ – zgodnie z obowiązującymi przepisami i normami;
e) System klimatyzacji precyzyjnej;
f) Instalacje teletechniczne (okablowanie strukturalne) kable światłowodowe (FO - fiber optic) i miedziane min. kat. 6;
g) Wymaga się stosowanie rozwiązań, ograniczających zjawisko tzw. ulotu elektromagnetycznego (emisji ujawniającej).

3.2 Postępowanie z elektronicznymi nośnikami danych nie zawierającymi informacji niejawnych

a) Nośniki zawierające dane osobowe muszą być przechowywane i wykorzystywane w sposób uniemożliwiający dostęp osobom nieupoważnionym.
b) Użytkownik końcowy jest odpowiedzialny za wydane mu elektroniczne nośniki danych. Nadzoruje ich jakość, sposób przechowywania a także inicjuje proces wymiany nośników i ich kwalifikacji do utylizacji.
c) Utylizacja oraz nadzór nad elektronicznymi nośnikami danych musi odbywać się zgodnie z procedurami przyjętymi w danej jednostce organizacyjnej Policji.
d) Czynność niszczenia nośników/utylizacji, musi być przeprowadzona w sposób uniemożliwiający dostęp do jeszcze nie zniszczonych nośników osobom nieuprawnionym oraz musi być udokumentowana.

3.3 Elementy bezpieczeństwa sieci teleinformatycznej

3.3.1 Podstawowym zadaniem systemu bezpieczeństwa jest zapewnienie poufności, integralności, dostępności informacji przetwarzanych w systemie TI a także rozliczalności, autentyczności i niezawodności w dostępie do tych informacji. W tym celu należy zapewnić funkcjonowanie w warstwie sieciowej takich rozwiązań jak:

- stosowanie technologii VPN z kryptografią, zapewniających akceptowany poziom bezpieczeństwa przesyłania danych w różnych środowiskach WAN,
- stosowanie co najmniej dwóch podstawowych typów systemów zaporowych: działające w warstwie aplikacji oraz w warstwie sieciowej modelu ISO OSI RM (ISO Open Systems Interconnection Reference Model).

oraz zapewnić realizację następujących zasad:

- mechanizmy kontroli dostępu do systemów teleinformatycznych Policji, muszą zapewnić, że z tych systemów będą mogły korzystać w ramach autoryzowanych uprawnień jedynie osoby zidentyfikowane i pozytywnie uwierzytelnione. Zastosowane mechanizmy i środki kontroli dostępu (np.: AAA, NAC itp.) do systemów TI muszą być adekwatne do specyfiki i zawartości informacyjnej systemu (systemy jawne, systemy w których przetwarzane są dane osobowe, systemy niejawne),
- wszystkie centralne systemy teleinformatyczne dołączone do sieci PSTD muszą korzystać z systemu BTUU, jako podstawowego mechanizmu kontroli dostępu użytkowników. W uzasadnionych przypadkach Dyrektor BŁiI KGP może wyrazić zgodę na odstępstwo od tej zasady. W przypadku systemów funkcjonujących lokalnie, a dołączonych do sieci PSTD, w KWP/KSP oraz komórkach organizacyjnych KGP, dopuszcza się inne mechanizmy kontroli dostępu, np. autoryzacja użytkowników z wykorzystaniem loginu i hasła.

3.3.2 Cele systemu bezpieczeństwa:

a) zapewnienie kontroli dostępu, zgodności zabezpieczeń i identyfikacji - weryfikacja użytkownika,
b) zapewnienie integralności danych,

wymagana jest akredytacja Departamentu Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego.

b) wykorzystuje się protokół GET VPN na wszystkich routerach CE (Customer Edge) w sieciach VPN MPLS OST 112 lub SSL/TLS dla przesyłania informacji jawnych.

3.4.2 Jako standard dla zarządzania certyfikatami kluczy publicznych przyjmuje się infrastrukturę PKI (Public Key Infrastructure).

Infrastruktura klucza publicznego musi być oparta na standardzie ITU-X.509 oraz zaimplementowana zgodnie z normą PN-I-02000:2002, a centrum autoryzacji musi wykorzystywać funkcję haszującą min. SHA-2 o rozmiarze skrótu co najmniej 224 bitów.

3.4.3 Aplikacje korzystające z infrastruktury PKI, muszą wykorzystywać przy transmisji danych:

a) szyfrowanie danych dla zapewnienia ich poufności,
b) podpisy cyfrowe dla zapewnienia niezaprzeczalności i weryfikacji integralności danych,
c) certyfikaty dla uwierzytelnienia osób, aplikacji, urządzeń i serwisów oraz dla zapewnienia kontroli dostępu (uwierzytelnienia), listy CRL.

3.5 Mechanizmy ochrony korespondencji głosowej

3.5.1 Bezpieczeństwo korespondencji w systemach łączności radiowej

3.5.1.1 Bezpieczeństwo korespondencji w systemie TETRA

a) System musi zapewniać pracę w klasach bezpieczeństwa SC1, SC2, SC3 (z i bez kluczy GCK).
b) W klasach SC2 i SC3 (z i bez kluczy GCK) maskowany w interfejsie radiowym musi być cały ruch radiowy z sygnalizacją i adresowaniem włącznie.
c) Maskowanie korespondencji musi być realizowane w interfejsie radiowym za pomocą zmiennych nw. kluczy szyfrujących:
   - Wspólny klucz szyfrujący - CCK;
   - Grupowy klucz szyfrujący - GCK;
   - Pochodny klucz szyfrujący - DCK;
   - Statyczny klucz szyfrujący - SCK;
d) System musi umożliwiać pracę w klasie bezpieczeństwa SC1 niezależnie od pracy z klasami SC2 lub SC3 (z i bez kluczy GCK).
e) W klasie bezpieczeństwa SC1 i SC2 system musi zapewniać przynajmniej uwierzytelnianie terminala przez system, przy czym funkcjonalność ta musi mieć charakter opcjonalny, zależny od bieżących potrzeb konfiguracyjnych.
f) BS w trybie trankingu lokalnego musi umożliwiać przynajmniej maskowanie korespondencji kluczem SCK, gdy możliwość maskowania korespondencji kluczem DCK jest niedostępna.
g) System musi zapewniać uwierzytelnianie terminali przy rejestracji do systemu, zmianie BS i wyjściu BS z trankingu lokalnego, w którym uwierzytelnianie nie było dostępne.
h) W klasie bezpieczeństwa SC3 (z i bez kluczy GCK) system musi realizować procedury autoryzacji terminali poprzez uwierzytelnienie inicjowane przez SwMI. System musi także umożliwiać uwierzytelnienie SwMI na żądanie terminala.

i) System musi umożliwiać stosowanie maskowania korespondencji E2E w relacjach terminal - terminal, oraz terminal - konsola dyspozytorska za pomocą klucza o długości 256 bitów (AES256). Wymaganie to nie może ograniczać pracy terminali bez funkcji szyfrowania E2E.
j) System musi realizować maskowanie korespondencji radiowej z wykorzystaniem algorytmu TEA2.
k) W zakresie zarządzania kluczami:
   - System musi być wyposażony w centrum dystrybucji kluczy maskujących,
   - System musi być wyposażony w centrum zarządzania kluczami do celów uwierzytelniania,
   - Każda z Agencji musi mieć możliwość techniczną generowania i zarządzania własnymi kluczami GCK;
   - Bazy danych przechowujące klucze służące do uwierzytelniania i maskowania interfejsu radiowego muszą być zaszyfrowane z wykorzystaniem narzędzi odpornych na próby włamania i uniemożliwiających dostęp osób nieuprawnionych.
   - System musi zapewniać dynamiczną zmianę kluczy maskujących SCK, CCK i GCK drogą radiową (OTAR) oraz umożliwiać przekazywanie drogą radiową danych potrzebnych do wygenerowania klucza DCK.

3.5.1.2 Bezpieczeństwo korespondencji w systemie DMR

Wdrażane rozwiązania muszą zapewniać maskowanie korespondencji głosowej algorytmem ARC4 o długości klucza 40 bitów, kodek głosu AMBE+2.

3.5.2 Telefonia IP

Wymagania techniczno-użytkowe w systemach łączności IP:

a) CallProcesor – system sterujący połączeniami telefonicznymi;
b) Brama głosowa – styk sieci VoIP z innymi systemami teleinformatycznymi z pomocą technologii ISDN;
c) Session Border Controller – styk sieci VoIP z innymi systemami telefonicznymi opartymi o technologie VoIP;
d) Gatekeeper – urządzenie sterujące połączeniami telefonicznymi, zapewniające między innymi call admission controll, translację adresów itp.
e) Urządzenia końcowe – aparaty telefoniczne, aparaty video, aplikacje
f) Sieć IP – transport dla pakietów rozmównych,
g) Protokoły sygnalizacyjne:
   - H.323
   - MGCP,
   - SIP,
   - SCCP
h) Protokoły transmisji danych:

3.7.1.1 Urządzenia zapewniające obsługę aplikacji centralnych, dostęp do tych aplikacji oraz sprzęt łączności zapewniający mobilność dla służb dyżurnych Policji muszą być objęte zasilaniem:

- bezprzerwowym na poziomie KGP, komend wojewódzkich (Stołecznej), miejskich, powiatowych Policji, komisariatów Policji o stanie etatowym powyżej 60 etatów oraz szkół policji,
- podstawowym lub bezprzerwowym, na poziomie pozostałych komisariatów Policji,
- wymaga się by, fizyczne okablowanie budynków Policji zapewniało wydzieloną, dedykowaną sieć elektroenergetyczną dla sieci LAN,
- bezprzerwowe zasilanie i napięcie gwarantowane powinno być dostępne w Centralnych Punktach Dystrybucyjnych.

3.7.1.2 Zasilaniem bezprzerwowym na poziomie KGP, komend wojewódzkich (Stołecznej), miejskich, powiatowych, rejonowych, komisariatów Policji o stanie etatowym powyżej 60 etatów, oraz szkół policji obejmuje się urządzenia wchodzące w skład:

- węzłów teleinformatycznych (WWT, PWT, WT),
- centralnych oraz lokalnych punktów dystrybucyjnych,
- sieci energetycznej w zakresie krytycznych systemów i stanowisk pracy (stanowisko kierowania, kontrola dostępu, monitoring wizyjny) dedykowanej dla infrastruktury sieci LAN,
- systemów telewizji przemysłowej CCTV,
- kontroli dostępu,
- systemów rozgłoszeniowych.

3.7.1.3 Zasilaniem rezerwowym na poziomie komend wojewódzkich (Stołecznej), miejskich, powiatowych, rejonowych, komisariatów Policji o stanie etatowym powyżej 60 etatów, oraz szkół policji obejmuje się urządzenia wchodzące w skład:

- systemów klimatyzacyjnych w węzłach teleinformatycznych.

3.7.1.4 Zasilanie podstawowe stosuje się do zasilania urządzeń teleinformatycznych w pozostałych komisariatach Policji i komórkach niższego szczebla. W celu ochrony instalowanych urządzeń przed zanikami napięcia zasilającego, wymaga się stosowanie zasilaczy UPS lub siłowni telekomunikacyjnych małej mocy.

3.7.2 Zasilanie węzłów TI

Przy projektowaniu podstawowych parametrów siłowni telekomunikacyjnych wymaga się stosowanie postanowień zawartych w rozporządzeniu Ministra Łączności z dnia 21 kwietnia 1995 r. w sprawie warunków technicznych zasilania energią elektryczną obiektów budowlanych łączności (Dz. U. Nr 50, poz. 271).

Przy projektowaniu siłowni telekomunikacyjnych należy dążyć do rezerwowania prostowników i inwertorów zgodnie z zasadą redundancji n + 1.

3.7.2.1 Podstawowe wymagania w zakresie zasilania energią elektryczną węzłów TI:

a) konstrukcja modulowa siłowni telekomunikacyjnych,
b) zdalne monitorowanie oraz możliwość zdalnej zmiany parametrów poprzez sieć Ethernet wykorzystując protokół TCP/IP z możliwością kontroli pracy systemów zasilania zainstalowanych w podległych jednostkach,

c) stacjonarny agregat prądotwórczy w jednostkach Policji szczebla KGP, komendy wojewódzkiej Policji i komendy miejskiej Policji oraz szkoły Policji, posiadający funkcję automatycznego uruchamiania się,
d) zapas paliwa dla stacjonarnego agregatu prądotwórczego musi zapewnić ciągłość jego pracy przez okres co najmniej 24 godzin,
e) baterie bezobsługowe, o żywotności zgodnie z normą EUROBAT 12,
f) czas rezerwy bateryjnej na szczeblu KGP, komendy wojewódzkiej (Stołecznej) Policji i komendy miejskiej Policji oraz szkoły Policji musi wynosić min. 3 godziny przy znamionowym obciążeniu siłowni. W przypadku zastosowania agregatu prądotwórczego, czas ten może być krótszy, jednak musi wystarczyć do wystartowania i zsynchronizowania agregatu,
g) do zasilania urządzeń w węzłach TI na szczeblu komendy powiatowej Policji, komendy rejonowej Policji, komisariatów Policji o stanie etatowym powyżej 60 etatów, stosuje się:
   - centralne zasilacze UPS o min. 15 minutowej autonomii pracy, przy obciążeniu znamionowym,
   - ogólno-budynkowe samo-startujące spalinowe agregaty prądotwórcze z zapasem paliwa na min. 24 godziny pracy przy obciążeniu znamionowym,
   - siłownie telekomunikacyjne.

3.7.2.2 Zasilacze UPS

Do zasilania urządzeń teleinformatycznych w pozostałych jednostkach organizacyjnych podległych komendom miejskim, powiatowym i rejonowym należy stosować:

a) siłownie inwertorowe lub zasilacze UPS typu kompakt (tzn. zintegrowane z szafą teleinformatyczną) o min. 15 minutowej autonomii pracy przy obciążeniu znamionowym,
b) zasilacze UPS w zakresie mocy 1-120kVA należy projektować zgodnie z zasadą redundancji n+1, stosując konstrukcję modułową, z zachowaniem możliwości rozbudowy o kolejne moduły. W zakresie mocy 100-500kVA stosować należy konstrukcję monoblokową z możliwością pracy równoległej szaf,
c) zasilacze UPS w technologii VFI - SS 111, posiadające certyfikat zgodności z zasadniczymi wymaganiami wydany przez notyfikowaną jednostkę certyfikującą lub deklarację zgodności z wymaganiami szczegółowymi wydany przez producenta lub importera,
d) zasilacze UPS spełniające normy:
   - PN-EN-62040-1-1:2006 (Systemy bezprzerwowego zasilania (UPS) - Część 1-1: Wymagania ogólne i wymagania dotyczące bezpieczeństwa UPS stosowanych w miejscach dostępnych dla operatorów),
   - PN-EN 50091-2:2002 (U) (Systemy bezprzerwowego zasilania (UPS) - Część 2: Wymagania dotyczące kompatybilności elektromagnetycznej (EMC)) [norma o takim samym numerze, ale bez indeksu "U" - dotyczy ogólnych wymagań technicznych dla domowych i budynkowych systemów elektronicznych (HBES)],
   - PN-EN 62040-3:2005 (Systemy bezprzerwowego zasilania (UPS) - Część 3: Metody określania właściwości i wymagania dotyczące badań).
e) zasilacze UPS zapewniające instalację kolejnych modułów bez konieczności montażu dodatkowego okablowania na obiekcie, z możliwością komunikacji z zasilaczem UPS poprzez adapter SNMP,

wprowadzany do obrotu spełnia wymagania zasadnicze określone w przepisach o systemie oceny zgodności CE (Conformability European - Zgodność Europejska),

b) główne parametry
   - silnik wyposażony w automatyczny, elektroniczny regulator prędkości obrotowej silnika zapewniający stabilność częstotliwości ±0.25 % w całym zakresie obciążeń,
   - prądnica synchroniczna, samowzbudna, bezszczotkowa, posiadająca automatyczny, elektroniczny regulator napięcia prądnicy, zapewniający stabilność napięcia ±0,5 % w całym zakresie obciążeń,
   - zakłócenia radioelektryczne zgodne ze standardami VDE 0875 stopień G i MIL 461 AB,
   - współczynnik THD (bez obciążenia) < 2,0 %,
   - stopień ochrony IP23,
   - klasa izolacji stojana i wirnika: H,
   - sprawność prądnicy przy 100% obciążenia należy określać dla konkretnej mocy agregatu (np. 85 kVA ≥ 91,5%, 150 kVA ≥ 92,2%, 250 kVA ≥ 92,4%, 400kVA≥ 94,1%).

c) wymagania w przypadku zabudowy kontenerowej:
   - wielkość kontenera powinna być zależna od wielkości agregatu i zastosowanego wyciszenia,
   - powierzchnia podłogi antypoślizgowa, odporna na rdzę: np. blacha ryflowana aluminiowa,
   - oświetlenie podstawowe (230 V) i awaryjne (12 lub 24 V) wnętrza kontenera,
   - wyłącznik „STOP" awaryjny przy każdych drzwiach wejściowych do kontenera,
   - poziom hałasu: max. 69 dB, mierzony w odległości 7 m od agregatu.

d) dobierając moc agregatu należy uwzględnić:
   - oczekiwaną moc zapotrzebowaną przez odbiorniki, które mają zostać objęte zasilaniem z agregatu,
   - pokrycie potrzeb częściowo rozładowanych akumulatorów współpracującego z agregatem zasilacza UPS lub siłowni,
   - zapas mocy ze względu na urządzenia klimatyzacyjne.

3.7.3 Monitoring urządzeń:

a) w pomieszczeniach całodobowej służby dyżurnej jednostek Policji należy montować wizualno-akustyczne panele sygnalizacyjne informujące o aktualnym stanie urządzeń zasilających (UPS, siłownie, agregat) oraz sygnalizujące ich ewentualne awarie,
b) całodobowej służbie dyżurnej Wojewódzkiego Węzła Teleinformatycznego należy zapewnić zdalne monitorowanie systemów zasilania zainstalowanych w podległych jednostkach Policji z możliwością kontroli ich parametrów w oparciu o protokół SNMP,
c) należy stosować układy monitorujące stan akumulatorów oraz systemów zarządzających ładowaniem akumulatorów,
d) obiekty komisariatów Policji wymaga się wyposażać w przyłącze dla agregatu przewoźnego,
e) wymaga się przeprowadzanie okresowych testów potwierdzających sprawność urządzeń zasilających.

3.7.4 Zasilanie urządzeń radiotelefonicznych

3.7.4.1 Zasilanie stacjonarnych obiektów infrastruktury TETRA

1) Urządzenia Systemu muszą zostać zaprojektowane i wykonane z uwzględnieniem przepisów bezpieczeństwa użytkowania, ograniczenia zaburzeń radioelektrycznych oraz ochrony środowiska.
2) Użyte określenia:
- Zasilanie podstawowe - zasilanie z sieci elektroenergetycznej niskiego napięcia 230/400V AC 50 HZ;
- Zasilanie dwustronne - zasilanie dwiema liniami niskiego napięcia z dwóch niezależnych stacji transformatorowych;
- Zasilanie jednostronne - zasilanie z jednej linii niskiego napięcia;
- Zasilanie rezerwowe - zasilanie z baterii akumulatorów lub spalinowego agregatu prądotwórczego lub ogniw paliwowych;
- Czas rezerwy bateryjnej - czas, w ciągu którego baterie akumulatorów mogą zasilać urządzenia przy maksymalnym poborze prądu i zachowaniem dolnej dopuszczalnej wartości napięcia rozładowania baterii;

3) Odnośnie warunków zasilania urządzeń infrastruktury przyjęto następujące wymagania:
- Czas zasilania ze źródła rezerwowego określony w niniejszych wymaganiach jest czasem minimalnym;
- Pojemność baterii akumulatorów musi być dobrana z uwzględnieniem zasilania wszystkich urządzeń wymagających rezerwowania;
- Obiekty, których dotyczą niniejsze wymagania powinny być wyposażone w przyłącza do przewoźnego zespołu agregatu prądotwórczego;
- Moc zespołu agregatu prądotwórczego (lub ogniwa paliwowego) musi być wystarczająca do zasilania wszystkich urządzeń wymagających rezerwowania;
- Zanik / powrót napięcia lub zmiana źródła zasilania nie mogą przerywać lub zakłócać działania zasilanych urządzeń;
- Obiekty, zależnie od ich rodzaju i wymaganego czasu zasilania ze źródła rezerwowego, muszą być zasilane w sposób określony w poniższej tabeli.

4) Wymagana dokumentacja dostarczonych urządzeń zasilania:
- Deklaracje zgodności, potwierdzające spełnienie wymagań zasadniczych w zakresie bezpieczeństwa użytkowania w związku z dyrektywą 2014/35/UE oraz w zakresie kompatybilności elektromagnetycznej w związku z dyrektywą 2014/30/UE;
- Aktualne pomiary elektryczne, potwierdzone protokołem i wykonane przez uprawnioną osobę, zastosowanych urządzeń i instalacji zasilającej urządzenia (od tablicy głównej zasilania do urządzeń, w tym zasilania rezerwowego).

5) Ponadto w pomieszczeniu musi być dostępna tablica główna zasilania (TGZ) a obwody zasilania zabezpieczone wyłącznikiem nadprądowym typu „S" o parametrach wynikających z projektu technicznego. Dedykowany obwód BS musi być zakończony złączem umożliwiającym podłączenie BS oraz zasilania rezerwowego. Obwód zasilania BS musi zawierać elementy ochrony przepięciowej I i II stopnia. W pomieszczeniu gdzie wykonana będzie instalacja BS musi być dostępna listwa wyrównania potencjałów.
6) Ogólne wymagania dotyczące zasilania obiektów:

i) wymaga się stosowanie szaf dystrybucyjnych o konstrukcji zgodnej do zastosowanego w pomieszczeniu systemu klimatyzacji,
j) szafa dystrybucyjna powinna posiadać odpowiednie dedykowane do danego typu produktu: organizery kabli i uchwyty kablowe zapewniające uporządkowanie i zarządzanie kablami,
k) szafa powinna być uziemiona w sposób zapewniający poprawną pracę instalacji elektrycznej,
l) wymaga się, aby całość oferowanej instalacji okablowania strukturalnego dla wskazanych lokalizacji miała możliwość dalszej rozbudowy w części logicznej: posiadać przekroje tras kablowych oraz wielkość szafy dystrybucyjnej dostosowane do zwiększenia struktury o 25%,
m) wymaga się, aby w Centralnych i Lokalnych Punktach Dystrybucyjnych w pomieszczeniach technicznych stosować odpowiednie urządzenia klimatyzacyjne zapewniające poprawną pracę urządzeń aktywnych sieci,
n) wymaga się, aby w trakcie budowy lub modernizacji systemów okablowań strukturalnych dokonywać integracji z istniejącą siecią telefoniczną,
o) gwarancja producenta na okablowanie powinna wynosić min. 20 lat,
p) pomiary połączenia powinny być wykonane metodą Permanent Link za pomocą mierników dla danej kategorii kabla i posiadających aktualną kalibrację,
q) dokumentacja powykonawcza powinna zawierać przynajmniej: informacje ogólne, normy i zalecenia techniczne, ogólną strukturę okablowania, okablowanie pionowe, okablowanie poziome, opis instalacji zasilającej - gdy wchodzi w skład projektu, punkty dystrybucyjne, testowanie systemu, opis sposobu oznaczania przebiegów poziomych, specyfikacje materiałową oraz certyfikat zastosowanych komponentów, rysunki i schematy, wyniki pomiaru sieci, informację na temat posiadanych przez pracowników świadczących usługę uprawnień, kalibrację miernika, jak również dane na temat udzielanej gwarancji,
r) okablowanie strukturalne powinno być zakończone w pomieszczeniu punktem PEL 4xRJ45 i 4x230V,
s) liczba PEL-i w danym pomieszczeniu powinna być określana na etapie projektowania sieci LAN w uzgodnieniu z użytkownikami końcowymi,
t) wymaga się aby w miarę możliwości projektowych, w serwerowniach projektować podłogę teletechniczną zgodnie z obowiązującymi standardami, w przypadku braku możliwości wykonania podłogi teletechnicznej w pomieszczeniach takich jak serwerownia lub lokalny punkt dystrybucyjny, należy zastosować wykładzinę antyelektrostatyczną,
u) wymaga się aby w miarę możliwości budowlanych, projektować na korytarzach wnęki dla urządzeń wielofunkcyjnych,
v) okablowanie strukturalne dla systemów niejawnych musi być budowane zgodnie z wymaganiami instytucji akredytujących takie systemy.

4.3 Systemy operacyjne, protokoły i systemy zarządzania bazami danych

a) w serwerach przeznaczonych dla obsługi aplikacji bazodanowych stosować należy systemy operacyjne zapewniające poziom ochrony nie niższy niż EAL3 (według *PN-ISO/IEC 15408-3: 2016-10*),

b) standardami systemów operacyjnych dla serwerów baz danych oraz serwerów aplikacji są:
   - RedHat Linux,
   - HP-UX,
   - IBM-AIX,
   - SUN-Solaris,
   - SUSE Linux Enterprise Server
   - system operacyjny z rodziny Windows Server,
   - wymaga się stosowanie komercyjnych wersji systemów LINUX i UNIX, tym niemniej dopuszcza się wykorzystanie innych dystrybucji, spośród których zalecany jest CentOS, openSUSE, Debian i FreeBSD.
c) wszystkie nowotworzone bazy danych muszą być relacyjne (jednak, gdy jest to konieczne i uzasadnione dopuszcza się, za zgodą Dyrektora Biura Łączności i Informatyki KGP, implementowanie innych baz danych), obsługujące polską stronę kodową ISO 8859-2 lub UTF-8 (preferowane jest UTF-8),
d) interfejs użytkownika w aplikacjach policyjnych (wszystkie systemy) musi być w języku polskim,
e) zarządzanie serwisami, systemami operacyjnymi/wirtualizatorami centralnych systemów odbywa się tylko i wyłącznie z poziomu Biura Łączności i Informatyki KGP. Wyjątek mogą stanowić elementy systemów budowanych w architekturze rozproszonej zlokalizowane w jednostkach terenowych,
f) wymaga się stosowanie formatu XML jako standardu wymiany danych pomiędzy systemami w strukturze organizacyjnej Policji, w tym dla nowo tworzonych rozwiązań, dopuszcza się także stosowanie formatu JSON,
g) wymaga się, aby wymiana danych pomiędzy systemami odbywała się za pośrednictwem usług sieciowych (web services) z wykorzystaniem PPU, dla nowo tworzonych rozwiązań,
h) wymaga się, aby bezpieczeństwo logowania na serwerach z systemami UNIX, LINUX obsługiwał protokół KERBEROS,
i) zgodę na wykorzystywanie innych systemów lub sprzętu niezgodnego z przyjętym standardem i ich eksploatację w sieci LAN (PSTD) każdorazowo wydaje Dyrektor Biura Łączności i Informatyki KGP,
j) do przechowywania informacji o użytkownikach i ich uprawnieniach, wykorzystywany jest protokół oparty o usługi katalogowe zgodne z otwartymi standardami (np.: LDAP, AD – Active Directory),
k) do identyfikacji użytkowników i zasobów stosowane są metody oparte o PKI,
l) funkcjonujące środowiska rozwojowe, testowe i produkcyjne muszą być odpowiednio odseparowane. Wybrana metoda separacji (np. separacja logiczna z zastosowaniem wirtualizacji, separacja fizyczna itp.) powinna odpowiadać poziomowi ryzyka i uwarunkowaniom technicznym związanym z danym środowiskiem i funkcjonującymi w nim systemami. Środowiska rozwojowe i testowe nie mogą zawierać danych rzeczywistych (produkcyjnych). Dane wykorzystywane na potrzeby tych środowisk muszą być zanonimizowane w sposób nieodwracalny lub testowo wprowadzone, np. w trakcie szkoleń.
m) w systemie, w którym jego gestor zarządzi anonimizację danych i wskaże, które z tabel (danych) muszą być zanonimizowane, proces anonimizacji polegać będzie na losowym wymieszaniu danych (lub nadpisaniu danych wg ustalonych zasad)

k) możliwość automatycznego wyłączania kompresji głosu dla konkretnych numerów abonentów,
l) możliwość stworzenia systemu łączności dyspozytorskiej,
m) skalowalność,
n) akceptowanie numeracji o zmiennej liczbie cyfr; możliwość wykonywania operacji na numeracjach telefonicznych (np. dodawanie prefixów, postfixów, podmiana),
o) automatyczna rekonfiguracja sieci w stanach awaryjnych,
p) nadzór, konfigurowanie, zarządzanie, testowanie urządzeń i sieci ze stanowiska zarządzania z poziomu węzła w Komendzie Głównej Policji / komendzie wojewódzkiej Policji / Komendzie Stołecznej Policji,
q) zasilanie urządzeń sieci napięciem przemiennym 230V lub napięciem stałym 48V.

4.5.2 Urządzenia teletransmisyjne, routery CE (Customer Edge) umiejscowione w obiektach komisariatach Policji, posterunkach Policji, referatach dzielnicowych

a) współpraca z łączami Ethernet, E&M, FXO, FXS, ISDN PRI, ISDN BRI oraz E1 (nx64kb/s),
b) obsługa protokołów sygnalizacji: SIP, H.323, ETSI oraz Q.sig,
c) obsługa faksów grupy G3 i G4,
d) możliwość tworzenia oddzielnych kanałów wirtualnych dla tworzenia podsieci na bazie infrastruktury urządzeń,
e) obsługa kanałów Frame Relay (PVC i SVC),
f) port LAN Ethernet 10Mb/s lub 10/100/1000 Mb/s,
g) obsługa standardu VLAN 802.1p oraz 802.1q na portach Ethernet,
h) konfiguracja styków do transmisji danych:
   - styk interfejsu V.36, V.35, Ethernet,
   - routing protokołów IP.
i) styk do operatorów telekomunikacyjnych: E1, ułamkowy E1 na styku G.703/G.704/G.706; możliwość tworzenia na interfejsach ułamkowych E1, co najmniej trzech grup kanałów, Ethernet, V.36, V.35,
j) efektywne wykorzystanie pasma:
   - kompresja głosu, tylko w miejscach wejścia-wyjścia z sieci, bez pośrednich stopni dekompresji-kompresji,
   - możliwość kompresji połączeń głosowych do wartości poniżej 8 kb/s, przy czym musi istnieć możliwość wybierania przez użytkownika dowolnej wartości współczynnika kompresji, głos w kanałach TDM po skompresowaniu ma być przenoszony przez sieć wraz z sygnalizacją międzycentralową,
   - dynamiczny przydział pasma,
   - dynamiczna aktywacja usługi fragmentacji pakietów w sytuacji, kiedy w sieci pojawiają się pakiety głosowe,
   - w celu zapewnienia odpowiedniej jakości skompresowanego głosu dla połączeń VoFR lub VoIP parametr MOS (Mean Opinion Score) nie może być gorszy niż 3,7 według pomiaru określonego w normie ITU-P.800,
k) możliwość tworzenia połączeń dyspozytorskich,
l) możliwość automatycznego wyłączania kompresji głosu dla konkretnych numerów abonentów,
m) akceptowanie numeracji o zmiennej liczbie cyfr,

n) nadzór, konfigurowanie, zarządzanie, testowanie urządzeń i sieci ze stanowiska zarządzania z poziomu węzła w komendzie wojewódzkiej (Stołecznej) Policji,
o) automatyczna rekonfiguracja sieci w stanach awaryjnych,
p) zasilanie urządzeń sieci napięciem przemiennym 230V lub napięciem stałym 48V.

4.5.3 Urządzenia teletransmisyjne, routery PE (Provider Edge) WAN/MAN

Wymaga się, aby nowobudowane sieci miejskie wykorzystywały technologię MPLS *(Multi Protocol Label Switching)* i MetroEthernet.

4.5.3.1 Wymagania dla urządzeń WAN/MAN w technologii MPLS:

a) budowa modularna,
b) możliwość przełączania w oparciu o standard MPLS i IP v4, IP v6,
c) architektura elementu przełączającego oparta o w pełni nieblokowalną matrycę przełączającą,
d) wymaga się redundancję wszystkich krytycznych elementów urządzenia: zasilacze, karty kontroli (procesorowe), matryce przełączające,
e) możliwość rozbudowy bez ponoszenia kosztów zmian w oprogramowaniu,
f) wymiana karty w urządzeniu musi odbywać się bez konieczności wyłączania całego urządzenia („wymiana na gorąco"),
g) zapewnienie wsparcia dla następujących mechanizmów związanych z zapewnieniem ciągłości pracy sieci:
   - protokół Fast Reroute,
   - protokół VRRP albo analogiczne rozwiązanie,
h) zasilanie ze źródeł prądu zmiennego 230V lub stałego 48V,
i) zapewnienie jednoczesnej obsługi protokołów:
   - Label Distribution Protocol (LDP),
   - MPLS VPN L2 i L3,
   - MPLS-RSVP-TE,
   - Mechanizmy QoS z użyciem tzw. bitów eksperymentalnych (EXP),
   - MPLS Differentiated Services (DiffServ)-Aware Traffic Engineering (MPLS-DS-TE),
   - IP v6 edge over MPLS,
   - EoMPLS,
   - EloMPLS
   - AToM
   - VPLS,
j) możliwość pracy w trybie LER i LSR,
k) zapewnienie instalacji następujących typów portów:
   - Ethernet 10/100/1000 BASE-T, Gigabit Ethernet,
   - 10 GB Ethernet,
l) zapewnienie wsparcia dla transmisji video poprzez Ethernet z obsługą tzw. ramek „jumbo" o wielkości nie mniejszej niż 9 tysięcy bajtów oraz możliwość obsługi ruchu multicast z wykorzystaniem IGMP v1, v2, PIM, DVMRP,
m) możliwość przełączania w warstwie trzeciej oraz definiowania routingu w oparciu o routing statyczny lub dynamiczny dla protokołu IP v4 i v6,
n) zapewnienie wsparcia dla następujących mechanizmów związanych z zapewnieniem jakości usług w sieci:

- łącza MB,
- analogowe łącza dwukierunkowe jedno- i dwutorowe E&M (sygnalizacja liniowa prądem stałym, R2 i impulsowa) o napięciu międzyżyłowym na żylach sygnalizacyjnych RON TRON min. 20V.

c) wymagania dla łączy cyfrowych ISDN 30B+D:
- parametry elektryczne zgodne z zaleceniami ITU-T G.703, impedancja falowa 120 Ω, przepływność 2 Mb/s,
- parametry jakościowe zgodne z zaleceniami ITU-T M.2100, M.2101 oraz G.821, G.826,
- dopuszczalne fluktuacje fazy i przepływności zgodne z zaleceniami ITU-T G.823 i G.921,
- struktura ramki zgodna z G.704 (bity E wykorzystane do kontroli parzystości CRC4) i G.705,
- wartość maksymalna bitowej stopy błędów BER wynosi 10^{-6}.

d) protokół (sygnalizacja) w sieci policyjnej oraz współpraca z innymi sieciami niepublicznymi:
- Q.sig zgodnie z zaleceniami ITU Q.931 BC/GF,
- IETF Session Initiation Protocol (SIP),
- ITU H.323.

e) protokół (sygnalizacja) do współpracy z sieciami publicznymi:
- EuroISDN DSS-1 zgodnie ETS 300 102-1.

f) kodowanie głosu:
- kodek audio: G.711 A-law, G.729A, G.723.1, G.718, G.719, G.722, G.722.1, G.722.2, G.726, G. 728, G. 279.

4.6.3 Wytyczne dotyczące wyposażenia i konfiguracji serwerów telefonicznych, realizujących sterowanie połączeniami telefonicznymi:

a) wyposażenie podstawowe:
- stanowisko administratora,
- stanowisko pośredniczące (awizo, call center) wraz z elektroniczną książką telefoniczną,
- pulpity dyspozytorskie,
- aparaty IP, umożliwiające połączenia telefoniczne i video,
- możliwość użycia lokalnych aplikacji, typu poczta głosowa, IVR itp.,
- system rejestracji i taryfikacji połączeń, rejestrujący cały ruch telefoniczny i przechowujący dane przez okres co najmniej 12 miesięcy, posiadający możliwość zdalnego dostępu do danych taryfikacyjnych, zbierania informacji o wszystkich połączeniach, również w sieci resortowej, generowania zestawień statystycznych, rachunków zbiorczych oraz umożliwiający pełną archiwizację danych na standardowych nośnikach,
- system zapowiedzi słownych,
- system rejestracji treści korespondencji w zależności od potrzeb.

b) podstawowe wymagania techniczno-użytkowe serwera telefonicznego:
- zgodność z zasadniczymi bądź szczegółowymi wymaganiami lub specyfikacjami technicznymi,

- zgodność ze szczególnymi wymaganiami bezpieczeństwa dotyczącymi urządzeń przeznaczonych do podłączenia do sieci telekomunikacyjnych w europejskiej normie zharmonizowanej EN 41003:1998 (lub w PN-EN 41003:2001),
- architektura wspierająca otwarte standardy współpracy z systemami innych producentów oraz zapewniająca elastyczność konfiguracji interfejsów i sieciowanie w oparciu o pakietową sieć IP,
- możliwość tworzenia podsystemów dyspozytorskich i grup zamkniętych,
- możliwość zestawiania, co najmniej 3 jednoczesnych telekonferencji do min. 8 abonentów w grupie,
- możliwość rozbudowy o zintegrowany sprzętowo i/lub funkcjonalnie system telefonii bezprzewodowej DECT lub DECT IP,
- system poczty głosowej oraz IVR,
- możliwość zdalnego wykonania podstawowych zmian konfiguracyjnych oraz nadzoru,
- skalowalność rozwiązań umożliwiająca prostą rozbudowę systemu,
- zasilanie napięciem stałym 48V lub ~230V).

c) podstawowe wymagania techniczno-użytkowe serwera przetwarzania połączeń:
- architektura wspierająca otwarte standardy współpracy z systemami innych producentów (IETF H.323, SIP, MGCP) oraz zapewniająca elastyczność konfiguracji interfejsów i sieciowanie w oparciu o sieć IP,
- przesyłanie pakietów głosowych w sieci LAN musi być realizowane przy zastosowaniu mechanizmów jakości usług QoS oraz mechanizmów separacji podsieci (np. VLAN L2, L3, VPLS – bez konieczności budowy oddzielnego okablowania sieci LAN), natomiast przenoszenie telefonii IP poprzez sieć WAN musi być realizowane przy użyciu sieci pakietowej IP,
- dedykowane rozwiązanie sprzętowe i programowe posiadające możliwość rozbudowy pojemności oraz zwiększenia jego niezawodności poprzez zastosowanie klastra serwerów przetwarzających połączenia telefoniczne,
- co najmniej dwa interfejsy Ethernet w celu realizacji redundantnego podłączenia do sieci LAN,
- skalowalność systemu umożliwiająca prostą rozbudowę,
- serwer musi realizować następujące funkcje telefoniczne,
  - identyfikację numeru dla połączeń przychodzących,
  - przenoszenie wywołań warunkowe oraz bezwarunkowe,
  - parkowanie połączeń (możliwość „zawieszenia" połączenia przychodzącego, a następnie odebranie tego samego połączenia z innego aparatu w systemie),
  - obsługę połączeń oczekujących – możliwość obsługi przez abonenta kilku połączeń jednocześnie (jedno aktywne, pozostałe zawieszone),
  - obsługę klawiszy szybkiego wybierania,
  - transferowanie połączeń,
  - funkcję zamawiania połączeń,
  - zestawianie telekonferencji,
  - automatyczny wybór standardu kompresji głosu dla obsługiwanych połączeń,
  - automatyczne zestawianie najtańszej drogi połączenia wychodzącego,
  - automatyczne uaktualnianie oprogramowania telefonów IP z serwera przetwarzania połączeń,

- sieć Polifax-Z – sieć zamknięta, co oznacza, że dokonywanie połączeń telekopiowych jest możliwe wyłącznie w ramach zamkniętej grupy abonentów telekopiowych.

4.7 Systemy radiokomunikacyjne

Jako docelowy do wdrożenia i eksploatacji w Policji planowany jest system TETRA. Przesłankami dla wprowadzenia standardu TETRA są jego cechy użytkowe i funkcjonalne, skalowalność, duża niezawodność eksploatacyjna oraz zabezpieczenia poufności przekazywanych danych. Rolę uzupełniającą do systemu TETRA w Policji mogą pełnić rozwiązania DMR tier II.

W Policji użytkowane są analogowe (EDACS, konwencjonalny) systemy łączności radiotelefonicznej. Jednostki organizacyjne Policji mają prawo użytkować te systemy, podejmując jednocześnie działania zmierzające do ich wycofania. Modernizacja i rozbudowa systemów lokalnych lub budowa nowych niestandardowych systemów lokalnych wymaga zgody Dyrektora Biura Łączności i Informatyki Komendy Głównej Policji. Każdorazowej zgody wymaga również doposażenie istniejących systemów (innych niż TETRA i DMR tier II) w sprzęt abonencki.

4.7.1 TETRA

KWP/KSP mają prawo użytkować dotychczas eksploatowane systemy TETRA. Celem zapewnienia kompatybilności rozwiązań TETRA w skali całej Policji modernizacja i rozbudowa tych systemów wymaga zgody Dyrektora Biura Łączności i Informatyki Komendy Głównej Policji. Zgody nie wymaga doposażanie istniejących systemów w sprzęt abonencki z uaktywnionym szyfrowaniem TEA2.

4.7.1.1 Wymagania ogólne:

- połączenia pomiędzy użytkownikami sieci w 95% przypadków, powinno być zestawione w czasie: $\leq 0,5$ s, a w pozostałych przypadkach w czasie < 2 s,
- czas uwalniania kanału komunikacyjnego po zakończeniu połączenia (czas podtrzymania) powinien być programowalny,
- system powinien dynamicznie przydzielać kanały komunikacyjne bez względu na rodzaj transmisji, głos lub dane pakietowe,
- system powinien umożliwiać jednoczesną transmisję głosu i danych pakietowych,
- przenoszenie trwającego połączenia pomiędzy sąsiednimi stacjami bazowymi nie powinno przerywać komunikacji i zmuszać użytkownika do ponownego zestawiania połączenia,
- dane lokalizacyjne stacji ruchomych powinny być przesyłane w kanale sterującym.

4.7.1.2 Połączenia grupowe:

- połączenia grupowe powinny być zestawiane przez dedykowaną dla służb cyfrową sieć radiokomunikacyjną,
- powinno być możliwe zestawienie połączenia do wszystkich użytkowników zarejestrowanych w danej grupie, bez względu na liczbę aktywnych użytkowników i ich rodzaj (radiotelefony, konsole dyspozytorskie) oraz liczbę stacji bazowych uczestniczących w realizacji połączenia,

- system powinien dynamicznie dla połączenia grupowego przydzielać kanały komunikacyjne tylko w tych stacjach bazowych, w których są zarejestrowani członkowie danej grupy,
- w każdej stacji bazowej, w której są zarejestrowani członkowie danej grupy, dla połączenia grupowego system powinien dynamicznie przydzielać tylko jeden kanał komunikacyjny,
- rejestracja do grupy rozmównej powinna odbywać się w sposób automatyczny,
- system powinien umożliwiać dostęp do połączeń grupowych tylko autoryzowanym użytkownikom,
- w trybie połączeń grupowych radiotelefon powinien automatycznie odbierać wszystkie wywołania skierowane do grupy, do której jest dołączony, bez konieczności wykonywania jakichkolwiek działań ze strony użytkownika,
- w trybie połączenia grupowego system powinien umożliwiać transmisję w tym samym czasie tylko jednemu użytkownikowi z danej grupy,
- zgłoszeniem żądania przydziału kanału komunikacyjnego do nadawania w komunikacji grupowej powinno być naciśnięcie przycisku PTT,
- możliwość połączeń grupowych na rozległym obszarze z możliwością zestawienia transmisji z użyciem wybranych stacji bazowych,
- system powinien przekazywać informację członkom grupy, jeżeli znajdą się oni poza zdefiniowanym obszarem działania grupy,
- system powinien realizować połączenia rozsiewcze do wszystkich użytkowników zarejestrowanych w wybranej stacji bazowej (Site Call) lub wybranych stacji bazowych (Multi-Site Call),
- system powinien umożliwiać opóźnione dołączenie użytkownika do połączenia grupowego,
- podczas trwania połączenia grupowego system powinien zapewnić prezentację identyfikatora strony nadającej pozostałym członkom grupy,
- system powinien przerwać połączenie grupowe w przypadku: upłynięcia zdefiniowanego w systemie czasu podtrzymania kanału komunikacyjnego, upłynięcia zdefiniowanego w systemie maksymalnego czasu trwania połączenia grupowego lub wywłaszczenia połączenia,
- w zadanym czasie przed planowanym przerwaniem połączenia, system powinien automatycznie powiadomić użytkownika o zbliżającym się momencie zakończenia komunikacji. Wymóg ten nie dotyczy wywłaszczania połączeń.

4.7.1.3 Połączenia indywidualne:

- połączenia indywidualne powinny być zestawiane przez dedykowaną dla służb cyfrową sieć radiokomunikacyjną,
- system powinien umożliwiać zestawianie połączeń indywidualnych, którymi są połączenia pomiędzy dwoma radiotelefonami, albo pomiędzy radiotelefonem a konsolą dyspozytorską,
- użytkownik, do którego jest skierowane wywołanie indywidualne, powinien mieć możliwość manualnej akceptacji tego wywołania przed zestawieniem połączenia (odbiór wywołania),
- system powinien umożliwić użytkownikowi wywoływanemu bezwarunkowo, lub wskutek spełnienia określonego warunku (zajęty, nie odpowiada, nieosiągalny) przekierowanie połączenia do innego użytkownika niż zdefiniowany przez użytkownika wywołującego,
- użytkownik, który nie odebrał przychodzącego wywołania, powinien być powiadomiony o niezrealizowanym połączeniu,
- wywoływanie skierowane do numeru zajętego, pomimo zajętości powinno być sygnalizowane,
- powinno być możliwe zakończenie połączenia indywidualnego:
  - w dowolnym momencie, przez jednego z uczestników, albo przez system,

4.7.1.9 Transmisja krótkich wiadomości tekstowych:

- użytkownicy systemu powinni mieć możliwość nadawania i odbioru krótkich wiadomości tekstowych o długości przynajmniej 255 bajtów,
- nadawanie i odbiór krótkich wiadomości tekstowych powinno być możliwe podczas komunikacji głosowej,
- opóźnienia transmisyjne usługi krótkich wiadomości tekstowych: całkowity czas przesłania wiadomości tekstowej o długości do 50 bajtów w 95% przypadków nie powinien przekraczać 5 s., w pozostałych przypadkach 10 s., całkowity czas przesłania wiadomości tekstowej o długości od 51 do 255 bajtów w 95% przypadków nie powinien przekraczać 6 s., w pozostałych przypadkach 12 s.,
- w przypadku, gdy krótka wiadomość tekstowa nie może być dostarczona do odbiorcy/odbiorców, nadawca powinien otrzymać informację o braku możliwości jej dostarczenia.

4.7.1.10 Transmisja danych pakietowych:

- system powinien umożliwiać przesyłanie danych pakietowych. Rozmiar przesyłanych danych pakietowych może być dowolny,
- brama po stronie infrastruktury systemu powinna wykorzystywać protokoły IP do przesyłania danych pakietowych między terminalami,
- opóźnienie przesyłu danych pakietowych o wielkości od 256 do 1500 bajtów, liczone od nadania pierwszego bitu datagramu IP z radiotelefonu do dostarczenia jego ostatniego bitu do bramy IP, przy założeniu, że transmisja danych z radiotelefonu odbywa się bez przerw, w 95% przypadków nie powinno przekroczyć 10 s., a w pozostałych przypadkach 20 s.,
- w przypadku, gdy dane pakietowe nie mogą być skutecznie przesłane, inicjujący transmisję powinien otrzymać informację o braku możliwości ich przesłania.

4.7.1.11 Organizacja łączności:

- system powinien umożliwiać dynamiczne tworzenie grup użytkowników zgodnie z aktualnymi potrzebami operacyjnymi poprzez zdalne dołączanie użytkowników do grupy lub odłączanie od grupy,
- system powinien umożliwiać zachowanie autonomii działania różnych organizacji poprzez wydzielenie w ramach zbudowanej sieci osobnych, wirtualnych podsieci,
- wymaga się, aby system mógł obsługiwać nie mniej niż 10 wirtualnych podsieci użytkowników, umożliwiając tworzenie rozbudowanych struktur hierarchicznych,
- system powinien umożliwiać nadawanie użytkownikom skróconych nazw, aliasów,
- adresowanie skróconymi numerami - wysyłanie do infrastruktury skróconego numeru zamiast pełnego identyfikatora,
- powinna być zapewniona możliwość bezpośredniej komunikacji pomiędzy radiotelefonami, bez udziału infrastruktury sieci,
- w trybie bezpośredniej komunikacji DMO powinny być realizowane, co najmniej następujące usługi:
  - połączenia grupowe,
  - połączenia indywidualne,
  - połączenia alarmowe,

  - przesyłanie statusów.
- w przypadku utraty komunikacji pomiędzy stacją bazową a stacjonarną infrastrukturą (węzłem sterującym) sieci, stacja bazowa powinna działać w trybie jednostrefowej lokalnej łączności trankingowej,
- w trybie jednostrefowej lokalnej łączności trankingowej stacja bazowa powinna realizować, co najmniej następujące usługi:
  - połączenia grupowe,
  - połączenia indywidualne,
  - połączenia alarmowe,
  - szyfrowanie transmisji radiowej z kluczem statycznym.
- wszyscy użytkownicy pozostający w zasięgu stacji bazowej powinni automatycznie otrzymywać informację o stanie sieci: tranking rozległy/tranking lokalny,
- użytkownik terminala powinien otrzymywać informacje o tym, że znajduje się poza zasięgiem stacji bazowej,
- system powinien umożliwiać zdalną zmianę konfiguracji infrastruktury sieci,
- system powinien umożliwiać:
  - monitorowanie ruchu w kanałach radiowych,
  - sprawdzenie rejestracji radiotelefonów,
  - raportowanie aktywności grup,
  - raportowanie aktywności indywidualnych użytkowników.
- radiotelefon powinien skanować grupy rozmówne, do których jest dołączony,
- system powinien umożliwiać zdefiniowanie, co najmniej 20 000 identyfikatorów grupowych,
- system powinien umożliwiać zdefiniowanie co najmniej 140 000 identyfikatorów indywidualnych.

4.7.1.12 Szybkie rozszerzenie zasięgu łączności:

- możliwość połączeń pomiędzy użytkownikami wykonującymi zadania w zasięgu sieci trankingowej oraz poza nią w trybie łączności bezpośredniej z wykorzystaniem dedykowanego radiotelefonu spełniającego funkcje bramy (TMO/DMO Gateway),
- w połączeniach realizowanych z wykorzystaniem bramy (Gateway) powinny być dostępne, co najmniej następujące usługi:
  - połączenia grupowe,
  - połączenia alarmowe.
- użytkownicy uczestniczący w połączeniach realizowanych z wykorzystaniem bramy powinni uzyskać sygnalizację trybu pracy "Gateway",
- możliwość połączeń dla zamkniętej grupy użytkowników wykonujących zadania poza zasięgiem stacji sieci trankingowej, wykorzystująca tryb łączności bezpośredniej z zastosowaniem dedykowanego radiotelefonu spełniającego funkcje stacji retransmisyjnej (DMO Repeater),
- w połączeniach realizowanych z wykorzystaniem stacji retransmisyjnej (DMO Repeater) powinny być dostępne, co najmniej następujące usługi:
  - połączenia grupowe,
  - połączenia indywidualne,
  - połączenia alarmowe.
- użytkownicy uczestniczący w połączeniach realizowanych z wykorzystaniem stacji retransmisyjnej powinni uzyskać sygnalizację trybu pracy "Repeater",

- znacznik daty i czasu,
- rodzaj połączenia (grupowe, indywidualne, telefoniczne, alarmowe, wysłanie statusu, wysłanie krótkich wiadomości tekstowych, głosowe, transmisja danych, afiliacja do systemu itp.),
- status połączenia (rozpoczęte, zakończone, szyfrowane, nieszyfrowane, odrzucone, dopuszczone, kolejkowane itp.),
- kierunek połączenia (radiotelefon – radiotelefon, radiotelefon - konsola, radiotelefon - grupa, radiotelefon - telefon itp.),
- identyfikatory, aliasy, adresy IP itp. stron biorących udział w połączeniu,
- czas trwania połączenia,
- ilość przesłanych danych pakietowych,
- identyfikatory stacji bazowych zaangażowanych w połączenie z jednoznacznym wskazaniem stacji, do której był zalogowany wywołujący.

- konfiguracja podsystemu powinna umożliwiać - po wprowadzeniu numeru identyfikacyjnego grupy oraz zadanego okresu, uzyskanie następujących danych o aktywności grupy rozmównej w systemie:
  - znacznik daty i czasu,
  - rodzaj połączenia (grupowe, telefoniczne, alarmowe, wysłanie statusu, wysłanie krótkich wiadomości tekstowych itp.),
  - status połączenia (rozpoczęte, zakończone, szyfrowane, nieszyfrowane, odrzucone, dopuszczone, kolejkowane itp.),
  - kierunek połączenia (konsola – grupa, radiotelefon – grupa, telefon – grupa itp.),
  - identyfikatory, aliasy, adresy IP itp. stron biorących udział w połączeniu,
  - czas trwania połączenia,
  - identyfikatory stacji bazowych zaangażowanych w połączenie z jednoznacznym wskazaniem stacji, do której był zalogowany wywołujący.
- konfiguracja podsystemu powinna umożliwiać - po wprowadzeniu numeru identyfikacyjnego radiotelefonu lub zakresu numerów identyfikacyjnych lub listy numerów identyfikacyjnych z możliwością jej importu z pliku utworzonego przynajmniej w jednym z popularnych formatów, takich jak .txt, .xls, .doc itp. - uzyskanie bieżących danych na temat użytkownika(ów):
  - bieżąca afiliacja do strefy lub jej brak,
  - bieżąca afiliacja do grupy lub jej brak,
  - ostatnie dane lokalizacyjne GPS (opcjonalnie).
- podstawowe dane z bazy użytkowników – identyfikator, alias, numer fabryczny, obecny użytkownik, status pracy w systemie (radiotelefon aktywny, wykluczony, zablokowany, przegrupowany, oczekujący na przegrupowanie lub zablokowanie, zaginiony itp.),
- procesy zarządzania wydajnością powinny określać zdolność systemu do obsługiwania generowanego ruchu poprzez charakterystykę efektywności zaspokajania potrzeb użytkowników przez system łączności,
- parametryzowanie wydajności systemu powinno odbywać się poprzez bieżące monitorowanie obciążenia stref oraz raportowanie zidentyfikowanych cech właściwych dla opisu przebiegu łączności,
- w skład powyższych cech powinny wchodzić:
  - całkowita liczba wywołań dla wskazanego obszaru, rozpatrywana jako sumaryczna liczba połączeń oraz liczba wywołań w jednostce czasu,
  - rodzaj transmisji (połączenia głosowe, transmisja danych),

  - czas trwania transmisji,
  - liczba i typ stanów niedostępności zasobów,
  - liczba stref uczestniczących w połączeniach,
  - zajętość kanałów komunikacyjnych w zadanym obszarze i jednostce czasu,
  - liczba aktywnych użytkowników oraz grup rozmównych w zadanym obszarze i jednostce czasu.
- podsystem powinien umożliwiać wgląd w historię parametrów wydajnościowych za okres min. 90 dni,
- we wszystkich podsystemach powinna być zapewniona możliwość raportowania przechowywanych danych wg zadanych parametrów czasu, zakresu i sposobu sortowania,
- raportowanie powinno zapewniać zarówno bezpośredni wydruk, jak również eksport w logicznie sformatowanej postaci do pliku w jednym, wybranym przez użytkownika formacie: tekstowym, oddzielonym tabulatorami lub innymi charakterystycznymi znakami, bazy SQL, MS Office, OpenOffice.

4.7.1.16 Łączność ziemia – powietrze:

- na etapie uzyskania pokrycia zasięgiem radiowym obszarów całych województw (zgodnie z odrębnymi wymaganiami dla zasięgów radiowych) w relacji do naziemnych urządzeń łączności radiowej TETRA. System powinien również zapewniać pokrycie dla dwukierunkowej łączności ze statkami powietrznymi (AGA) poruszającymi się z prędkością do 300 km/h na wysokości do 500 m ponad powierzchnią ziemi.
- na etapie uzyskania pokrycia zasięgiem radiowym obszarów całych województw (zgodnie z odrębnymi wymaganiami dla zasięgów radiowych) w relacji do naziemnych urządzeń łączności radiowej TETRA wymaga się wykorzystanie dla potrzeb łączności AGA europejskich zharmonizowanych zakresów częstotliwości 384,800 ÷ 385,000 MHz i 394,800 ÷ 395,000 MHz. Radiotelefony przeznaczone do łączności AGA powinny automatycznie wybierać kanał sterujący/częstotliwość stacji bazowej AGA. Wymaga się, aby konfiguracja sieci uniemożliwiała rejestrację naziemnych stacji ruchomych w komórkach przeznaczonych do łączności AGA. Dopuszcza się, aby terminal łączności AGA wykorzystywał sieć łączności lądowej, gdy statek powietrzny znajduje się na ziemi. Przenoszenie trwającego połączenia AGA pomiędzy sąsiednimi stacjami bazowymi nie może powodować zrywania komunikacji. Usługi dostępne dla użytkowników radiotelefonów na statkach powietrznych powinny być takie same jak dla użytkowników radiotelefonów w pojazdach lądowych. W przypadku braku komunikacji stacji bazowej AGA z infrastrukturą sieci, stacja bazowa powinna wstrzymać nadawanie, aby umożliwić awaryjną komunikację terminali AGA za pośrednictwem sieci naziemnej.

4.7.1.17 Rejestracja oraz archiwizacja aktywności użytkowników:

- podsystem rejestracji i archiwizacji powinien zapewniać cyfrowy zapis korespondencji głosowej wraz ze znacznikami daty i godziny umożliwiającymi odsłuch, wyszukiwanie i katalogowanie nagrań.
- podsystem rejestracji i archiwizacji powinien umożliwiać kopiowanie nagrań na przenośne nośniki danych,
- scentralizowane zarządzanie rejestracją korespondencji z możliwością zdalnego dostępu i eksportu z poziomu lokalnych stanowisk odsłuchowych z możliwością nadawania uprawnień wynikających z użytkowania wirtualnych podsieci poszczególnych użytkowników oraz struktur

- dyspozytor musi mieć możliwość zainicjowania wywłaszczającego priorytetowego połączenia indywidualnego, które poprzez wywłaszczenie otrzyma zasoby ruchowe i przerwie połączenie indywidualne lub telefoniczne niższego priorytetu, w które zaangażowana będzie strona wywoływana,
- konsola dyspozytorska musi zapewniać interfejs użytkownika do wysyłania i odbierania wiadomości tekstowych (SDS),
- konsola dyspozytorska musi umożliwiać rozsyłanie wiadomości tekstowych do wielu terminali jednocześnie,
- w momencie odebrania połączenia alarmowego, każda konsola dyspozytorska monitorująca daną grupę rozmówną musi zacząć emitować specyficzny sygnał dźwiękowy do momentu podjęcia działania przez dyspozytora;
- prezentowane na ekranie wpisy historii połączeń dla przychodzącej komunikacji alarmowej muszą być oznaczone w sposób wyróżniony. Gdy dyspozytor podejmie obsługę sytuacji alarmowej, wszystkie konsole dyspozytorskie monitorujące dana grupę rozmówną muszą otrzymać wizualną sygnalizację,
- z poziomu konsoli dyspozytorskiej dyspozytor musi mieć możliwość odsłuchu co najmniej ostatnich 12 godzin korespondencji prowadzonej na własnym stanowisku. Nagrania na liście nagrań muszą być oznaczone graficznym wyróżnikiem typu połączenia. Wyszukiwanie nagrań poprzez co najmniej przewijanie w przód i wstecz listy zarejestrowanych nagrań. Odtwarzanie nagrania z możliwością pauzy, przewijania do przodu i wstecz;
- konsole muszą posiadać wbudowany mechanizm uniemożliwiający pojawienie się sprzężeń akustycznych na sąsiadujących konsolach,
- przestrzeń robocza każdego dyspozytora konsoli musi być konfigurowalna przez administratora systemu. Administrator musi mieć także możliwość zdefiniowania kilku profili dyspozytorskich (obejmujących konkretną konfigurację konsoli) możliwych do pobrania przez dyspozytora,
- konsola Dyspozytorska musi zapewniać dostęp do zobrazowanych graficznie co najmniej 128 zasobów: TETRA, DMR, z jednoczesną obsługą co najmniej 128 sesji audio na jednej konsoli. Limity te muszą być niezależne dla każdej konsoli,
- konsola musi zapewniać tworzenie co najmniej 16 scaleń, w każdym scaleniu musi by możliwość umieszczenia co najmniej 10 zasobów. Limity te muszą być niezależne dla każdej konsoli,
- konsola musi zapewniać tworzenie co najmniej 3 multiwyborów, w każdym multiwyborze musi być możliwość umieszczenia co najmniej 20 zasobów. Ograniczenie sumarycznej liczby wszystkich zasobów w multiwyborach nie może być mniejsze niż 40,
- dostępne na konsolach dyspozytorskich zasoby grupowe, muszą być pozyskiwane poprzez bezpośrednie połączenie z systemem. Niedopuszczalne jest pozyskiwanie tych zasobów poprzez wykorzystywanie terminali,
- cała korespondencja prowadzona z wykorzystaniem konsoli dyspozytorskiej musi być rejestrowana w module rejestracji.

4.7.1.20 Radiotelefon noszony TETRA

a) wymagania ogólne:
- zgodność ze standardem ETSI TETRA,
- zakres częstotliwości pracy w trybie TMO min. 380 - 430 MHz,
- zakres częstotliwości pracy w trybie DMO min. 380 - 430 MHz,
- minimalny zakres temperatury pracy MS, anteny, akumulatora, klipsa, od -25°C do + 55°C,

- nadajnik klasy 3L (1,8W),
- kolorowy wyświetlacz,
- minimalna klasa ochrony obudowy przed wnikaniem pyłu i wody IP 65,
- pełna klawiatura alfanumeryczna.

b) wymagania funkcjonalne:
- praca w trybach TMO, DMO,
- transmisja danych pakietowych,
- wysyłanie, odbieranie krótkich wiadomości SDS,
- praca na dowolnej z co najmniej 800 zaprogramowanych grup rozmownych TMO,
- programowe definiowanie wyświetlanej nazwy grupy (minimum 12 znaków alfanumerycznych),
- programowy podział zaprogramowanych grup rozmownych na minimum 50 folderów po minimum 16 grup każdy, przy czym ta sama grupa może być przydzielona do dowolnej liczby folderów,
- programowe ograniczanie czasu nadawania,
- programowe i ręczne ustawienia grup rozmownych do pracy w skaningu ze zróżnicowanym priorytetem skanowania,
- tworzenie przynajmniej 20 różnych list skanowania po przynajmniej 16 pozycji każda, które będą uaktywniane stosownie do potrzeb użytkownika,
- wybór grup rozmównych z użyciem dedykowanego przełącznika obrotowego lub dedykowanych do tego celu przycisków,
- regulację głośności przełącznikiem obrotowym lub dedykowanymi do tego celu przyciskami,
- realizację wywołań: alarmowych, grupowych, indywidualnych i telefonicznych,
- wysyłanie i odbieranie wiadomości statusowych,
- programowe definiowanie wyświetlanej nazwy grupy DMO (minimum 12 znaków alfanumerycznych),
- programowy podział zaprogramowanych grup DMO na foldery,
- programowe przypisanie dowolnej grupy DMO do dowolnej grupy TMO, z możliwością powtórzenia tego samego kanału DMO dla dowolnej ilości grup TMO,
- korzystanie z interfejsu użytkownika w języku polskim,
- włączenie trybu alarmowego dedykowanym przyciskiem,
- realizację połączeń telefonicznych w trybie dupleks,
- realizację połączeń indywidualnych w trybie simpleks oraz w trybie dupleks,
- programowe zdefiniowanie skróconych numerów wybierania ISSI,
- programowe i ręczne zdefiniowanie listy kontaktów radiowych i telefonicznych o pojemności przynajmniej 500 pozycji,
- ładowanie kluczy maskujących do terminala za pomocą sprzętu dostarczonego przez wykonawcę w ramach zamówienia,
- zabezpieczenie kluczy maskujących; klucze nie mogą być przechowywane w terminalu w sposób jawny a ich odczyt lub przepisanie pomiędzy dwoma terminalami musi być niemożliwe;
- przystosowanie do obsługi maskowania E2E,
- realizację funkcjonalności OTAR,
- użycie programowalnych przycisków funkcyjnych (min. 2), umieszczonych w sposób umożliwiający szybki i łatwy dostęp do uprzednio zdefiniowanych funkcji,
- pracę w klasach bezpieczeństwa SC1, SC2, SC3, SC3 (z i bez GCK),
- maskowanie korespondencji TETRA–TEA2. W okresie przejściowym dopuszcza się stosowanie maskowania TEA1,

- zasilacz sieciowy 230V AC do pracy buforowej z akumulatorem – czas podtrzymania co najmniej 8h (w trybie pracy 5/5/90),

d) wymagania dla instalacji antenowej:
- antena dookólna - zależnie od projektu lokalizacyjnego, wymaga się użycie anten o wzmocnieniu >=3dBd,
- WFS ≤ 1,5 w wymaganym zakresie częstotliwości,
- dopuszczalna moc maksymalna nie mniej niż 20W,
- polaryzacja pionowa,

4.7.1.23 Radiotelefon biurkowy TETRA ze sterowaniem

a) wymagania ogólne:
- połączenie modułu biurkowego i modułu N/O, realizowane z użyciem interfejsu sieciowego TCP/IP RJ-45, bez konieczności połączenia z zewnętrzną siecią
- pozostałe parametry techniczne ogólne takie same jak dla radiotelefonu przewoźnego.

b) wymagania funkcjonalne:
- wymagania funkcjonalne takie same jak dla radiotelefonu biurkowego.

c) wymagania sprzętowe:
- moduł biurkowy z wbudowanym głośnikiem:
- mikrofon biurkowy z przyciskiem PTT,
- nożny przycisk nadawania,
- przewód zasilający DC
- moduł N/O musi stanowić zwartą konstrukcję wyposażoną zgodnie z rozwiązaniem przyjętym przez wykonawcę,

d) wymagania dla instalacji antenowej:
- wymagania dla instalacji antenowej takie same jak dla terminala biurkowego.

4.7.2 DMR

W wybranych lokalizacjach eksploatowany jest system analogowo-cyfrowy DMR, który posiada również możliwości koniecznego do wycofania systemu łączności analogowej. Rozwiązania DMR pełnią w Policji jedynie rolę uzupełniającą w stosunku do systemu TETRA. Rozwiązania DMR mogą być wdrażane jedynie w przypadku braku możliwości lub znacznych utrudnień we wdrażaniu systemu TETRA przy każdorazowym uzyskaniu zgody od Dyrektora Biura Łączności i Informatyki Komendy Głównej Policji.

4.7.2.1 Stacja retransmisyjna DMR

a) ogólne cechy użytkowe:
- praca w standardach: cyfrowym ETSI TS 102 361 oraz analogowym; w trybach simpleks/duosimpleks, dupleks

- złącze akcesoriów na obudowie umożliwiające podłączanie dodatkowych urządzeń,
- złącze umożliwiające programowanie stacji oraz transmisję danych zgodną ze standardem USB,
- programowalny adres IP,
- przypisany adres sprzętowy (MAC adres),
- zabezpieczenie hasłem przed odczytem parametrów konfiguracyjnych ze stacji retransmisyjnej,
- obsługa transmisji maskowanych i jawnych,
- zabezpieczenie przepięciowe i przeciw odwrotnemu podłączeniu biegunów zasilania,
- automatyczne ładowanie „on-line" baterii akumulatorów zasilania rezerwowego,
- automatyczne, bezzwłoczne przełączenie z zasilania sieciowego na rezerwowe i odwrotnie, zapewniające ciągłą pracę,
- automatyczne zabezpieczenie baterii przed nadmiernym rozładowaniem.

b) parametry techniczne
- minimalny zakres częstotliwości pracy 148 ÷174 MHz,
- maksymalna dopuszczalna odchyłka częstotliwości kanału ± 2 ppm,
- czułość analogowa odbiornika lepsza niż 0,4 µV dla SINAD 20 dB oraz 0,3 µV dla SINAD 12 dB,
- kodowa blokada szumów (CTCSS) wybierana programowo na dowolnym kanale analogowym z możliwością zaprogramowania dowolnego kodu z zakresu 67÷255 Hz (programowana ze skokiem 0,1 Hz),
- retransmisja tonów CTCSS,
- czułość cyfrowa 5% BER/0,3 µV,
- modulacja na kanale analogowym: częstotliwości (11K0F3E),
- modulacja na kanale cyfrowym: 2 szczelinowa TDMA (7K60FXD dane, 7K60FXW dane i głos),
- odporność na intermodulacje ≥70 dB,
- tłumienie emisji niepożądanych ≥70 dB,
- selektywność sąsiedniokanałowa ≥60 dB dla kanału 12,5 kHz,
- programowalny odstęp sąsiedniokanałowy 12,5 kHz,
- praca na dowolnym z co najmniej 16 zaprogramowanych kanałów,
- praca z dużą lub małą mocą fali nośnej nadajnika programowana w zakresie 1-25 W,
- programowe ograniczenie czasu nadawania w granicach od 15 do 480 s ze skokiem 15 s,
- protokół cyfrowy zgodny z ETSI TS102 361,
- zasilanie sieciowe 230 V ± 10 %, 50 Hz,
- minimalny zakres temperatury pracy od -30°C do +60°C.

c) wymagania uzupełniające
- metody pomiarów i parametry radiowe nie ujęte w niniejszych wymaganiach muszą być zgodne z normami: ETSI EN 300 086, ETSI EN 300 113, ETSI EN 102 361-2,

- klasa odporności na warunki środowiskowe IP 54,
- odporność na przepięcia (ESD) zgodnie z normą IEC 801-2 KV.

d) **wymagania uzupełniające**
- metody pomiarów i parametry radiowe nie ujęte w niniejszych wymaganiach muszą być zgodne z normami: ETSI EN 300 086, ETSI EN 300 113, ETSI EN 102 361-2,
- wymagania dotyczące kompatybilności elektromagnetycznej muszą być zgodne z normami: ETSI EN 301 489-1 i ETSI EN 301 489-5,
- wymagania odnośnie bezpieczeństwa urządzeń nadawczych muszą być zgodne z normą EN 60950-1.

4.7.2.3 Radiotelefon noszony DMR

a) **ogólne cechy użytkowe**
- praca w standardach: cyfrowym ETSI TS 102 361 oraz analogowym, w trybach simpeks/duosimpleks,
- możliwość zaprogramowania min. 250 kanałów z możliwością podziału na strefy,
- czytelny wyświetlacz z matrycą punktową i podświetlaniem (min. 2 wiersze), umożliwiający wizualizację odbieranych i wysyłanych wywołań, poziomu sygnału w trybie cyfrowym, stanu naładowania baterii,
- programowanie wyświetlanej nazwy kanału – min. 16 znaków alfanumerycznych,
- praca z dużą lub małą mocą fali nośnej nadajnika, programowana indywidualnie dla każdego kanału,
- programowe ograniczanie czasu nadawania,
- możliwość skanowania kanałów analogowych z kanału cyfrowego oraz użytkowników, grup i kanałów cyfrowych z kanału analogowego,
- możliwość wysyłania i odbierania wiadomości tekstowych,
- wizualna sygnalizacja (np. diodowa) stanów pracy radiotelefonu, w tym: wywołań, skaningu i stanów monitora,
- wbudowany odbiornik GPS,
- wywołanie indywidualne, grupowe, alarmowe oraz okólnikowe (wszystkich) w trybie cyfrowym z identyfikacją na wyświetlaczu abonenta wywołującego i sygnalizacją akustyczną (z możliwością wyłączenia sygnalizacji akustycznej),
- programowalny adres IP radiotelefonu,
- dedykowany łatwo dostępny przycisk sygnału alarmowego.
- radiotelefon musi posiadać poniższe funkcje sygnalizacji :
  - zdalne sprawdzenie obecności radiotelefonu w sieci,
  - zdalny monitoring,
  - zdalne zablokowanie radiotelefonu,
  - zdalne odblokowanie radiotelefonu.
- kodowa blokada szumów CTCSS wybierana programowo na dowolnym kanale analogowym,
- możliwość maskowania korespondencji w trybie cyfrowym,
- możliwość utworzenia min. 16 kluczy kodowych i przypisywania ich do kanałów,
- sterowanie MENU dedykowanymi do tego celu przyciskami oraz dodatkowo min. 3 programowalne przyciski,

- wybór kanałów – przełącznikiem obrotowym,
- regulacja głośności potencjometrem obrotowym lub dedykowanymi do tego celu przyciskami,
- złącze akcesoryjne: umożliwiające programowanie radiotelefonu i transmisję danych zgodną ze standardem USB, podłączenie dodatkowego mikrofonogłośnika z przyciskiem nadawania itp.,
- możliwość programowego tworzenia listy kontaktów (książki adresowej) - wywołań indywidualnych w trybie cyfrowym,
- możliwość wyłączenia sygnalizacji akustycznej i optycznej, tzw. „cicha praca",
- możliwość pracy w systemie cyfrowym z wieloma urządzeniami retransmisyjnymi pracującymi na tej samej parze częstotliwości, z możliwością rozróżnienia urządzeń retransmisyjnych,
- pełna klawiatura numeryczna,
- wbudowany głośnik,
- menu radiotelefonu w języku polskim.

b) **parametry techniczne**
- pasmo częstotliwości pracy 148÷174 MHz,
- modulacja na kanale analogowym: częstotliwości (11K0F3E),
- modulacja na kanale cyfrowym: 2 szczelinowa TDMA (7K60FDX dane, 7K60FXE dane i głos),
- odstęp międzykanałowy-12,5/25 kHz,
- maksymalna moc nadajnika 5 W, z możliwością ustawienia dwóch poziomów mocy: poziom niski 1W, poziom wysoki 5 W, programowana w całym zakresie częstotliwości,
- maksymalna dopuszczalna dewiacja częstotliwości ± 2,5 kHz (dla odstępu 12,5 kHz),
- stabilność częstotliwości +/- 2 ppm,
- charakterystyka pasma akustycznego (+1,-3 dB),
- łączne zniekształcenia modulacji ≤ 5%, przy 1 kHz, dewiacja 60% wartości maksymalnej,
- odstęp od zakłóceń - 40 dB dla odstępu 12,5 kHz,
- moc emitowana na kanałach sąsiednich ≤ 60 dB dla odstępu 12,5 kHz,
- wokoder cyfrowy,
- protokół cyfrowy zgodny z ETSI-TS102 361,
- czułość analogowa nie gorsza niż 0,30 µV przy SINAD wynoszącym 12 dB,
- czułość cyfrowa 5% BER/0,3 µV,
- współczynnik zawartości harmonicznych ≤ 5 %, przy 1 kHz, dewiacja 60% wartości maksymalnej i mocy akustycznej 0,5 W,
- charakterystyka pasma akustycznego (+1, -3 dB),
- selektywność sąsiedniokanałowa min. 60 dB dla odstępu 12,5 kHz,
- tłumienie sygnałów niepożądanych ≥ 70 dB dla odstępu 12,5 kHz,
- przydźwięki i szumy nie więcej niż –40 dB dla odstępu 12,5 kHz,
- moc wyjściowa akustyczna dla głośnika wewnętrznego minimum 0,5 W.

b) **pozostałe wymagania:**

- Wbudowany czytnik kart RFID, komunikacja na częstotliwości 13,56 MHz, wspierane standardy: ISO/IEC 14443-4 Typ A & B, MIFARE (Classic 1K and 4K, DESFire, MIFARE Plus), NFC forum (tag type 1, 2, 3, 4)
- Wbudowana kamera tylna min. 8 Mpix, wyposażona w lampę doświetlającą LED
- Możliwość wykonywania połączeń głosowych w sieci GSM
- uwierzytelnienie użytkowników w zakresie dostępu do aplikacji KM SWD musi odbywać się poprzez wykorzystywany w Policji serwer uwierzytelniający BTUU,
- oprogramowanie/biblioteka musi umożliwiać przeprowadzenie uwierzytelnienia i autoryzacji użytkownika w BTUU na podstawie hasła użytkownika do konta w LDAP oraz dostęp do jawnych systemów informatycznych w sieci PSTD poprzez dedykowaną aplikację KM SWD,
- mechanizm uwierzytelnienia i autoryzacji musi zapewniać jednoznaczną identyfikację użytkownika, - certyfikaty urządzenia, CUID, SSL muszą znajdować się w obszarze pamięci chronionej,
- terminal musi umożliwiać nawiązanie bezpiecznej sesji SSL/TLS,
- proces uwierzytelnienia zgodny z BTUU z wykorzystaniem serwera Proxy,
- czas logowania do systemu operacyjnego terminala z wykorzystaniem oprogramowania uwierzytelniającego nie może wynosić więcej niż 1 minuta.

4.8.2 Mobilny Terminal Przewoźny (MTP)

a) **wymagania użytkowe:**

- procesor z funkcjonalności skalowania częstotliwości jego pracy, dostosowujący wydajność do aplikacji i obciążenia w celu zwiększenia wydajności i energooszczędności, wielozadaniowy, zapewniający długi czas pracy na baterii, wydajność w testach Pass Mark, CPU Benchmark na poziomie min. 3000 pkt
- pamięć RAM min. 2GB,
- system operacyjny Microsoft Windows 10 bądź równoważny lub Android w wersji min. 8.0, w polskiej wersji językowej wraz z bezterminową licencją, dokumentacja w języku polskim,
- dokumentacja w języku polskim,
- zasilacz sieciowy AC (230V 50Hz),
- ładowarka samochodowa do terminala umożliwiająca ładowanie akumulatora terminala przewodem elastycznym z gniazda zapalniczki (bez pośrednictwa stacji dokującej), ładowarka musi obsługiwać poziom napięcia 12V, 24V DC z gniazda zapalniczki i przetwarzać napięcie do napięcia znamionowego terminala, umożliwiającego ładowanie baterii zasilającej,
- akumulator o mocy nie mniejszej niż 30Wh
- wymaga się, aby waga urządzenia nie przekraczała 1500g,
- wymaga się, aby wymiary nie były większe niż 300 mm x 200 mm x 30 mm,
- kolorowy ekran dotykowy o rozdzielczości minimum 1280x768 pixeli, przekątna ekranu nie mniejsza, niż 9,8", jasność nie mniejsza niż 350 NIT's,
- ilość kolorów co najmniej 16 mln., możliwość regulacji natężenia podświetlania ekranu, podświetlanie równomierne na całej powierzchni ekranu.
- opcjonalny rysik

- slot na kartę SD (dopuszczalny Mini, Micro),
- przestrzeń na dane min. 32 GB, SSD/eMMC,
- klawiatura wirtualna (ekranowa),
- slot standardowej karty miniSIM/microSIM,
- wbudowany głośnik, wbudowany mikrofon,
- wbudowany modem min. GPRS/EDGE/ WCDMA/HSDPA/ HSUPA/HSPA+/LTE/LTE+/5G bez blokady typu sim-lock, umożliwiający pracę w sieci każdego krajowego operatora telefonii komórkowej,
- wbudowany moduł GPS (Global Positioning System), który umożliwia jednoczesną bezkolizyjną pracę urządzeń radiowych,
- funkcjonalność określania pozycji GPS, oraz transmisji danych o położeniu z GPS poprzez łączność bezprzewodową pod wskazany adres sieciowy APN, jak również udostępnienie informacji o położeniu terminala na potrzeby aplikacji pracujących pod kontrolą systemu operacyjnego zainstalowanego w MTN,
- dane o lokalizacji muszą być przekazywane przez moduł GPS poprzez narzędzie (aplikacje) następnie do systemów centralnych Policji zgodnie z wykorzystywanym formatem. Terminal musi realizować powyższe funkcjonalności samodzielnie bez udziału operatora.
- znak CE potwierdzający że spełnienie zasadniczych wymagań określonych w przepisach wykonawczych do ustawy o systemie oceny zgodności z dnia 30 sierpnia 2004 r. (Dz. U. 2002 r. Nr 166, poz. 1360),

b) **pozostałe wymagania:**

- Wbudowana kamera tylna min. 8 Mpix, wyposażona w lampę doświetlającą LED
- uwierzytelnienie użytkowników w zakresie dostępu do aplikacji KM SWD musi odbywać się poprzez wykorzystywany w Policji serwer uwierzytelniający BTUU,
- oprogramowanie/biblioteka musi umożliwiać przeprowadzenie uwierzytelnienia i autoryzacji użytkownika w BTUU na podstawie hasła użytkownika do konta w LDAP oraz dostęp do jawnych systemów informatycznych w sieci PSTD poprzez dedykowaną aplikację KM SWD,
- mechanizm uwierzytelnienia i autoryzacji musi zapewniać jednoznaczną identyfikację użytkownika, - certyfikaty urządzenia, CUID, SSL muszą znajdować się w obszarze pamięci chronionej,
- terminal musi umożliwiać nawiązanie bezpiecznej sesji SSL/TLS,
- proces uwierzytelnienia zgodny z BTUU z wykorzystaniem serwera Proxy,
- czas logowania do systemu operacyjnego terminala z wykorzystaniem oprogramowania uwierzytelniającego nie może wynosić więcej niż 1 minuta.
- System operacyjny umożliwiający uruchamianie aplikacji napisanych w technologii Universal Windows Platform (UWP) oraz umożliwiający uruchomienie i działanie aplikacji Klienta Mobilnego SWD, działająca w trybie modern UI, napisanej w technologii Universal Windows Platform (UWP)
- wbudowany port USB min. 2.0
- Temperatury pracy: +5°C - +35°C
- Temperatury przechowywania: -10°C do +55 °C

PSW musi posiadać bezpieczny styk z siecią Internet umożliwiający realizację połączeń z terminalami policyjnymi funkcjonującymi w sieci Internet (mobilne terminale wideokonferencyjne) jak i użytkownikami spoza Policji.

System musi być zintegrowany z resortowym systemem łączności telefonicznej oraz systemem telefonii IP w sieci OST 112.

Elementy infrastruktury serwerowej jak i terminale powinny należeć do Policji.

Dopuszcza się podłączanie do PSW terminali i wideokonferencyjnych systemów pozapolicyjnych należących do organów administracji państwowej z zastosowaniem bezpiecznego punktu styku.

System musi:

- umożliwiać zabezpieczenie przed nieuprawnionym dostępem do urządzeń połączeń i zarejestrowanych danych w celu zabezpieczenia przed zmianą konfiguracji i utratą poufności i integralności,
- umożliwiać rozbudowę bez konieczności wymiany istniejących elementów systemu,
- umożliwiać zestawienie połączeń wideokonferencyjnych wraz z przesyłaniem treść z systemami wideokonferencyjnymi instytucji zewnętrznych obsługujących standardy SIP i H323.

4.9.3.1 Wymagania minimalne dla PSW.

a) system powinien być spójny i posiadać wbudowane funkcje w zakresie:
   - centralnego zarządzania serwerami, terminalami, użytkownikami, połączeniami,
   - wykrywania oraz diagnozowania błędów i awarii,
   - aktualizacji oprogramowania,
   - zabezpieczania i odtwarzania konfiguracji serwerów oraz terminali,
   - monitorowania bieżących parametrów połączeń i statusu terminali i serwerów,
   - planowania wideokonferencji,
   - rejestracji i udostępniania nagrań, streamingu do sieci wewnętrznej oraz do sieci Internet.
b) możliwość zastosowania terminali sprzętowych jak i dedykowanego oprogramowania na platformy PC lub urządzenia mobilne,
c) urządzenia systemu muszą być dostosowane do zasilania napięciem ~ 230V, 50 Hz.

4.9.3.2 Minimalne wymagane techniczno-użytkowe:

a) obsługa połączeń wielopunktowych i punkt-punkt ,
b) jednoczesna obsługa połączeń wideokonferencyjnych w oparciu o protokoły H.320, H.323 i SIP,
c) możliwość dołączenia do wideokonferencji telefonów w trybie audio,
d) możliwość dołączenia do wideokonferencji telefonów IP w trybie audio-wideo,
e) wsparcie dla WebRTC,
f) obsługa standardów kodowania wideo: H.261, H.263, H263+, H.264 AVC/SVC,
g) obsługa standardów kodowani audio: G.711 G.722. G.722.1, ,
h) obsługa H.239 i BFCP, również w połączeniach kaskadowych,

i) wsparcie dla IPv4, IPv6,
j) wsparcie dla IP QoS,
k) wsparcie dla H.460 NAT/Firewall Traversal (STUNT/TURN/ICE),
l) obsługa połączeń wideokonferencyjnych w jakości wideo HD 720p 30, Full HD 1080p 60,
m) transkodowanie w czasie rzeczywistym pomiędzy protokołami audio, protokołami wideo, protokołami sieciowymi, rozdzielczością obrazu,
n) możliwość konfiguracji wirtualnych pokoi wideokonferencyjnych z zabezpieczeniem przed nieuprawnionym dostępem kodem PIN,
o) możliwość niezależnego nagrywania minimum 20 wideokonferencji w jakości minimum HD 720p 30 każda,
p) możliwość integracji z zewnętrznym systemem pamięci masowej,
q) IVR z funkcją zapowiedzi głosowych rozpoczęcia/zakończenia nagrywania, oraz możliwością dodawania własnych zapowiedzi,
r) centralna książka adresowa,
s) integracja z LDAP,
t) edycja i wyświetlanie komunikatów tekstowych.
u) funkcje poprawy jakości obrazu w przypadku pogorszenia parametrów sieci transmisyjnej,
v) zarządzanie serwerami przez http/https przy wykorzystaniu przeglądarki internetowej,
w) obsługa połączeń wideokonferencyjnych oraz połączeń głosowych z/do sieci ISDN,
x) konfiguracja systemu musi umożliwiać logiczne wydzielenie grup z możliwością przypisania do nich zasobów sprzętowych (terminale) i licencyjnych na połączenia. Każda z grup powinna posiadać możliwość odrębnego administrowania oraz swobodę dysponowania przypisanymi zasobami. Administrator całego systemu powinien mieć możliwość zarządzania zasobami wszystkich grup.

4.9.3.3 Elementy składowe terminali sprzętowych:

a) kodek sprzętowy,
b) pilot zdalnego sterowania lub inne urządzenie zapewniające zdalne bezprzewodowe sterownie funkcjami,
c) monitor/telewizor ze stojakiem lub wieszakiem lub inne urządzenie wyświetlające obraz,
d) kamera lub zestaw kamer z systemem śledzenia i kadrowania osoby mówiącej,
e) minimum 2 mikrofony,
f) niezbędne okablowanie,
g) terminale sprzętowe powinny być wyposażone w interfejsy sygnałowe audio-wideo stosownie do wymagań użytkowników w zależności od możliwych do wykorzystania innych źródeł sygnałów audio-wideo niż kamera systemowa.
h) dopuszcza się wyposażenie dodatkowe w postaci terminali w postaci tablic interaktywnych, itp. lub stosowanie terminali specjalnych, np. o podwyższonej odporności na warunki atmosferyczne.

4.9.3.4 Wymagania minimalne dla terminala wideokonferencyjnego

a) Obsługa połączeń wideo przez sieć IP zgodnie ze standardem H323 i SIP,
b) nawiązywanie połączeń wideokonferencyjnych z poziomu terminala,
c) wsparcie dla WebRTC,
d) obsługa standardów kodowania wideo: H.261, H.263, H263+, H.264 AVC/SVC,
e) obsługa standardów kodowani audio: G.711; G.722. G.722.1, ,

6.3 Oprogramowanie biurowe

Do tworzenia dokumentów tekstowych, arkuszy kalkulacyjnych, prezentacji wizualnych, rysunków, formuł i baz danych wymaga się wykorzystywanie na Samodzielnych Stanowiskach Roboczych oraz stanowiskach dostępowych, narzędzi zawartych w darmowych dystrybucjach pakietów OpenOffice/LibreOffice/Lotus Symphony. Dopuszcza się zakup pakietów komercyjnych.

Wykaz standardowych programów obecnie wykorzystywanych w Policji:

1) Edytory tekstowe (format domyślny zapisu danych - „ .doc"):
   - OpenOffice/LibreOffice Writer,
   - MS Office Word.
2) Arkusze kalkulacyjne (format domyślny zapisu - „ .xls"):
   - OpenOffice/LibreOffice Calc,
   - MS Office Excel.
3) Programy do tworzenia prezentacji (format domyślny zapisu danych - „ .ppt"):
   - OpenOffice/LibreOffice Impress,
   - MS Office PowerPoint.
4) Programy do przeglądania dokumentów w formacie „ .pdf":
   - Adobe Reader PL,
   - Foxit Reader.
5) Programy umożliwiające odczyt formatów zapisu danych MS Office:
   - Word Viewer,
   - Excel Viewer,
   - Power Point Viewer,
   - Visio Viewer.

Zalecany wykaz programów **niestandardowych** wykorzystywanych w Policji, z uwagi na szczególne, indywidualne potrzeby:

1) Programy do tworzenia baz danych:
   - OpenOffice/LibreOffice Base
   - MS Access.
2) Programy do OCR (bezpośrednie konwertowanie skanowanych dokumentów na formaty edytowalne):
   - Abbyy Finereader PL.
3) Konwertery i generatory PDF:
   - Bullzip PDF Printer,
   - PDFCreator.

Naczelnik właściwy ds. łączności/informatyki może, w uzasadnionych przypadkach podjąć decyzję o dopuszczeniu, innych niż wymienione powyżej, rodzajów oprogramowania.

6.4 Oprogramowanie internetowe i pocztowe

Wykaz programów **standardowych** wykorzystywanych w Policji:

1) Przeglądarki internetowe (wersje posiadające wsparcie producenta),
   - Internet Explorer/Microsoft Edge,
   - Mozilla Firefox,
   - Opera,
   - Google Chrome,
2) Klienci poczty e-mail:
   - Lotus Notes,
   - MS Outlook Express,
   - MS Outlook,
   - Poczta systemu Windows,
   - Mozilla Thunderbird
   - lub inne aktualnie wdrożone w Policji

6.5 Oprogramowanie pozostałe

1) Wtyczki i rozszerzenia:
   - ActiveX,
   - Java,
   - Silverlight,
   - lub inne, niezbędne do prawidłowego działania przeglądarek internetowych.
2) Programy do nagrywania nośników optycznych:
   - Nero OEM,
   - InfraRecorder, AnyBurn,
   - wbudowane oprogramowanie systemowe,
   - lub inne do zastosowań komercyjnych.
3) Programy do archiwizacji danych:
   - 7-zip,
   - WinRAR,
   - lub inne do zastosowań komercyjnych.
4) Oprogramowanie inne niż wymienione w pkt 1) do 3), dostosowane do szczególnych potrzeb wynikających z charakteru realizowanych zadań, np. oprogramowanie Apple Mac OS, najnowsze, stabilne wersje, preinstalowane na komputerach Mac i MacBook.
5) **Oprogramowanie antywirusowe.** Na Samodzielnych Stanowiskach Roboczych oraz stanowiskach dostępowych powinno być zainstalowane oprogramowanie antywirusowe dystrybuowane centralnie lub zakupione przez jednostki organizacyjne Policji wraz z aktualizowaną bazą antywirusową.
6) **Sterowniki i niezbędne oprogramowanie.** Na Samodzielnych Stanowiskach Roboczych oraz stanowiskach dostępowych musi zostać zainstalowane niezbędne oprogramowanie oraz sterowniki w najnowszej wersji.
7) **Oprogramowanie narzędziowe.** Zaleca się administratorom wykorzystywanie oprogramowania do zarządzania środowiskiem stacji roboczych, umożliwiającym zdalne instalowanie poprawek systemowych i aplikacyjnych oraz innych niezbędnych narzędzi.

9.3.4 Ustawienia dzienników zdarzeń

Ustawienia Dziennika Zdarzeń	Wartość Ustawiona
Maksymalny rozmiar dziennika aplikacji	*20480KB*
Maksymalny rozmiar dziennika bezpieczeństwa	*20480KB*
Maksymalny rozmiar dziennika systemowego	*20480KB*
Archiwizuj dziennik po zapełnieniu, nie zastępuj zdarzeń	

Rozdział 10 Zadania Lokalnych Administratorów

Zadania lokalnych administratorów wykonują policjanci/pracownicy komórek łączności i informatyki oraz policjanci/pracownicy komórek organizacyjnych Policji, zgodnie z zakresami obowiązków.

Jeżeli sytuacja tego wymaga, kierownik jednostki lub komórki organizacyjnej Policji może podjąć decyzję o powierzeniu niektórych zadań realizowanych przez administratorów lokalnych, pracownikom zatrudnionym w tej komórce lub jednostce organizacyjnej Policji. Zakres zadań, które mogą być powierzone tym policjantom lub pracownikom Policji jest następujący:

1. Monitorowanie sieci i reagowanie na wszelkie niebezpieczeństwa mogące zagrażać poprawnym działaniu systemów/oprogramowania.
2. Zarządzanie siecią PSTD w ramach sieci wewnątrzwojewódzkiej lub sieci lokalnej, danej komórki organizacyjnej Policji (zgodnie z zakresem przyznanych uprawnień).
3. Ustanawianie wszelkich praw dostępu do zasobów plików, zgodnie z regulacjami obowiązującymi dla danego systemu.
4. Definiowanie i konfigurowanie stacji lokalnych.
5. Weryfikacja legalności oraz aktualizacja zainstalowanego oprogramowania.
6. Szkolenie policjantów i pracowników komórki organizacyjnej jednostki Policji w zakresie użytkowania posiadanych stanowisk dostępowych oraz SSR.
7. Nadzór nad prawidłową obsługą urządzeń teleinformatycznych, w tym diagnostyka i nadzór, przez użytkowników końcowych i współpraca z komórkami ds. łączności i informatyki w usuwaniu awarii.
8. Wykonywanie podłączeń i konfiguracji sprzętu informatycznego użytkowników końcowych do urządzeń peryferyjnych
9. Wymiana tuszy i tonerów w urządzeniach drukujących.
10. Wymiana uszkodzonych peryferii komputerowych.
11. Wykonywanie zestawień zawierających dane sprzętu teleinformatycznego użytkowanego w biurze/jednostce, uwzględniających wersję programu antywirusowego, adresy IP, lokalizację sprzętu, numery inwentarzowe i seryjne urządzeń oraz dane użytkowników.
12. Zgrywanie danych użytkowników sprzętu, w celu przeinstalowania systemu operacyjnego lub migracji na inny sprzęt.

Zadania administratorów lokalnych, w odniesieniu do systemów teleinformatycznych, w których są przetwarzane informacje niejawne, są uregulowane w dokumentacji bezpieczeństwa tych systemów.

Rozdział 11 Wymagania w zakresie dokumentacji systemu teleinformatycznego

Wraz z systemami teleinformatycznymi, budowanymi na potrzeby jednostek organizacyjnych Policji, powinna być dostarczana dokumentacja, umożliwiająca ich poprawne użytkowanie i administrowanie a także dalszy rozwój i modyfikacje, w tym takie rodzaje dokumentacji, jak:

I. **Dokumentacja Systemowa**, obejmująca m.in.:

- opis otoczenia systemu;
- opis wymagań funkcjonalnych i niefunkcjonalnych systemu;
- opis architektury systemu w podziale na komponenty/moduły;
- opis modelu logicznego i fizycznego systemu;
- opis relacji pomiędzy komponentami/modułami systemu oraz powiązań z innymi systemami;
- specyfikacje przypadków użycia komponentów/modułów systemu.

II. **Dokumentacja Techniczna**, obejmująca m.in.:

- opis wykonanych instalacji technicznych;
- opis struktur danych;
- opis zainstalowanego sprzętu i oprogramowania wraz z informacjami o parametrach i sposobie konfiguracji;
- instrukcje obsługi sprzętu i oprogramowania, dostarczane standardowo przez wykonawcę, wraz z informacjami o warunkach licencjonowania;
- materiały szkoleniowe i podręczniki w zakresie dotyczącym administracji i użytkowania systemu;
- opis struktury i mechanizmów funkcjonowania wszystkich interfejsów systemu;
- kod źródłowy oprogramowania z objaśnieniami/komentarzem (jeżeli wytworzono, bądź zmodyfikowano oprogramowanie dedykowane na potrzeby systemu).

III. **Dokumentacja Eksploatacyjna (procedury utrzymaniowe i awaryjne), obejmująca** m.in.:

- procedury związane z administracją i eksploatacją systemu, w tym procedury działania administratorów systemu oraz procedury działania użytkowników systemu;
- procedury o charakterze testowym;
- procedury konserwacji systemów;