Cyberbezpieczeństwo bezkluczowego zarządzania dostępem

Biała księga dla Infrastruktury Krytycznej

ASSA ABLOY
Global Solutions

assaabloyglobalsolutions.com

Experience a safer
and more open world

Spis treści

1. Wprowadzenie

Cyfryzacja kształtuje wszystkie branże. Nowe technologie są rozwijane i dostosowywane w infrastrukturze krytycznej, aby usprawniać operacje. Bezprzewodowe urządzenia bezpieczeństwa oferują nieograniczone możliwości ochrony infrastruktury, ale mogą rodzić też pytania dotyczące cyberbezpieczeństwa. W tym dokumencie chcemy wskazać jak technologia bezprzewodowa umożliwia bezpieczne zarządzanie dostępem.

Dostęp do miejsc bliskich i odległych za pomocą cyfrowego klucza

Dla większości pracowników smartfon jest prawdziwym wielofunkcyjnym urządzeniem do pracy. Może wykonywać i odbierać połączenia, organizować spotkania, asystować i pomagać, a nawet działać jako urządzenie do uwierzytelniania i płatności. Dodatkowo, może być łatwo używany jako bezpieczny cyfrowy klucz – lub token uwierzytelniający – do uzyskiwania dostępu do różnych miejsc i obiektów.

Zaufanie jako najważniejszy element rozwiązań cyfrowych

Gdy cyberbezpieczeństwo jest uwzględniane i priorytetowo traktowane we wszystkich rozwiązaniach cyfrowych, działaniach i punktach dostępu, rozwiązania bezprzewodowe mogą uczynić krytyczne obiekty infrastruktury bardziej inteligentnymi, lepiej połączonymi i bezpieczniejszymi. Cyberbezpieczeństwo dotyczy urządzeń, ludzi i praktyk. W centrum wszystkiego znajduje się zaufanie – zarówno do urządzeń, jak i do wiedzy, że Twoi pracownicy i kontrahenci są wyposażeni w umiejętności bezpiecznego korzystania z tych urządzeń.

1.1 Dlaczego cyberbezpieczeństwo jest tak ważne?

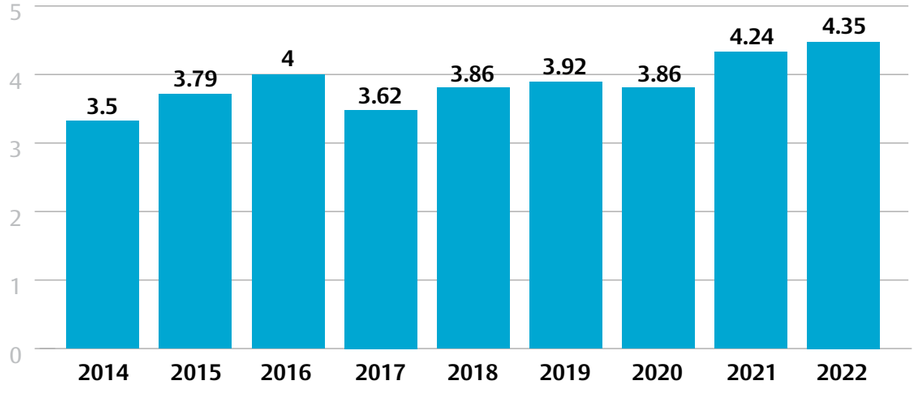
Otaczająca nas rzeczywistość staje się coraz bardziej cyfrowa i połączona. Firmy polegają na Internecie, a wiele naszych danych osobowych jest przechowywanych online i na naszych urządzeniach. Napotkanie ryzyk, które zagrażają naszemu bezpieczeństwu jako jednostkom lub powodują szkody dla firm i infrastruktury publicznej, jest realne, nawet podczas korzystania z otwartej sieci. Dlatego potrzebne są środki cyberbezpieczeństwa, aby wzmocnić integralność i bezpieczeństwo.

Czy wiesz, że...

Cyberprzestępczość można podzielić na dwa typy: naruszenia bezpieczeństwa danych i sabotaż. Naruszenia mają na celu uzyskanie nie tylko danych osobowych, ale także własności intelektualnej. Sabotaż ma na celu zniszczenie infrastruktury i ważnych systemów. Średni globalny koszt naruszeń danych rośnie. W 2022 roku średni koszt jednego naruszenia wyniósł 4,35 miliona USD. (Statista)

Średni koszt naruszenia danych na świecie w latach 2014-2022

(w milionach USD)



Szczegóły: na całym świecie, Instytut Ponemon, od 2014 do 2022 roku, 550 firm

2. Obawy i wyzwania wobec cyberbezpieczeństwa Infrastruktury Krytycznej

Menedżerowie ds. bezpieczeństwa, ochrony i operacji pracujący w infrastrukturze krytycznej nadzorują wiele operacji, co wymaga pełnej świadomości sytuacyjnej. Wiele usług musi być świadczonych 24/7, bez przerw, dlatego infrastruktura, zasoby i personel muszą być chronione. Operacje i sprzęt, w tym pojazdy, wymagają monitorowania, śledzenia i zarządzania dostępem. Wszystko to musi być zgodne z lokalnymi przepisami i regulacjami.

Z punktu widzenia bezpieczeństwa informacji, profesjonaliści zajmujący się infrastrukturą mogą mieć trudności z porównaniem aspektów cyberbezpieczeństwa między dostępnymi rozwiązaniami i nadążaniem za najnowszymi zagrożeniami i rozwojem w dziedzinie cyberbezpieczeństwa. Nawet jeśli dostawca ma odpowiedzi i opisy, praktyczny wpływ może być trudny do zrozumienia – nie mówiąc już o porównaniu. Dlatego chcemy podzielić się informacjami na temat niektórych aspektów dotyczących bezpieczeństwa bezprzewodowego i cyberbezpieczeństwa w tym dokumencie.

2.1 Bezprzewodowe zarządzanie dostępem: Czym są poświadczenia mobilne?

Poświadczenia mobilne to cyfrowy klucz, którego używasz za pomocą smartfonu. Zastępują klucze fizyczne, karty i breloki do budynków i infrastruktury. Zaletami poświadczeń mobilnych są łatwośc użycia i wielowarstwowe bezpieczeństwo. Dla przykładu: prawa dostępowe ABLOY BEAT to poświadczenia mobilne, które mogą byc użyte przy pomocy dedykowanej aplikacji BEAT oraz innej zintegrowanej aplikacji Klienta.

Jakie warstwy bezpieczeństwa oferują poświadczenia mobilne?
Po pierwsze to cyberbezpieczeństwo oferowane przez producenta urządzenia oraz dostawcę sieci komórkowej. Po drugie cyfrowe poświadczenia są przechowywane w postaci zaszyfrowanej w telefonie. Poświadczenia Seos od ASSA ABLOY oferują zaawansowane szyfrowanie oraz ochronę prywatności co oznacza, że nawet jeśli osobie niepowołanej uda się uzyskać dostęp do danych to będą one dla niej niezrozumiałe.

A co z bezpieczeństwm urządzenia?
Smartfony już wykorzystują odciski palców, rozpoznawanie twarzy i inne dane biometryczne oraz hasła zabezpieczające. Ponadto, dodatkowe uwierzytelnianie może być wymagane w samej aplikacji poświadczeń. Istnieje również ochrona innego rodzaju - ludzie prawdopodobnie zauważą brak telefonu znacznie wcześniej niż zgubienie klucza. Wszystko to tworzy wielowarstwową ochronę dla bezprzewodowego i mobilnego rozwiązania dostępu.

2.2 Wdrażanie niezbędnych warstw cyberbezpieczeństwa

Kolejne warstwy cyberbezpieczeństwa zwiększają bezpieczeństwo fizyczne. Istnieją trzy ważne procedury, które powinny być wykorzystane – szyfrowanie, uwierzytelnianie i autoryzacja.

1. Szyfrowanie
Informacje mogą być ukryte za pomocą szyfrowania. Szyfrowanie chroni wszystkie dane, które przemieszczają się między urządzeniami, kodując informacje lub mieszając czytelny tekst, aby uczynić go bezsensownym i chronić go przed nieautoryzowanymi użytkownikami. Na następnej stronie wyjaśnimy szyfrowanie bardziej szczegółowo.

2.Uwierzytelnianie
Uwierzytelnianie identyfikuje użytkownika i system zarządzania dostępem. Gdy obie strony mogą być pewne, kto jest po drugiej stronie, prawa dostępu mogą być przyznane i używane. Uwierzytelnianie użytkownika obejmuje środki identyfikacyjne aplikacji, a także biometrię lub hasła telefonu w celu weryfikacji użytkownika. Te informacje są również uwierzytelniane przez system zarządzania dostępem. Jeśli otrzymane dane są nieprawidłowe, system zarządzania lub zamek nie odczyta danych.

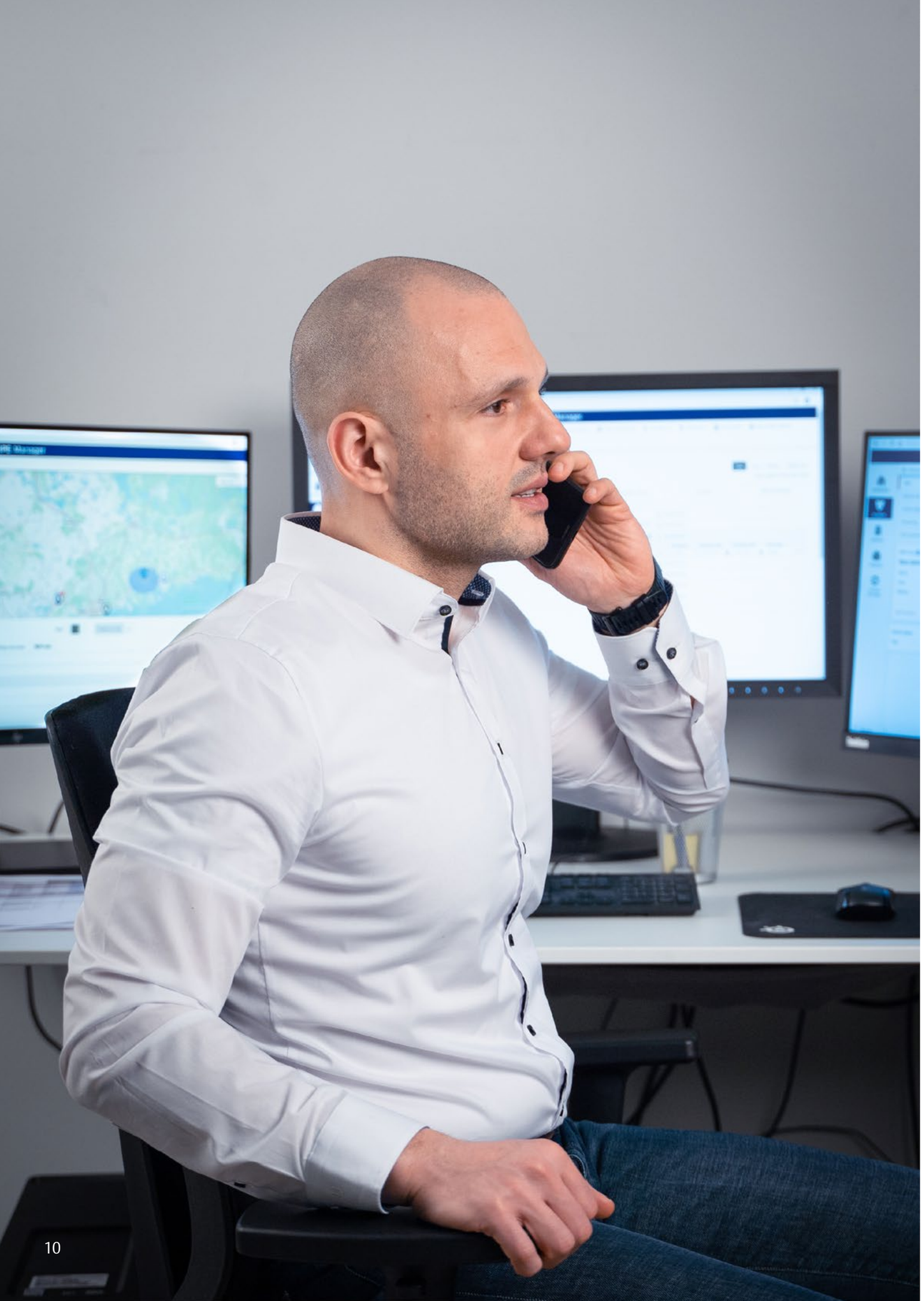
3. Autoryzacja
Autoryzacja określa, co każdy użytkownik może zrobić w aplikacji lub z otrzymanymi danymi, na przykład, czy użytkownik może najpierw otrzymać prawa dostępu, a następnie osobiście je udostępnić. Dzięki prawom dostępu użytkownicy mogą być ograniczeni do otrzymywania i używania tylko swoich osobistych praw dostępu i nigdy ich nie udostępniać dalej. To również zwiększa bezpieczeństwo fizyczne.

2.3 Co to jest szyfrowanie?

Szyfrowanie miesza czytelne dane, aby wyglądały na losowe, co pomaga zapobiegać nieautoryzowanemu użyciu danych. Istnieją dwie popularne metody szyfrowania danych. Pierwsza to szyfrowanie symetryczne, gdzie wszystkie urządzenia używają tego samego tajnego klucza do szyfrowania i deszyfrowania. Druga to szyfrowanie asymetryczne, gdzie każde urządzenie ma swój unikalny klucz szyfrujący.

Rozwiązanie ABLOY BEAT wykorzystuje szyfrowanie asymetryczne, co oznacza, że dane dotyczące praw dostępu są zawsze unikalnie szyfrowane od punktu do punktu. W szyfrowanym kanale bezpieczeństwa typu end-to-end dane, które przemieszczają się od systemu zarządzania do zamka i smartfona, będą szyfrowane wielokrotnie.

Wszystkie zamki BEAT są unikalnie szyfrowane za pomocą klucza prywatnego. Oznacza to, że dane zamka nie mogą być odszyfrowane za pomocą kluczy deszyfrujących innego zamka. Jeśli ktoś odszyfruje jeden zamek w systemie zabezpieczeń, wszystkie pozostałe zamki nadal mają swoje unikalne klucze i pozostają chronione. Jedno skompromitowane urządzenie nie złamie systemu ani nie wpłynie na inne urządzenia w systemie.



Jakie są ataki i zagrożenia cyberbezpieczeństwa?

Ataki siłowe
Hakerzy mogą próbować złamać hasła i poświadczenia, zgadując różne kombinacje, aż znajdą właściwe dane logowania, aby uzyskać nieautoryzowany dostęp. Tego typu atak można skutecznie powstrzymać za pomocą zaszyfrowanych poświadczeń. Nawet jeśli teoretycznie system mógłby zostać zhakowany metodą ataku siłowego, w praktyce odszyfrowanie wszystkich danych zajęłoby około 10 000 lat.

Kradzież zamka
Haker może próbować ukraść zamek, ale skradziony zamek nie spowoduje szkody dla innych zamków w systemie zabezpieczeń. Dzieje się tak, ponieważ wszystkie zamki są unikalne i mają swoje unikalne klucze deszyfrujące. Mówiąc prościej, skradziony zamek nie ma wpływu na inne zamki.

Skradziony lub skompromitowany telefon
Smartfon z prawami dostępu może zostać skradziony. Po pierwsze, większość nowoczesnych smartfonów wymaga biometrii i haseł do odblokowania. Po drugie, wszystkie przyznane prawa dostępu automatycznie wygasną po określonym czasie. Jednak jeśli telefon zostanie zgubiony lub skradziony, prawa dostępu mogą zostać natychmiast unieważnione za pomocą backend BEAT, gdy tylko użytkownik zorientuje się, że jego urządzenie zaginęło. Jeśli smartfon zostanie zhakowany, można również podjąć działania naprawcze i unieważnić prawa dostępu z systemu zabezpieczeń.

3. Rynek zamknięć cyfrowych

Cyfrowe zamknięcia zapewniają wyjątkowe bezpieczeństwo i ochronę prywatności dla Infrastruktury Krytycznejz. Istnieją rozwiązania przewodowe i bezprzewodowe, a rozwiązania bezprzewodowe często wykorzystują technologię NFC lub Bluetooth®. Rozwiązania przewodowe mają ograniczenia i wymagania dotyczące miejsca, w którym mogą być umieszczone. NFC to rozwiązanie bezprzewodowe, które może działać bez ciągłego źródła zasilania, ale te urządzenia aktywują się tylko wtedy, gdy są w bardzo bliskiej odległości.

Zasilane bateriami zamki z Bluetooth® oferują ciągłe źródło zasilania i bezprzewodową elastyczność, dlatego wybraliśmy tę technologię dla naszego rosnącego cyfrowego portfolio BEAT. Konkurencyjne rozwiązania wydają się rozwiązywać te same wyzwania, z którymi borykają się nasi klienci, ale w przeciwieństwie do BEAT, te urządzenia zamykające mogą nie być zaprojektowane do celów bezkluczowych, co skutkuje trudnościami w obsłudze, mnieszym bezpieczeństwem i ograniczoną wytrzymałością.

Przyszłościowa technologia oraz projekt dedykowany dostępowi bezkluczowemu

- Możesz otworzyć zamek za pomocą smartfona. Żywotnośc baterii w urządzeniach BEAT pozwala na więcej niż 5 000 użyć lub 5 lat funkcjonowania.
- BEAT zaczyna jako rozwiązanie offline, a urządzenia zamykające mogą być umieszczone w zasięgu sieci lub poza nim. Zamki mogą być obsługiwane bez aktywnego połączenia komórkowego, jeśli prawa dostępu są zaktualizowane na smartfonie przed wejściem w obszar offline.
- Bluetooth® to łączność, która pozwala na zdalne otwieranie i monitorowanie IoT za pomocą oprogramowania do zarządzania dostępem i urządzeń bramkowych. W ten sposób można szybciej reagować na wandalizm i nieautoryzowany dostęp – oraz mieć spokój ducha, mając pełną świadomość swojej sytuacji bezpieczeństwa bez konieczności wizyt na miejscu.

4. Wprowadzenie ABLOY BEAT

ABLOY BEAT to bezkluczowe rozwiązanie stworzone specjalnie do ochrony infrastruktury krytycznej. Wszystkie produkty BEAT są obsługiwane za pomocą aplikacji mobilnej przez połączenie Bluetooth®. Bezkluczowe rozwiązania BEAT są zaprojektowane do bezpiecznego zarządzania dostępem bezprzewodowym, a aby zapewnić bezpieczeństwo BEAT teraz i w przyszłości, wdrażamy wiele warstw cyberbezpieczeństwa.

Dlaczego BEAT jest bezpieczny?

1. Szyfrowanie chroni wszystkie dane przesyłane między urządzeniami poprzez kodowanie informacji lub mieszanie czytelnego tekstu, aby ukryć i zabezpieczyć go przed nieautoryzowanymi użytkownikami. Używamy zaawansowanej technologii szyfrowania Seos® nowej generacji z ulepszonymi możliwościami IoT, a także standardowych protokołów i praktyk bezpieczeństwa w branży.

2. Uwierzytelnianie identyfikuje użytkownika i system zarządzania dostępem. Kazdy zamek i użytkownik w systemie ma indywidualną, zweryfikowaną i zaufaną tożsamość, a dostęp do zamków BEAT mogą uzyskać tylko autoryzowane osoby. Uwierzytelniamy cały ruch użytkowników i stosujemy politykę braku zaufania, co oznacza, że żadne urządzenie ani użytkownik nie mogą ominąć naszego procesu uwierzytelniania.

3. Autoryzacje są bezpiecznie dostarczane z systemu backendowego BEAT do zamków. Każda autoryzacja na urządzeniu mobilnym jest ważna przez ograniczony, krótki okres. Wszystkie dane przesyłane z zamków są szyfrowane od końca do końca, więc nawet autoryzowani mobilni klienci nie mogą odczytać zawartości. Naruszone i skradzione urządzenia mogą być unieważniane przez backend.

Aktualizacje oprogramowania sprzętowego dla wykrytych luk
Wykrywamy możliwe problemy i luki w zabezpieczeniach we współpracy z testerami. Poprawki do oprogramowania sprzętowego naszych produktów są łatwo implementowane w trakcie użytkowania. Za każdym razem, gdy zamek jest używany, przechodzi w tryb online i aktualizuje się w tle.

Aspekty bezpieczeństwa BEAT

Wygodna identyfikacja użytkownika bez kompromisów w zakresie bezpieczeństwa

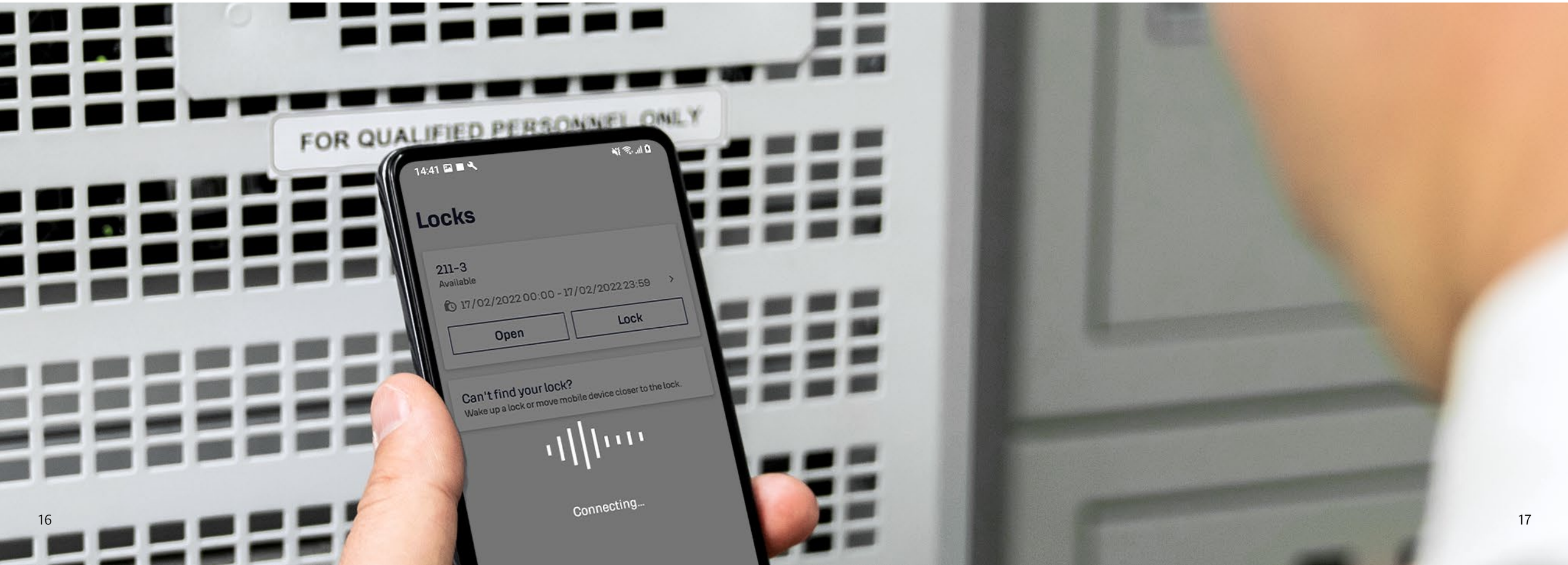
Funkcja offline zapewnia funkcjonowanie systemu mimo braku zasięgu

Aktualizacja oprogramowania sprzętowego smartfonem dowolnego, zaufanego użytkownika

Szyfrowanie wiadomo-sci od końca do końca (E2E)

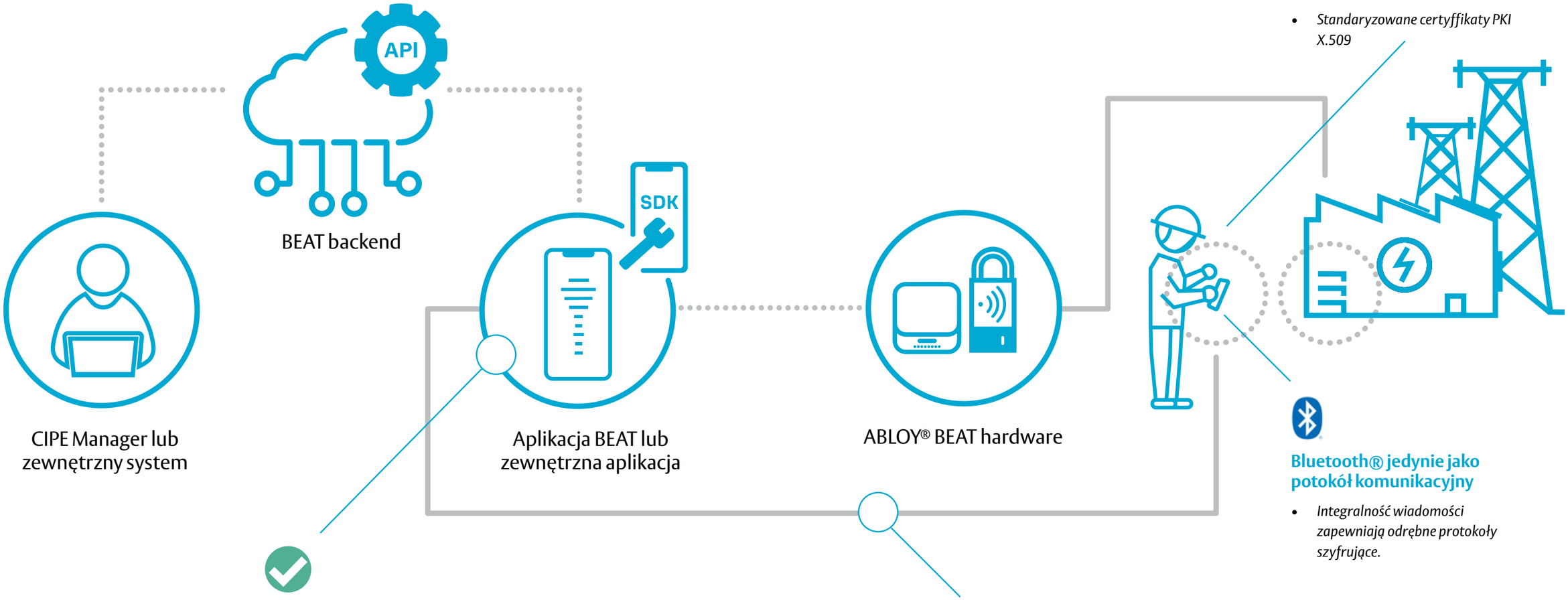
Globalne PKI jako now-oczesne podejście IoT do uwierzytelniania

Weryfikowane przez niezależne instytuty bezpieczeństwa



Jak działa BEAT

Mobilne poświadczenia i prawa dostępu są przechowywane na smartfonie użytkownika w “bezpiecznej enklawie”, a informacje o poświadczeniu są przechowywane w chmurze. Wszystkie informacje między urządzeniami są przesyłane przez Internet. To, co sprawia, że produkt jest cyberbezpieczny, to fakt, że na każdym etapie używania poświadczenia stosowane są protokoły bezpieczeństwa, które zapobiegają atakom.



Infrastruktura klucza publicznego (PKI)

i tożsamośc klucza prywatnego

- *Asymetryczne szyfrowanie bez współdzielonych sekretów*
- *Standaryzowane certyffikaty PKI X.509*

Bluetooth® jedynie jako potokół komunikacyjny

- *Integralność wiadomości zapewniają odrębne protokoły szyfrujące.*

Trusted Service Manager (TSM)

- *Umożliwienie bezpieczenej rejestracji urządzenia mobilnego*
- *Zaproszenia pochodzą tylko z oryginalnej organizacji*

Bezpieczny kanał end-to-end

- *Tylko naszemu backend admininstratorowi ufa zamek*
- *Mniej podatne na ataki “człowiek w środku”*

5. Podręcznik: czy BEAT jest odpowiedni dla Ciebie?

Nasz rozwijający się portfel produktów BEAT oferuje przyszłościowe rozwiązania zapewniające bezpieczeństwo i łączność. Te pytania mogą pomóc Ci zdecydować, czy BEAT jest rozwiązaniem, którego szukasz:

- Czy chciałbyś uzyskać lepszą świadomość sytuacyjną dzięki mobilnemu systemowi kontroli dostępu?
- Czy chcesz wyeliminować ryzyko zgubienia kluczy i pozbyć się fizycznego zarządzania kluczami?
- Czy chciałbyś śledzić przepływ osób i pracowników na swoim terenie?
- Czy potrzebujesz zarządzać kluczami, zamkami i prawami dostępu niezależnie od swojego fizycznego położenia?
- Czy mógłbyś obniżyć koszty i zaoszczędzić czas podróży dzięki prostszej logistyce?
- Czy szukasz rozwiązania dostępowego, które można zintegrować z istniejącymi systemami?
- Czy chcesz być na czele ochrony infrastruktury krytycznej?

Jeśli choć jedna odpowedź brzmi "tak" lub "może" skontaktuj się z nami i dowiedz się więcej:

KONTAKT DO NAS

6. Dlaczego cyberbezpieczeństwo ma dla nas znaczenie

Odpowiedzialne ujawnianie luk w zabezpieczeniach zapewnia, że infrastruktura dostępu do bezpieczeństwa jest testowana i sprawdzana pod kątem niezawodności. Dlatego ASSA ABLOY ceni wnikliwość i zaangażowanie testerów bezpieczeństwa oraz innych osób badających luki w zabezpieczeniach, aby uczynić świat bezpieczniejszym miejscem. Dla nas ujawnianie jest kluczowe dla poprawy jakości naszych produktów i usług oraz bezpieczeństwa naszych klientów, którzy na nich polegają.

Przyjęliśmy politykę bezpieczeństwa dotyczącą odpowiedzialnego ujawniania, która obejmuje na przykład:

- ASSA ABLOY ujawni znane luki w zabezpieczeniach i ich poprawki swoim klientom w sposób, który chroni ASSA ABLOY i jej klientów.
- ASSA ABLOY jest otwarta na komunikację i współpracę z badaczami bezpieczeństwa, którzy przychodzą do nas z wspólnym zainteresowaniem poprawą bezpieczeństwa i koordynacją dystrybucji informacji, które obejmują zarówno lukę, jak i rozwiązanie, które ją eliminuje.
- Przeczytaj naszą politykę bezpieczeństwa.

7. Słownik

- **Szyfrowanie asymetryczne** = w szyfrowaniu asymetrycznym używane są różne klucze do szyfrowania i deszyfrowania. Szyfrowanie asymetryczne jest również znane jako szyfrowanie infrastruktury klucza publicznego.
- **Uwierzytelnianie** = ważna warstwa cyberbezpieczeństwa, która identyfikuje użytkownika i system zarządzania dostępem.
- **Autoryzacja** = ważna warstwa cyberbezpieczeństwa, która określa, co każdy użytkownik może zrobić z otrzymanymi danymi.
- **BLE** = Bluetooth® Low Energy to standard bezprzewodowej łączności o niskim zużyciu energii.
- **Chmura** = chmura przechowuje dane na serwerach internetowych, do których można uzyskać dostęp zdalnie, gdy jest to potrzebne.
- **Szyfrowanie** = ważna warstwa cyberbezpieczeństwa, która miesza czytelne dane, aby wyglądały na losowe, co pomaga zapobiegać nieautoryzowanemu użyciu zaszyfrowanych danych.
- **Szyfrowanie end-to-end (E2EE)** = metoda zabezpieczeń, która zapobiega potajemnej modyfikacji lub dostępowi do danych przez kogokolwiek innego niż prawdziwy nadawca i odbiorca. Dane są szyfrowane przez nadawcę i przechowywane w postaci zaszyfrowanej, a odszyfrowywane tylko przez odbiorcę.
- **Haker** = osoba, która próbuje włamać się do systemu komputerowego, na przykład w celu uzyskania nieautoryzowanego dostępu do określonych danych.
- **IoT (Internet rzeczy)** = Opisuje urządzenia z czujnikami, które są połączone, komunikują się i wymieniają dane z innymi urządzeniami.
- **NFC (Near Field Communication)** = technologia bezprzewodowa krótkiego zasięgu, która umożliwia urządzeniom komunikowanie się ze sobą.
- **PKI (Infrastruktura klucza publicznego)** = asymetryczna metoda szyfrowania, która składa się z polityk, procedur, sprzętu i oprogramowania używanych do tworzenia i dystrybucji cyfrowych poświadczeń.
- **SaaS (Oprogramowanie jako usługa)** = aplikacje oparte na chmurze jako usługę przez Internet. Dostawca SaaS uruchamia aplikację na swoich serwerach i zarządza dostępem oraz bezpieczeństwem aplikacji. Na przykład ABLOY BEAT jest SaaS.
- **Seos®** = zaawansowana technologia szyfrowania opracowana przez HID Global, firmę należącą do ASSA ABLOY.
- **Szyfrowanie symetryczne** = w szyfrowaniu symetrycznym wszystkie urządzenia używają tego samego tajnego klucza do szyfrowania i deszyfrowania.
- **Trust no one (Brak zaufania)** = model TNO eliminuje ryzyko przeoczenia „zaufanych" użytkowników, wymagając, aby wszyscy użytkownicy byli zawsze weryfikowani i uwierzytelniani.
- **TSM (Zaufany menedżer usług)** = koordynuje techniczne połączenia i umowy biznesowe, np. z operatorami sieci komórkowych, dostawcami usług i producentami urządzeń. TSM BEAT umożliwia bezpieczną rejestrację urządzenia mobilnego.
- **X.509** = międzynarodowy standard definiujący certyfikaty klucza publicznego. W kryptografii certyfikaty te są używane w różnych protokołach internetowych, takich jak HTTPS i TLS. Na przykład BEAT posiada certyfikat TLS 1.3.

The ASSA ABLOY Group is the global leader in access solutions. Every day we help people feel safe, secure and experience a more open world.

ASSA ABLOY
Global Solutions

assaabloyglobalsolutions.com