I. Wymagania i zakres techniczny Kaufland dotyczący stacji ładowania pojazdów elektrycznych:

1. Moc przyłączeniowa 75–77 kVA.
2. Stacja zasilana trójfazowo.
3. Moc po stronie ładowania AC 1x22 kW.
4. Wyjście / gniazdo AC (Typ 2) – 1 szt, 22 kW, 3 x 32 A, zakres napięcia wyjściowego: 400 V (+/– 10%).
5. Moc po stronie ładowania DC 50kW**,** system ładowania Mode 4.
6. Wyjście / złącze typ CCS 2– 1 szt, 50 kW, 125 A DC (+/– 5%), zakres napięcia wyjściowego: 200 – 500 V, długość złącza (przewodu z wtyczką do ładowania) – co najmniej 3m.
7. Wyjście / złącze typ CHAdeMO – 1 szt, 50 kW, 120 A DC, zakres napięcia wyjściowego: 200 – 500 V, długość złącza (przewodu z wtyczką do ładowania) – co najmniej 3m.
8. Zabezpieczenie bezpiecznikowe 125A.
9. Ochrona przeciwprzepięciowa CPTPSM4–40/400 TNS.
10. Możliwość balansowania mocą (zdalna, programowa możliwość ograniczenia prądu ładowania)
11. Możliwość jednoczesnego ładowania dwóch pojazdów (1 auto po stronie DC, 1 auto po stronie AC).
12. Zabudowa wolnostojąca, o stopniu szczelności co najmniej IP54 oraz IK 10.
13. Zakres temperatury pracy – eksploatacja: – 30°C do + 50°C.
14. Zakres temperatury pracy – podczas składowania: – 40°C do + 70°C.
15. Niski poziom hałasu, tj: <45 dBA.
16. Montaż przez posadowienie na stopie / ławie fundamentowej
17. Zachowanie ciągłości pracy, tj. możliwości ładowania pojazdów w przypadku awarii jednego z prostowników.
18. Możliwość zastosowania kolorystyki i malowania stacji ładowania wg. wzoru ustalonego z Zamawiającym.
19. Praca w trybie bezpłatnym z możliwością zmiany **na płatny**, możliwość dokonywania płatności kartą kredytową oraz debetową lub rozbudowy stacji ładowania pozwalającej na montaż terminalu płatniczego lub innych urządzeń elektronicznych umożliwiających płatność elektroniczną zgodną z polskim prawem.
20. Obudowa wykonana ze stali nierdzewnej.
21. Sygnalizacja procesu ładowania i zakończenia ładowania.
22. Możliwość obsługi stacji ładowania z autoryzacją lub bez autoryzacji (w zależności od konfiguracji).
23. Ładowanie pojazdów elektrycznych oparte na: identyfikacja RFID, kodzie PIN, lub internetowych metodach uwierzytelniania
24. Przycisk wyłącznika awaryjnego na obudowie
25. Komunikacja zgodnie z OCPP Standard 1.6, w tym zapewnienie komunikacji z EIPA (Ewidencja Infrastruktury Paliw Alternatywnych)
26. Certyfikat CE
27. Stacja ładowania pojazdów musi spełniać wymogi ustawy z dnia 11 tycznia 2018 r. o elektromobilności i paliwach alternatywnych (Dz. U. z 2019 r. poz.1124 z późniejszymi zmianami) oraz Rozporządzenie Ministra Energii z dnia 26 czerwca 2019 r. w sprawie wymagań technicznych dla stacji ładowania i punktów ładowania stanowiących element infrastruktury ładowania drogowego transportu publicznego (Dz. U. z 2019 r. poz. 1316 z późniejszymi zmianami).
28. Standardy i certyfikacja na zgodność z normami:

a) EN 61000–6–1:2000
b) EN 61000–6–2 (2005) + AC (2005)
c) EN 61000–6–3:2007 + A1 (2011), CLASS B
d) EN 61000–6–4:2007 + A1
e) EN 61643–11 (klasa II)
f) EN 61851–1
g) EN 61851–22
h) EN 61851–23
i) EN 301489–1 V 2.2.0:2017
j) EN 301489–52V 1.1.0:2016
k) EN 301489–3V 2.2.2:2017
l) EN 301908–2V 11.1.2:2017
m) EN 301511 V 12.5.1:2017
n) EN 30033V 2.2.2:2017

o) EN 50364:2001
p) ISO 14443 A/B
q) zgodność z Dyrektywą 2014/94/EU

II. Wymagania i zakres techniczny Kaufland – zakres IT

1. Ethernet

Urządzenie musi posiadać interfejs Ethernet.
Specyfikacja:
• złącze RJ45 (IEEE 802.3)
• Izolacja galwaniczna połączenia sieciowego
• Obsługa ICMP / Ping (RFC 4560, RFC 2925, RFC 1739) – patrz także ICMP
Wymagania firmy:
• Co najmniej 100 Mbit/s full-duplex (100 Base-TX)
• Auto negocjacja
Notatka: Zasilanie urządzeń o niskim poborze mocy jest możliwe poprzez Power-over-Ethernet (PoE – IEEE Standards 802.3AF/3AT) – do 12 Watt. Musi to być ściślej uzgodnione z osobami kontaktowymi w Schwarz IT.

2. Kabel światłowodowy

Urządzenie może posiadać dodatkowy interfejs kabla światłowodowego.
Specyfikacja:
Standardowe złącze SFP-Port (Small Form-Factor Pluggable)
Alternatywnie: 1000Base-SX (IEEE 802.3z)
Wymagania firmy:
LC lub SC (bez preferencji)

3. Sieć komórkowa

Urządzenie może komunikować się przez sieć komórkową. W takim przypadku należy spełnić następujące wymagania:
Funkcja Watchdog
Musi istnieć funkcjonalność Watchdog dotycząca komunikacji przez sieć komórkową. Można to zaimplementować, próbując dotrzeć do zewnętrznego adresu IP przez PING. Jeśli komunikacja przestanie działać, urządzenie musi automatycznie ponownie połączyć się z siecią komórkową.
Standardy komórkowe
Urządzenie musi obsługiwać 2G i 4G. Urządzenie powinno obsługiwać 5G.
Zdalna aktualizacja
Sprzęt musi być aktualizowany zdalnie.
Inne
Urządzenie powinno spełniać następujące wymagania:

- siła sygnału powinna być czytelna zdalnie
- powinno być możliwe zamontowanie anteny zewnętrznej
- powinno być możliwe ponowne uruchomienie urządzenia przez SMS

4. Protokół IP

IPv4
Urządzenie musi obsługiwać protokół IPv4.
Specyfikacja:
RFC 791
Gratuitous ARP (RFC 826)
Path MTU Discovery (RFC 791)

Wymagania firmy:
Gratuitous ARP
Urządzenie musi być skonfigurowane do wysyłania co najmniej 3 pakietów ARP przy starcie i cyklicznie co 15 minut. Pakiety ARP mają być wysyłane na adres IP z zakresu IP Grupy Schwarz.
W celu zapewnienia poprawnego przypisania urządzenia w tablicy adresów MAC dołączanych przełączników konieczna jest regularna wysyłka bezpłatnych pakietów ARP.

Path MTU Discovery
Path MTU Discovery to funkcja protokołu IPv4 służąca do określania maksymalnego rozmiaru pakietu. Użycie bitu „Nie fragmentuj" NIE jest dozwolone.
Ze względu na restrykcyjne ustawienia routera odpowiedź dotycząca maksymalnego rozmiaru pakietu jest tracona na drodze do nadawcy pakietów. Powoduje to nieprawidłowe działanie mechanizmu, powodując problemy z siecią.
Statyczny adres IP
Musi istnieć możliwość skonfigurowania statycznego IP z zakresu IP Grupy Schwarz.

IPv6

Urządzenie musi obsługiwać protokół IPv6 w perspektywie średnioterminowej. Niezbędne jest zapewnienie umownej obsługi IPv6 na urządzeniach w perspektywie średnioterminowej (w ciągu najbliższych 36 miesięcy), a także zapewnienie możliwości zdalnej aktualizacji do IPv6.
IPv6 musi być obsługiwany w tzw. trybie podwójnego stosu (IPv4 i IPv6 równolegle).

Specyfikacja:
RFC 2460

Podsieci

Podsieci pomiędzy komponentami muszą być oparte na protokołach magistrali szeregowej (np. Modbus RTU, CAN itp.) lub wykorzystywać wejścia/wyjścia analogowe/cyfrowe. Podsieci oparte na IP są zabronione.
Wymagania firmy:
Własne sieci oparte na Ethernet są dozwolone tylko po konsultacji z działem IT Grupy Schwarz.

Uwierzytelnianie sieci

Specyfikacja:
IEEE 802.1X
RFC3748 (EAP)

Wymagania firmy:
Urządzenie powinno być w stanie uwierzytelnić się w sieci za pomocą IEEE 802.1X.

Uwaga:
Jeśli urządzenie nie obsługuje uwierzytelniania zgodnego ze standardem IEEE 802.1X, można również zaimplementować białą listę adresów MAC.

Konfiguracja:
Korzystanie z EAP–TLS

5. **Procedury szyfrowania**
   Należy stosować następujące metody szyfrowania:

Szyfrowanie symetryczne
Specyfikacja:

Encryption algorithm	**minimum Key length (bit)**	**Operational modes**
AES	128	CBC, CCMP, GCM, CTR
Twofish	192	CBC, CTR
Serpent	192	CBC, CTR

MARS	192	CBC, CTR
CAMELLIA	192	CBC, CTR
ChaCha20	256	Poly1305

Szyfrowanie asymetryczne

Algorytm

Encryption algorithm	**Key length (bit)**	**Comments**
RSA	2048	
DSA	2048	If the value k is generated according to RFC6979 and SHA−2 is used as the hash algorithm
ElGamal	2048	

ECC

Wszystkie metody kryptografii krzywych eliptycznych (ECC) obsługują klucz o długości co najmniej 224 bity.
ECC umożliwia obliczenie mniejszych kluczy szyfrowania bez powodowania obniżenia poziomu bezpieczeństwa do poziomu porównywalnego z RSA.

Procedura wymiany kluczy

- DHE
- ECDH
- ECDHE
- SIDH
- PSK
- KRB5
- SRP
- PCT

Szyfrowanie danych
Specyfikacja:
AES (NIST 197)
Wymagania firmy:
AES z kluczem o długości 512 bitów
Certyfikaty
Należy stosować certyfikaty wystawione przez Grupę Schwarz lub uznany publiczny urząd certyfikacji (patrz poniżej).
Certyfikaty Grupy Schwarz
Jeżeli certyfikaty mają być wydawane przez Grupę Schwarz, są to certyfikaty wewnętrznie generowane i weryfikowane przez Grupę Schwarz o ważności 27 miesięcy. W tym celu Grupa Schwarz prowadzi własną infrastrukturę PKI.

Certyfikaty stworzone przez Grupę Schwarz mogą być dostarczone w jednym z następujących formatów:
*.pem
*.p12 (preferowane)
Publiczne urzędy certyfikacji
Publiczne jednostki certyfikujące uznane przez Grupę Schwarz:

- SwissSign

Z innych publicznych urzędów certyfikacji można korzystać po sprawdzeniu ich przydatności przez dział IT Grupy Schwarz.

Rejestracja certyfikatu
Ze względu na dużą liczbę urządzeń należy wdrożyć automatyczną rejestrację certyfikatów. Aktualizacja certyfikatów powinna być przeprowadzana nie rzadziej niż co 27 miesięcy. Istnieje kilka możliwości rejestracji certyfikatu. Należy określić wraz z informacją Schwarz, który z nich będzie używany:
SCEP
SCEP to protokół do automatycznej aktualizacji certyfikatów.

Specyfikacja:
IETF „projekt gutmann-scep-05"
EST
EST (Enrollment over Secure Transport) to protokół automatycznej aktualizacji certyfikatu.
Specyfikacja:
RFC7030
OCPP
Specyfikacja OCCP 2.0.1 opisuje, w jaki sposób ładowarka może zażądać nowego certyfikatu w CSMS wysyłając SignCertificateRequest.
Specyfikacja:
OCPP 2.0.1

6. Interfejsy komunikacyjne

Cała komunikacja musi odbywać się za pomocą szyfrowanych protokołów.
OCPP 1,6
Do komunikacji z backendem OCPP dane muszą być dostarczone przez OCPP1.6J. Należy przestrzegać wymagań dotyczących szyfrowania. OCPP 1.6 jest zaimplementowany zgodnie ze specyfikacją OCPP jako wariant JSON z Websocket (Open Charge Point Protocol 1.6 i Open Charge Point Protocol JSON 1.6).
Specyfikacja:
OCPP 1,6
OCPP 1.6 Rozszerzenia bezpieczeństwa
Specyfikacja:
Oficjalny dokument dotyczący bezpieczeństwa OCPP 1.6 (wydanie trzecie)
certyfikacja zgodności OCPP z oficjalnym programem certyfikacji OCA OCPP 1.6
Ładowarka powinna być certyfikowana przez oficjalny program certyfikacyjny OCPP 1.6 OCA.
Inteligentne ładowanie OCPP 1.6
OCPP 2.0.1
Specyfikacja:
OCPP 2.0.1
Dezaktywacja punktów ładowania
Jeśli punkty ładowania wykorzystują ten sam zasilacz i nie mogą być używane równolegle, nieużywany punkt ładowania musi być oznaczony jako „Niedostępny" lub „Zawieszony EVSE".

Adresowanie Backendu OCPP:
Adresowanie backendu OCPP musi być możliwe przy użyciu zarówno adresu IP, jak i nazwy hosta. Musi być możliwe korzystanie z serwera DNS grupy Schwarz.
Zdalna konfiguracja:
Następujące ustawienia muszą być zmieniane za pomocą polecenia SetConfiguration OCPP:
• URL backendu
• Identyfikator punktu ładowania
• Tryb autoryzacji ładowarki (z autoryzacją/bez konfiguracji)

7. ICMP (ping)

Należy zapewnić obsługę polecenia PING (ICMP / Ping).
Specyfikacja:
RFC 4560

RFC 2925
RFC 1739

8. DNS

Musi istnieć możliwość używania DNS jako klienta (rozpoznawanie nazw). Wpisy DNS nie mogą być tworzone przez samo urządzenie. Wpisy tworzone są przez działy IT Grupy Schwarz na podstawie adresu IP urządzenia. Urządzenie powinno być dostępne za pośrednictwem wpisu DNS.
Specyfikacja:
RFC 1034
RFC 1035
Wymagania firmy:
Nazwę hosta urządzeń należy określić w porozumieniu z działem IT Grupy Schwarz.

9. HTTPS (serwer WWW)

Jeśli na urządzeniu używany jest serwer WWW, należy spełnić następujące wymagania.

Specification:

- RFC 2660
- HTTPS (RFC 2818) – at least TLS 1.2 (RFC 5246), Technical guideline TR-02102-2 of the Federal Office for Information Security
- OWASP Application Security Verification Standard (ASVS) Project
- OWASP Top 10 Application Security Risks – 2017
- BSI Guidelines for the Development of Secure Web Applications
- W3C – Next Generation Web Technologies Build on Stable Foundation
- HSTS – RFC6797
- web.dev (Mozilla)

Wymagania firmy:
TLS:

- Minimum cipher suite key length 256 Bit (Recommended 512 Bit)
  Perfect forward secrecy is required if access is via external networks, otherwise recommended.
- Permissible protocols for key exchange are Diffie-Hellmann Group 15, 16, 17, 18, 20 and 21, whereby Group 16 is recommended.
- Client-initiated renegotiation must be rejected by the server.
- Authentication is carried out via user name / password.

10. HSTS:

„HTTP Strict Transport Security" musi być zaimplementowane po stronie serwera WWW.

11. ISO 15118

Ładowarka obsługuje wymienione funkcje:
Plug & Charge
Ładowarka musi obsługiwać normy ISO15118-2 i ISO15118-20.
Ładowarka musi posiadać certyfikat Hubject für ISO 15118 Plug & Charge.
Vehicle to Grid

12. Wymagania funkcjonalne

Zegar wewnętrzny
Urządzenie musi mieć wewnętrzny zegar – rekomendowany standard UTC.
Wymagania firmy:
Zmiana z czasu zimowego na letni musi odbywać się automatycznie na podstawie aktualnej daty i skonfigurowanej strefy czasowej.

13. Aktualizacja

Musi istnieć możliwość aktualizacji oprogramowania urządzenia (systemu operacyjnego i aplikacji) przez sieć. Jeśli urządzenie składa się z kilku komponentów (np. Routera,...) wszystkie komponenty muszą mieć możliwość zdalnej aktualizacji.

Wymagania firmy:
Należy zapewnić autentyczność/autentyczność zaimportowanej aktualizacji (np. poprzez podpisywanie na podstawie skrótu/certyfikatu)

Czas ostatniej aktualizacji musi być możliwy do prześledzenia
Aktualizacje powinny być aktualizowane za pomocą narzędzia wiersza poleceń (słowo kluczowe: przydatność masowa)
Zarządzanie przepustowością musi być zaimplementowane dla pakietów powyżej 50 MB
Rozdzielenie dwóch procesów „transmisja" i „instalacja". „Instalacja" powinna mieć możliwość odbycia się w określonym czasie
Wszystkie używane biblioteki (Log4j, OpenSSH itp.) muszą być regularnie aktualizowane, aby zamknąć znane luki w zabezpieczeniach.

14. Konfiguracja

Musi istnieć możliwość pobrania konfiguracji urządzenia lub zdalnego załadowania nowej konfiguracji na urządzenie.
Wymagania firmy:
Musi istnieć możliwość wyświetlenia konfiguracji w kilku językach. Język niemiecki i angielski muszą być domyślnie obsługiwane. Dodatkowe języki – w tym języki spoza obszaru języków niełacińskich (np. bułgarski, grecki) – powinny być dodawane.

15. Watchdog

Stan urządzenia musi być monitorowany przez watchdog (monitorowanie procesu).
Wymagania firmy:
Jeśli poszczególne usługi ulegną awarii, należy je automatycznie ponownie uruchomić. Gdy urządzenie nie będzie już w pełni funkcjonalne, watchdog musi zainicjować automatyczne ponowne uruchomienie urządzenia.

16. Ochrona fizycznych interfejsów

Ochrona fizycznych interfejsów, jeśli są dostępne
Ograniczanie dostępu fizycznego
Ograniczanie dostępu po stronie oprogramowania

17. Zamykana obudowa

Obudowa ładowarki musi być zamykana za pomocą wkładki bębenkowej. Musi istnieć możliwość wymiany standardowego wkładki bębenkowej na wkładki, które nie są używane u innych klientów.

18. Wyświetlacz

Ładowarka powinna mieć wyświetlacz. Należy spełnić następujące wymagania:
Szczegóły techniczne
Ekran powinien mieć minimalną wielkość 15". Wyświetlacz musi być w stanie pokazać kolory co najmniej 800x400 pikseli. Wyświetlacz powinien obsługiwać Full HD (1920 x 1080 pikseli).
Ekran powinien być dotykowy. Jeśli ekran nie jest ekranem dotykowym, muszą być przyciski do interakcji z użytkownikiem.
Ekran powinien mieć jasność >=1000nits.
Kod QR EVSE-ID
Powinno być możliwe wygenerowanie i pokazanie kodu QR z indywidualnymi identyfikatorami EVSE punktów ładowania.
Personalizacja
Wszystkimi ustawieniami personalizacji należy zarządzać za pośrednictwem scentralizowanego backend'u. Dlatego konfiguracja może być obsługiwana przez własny, zastrzeżony backend lub konfiguracja musi być wykonana za pomocą ustawień OCPP.
Wygaszacz ekranu

Musi istnieć możliwość zdefiniowania własnych ekranów dla wygaszacza ekranu wyświetlacza ładowarki.
Powinna istnieć możliwość zdefiniowania własnego wideo dla wygaszacza ekranu.
Identyfikacja wizualna ekranów
Powinna istnieć możliwość modyfikacji ekranów dotyczących identyfikacji korporacyjnej:
użycie własnego logo firmy
definiowanie kolorów
Nośniki uwierzytelniające
Musi istnieć możliwość skonfigurowania, które nośniki uwierzytelniania mają być wyświetlane jako dozwolone nośniki uwierzytelniania. Każda kombinacja następujących nośników musi być konfigurowalna:

- RFID
- app
- Direct Payment page
- card terminal

Wszystkimi ustawieniami personalizacji należy zarządzać za pośrednictwem scentralizowanego backend'u. Dlatego konfiguracja może być obsługiwana przez własny, zastrzeżony backend lub konfiguracja musi być wykonana za pomocą ustawień OCPP.

Język
Zawartość wyświetlacza musi być widoczna w różnych językach. Użytkownik powinien mieć możliwość przełączania się między językami. Po pewnym czasie język powinien wrócić do skonfigurowanego standardowego języka ładowarki.
Standardowy język ładowarki powinien być konfigurowalny przez OCPP.
Ponieważ ładowarka będzie używana w kilku krajach, ładowarka musi obsługiwać UTF-8. Musi istnieć możliwość łatwego dodawania nowych języków. Dlatego należy zaimplementować mechanizm eksportu i importu plików językowych.

19. Maksymalne obciążenie ładowarki

Musi istnieć możliwość zdalnej zmiany skonfigurowanej mocy połączenia (maksymalnego obciążenia ładowarki).
Moc przyłącza powinna być ustawiana w kW jako parametr OCPP.

20. Hasła

Musi istnieć możliwość odwzorowania koncepcji roli/autoryzacji na urządzeniu. W tym celu należy rozróżnić następujące role użytkowników. Role powinny być buforowane tylko lokalnie, a przy każdym logowaniu użytkownika konieczne jest sprawdzenie protokołu LDAP.

Wymagania firmy:

Role	Description	Functions	Type
Installation companies	Delivers and installs the initial configuration, if necessary	Configuration	Local / generic
Schwarz Group Administrator	Responsible for 1st level support	Remote access, restart, debugging	LDAP / personalized
Manufacturer	Responsible for 2nd level support and software maintenance	Remote access, restart, debugging, updates	LDAP / personalized

Użytkownicy lokalni
W zasadzie hasła muszą być osobiste. Wyjątki są dozwolone tylko po zatwierdzeniu przez dział bezpieczeństwa IT.
Wymagania firmy:
– Minimalna długość – 8 znaków
– kryteria złożoności: do uzgodnienia
Konta systemowe
Hasła systemowe są używane przez system do uwierzytelniania. Zmiana hasła musi być przeprowadzana przy każdej aktualizacji oprogramowania układowego. Producent jest odpowiedzialny za zapewnienie, że nowe hasło zostanie przekazane w odpowiednim czasie Grupie Schwarz i firmom instalacyjnym.

Wymagania firmy:
– Minimalna długość hasła: 8 znaków (zalecane 30)
– Złożoność hasła: należy rozróżnić wielkie i małe litery, znaki specjalne i cyfry muszą być możliwe do użycia.
– Złożoność hasła: należy użyć co najmniej dwóch czynników (cyfry, znaki specjalne lub wielkie/małe litery).
– Wymuszona przez system zmiana hasła co 24 miesiące

Przechowywanie haseł na urządzeniu
Wymagania firmy:
Hasła nie mogą być przechowywane w postaci zwykłego tekstu

21. System operacyjny
Jesteśmy otwarci na wybór systemu operacyjnego.
Musi to być system operacyjny, który w trakcie cyklu życia jest dostarczany z aktualizacjami zabezpieczeń. Nie można używać systemów, które nie są już obsługiwane przez producenta/dewelopera.
W przypadku korzystania z Linuksa należy użyć wersji jądra z LTS.
Jeśli używana wersja systemu operacyjnego nie jest już utrzymywana przez dostawcę lub organizację, zwłaszcza jeśli nie otrzymuje już poprawek bezpieczeństwa, urządzenie musi zostać zaktualizowane do nowszej wersji lub urządzenie musi zostać wycofane (informację o tym należy przesłać do Schwarz tak wcześnie, jak to możliwe).
Specyfikacja:
Różne w zależności od systemu operacyjnego
Wymagania firmy:
Usługi systemowe i porty, które nie są wymagane do działania aplikacji, należy dezaktywować lub usunąć.
Poprawki bezpieczeństwa muszą być regularnie instalowane.
Poprawki bezpieczeństwa dla krytycznych luk w zabezpieczeniach nie są cykliczne i muszą być testowane i instalowane natychmiast po ich pojawieniu się.

22. Dokumentacja
Przeglad komunikacji (porty)
Konieczna komunikacja sieciowa musi być udokumentowana.
Pełna lista otwartych portów (TCP i UDP) oraz ich kierunku komunikacji (niezbędne do prawidłowej aktywacji sieci).
Dla każdego portu należy podać nazwę korzyści oraz aplikacji/funkcji.
Używane oprogramowanie/biblioteki
Oprogramowanie i biblioteki używane w produkcie muszą być udokumentowane. Dokumentację należy udostępnić Schwarz IT ze szczegółami użytych wersji i wskazaniem licencji na bibliotekę.

23. Środowisko

Urządzenie musi spełniać co najmniej wymagania IP20.
Urządzenie musi być zaprojektowane do pracy w temperaturach od +0 do +50 °C.
Jeżeli napięcie zasilania odbiega od 220–230 V AC, należy dołączyć odpowiedni zasilacz. Zasilanie musi być wykonane za pomocą złącza wtykowego, które umożliwia nieprzeszkolonemu personelowi odłączenie zasilania.
Jeśli urządzenie jest używane w bardziej specyficznym środowisku (na zewnątrz, mrożonki), musi spełniać wymagania tam panujące.

24. Czytnik RFID
Jeśli używany jest czytnik RFID, czytnik musi spełniać następujące wymagania:
Specyfikacja:
support of ISO 14443 A
support of Legic Prime
support o Legic Advant
Wymagania firmy:
Identyfikator CID, który jest przechowywany w segmencie 1, musi zostać odczytany i użyty jako identyfikator
Powód:
Grupa Schwarz korzysta z kart Legic Prime i Legic Advant RID dla pracowników

25. Karty pamięci
Jeśli używana jest karta pamięci (karta SD, karta Flash,...) czytnik musi spełniać następujące wymagania:
Specyfikacja:
- Industrial Grade
- MTBF > 2.000.000 hours
- TBW > 120 TByte
- at least MLC flash, SLC flash is recommend

Wymagania firmy:
Temperatura pracy karty pamięci musi odpowiadać istniejącym temperaturom w otoczeniu.

26. Powiadamianie o incydentach bezpieczeństwa

W przypadku ujawnienia faktów krytycznych dla bezpieczeństwa w kontekście aplikacji, które negatywnie wpływają na zależne procesy biznesowe i/lub mogą w inny sposób zaszkodzić firmie, incydent związany z bezpieczeństwem należy jak najszybciej zgłosić Grupie Schwarz.

27. Regularne aktualizacje urządzeń
Aplikacje muszą być aktualizowane za pomocą aktualizacji zabezpieczeń i ustawień zabezpieczeń.
Aktualizacje zabezpieczeń dotyczące krytycznych luk w zabezpieczeniach należy natychmiast zainstalować lub natychmiast dostosować ustawienia zabezpieczeń.
W przypadku korzystania z produktów open source należy sprawdzać aktualność przynajmniej co sześć miesięcy i w razie potrzeby integrować nowsze wersje.
Zmiany muszą być wcześniej przetestowane, skoordynowane z Grupą Schwarz i udokumentowane.

28. Podawanie adresu MAC po zamówieniu
Dopóki stacja ładująca nie zostanie uwierzytelniona w sieci za pomocą certyfikatu, adres MAC jest używany jako obejście uwierzytelniania. Grupa Schwarz musi zostać poinformowana o adresie MAC przed dostawą stacji ładującej. Jest to jedyny sposób na zapewnienie, że uwierzytelnianie w sieci jest możliwe w momencie uruchomienia.