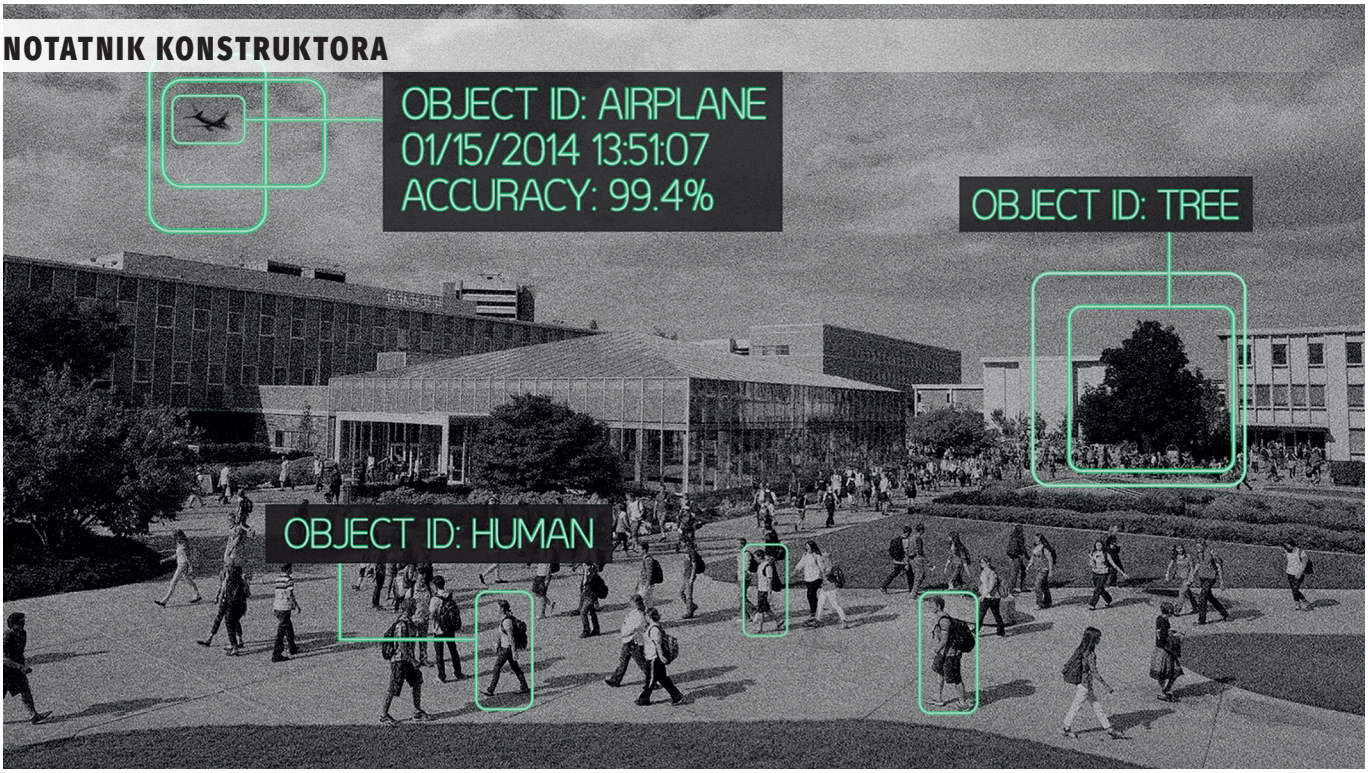


Identyfikacja elektroniczna (1)

Wstęp i układy znaczników RFID oraz NFC

Wraz z postępem technicznym coraz więcej procesów uległo automatyzacji. Dotyczy to nie tylko przemysłu, ale również prób konstruowania maszyn (robotów i innych) mających ułatwić nam codzienne życie. Podstawową „umiejętnością", którą muszą mieć takie maszyny jest zdolność do rozpoznawania obiektów. W artykule omówimy podstawowe, mające zastosowanie praktyczne techniki pozwalające ocenić maszynie, z jakim przedmiotem ma do czynienia.

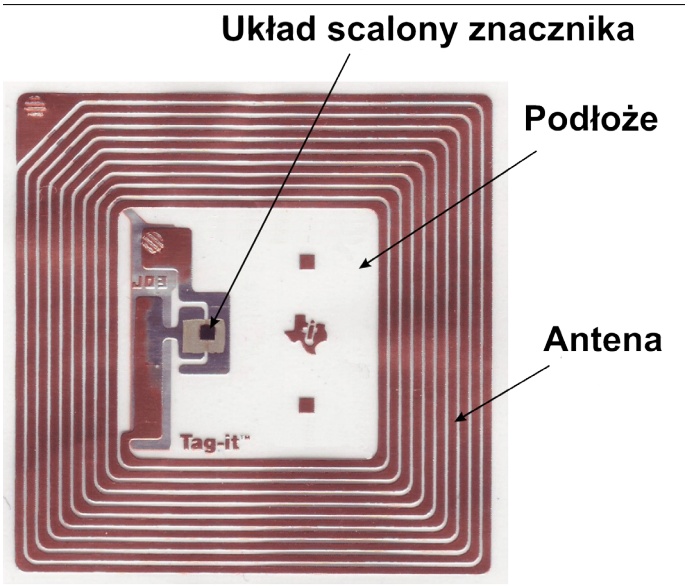
Dla potrzeb tego artykułu wprowadźmy umowny podział technik identyfikacji. Pierwsza metoda jest stosowana od lat. Za jej pomocą rozpoznawane są obiekty wyposażone w specjalne znaczniki (tagi). Jak dobrze wiemy z praktyki, takie znaczniki mogą być różnego typu, ale najczęściej używane są radiowe i optyczne. Rozwój drugiej metody, bardziej zbliżonej do naturalnego rozróżniania obiektów przez człowieka, umożliwiły postęp w dziedzinach szybkości przetwarzania danych oraz rozwój algorytmów oceny obrazu. W tej drugiej metodzie jako sensora najczęściej używa się kamery pracującej w zakresie światła widzialnego lub niewidzialnego i rozpoznaje obraz zapamiętany w buforze pamięci. Nie jest też regułą, że obraz jest odbierany przez kamerę – niekiedy może to być czujnik radarowy, ultradźwiękowy lub inny. Nie jest też powiedziane, że rozpoznawanie obiektu musi odbywać się o mechanizmy dostępne naszemu organizmowi, ponieważ czasami w tych bardziej zaawansowanych metodach wykorzystuje się metody numeryczne.

Identyfikacja RFID

Identyfikacja RFID jest dobrze znaną i powszechnie stosowaną od wielu lat. Najczęściej używa się w niej tzw. znaczników (tagów) pasywnych zasilanych energią pola elektromagnetycznego wytwarzanego przez antenę, najczęściej wykonaną w postaci cewki o kilku – kilkudziesięciu zwojach, zależnie od częstotliwości nośnej (**rysunek 1**). Innym rodzajem znaczników są rzadziej stosowane tagi aktywne lub pasywno - aktywne, zasilane z baterii lub w inny sposób, transmitujące dane na znaczną odległość (**fotografia 2**). Dodajmy przy tym, że w artykule zajmujemy się systemami „cywilnymi", a nie metodą identyfikacji np. samolotów, stosowaną w lotnictwie, aczkolwiek ona też opiera się na nadawaniu pewnego unikatowego numeru identyfikacyjnego lub komunikatu, które mogą być odbierane przez specjalny odbiornik.

Popularność metody, w której są stosowane znaczniki RFID zaczęła wzrastać na przestrzeni ostatnich 20 lat, a prawdziwy jej boom powodują znaczniki komunikujące się za pomocą interfejsu NFC, w który to jest wyposażona większość współczesnych smartfonów. Można zaryzykować twierdzenie, że dzięki znacznikom NFC ta technologia trafiła pod przysłowiowe strzechy i jest szeroko stosowana przez różnych użytkowników, nie tylko profesjonalistów. Co ważne, znaczniki NFC mające możliwość komunikacji dwukierunkowej oraz przechowywania danych, są tanie, powszechnie dostępne i wykonywane np. w postaci naklejki na przedmiot. Dzięki odpowiedniemu oprogramowaniu i możliwości komunikowania się z bazą danych za pomocą Wi-Fi lub GSM, nasz smartfon może pełnić rolę czytnika. Dzięki niemu można np. przekazać informację o odbiorze przesyłki, sprawdzić datę produkcji i numer seryjny urządzenia, daty jego przeglądów itp. Kiedyś był do tego wymagany specjalny czytnik, a dziś większość z nas nosi taki czynnik w kieszeni.

Pamiętam czasy, gdy znaczniki RFID były kosztowne, duże, a budując urządzenie trzeba było poważnie zastanowić się na kosztem użycia



Rysunek 1. Budowa typowego, pasywnego znacznika RFID

tej technologii identyfikacji. Współcześnie, czego dowodem są między innymi znaczniki NFC, udało się opracować takie metody produkcji, które pozwoliły na obniżenie ceny znaczników. Wprowadzono również wyższe częstotliwości nośne, co spowodowało miniaturyzację anten (a tym samym czytników) oraz tagów. Technologie komunikacji sieciowej – przewodowe i bezprzewodowe – umożliwiły sensowne wykorzystanie danych odczytywanych ze znaczników. Wprowadzono również mechanizmy kryptograficzne, dzięki którym „podsłuchana" komunikacja pomiędzy znacznikiem i czytnikiem jest trudna do rozszyfrowania. W końcu, coraz bardziej wdzierająca się w codzienność automatyzacja różnych aspektów życia, wymusiła przyjęcie pewnych rozwiązań zdalnej identyfikacji, bez których nie byłoby możliwe uproszczenie czy też przyspieszenie wykonywania różnego rodzaju operacji.

Na przestrzeni lat powstało wiele standardów RFID. Wiele z nich zyskało popularność w pewnych konkretnych zastosowaniach np. standardy Unique i Hitag pracujące w paśmie 125 kHz są do dziś chętnie stosowane w systemach kontroli dostępu. Co może być istotne z punktu widzenia inżyniera, istnieją pewne „mutacje" starych standardów, które opracowano w miarę rozwoju technologii i techniki.

Znaczniki aktywne mają własne źródło zasilania i mogą funkcjonować niezależnie, bez potrzeby inicjowania transmisji przez czytnik. Wbudowane źródło energii pozwala na przesyłanie sygnału na dużą odległość, ograniczoną przez zasoby zgormadzonej energii oraz stosowaną metodę transmisji sygnału. Znaczniki pasywno-aktywne również korzystają z własnego źródła energii, co pozwala im na transmisję sygnału na dużą odległość, ale mają mniej obwodów elektronicznych i nie mogą samodzielnie zainicjalizować komunikacji – czekają w uśpieniu do momentu, gdy wzbudzi je czytnik.

Znaczniki pasywne najczęściej są zbudowane w postaci anteny (zwykle cewki o kilku – kilkunastu zwojach), do której jest dołączony układ scalony zawierający znaczni. W stanie spoczynku znacznik nie jest zasilany i w ogóle nie pobiera prądu – oczekuje do momentu, gdy za pomocą pola elektromagnetycznego zasili i wzbudzi go czytnik. Dzięki odpowiedniej budowie oraz metodzie modulacji, antena służy jako swego rodzaju uzwojenie pierwotne transformatora zasilającego oraz komponent odbierający dane z czytnika. Zebrana przez znacznik energia jest też wykorzystywana do wyemitowania odpowiedzi, przy czym ze względu na jej ograniczoną ilość, dostępny zasięg transmisji jest niewielkie i zwykle wynosi kilka centymetrów.

W zależności od standardu, planowanego zasięgu i aplikacji, korzysta się z kilku pasm. Są to: 125 kHz, 13,56 MHz, 433 MHz, 866 MHz, 2,4…5,8 GHz, 3,1…10 GHz.

Do cech wspólnych różnych standardów tagów RFID należy też fakt, że mają one pamięć, w której jest zapisany unikatowy kod identyfikacyjny. W zależności od zastosowania, może on w pełni wystarczać do danej aplikacji, lub może być konieczne zapisanie w pamięci znacznika dodatkowych informacji. Tu pojawiają się większe różnice, gdyż pamięć ta może mieć różną pojemność i może być zapisywana jednokrotnie lub nadpisywana wiele razy, w zależności od standardu.

Standard Hitag

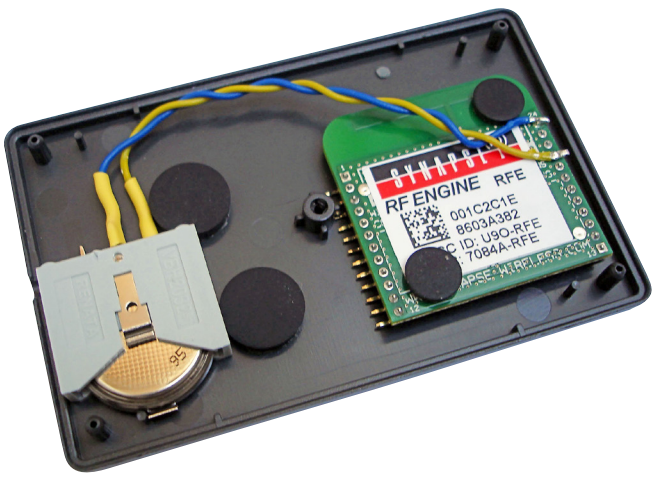
Znaczniki tego typu dzięki małej częstotliwości nośnej (zakres 100…150 kHz) świetnie sprawdzają się w trudnych warunkach eksploatacji, a więc tam, gdzie w tle transmisji występują zakłócenia. Znaczniki Hitag są zgodne z międzynarodowymi standardami: ISO 11784, ISO 11785, ISO 14223, ISO 18000-2. Opracowano cztery odmiany systemu Hitag:

1. Podstawowy standard Hitag 1 wykorzystuje nośną o częstotliwości 125 kHz i nie wymaga żadnych dodatkowych komponentów poza czytnikiem. Komunikacja odbywa się dwukierunkowo, w trybie half duplex, przy czym jest możliwe szyfrowanie danych. Dzięki zastosowani algorytmu antykolizyjnego można odczytać wiele znaczników umieszczonych w polu anteny. Hitag 1 zawiera też obsługę korekcji błędów na podstawie sumy kontrolnej. Tagi te mieszczą 2048 bitów. Wbudowana pamięć może być zapisywana wielokrotnie.
2. Tagi Hitag 2 mają 256 bitów pamięci, z czego tylko 128 może być zapisane przez użytkownika. Również obsługują szyfrowanie, przy czym jest możliwy wybór sposobu kodowania emitowanych danych (Manchester lub dwufazowy).
3. Hitag S jest dostępny jest w dwóch odmianach – o pojemności 256 lub 2048 bitów. Pozwala na szybszą transmisję i pracuje w zakresie częstotliwości 100…150 kHz. Tagi Hitag S mają 32-bitowy, unikalny identyfikator oraz 48-bitowy klucz szyfrujący.
4. Hitag μ zaprojektowano tak, aby znaczniki były jak najmniejsze, a jednocześnie zgodne z pozostałymi z tej rodziny. Są najbardziej zbliżone do standardu Hitag S.

Mifare

Popularnym standardem jest Mifare, nad którego rozwojem pracuje firma NXP Semiconductors. Producent ten jest jednym z liderów w tej dziedzinie, co zapewniło dużą popularność standardu. Charakteryzuje się dużą ilością pamięci dostępnej dla użytkownika. Jest to też standard obsługiwany przez wiele nowoczesnych smartfonów wyposażonych w czytniki NFC, choć sytuacja ta się zmienia, o czym dalej.

1. Jako pierwszy opracowano standard Mifare Classic 1K. Znaczniki mają pamięć mieszczącą 1024 bajty. Jest ona podzielona na 16 bloków, z których każdy może być zabezpieczony dwoma kluczami. Klucze mogą pełnić rolę kodu nadającego uprawnienia do odczytu, zapisu lub modyfikowania zapamiętanych danych.



Fotografia 2. Budowa przykładowego, aktywnego znacznika RFID

2. Mifare Classic 4K mają pamięć mieszczącą 4096 bajtów podzielonej na 40 bloków. 32 bloki mają pojemność po 64 bajtów, a pozostałe 8 po 256 bajtów. Istnieje także wersja Mifare Classic Mini, która ma 320 bajtów pamięci, podzielonych na 5 bloków po 64 bajty.
3. Mifare Ultralight EV1 ma pamięć mieszczącą 48 lub 128 bajtów, konfigurowalne liczniki, trzy niezależne, 24-bitowe licznikami jednokierunkowe, możliwość zabezpieczenia odczytu za pomocą hasła 32-bitowego oraz mechanizm podpisywania kart.
4. Mifare Ultralight C został zaprojektowany z myślą o jednorazowych biletach, ale dodatkowo wzbogacono go o funkcje bezpieczeństwa. Mifare Ultralight C obsługuje szyfrowanie 3DES, ma 192 bajty pamięci EEPROM podzielone na 4-bajtowe strony. Obsługuje mechanizm unikania kolizji (zgodny z ISO 14443) oraz ma unikalny, 42-bitowy numer identyfikacyjny. Karty te są kompatybilne ze standardem Mifare Ultralight oraz zgodne ze specyfikacją NFC Forum Tag Type 2.
5. Znaczniki Mifare DESFire są wyposażone w mikrokontroler z rdzeniem 8051, dzięki któremu „na pokładzie" jest realizowany nieskomplikowany system operacyjny obsługujący system plików. W zależności od wariantu, oferowane były z szyfrowaniem 3DES lub AES, z pamięcią o pojemności 2, 4 lub 8 kB. Obecnie karty te zostały zastąpione przez wstecznie kompatybilną wersję Mifare DESFire EV1. Obsługuje ona 128-bitowe szyfrowanie AES.
1. Mifare Plus miały zastąpić Mifare Classic, zwiększając ich bezpieczeństwo. Pomimo tego, że sposób obsługi zapisanych w nich danych jest identyczny, to wprowadzone zabezpieczenia wymuszają modyfikację czytników, stąd nie można mówić o pełnej kompatybilności wstecznej. Karty Mifare Classic mają 2048 lub 4096 bajtów pamięci oraz 42- lub 32-bitowe, unikalne numery identyfikacyjne. Obsługują 128-bitowe szyfrowanie AES i są oferowane w specjalnych odmianach Mifare Plus S oraz Mifare Plus X. Karty Mifare Plus można odczytywać w trybie kompatybilności z Mifare Classic, ale wymaga to ograniczenia zastosowanych zabezpieczeń.

W każdej z wersji Mifare Classic, 16 bajtów każdego bloku jest zarezerwowanych na klucze i informacje o sposobie ich użycia. Ponadto, pierwsze 16 bajtów karty zawiera jej numer seryjny oraz dodatkowe informacje wprowadzone przez producenta znacznika. Są to dane tylko do odczytu. Oznacza to, że pojemność dostępna dla użytkownika wynosi 3440 bajtów dla Mifare Classic 4k, 752 bajty dla zwykłego Mifare Classic 1K i 224 bajty dla Mifare Classic Mini.

Wszystkie odmiany Mifare pracują na częstotliwości 13,56 MHz.

Karty Mifare Classic korzystają z algorytmu szyfrującego, ale jest też wersja pozbawiona tej funkcji. Są to tagi Mifare Ultralight, których pojemność wynosi 64 bajty, podzielone na 16 stron. Ze względu na brak szyfrowania, ich zabezpieczenie polega na zapisaniu bitu blokującego nadpisanie danych na karcie.

Unique

Bardzo rozpowszechnionym standardem jest Unique. Obejmuje on znaczniki pasywne wyposażone w niewielką pamięć ROM zaprogramowaną w trakcie produkcji. 64-bity pamięci znaczników Unique zawierają 40-bitowy, unikalny numer seryjny, przesyłany na częstotliwości 125 kHz z użyciem modulacji ASK i kodowania Manchester. Na pozostałe 24 bity składa się 9 bitów nagłówka (w postaci samych jedynek), 14 bitów parzystości i bit stopu w postaci wartości 0. Sam numer seryjny zapisywany jest w postaci 10 wierszy po cztery 1-bitowe kolumny, przy czym pierwsze 12 bitów odpowiada identyfikatorowi nadawanemu klientowi przez producenta, natomiast pierwsze 10 bitów parzystości obliczanych jest dla wierszy, a pozostałe 4 – dla kolumn.

Rozwinięciem standardu Unique jest Q5. Podstawową różnicą jest możliwość zapisania danych w pamięci znacznika. Dostępną pamięć EEPROM można zabezpieczyć przed programowaniem. Dostępne są znaczniki wyposażone w pamięć mieszczącą 8 słów 4-bajtowych, z której 224 bity są dostępne dla użytkownika.

I-Code

Znaczniki I-Code pracują w paśmie 13,56 MHz. Są one wyposażone w pamięć mieszczącą 1024 bity. Charakteryzują się dużą prędkością transmisji – teoretycznie mogą przesyłać dane z prędkością do 53 kb/s, a pamięć może być zapisywana co najmniej 100 razy. Ich protokół komunikacyjny umożliwia odczyt do 30 znaczników umieszczonych w polu anteny. Pamięć znacznika jest podzielona na 32 bloki 4-bajtowe. Każdy może być zabezpieczony przed zapisem. Duży zasięg odczytu oraz unikalny, stały numer seryjny nadawany przez producenta (4 bloki po 4 bajty) ułatwiają zdalny monitoring przedmiotów. Pomocny jest też system antykradzieżowy EAS oraz mechanizm rozpoznawania grup znaczników.

Tiris

Standard został opracowany przez firmę Texas Instruments. Tiris to standard, który zdobył popularność w wielu zastosowaniach, ale nie jest używany w nowych aplikacjach. Obejmował znaczniki pasywne.

Pamiętam też rozwiązania czytników dużego zasięgu, które umożliwiały odczyt danych z odległości nawet 2-3 metrów. Były to jednak rozwiązania kosztowne, antena miała spore wymiary i przez to nie zyskały popularności.

EPC Global

Standard opracowany przez organizację GS1. Opracowano go z myślą o identyfikacji produktów. Konkretnie, twórcom chodziło o przygotowanie systemu RFID, który mógłby bezpośrednio zastąpić kody kreskowe. Nic w tym dziwnego – grupa GS1 odpowiada właśnie za nadzór nad kodami kreskowymi i przypisuje je producentom, którzy się do niej zgłoszą.

Standard EPC Global pracuje w paśmie UHF (Europa – 866 MHz). Znaczniki mają programowalną przez użytkownika pamięć mieszczącą 96-bitów. Zapisany w niej kod musi jednoznacznie identyfikować produkt, zgodnie z wytycznymi GS1. Dzięki niewielkiej pojemności, brakowi zabezpieczeń i nieskomplikowanej technologii, są bardzo tanie w produkcji, a koszt ich wdrożenia ma sens nawet w wypadku tak masowego zastosowania, jak sprzedaż detaliczna.

Opracowano też drugą generację znaczników – EPC Global Class 1 Gen 2, w którym rozszerzono funkcjonalność o możliwość zapisu znaczników „w terenie" oraz o nowe sposoby kodowania i przesyłania informacji. Zaimplementowano funkcję zliczania znaczników znajdujących się w zasięgu czytnika, a mających ten sam kod. Pamięć może być zabezpieczona hasłem przed odczytem i/lub zapisem. Mechanizm podziału transmisji na sesje umożliwia niezakłócające się odczytywanie znaczników za pomocą nawet 4 różnych czytników w tym samym czasie. Czytnikom można nadać identyfikator sesji, aby odróżnić odczyty wykonywane np. przez czytniki inwentaryzujące od skanerów przy kasach. EPC Global, dzięki algorytmom antykolizyjnym, pozwala również na szybkie skanowanie wielu produktów w polu anteny.

NFC

Rozwinięciem standardów RFID jest popularny w ostatnich latach standard NFC, pozwalający na komunikację dwóch urządzeń za pomocą metod podobnych, jak w przypadku RFID. Komunikacja nadal odbywa się w oparciu o próbę odczytu wartości znacznika przez czytnik, jednak ze względu na możliwości przetwarzania danych zaszyte w obu komunikujących się urządzeniach, potencjalne rozwiązania są znacznie bardziej rozbudowane.

Standard NFC może posłużyć do nawiązywania połączeń danych i transakcji w sposób wygodny, i względnie bezpieczny, z szybkością do 424 kb/s. Komunikacja NFC odbywa się na częstotliwości 13,56 MHz. Zasięg pracy NFC jest niewielki i wynosi kilkanaście centymetrów. W praktyce, szumy elektromagnetyczne tła oraz obudowy czytników sprawiają, że w urządzenia NFC zetknąć ze sobą, aby mogły się skomunikować. Pozwala to na selektywne łączenie urządzeń obsługujących NFC, bez konieczności każdorazowego, ręcznego uruchamiania trybu komunikacji, nawet jeśli w pobliżu znajduje się wiele znaczników NFC. Istotnie zwiększa się też bezpieczeństwo przesyłanych danych. Typowo, aby połączyć się przez NFC, trzeba mieć bezpośredni, fizyczny dostęp do wybranego urządzenia lub znacznika, prawie tak samo, jakby konieczne było przyłączenie do niego kabla.

Kompatybilność NFC i RFID

Fakt, że znaczniki NFC i RFID mogą zostać wykorzystane do tego samego rodzaju aplikacji sprawia, że warto się zastanowić, które z rozwiązań będzie bardziej korzystne. W tej kwestii kluczowym jest zrozumienie, czym jest NFC w stosunku do RFID oraz czym różnią się różne odmiany NFC.

NFC jest standardem (ISO18092 – Near Field Communication Interface and Protocol-1; ISO21481 – Near Field Communication Interface and Protocol-2), który oparto na licznych innych standardach,

w tym ISO14443, który stanowi podstawę RFID. Ponieważ na bazie ISO14443 powstała więcej niż jedna odmiana systemu znaczników RFID, zgodność tagów różnego typu jest ograniczona. W praktyce, NFC jest rozszerzeniem RFID, co oznacza, że próba skorzystania z czytnika NFC do zeskanowania klasycznego znacznika RFID może zakończyć się częściowym sukcesem.

Należy zauważyć, że system kart Mifare pracuje z wykorzystaniem tej samej częstotliwości nośnej, co NFC, a liderem w dziedzinie produkcji układów do RFID i NFC jest NXP. Ze względu na wagę, jaką NXP przywiązuje do Mifare, zdecydowana większość układów scalonych przeznaczonych do obsługi NFC, a wytwarzanych przez tego producenta, jest również kompatybilna z Mifare. Dlatego mając czytnik NFC oparty o układ NXP można swobodnie korzystać z tanich i pojemnych tagów Mifare. Jednakże Mifare nie jest w pełni zgodne z opisanymi przez NFC Forum w 2007 roku standardami (typami) znaczników. Zadeklarowano 4 typy:

- NFC Forum Type 1 Tag – bazuje na ISO14443A, możliwość wielokrotnego zapisu lub konfiguracji tylko do odczytu. Pamięć od 96 bajtów do 2 kB; szybkość komunikacji: 106 kb/s;
- NFC Forum Type 2 Tag – prawie taki sam, jak typ 1, ale dostępna pamięć może wynosić już od 48 bajtów do 2 kB;
- NFC Forum Type 3 Tag – bazuje na japońskim standardzie przemysłowym JIS X 6319-4, znanym też jako FeliCa. Znaczniki te są prekonfigurowane podczas produkcji, tylko do odczytu lub do wielokrotnego zapisu. Dostępność pamięci jest różna, ale nie powinna przekraczać 1 MB. Możliwa jest też większa szybkość komunikacji: 212 kb/s lub 424 kb/s;
- NFC Forum Type 4 Tag – w pełni kompatybilny z ISO14443A i ISO14443B, prekonfigurowany na etapie produkcji do wielokrotnego zapisu lub tylko do odczytu. Dostępna pamięć może wynosić do 32 kB, a szybkość komunikacji to 424 kb/s.

Obsługa Mifare nie jest zapewniona w standardzie NFC, co oznacza, że nie można na niej polegać. Praktyka pokazuje, że wszystko zależy od rodzaju układu zastosowanego w czytniku. W uniwersalnych zastosowaniach konsumenckich NFC liczą się przede wszystkim smartfony, więc to na nie należy zwrócić szczególną uwagę. Jeszcze do niedawna dominowały w nich układy do obsługi NFC firmy NXP, zgodne z Mifare. Obecnie, w najnowszych modelach telefonów spopularyzowały się układy marki Broadcom, które nie wspierają już Mifare.

Największą popularność zyskały znaczniki NFC typ 2. Producentem najczęściej stosowanych układów jest NXP, a najbardziej rozpowszechniony jest NTAG203. Zawiera on 168 bajtów pamięci podzielone na 42 strony 4-bajtowe. Dla użytkownika dostępne są 144 bajty w 36 stronach 4-bajtowych. Ponadto, NTAG203 pozwalają na zablokowanie do odczytu pierwszych 16 stron pamięci oraz mają 16-bitowy licznik. Mają też unikalny, 7-bitowy numer seryjny oraz obsługują mechanizm antykolizyjny. Szacowany czas przechowywania danych wynosi ok. 5 lat.

Jacek Bogusz, EP