21. Co to jest uwierzytelnianie i jakie metody się do tego stosuje.

Uwierzytelnianie (ang. authentication) – proces polegający na potwierdzeniu zadeklarowanej tożsamości podmiotu biorącego udział w procesie komunikacji. Celem uwierzytelniania jest uzyskanie określonego poziomu pewności, że dany podmiot jest w rzeczywistości tym, za który się podaje.

Metody uwierzytelniania

W zależności od kanału komunikacyjnego stosuje się różne metody i protokoły uwierzytelniania.

- w stosunku do dokumentów papierowych – podpisy, pieczęcie, parafowanie, znak wodny (metody), poświadczenie notarialne (protokół);
- w stosunku do osób i innych istot żywych – zabezpieczenie biometryczne, dokument tożsamości, hasło, karta elektroniczna (smart card), biochip, token (generator kodów);
- w stosunku do wiadomości i dokumentów elektronicznych – podpis cyfrowy, kod uwierzytelniania wiadomości (message authentication code);
- w stosunku do podmiotów w komunikacji elektronicznej – metody oparte na dowodzie posiadania hasła (kryptografia symetryczna – np. HMAC) lub klucza prywatnego (kryptografii asymetrycznej), dowód z wiedzą zerową, hasło jednorazowe.

Jedną z funkcjonalnych klasyfikacji uwierzytelniania jest podział na metody wykorzystujące:

- coś co wiesz (something you know) – informacja będąca w wyłącznym posiadaniu uprawnionego podmiotu, na przykład hasło lub klucz prywatny;
- coś co masz (something you have) – przedmiot będący w posiadaniu uprawnionego podmiotu, na przykład klucz (do zamka) lub token (generator kodów);
- coś czym jesteś (something you are) – metody biometryczne.