GDAŃSK UNIVERSITY
OF TECHNOLOGY

Uwierzytelnianie

Krzysztof Gierłowski

GDAŃSK UNIVERSITY OF TECHNOLOGY

Uwierzytelnianie stron (User authentication)

- Jeden z podstawowych elementów bezpieczeństwa i rozliczania.
- Służy określeniu i potwierdzeniu tożsamości stron (entities).

- Dwa podstawowe elementy:
  - Identyfikacja (Identification) – określenie lub deklaracja tożsamości,
  - Weryfikacja (Verification) – potwierdzenie i powiązanie strony i identyfikatora.

- Weryfikacja może być oparta na (Factors of authentication):
  - wiedzy (something you know, knowledge),
  - posiadaniu (something you have, possession),
  - cechach własnych (something you are, biometrics).

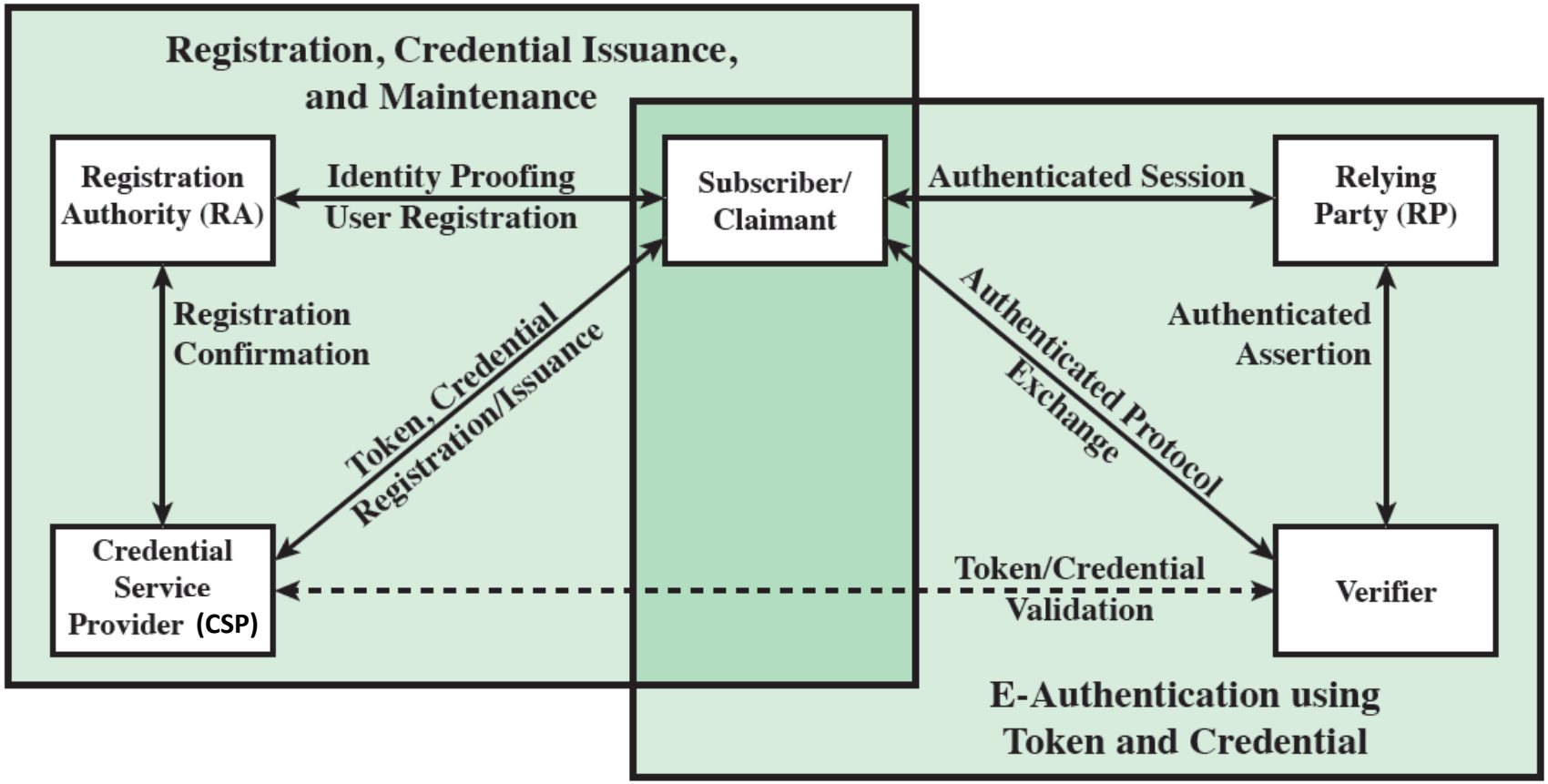
- Multifactor authentication – wykorzystuje kombinację kilku z powyższych.
- Multistep authentication – realizuje kilka kroków procesu uwierzytelniania sekwencyjne.

- Uwzględnienie lokalizacji (location factor) – uzależnienie procesu uwierzytelnienia od lokalizacji (geograficznej, sieciowej, sposobu dostępu, …).

- Uwierzytelnianie wiadomości (message authentication) jest osobnym procesem.

GDAŃSK UNIVERSITY OF TECHNOLOGY

NIST SP 800-63-3 model (End User Authentication)



- NIST SP 800-63-3 defines EUA as: the process of establishing confidence in user identity that are electronically presented.

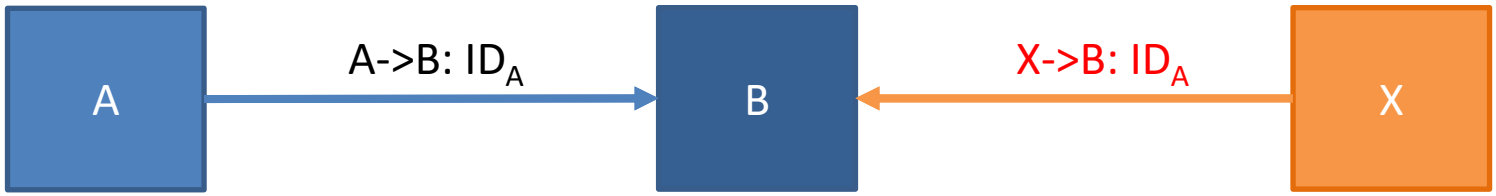
GDAŃSK UNIVERSITY OF TECHNOLOGY

Przykładowe zagrożenia

- Replay attacks – odtworzenie wcześniej przechwyconych wiadomości.
- Impersonation attacks – podszycie się pod jedną ze stron procesu uwierzytelniania,
  - Szczególnie łatwe w przypadku braku uwierzytelniania wzajemnego (mutual authentication).
- Reflection attacks – przekierowanie wiadomości.
- Przejęcie bazy danych uwierzytelniających.
- Oracle attacks – wymuszenie na jednej ze stron procesu uwierzytelniania dokonania określonych operacji,
  - celem uzyskania poszukiwanej wartości,
  - celem wygenerowania zbioru wartości do analizy (np. statystycznej),
- Wykorzystanie słabości zabezpieczeń po zakończeniu procesu uwierzytelniania (post-authentication),
  - mechanizmów dystrybucji kluczy, ochrony poufności i integralności.

GDAŃSK UNIVERSITY OF TECHNOLOGY

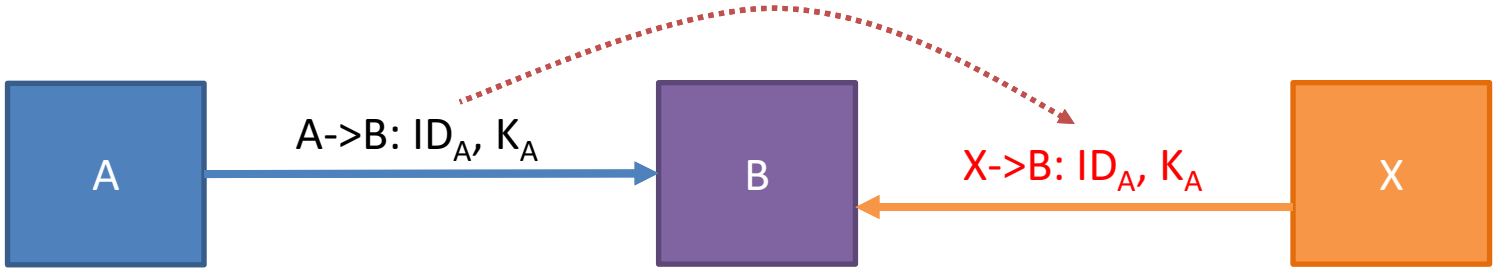
Identification



- Przesłanie identyfikatora użytkownika.
- Przykład:
  - „tajny” URL przekazywany lub wykorzystywany w niezabezpieczonym kanale komunikacji.
- Wyłącznie identyfikacja, bez weryfikacji.
- Każdy może podać się za dowolnego użytkownika.

GDAŃSK UNIVERSITY OF TECHNOLOGY

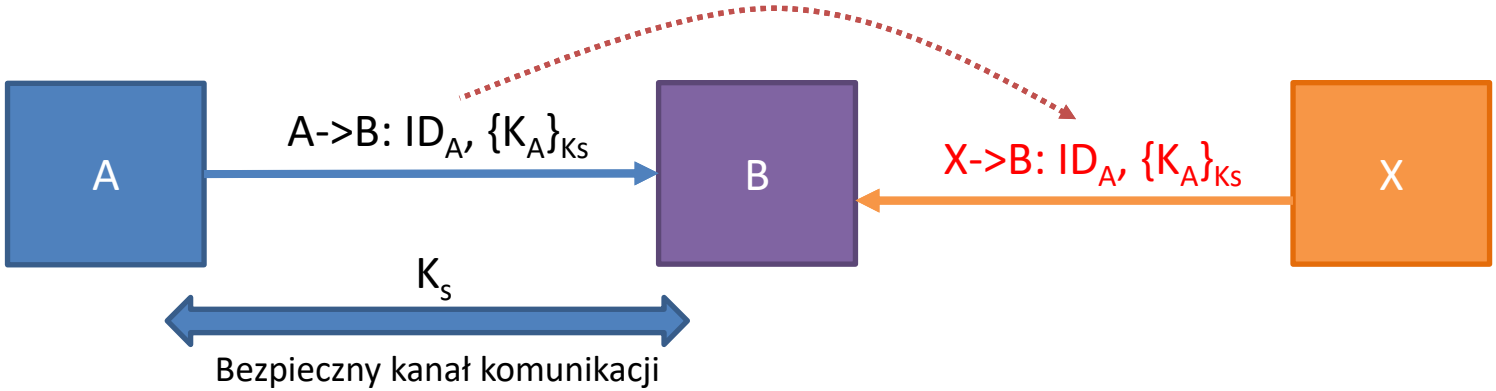
Plain-text password



- Przesłanie identyfikatora użytkownika oraz klucza znanego obu komunikującym się stronom.
- Przykład:
  - HTTP (basic), FTP, telnet, POP3, IMAP, …
- Każdy mający dostęp do użytego kanału komunikacyjnego jest w stanie poznać klucz.
- Uwierzytelnianie nie jest obustronne.
  - Użytkownik podaje dane weryfikujące pytającemu o niepotwierdzonej tożsamości.

GDAŃSK UNIVERSITY OF TECHNOLOGY

Encrypted password

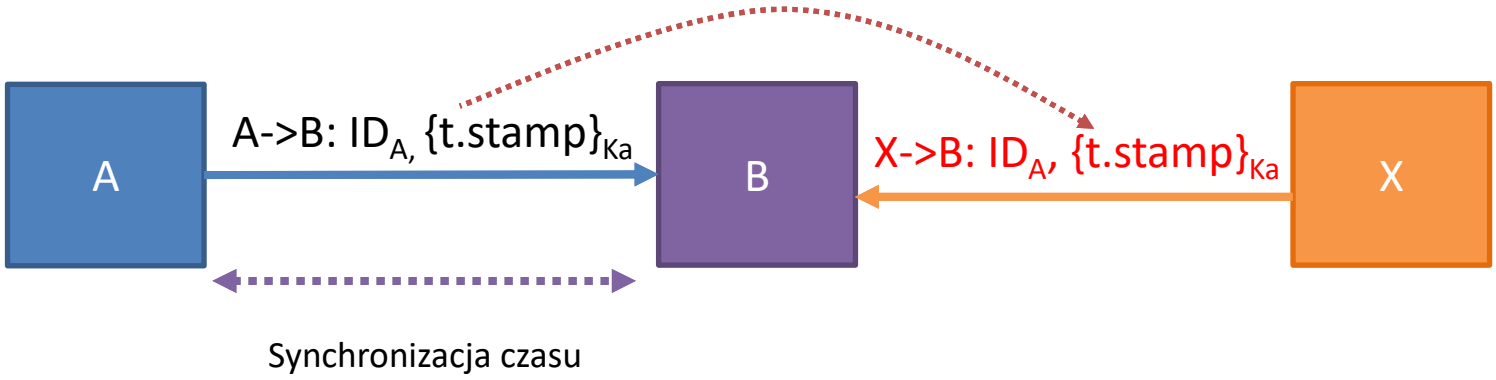


- Przesłanie identyfikatora użytkownika oraz klucza znanego obu komunikującym się stronom.
  - Wymaga już istniejącego, bezpiecznego kanału komunikacji.
- Klucz przesyłany jest w postaci zaszyfrowanej.
- Pozwala na zachowanie poufności klucza podczas transmisji oraz przed nieautoryzowanymi (nieznającymi K_s) odbiorcami – poznają jedynie $\{K_A\}_{Ks}$.

- Przy braku dodatkowych założeń, odtworzenie odpowiedzi uwierzytelniającej się strony ciągle działa.
- Uwierzytelnianie nie jest obustronne.

GDAŃSK UNIVERSITY OF TECHNOLOGY

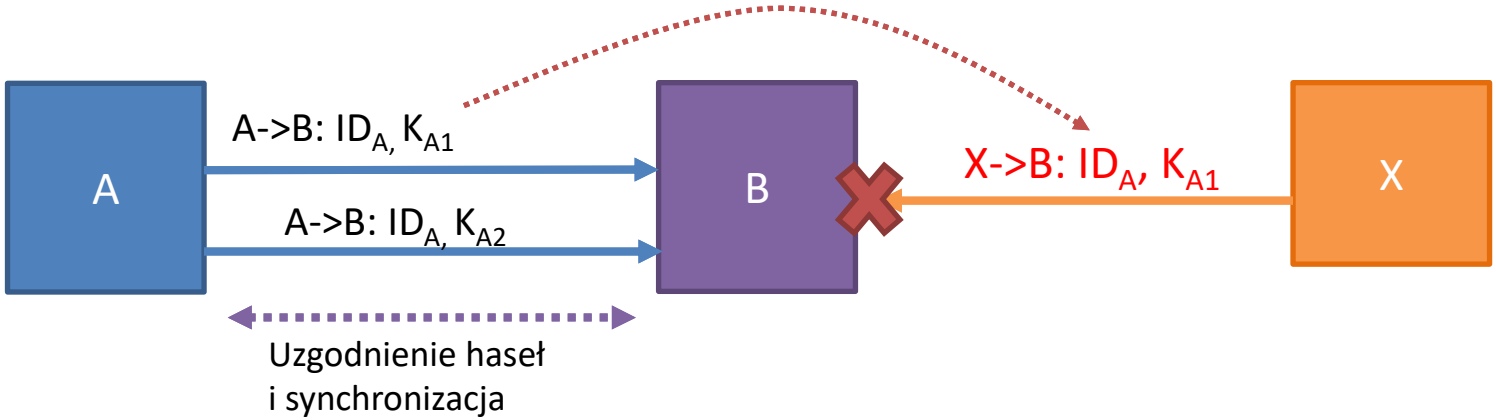
One-way with timestamp



- Wraz z identyfikacją przesyłany jest odpowiednio zmodyfikowany znacznik czasu.
  - Najczęściej zaszyfrowany przy wykorzystaniu hasła/klucza.
  - Sposób modyfikacji (np. znajomość K_a) potwierdza tożsamość.
- Wymaga synchronizacji czasu.
- Wymaga przyjęcia akceptowalnego opóźnienia odpowiedzi.
  - Opóźnienie komunikacji, niedokładność synchronizacji czasu.
- Przechwycenie wiadomości i odpowiednio szybkie wysłanie własnej pozwala na podszycie się pod A.
  - Niemożliwe jest już powtarzanie tego procesu bez ograniczeń.
- Obrona w postaci utrzymywania listy wykorzystanych już znaczników czasowych nie skutkuje w przypadku wielu serwerów B.

GDAŃSK UNIVERSITY OF TECHNOLOGY

One-time password (OTP)



- A i B posiadają wiedzę, jakie hasło powinno zostać użyte przy następnej próbie uwierzytelnienia, np.:
  - Lista haseł z zaznaczeniem wykorzystanych,
  - Lista haseł ze wskaźnikiem,
  - Sposób określenia kolejnego hasła na podstawie aktualnego stanu.
- Hasło używane jest jednokrotnie.

- Bezpieczne, jeśli kolejne hasła są rzeczywiście niemożliwe do przewidzenia.
  - Zadanie to należy to trudnych.
- Trudności sprawia też uzgodnienie haseł i/lub utrzymanie synchronizacji stron.

GDAŃSK UNIVERSITY OF TECHNOLOGY

OTP Generators (Tokens)

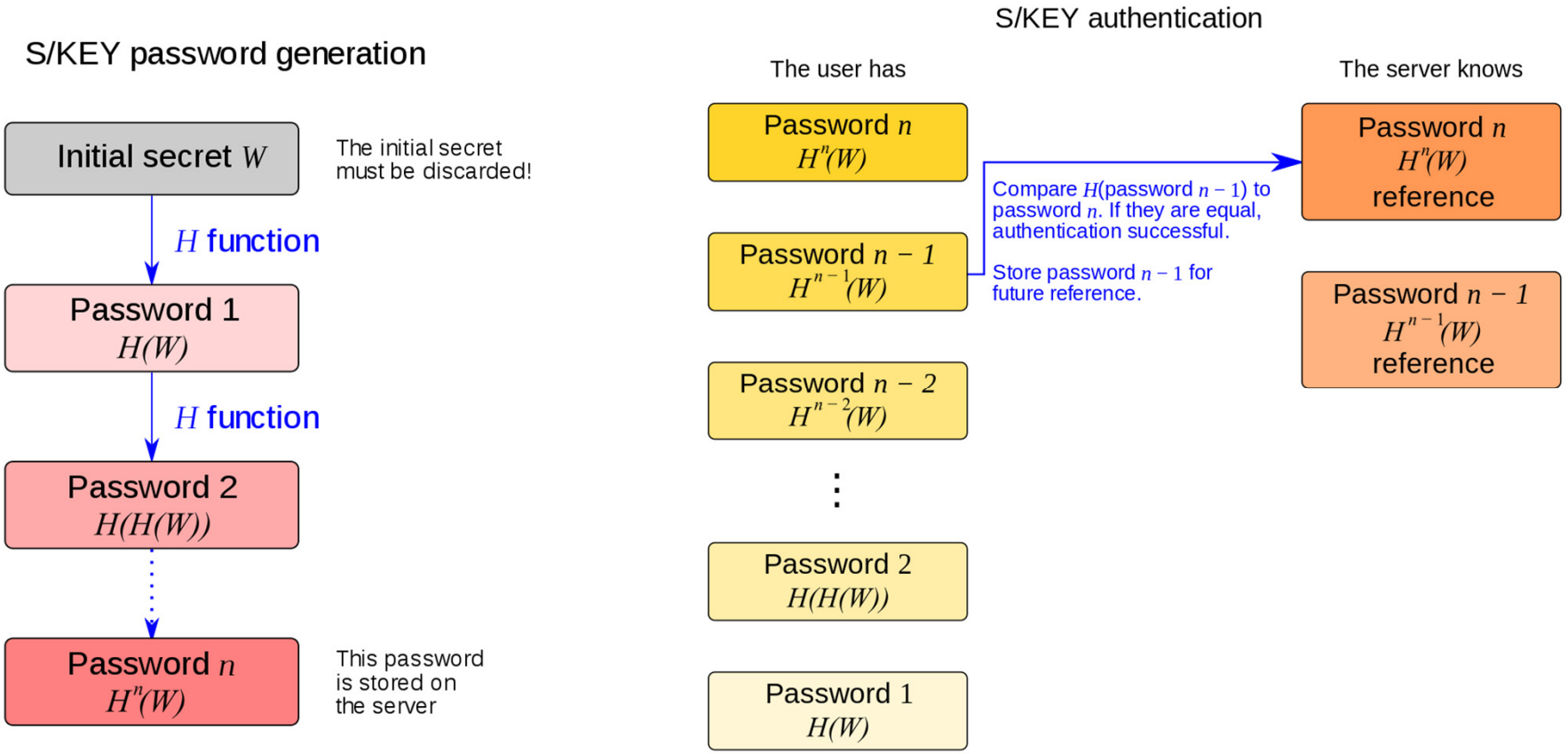
- Rodzaje:
  - Event OTP (H-MAC OTP, HOTP) – generują OTP na podstawie licznika żądań zsynchronizowanego z serwerem.
  - Time OTP (TOTP) – bazują na zegarze zsynchronizowanym z zegarem serwera uwierzytelniającego.
    - Popularnym rodzajem jest HOTP generujący wydarzenie do określony czas (np. 30-60 s).

- Popularnym rozwiązaniem przy generowaniu haseł jest użycie generatorów liczb pseudolosowych w postaci:
  - kodera blokowego – wielokrotne szyfrowanie,
  - funkcji skrótu – np. SHA-1.
- Najlepszym rozwiązaniem jest wykorzystanie dobrego źródła (np. fizycznego) wartości losowych.

- Ważnym elementem systemu jest sposób przechowywania haseł.

GDAŃSK UNIVERSITY OF TECHNOLOGY

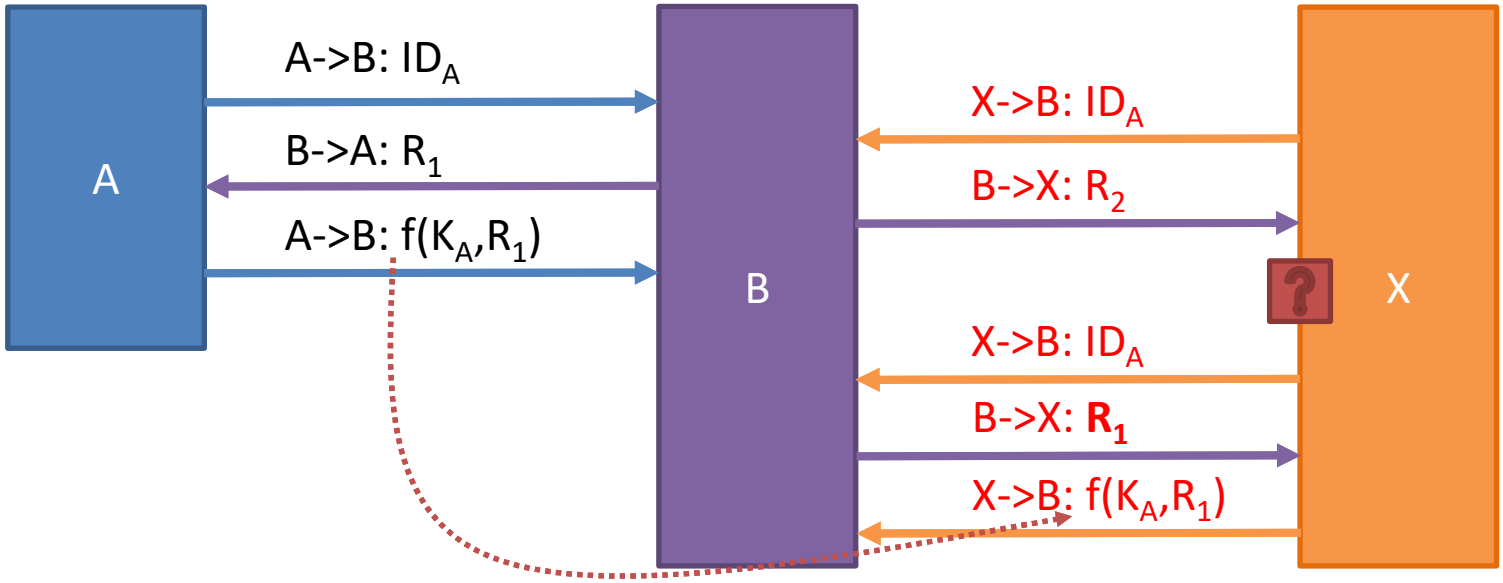
One-time password auth – Lamport's scheme (S/Key)



Założenie: Nie można łatwo uzyskać hasła $H^{n-1}(W)$ z hasła $H^n(W)$.

GDAŃSK UNIVERSITY OF TECHNOLOGY

One-way challenge-response

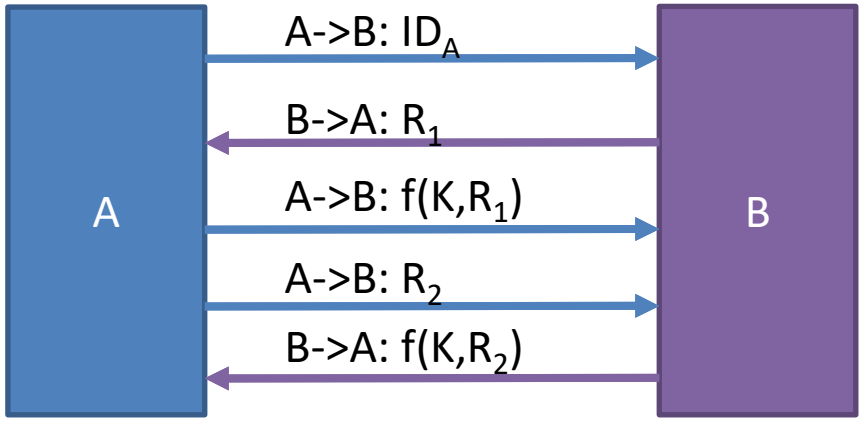


- W odpowiedzi identyfikację, przesyłana jest wartość challenge (R).
- Musi ona zastać w odpowiedni sposób przekształcona i odesłana.
  - Przy użyciu klucza użytkownika (K).
- Potwierdzeniem identyfikacji jest poprawność przekształcenia.
- Wartość challenge nie może być wykorzystywana wielokrotnie.
  - Przy powtórzeniu R wystarczy atak Reply.
- Uwierzytelnianie nie jest obustronne.
- Analiza odpowiedniej liczby wymian R – f(K,R) pozwala na odtworzenie K.

GDAŃSK UNIVERSITY OF TECHNOLOGY

Wzajemne uwierzytelnianie kluczem współdzielonym

(Mutual authentication with secret key)



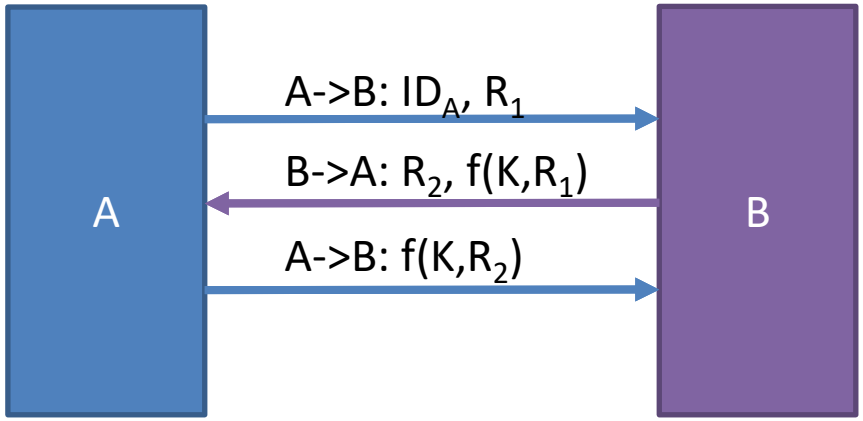
- Obie strony przeprowadzają uwierzytelnienie typu challenge-response.
  - Stosując odmienne wartości R.

- Kolejność uwierzytelnienia – pierwszy uwierzytelnia się inicjator (A).
  - ochrona przed atakiem DoS,
  - bardziej przydatna byłaby kolejność odwrotna.
- Niepotrzebnie duża liczba wiadomości.

GDAŃSK UNIVERSITY OF TECHNOLOGY

Wzajemne uwierzytelnianie kluczem współdzielonym

(Mutual authentication with secret key)



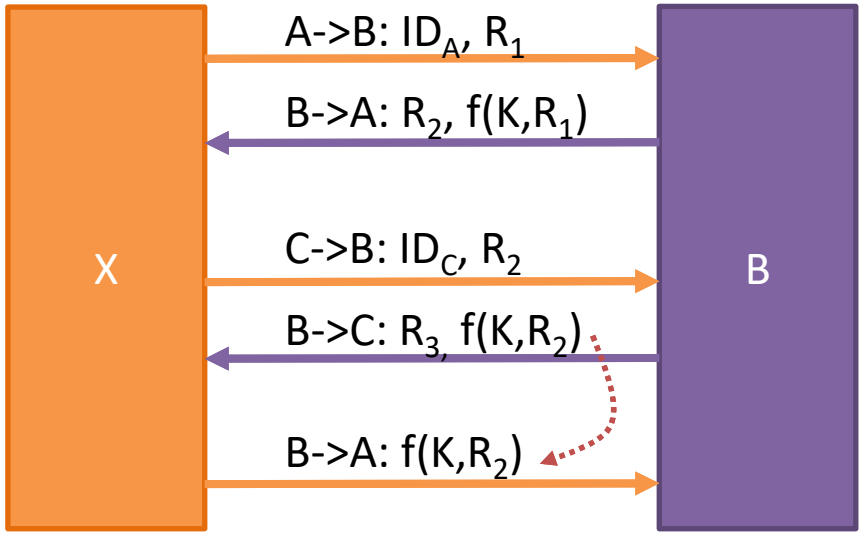
- Obie strony przeprowadzają uwierzytelnienie typu challenge-response.
- Strona inicjująca (A) uzyskuje potwierdzenie tożsamości B przed odesłaniem odpowiedzi.

- Strona B musi przeprowadzić operację $f(K,R_1)$ na żądanie inicjującego.
  - Potencjalny atak typu DoS, jeśli f() jest kosztowne obliczeniowo.
  - Możliwość uzyskania rozwiązań dla dowolnego dozwolonego R.
  - Możliwość uzyskania danych do analizy pozwalającej na określnie K.

GDAŃSK UNIVERSITY OF TECHNOLOGY

Wzajemne uwierzytelnianie kluczem współdzielonym

(Mutual authentication with secret key)



- Zagrożenie – Reflection attack.
  - zażądanie od atakowanej strony odpowiedzi na pytanie zadane atakującemu.

- Zróżnicowanie kluczy dla obu stron.
- Rozdzielenie zbiorów możliwych R.
- Zróżnicowanie sposobu przetwarzania.

GDAŃSK UNIVERSITY OF TECHNOLOGY

Nonce

- Nonce – Number Used Once
  - Wartość którą dana strona protokołu wykorzystuje jeden raz.
  - Składnik gwarantujący „świeżość” (freshness).
- Ochrona przed atakami polegającymi na odtworzeniu wiadomości (replay attacks).
- Powiązanie wiadomości wymienianych pomiędzy stronami.
- Rodzaje:
  - Licznik – wymaga utrzymywania stanu.
  - Znacznik czasu – wymaga synchronizacji czasu oraz określenia akceptowalnego przedziału opóźnienia.
  - Liczba losowa – oferuje jedynie prawdopodobieństwo unikalności. Wymaga liczb z dużego przedziału.

GDAŃSK UNIVERSITY OF TECHNOLOGY

Przechowywanie haseł

- W postaci otwartej (plain text) lub z użyciem odwracalnego szyfrowania (reversible encryption).
  - Każda z komunikujących się stron jest w stanie podać się za drugą.
  - Uzyskanie dostępu do bazy danych (potencjalnie) pozwala na poznanie haseł użytkowników.
- Najczęściej hasła przechowywane są (powinny być) w postaci nieodwracalnego skrótu (md5, sha1, sha256, sha512, …).
  - Przy weryfikacji otrzymane hasło jest poddawane temu samemu przekształceniu i porównywane.

- **Wymagania** dotyczące funkcji skrótu:
  - Oczywiste: przekształcenie jednokierunkowe – na podstawie hash(A) nie można jednoznacznie ustalić A.
  - Determinizm: hash(A) = hash(A)
  - Wysoki poziom entropii:
    - md5('security') = e91e6348157868de9dd8b25c81aebfb9
    - md5('security1') = 8632c375e9eba096df51844a5a43ae93
    - md5('Security') = 2fae32629d4ef4fc6341f1751b405e45
  - Małe prawdopodobieństwo kolizji:
    - Znalezienie A' takiego, że hash(A) = hash(A') jest czasochłonne.

GDAŃSK UNIVERSITY OF TECHNOLOGY

Przechowywanie haseł

- Hasła przechowywane w postaci skrótów mogą zostać złamane:
  - Atak brute force – powtórzenie operacji obliczenia skrótu i porównania wyniku dla wszystkich możliwych wartości hasła,
  - Atak słownikowy – ograniczenie powyższej metody do popularnych haseł zawartych w (szeroko pojętym) słowniku,
  - Wykorzystanie przeliczonych wcześniej wartości skrótów – ze względu na determinizm funkcji skrótu, można stworzyć bazę odwzorowań hasło->hash(hasło).

- Możliwe jest porównanie pojedynczego wyniku obliczeń z całym posiadanym zbiorem skrótów haseł wielu użytkowników: jedno obliczenie – n porównań.

- Obliczanie skrótu powinno wymagać możliwie długiego czasu (np. 1 s).
  - Czyni to ataki brute force mało efektywnymi. Utrudnia też ataki słownikowe.

GDAŃSK UNIVERSITY OF TECHNOLOGY

Salt

- Salt – losowa, (potencjalnie) inna dla każdego użytkownika, wartość modyfikująca hasło przed obliczeniem skrótu,
  - Skrót hasła = hash(salt + hasło).
  - Wartość salt musi być dostępna przy próbie weryfikacji hasła.
- Zastosowanie wartości salt:
  - Uniemożliwia wykorzystanie wcześniej przeliczonych tablic skrótów.
  - Wymusza przeprowadzenie obliczenia skrótu dla konkretnego użytkownika.

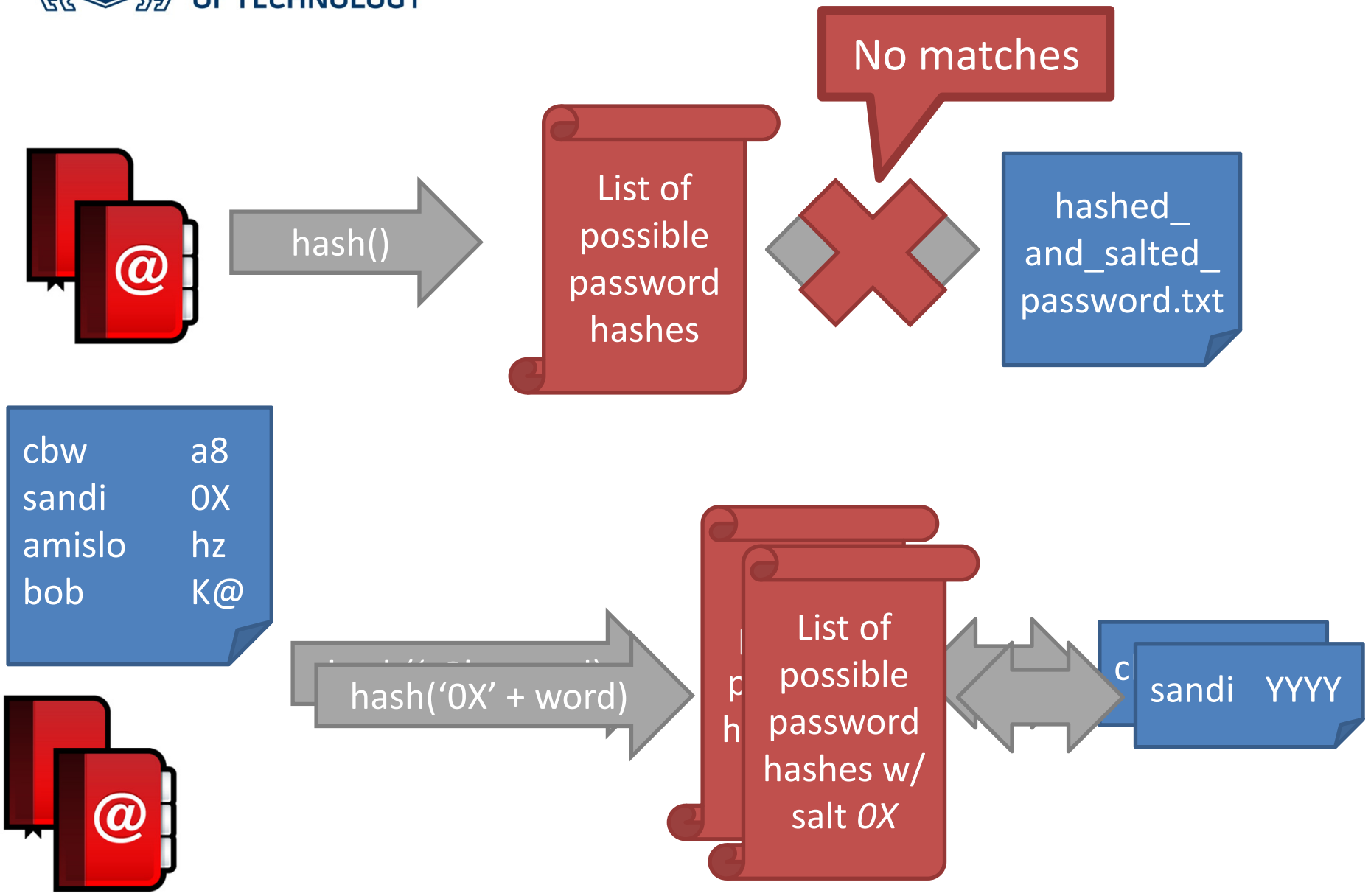
First two characters are the salt

/etc/shadow

username:password:last:may:must:warn:expire:disable:reserved

cbw:a8ge08pfz4wuk:9479:0:10000::::
amislo:hz560s9vnalh1:8172:0:10000::::

GDAŃSK UNIVERSITY OF TECHNOLOGY



GDAŃSK UNIVERSITY OF TECHNOLOGY

Stretching

- Funkcje skrótu dają się policzyć zbyt szybko.
- Można próbować wydłużyć ten czas wprowadzając wymóg wielokrotnego powtarzania obliczeń: hash(hash(hash(hash(…))))

- Password-Based Key Derivation Function 2 (PBKDF2, zdefiniowane w PKCS #5 2.0)
  - Wielokrotne przekształcenie hasła, uzupełnionego wartością salt, z użyciem funkcji skrótu, kodera blokowego lub funkcji HMAC (Hash-based Message Authentication Code).

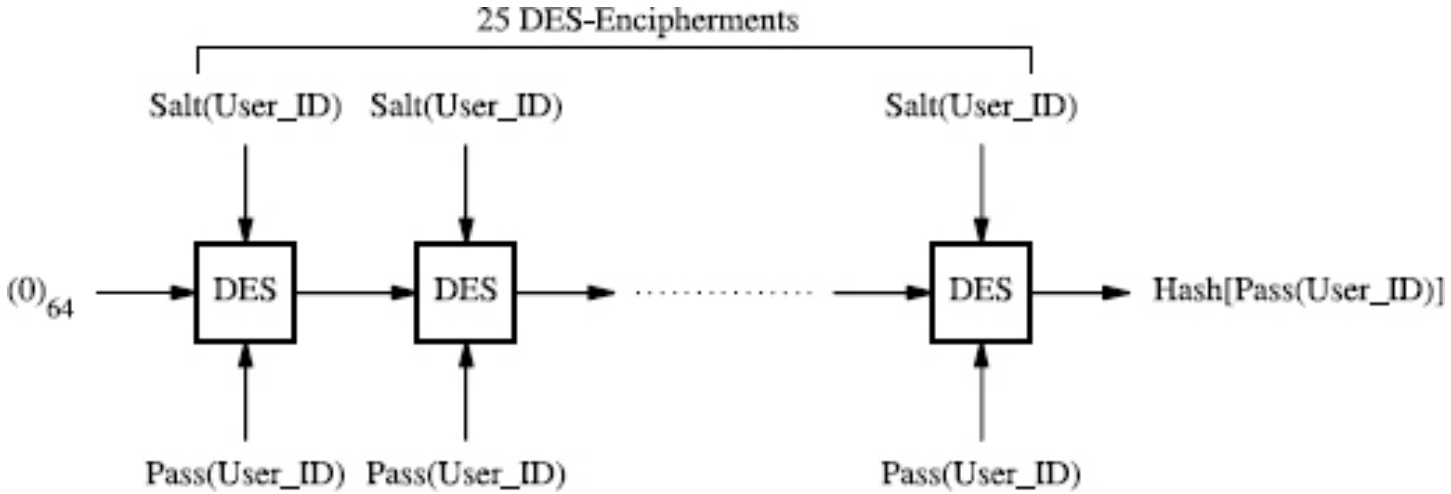
- bcrypt
  - Wielokrotne szyfrowanie hasła, uzupełnionego wartością salt, algorytmem Blowfish.
  - Parametr work factor pozwala kontrolować wprowadzane obciążenie obliczeniowe.

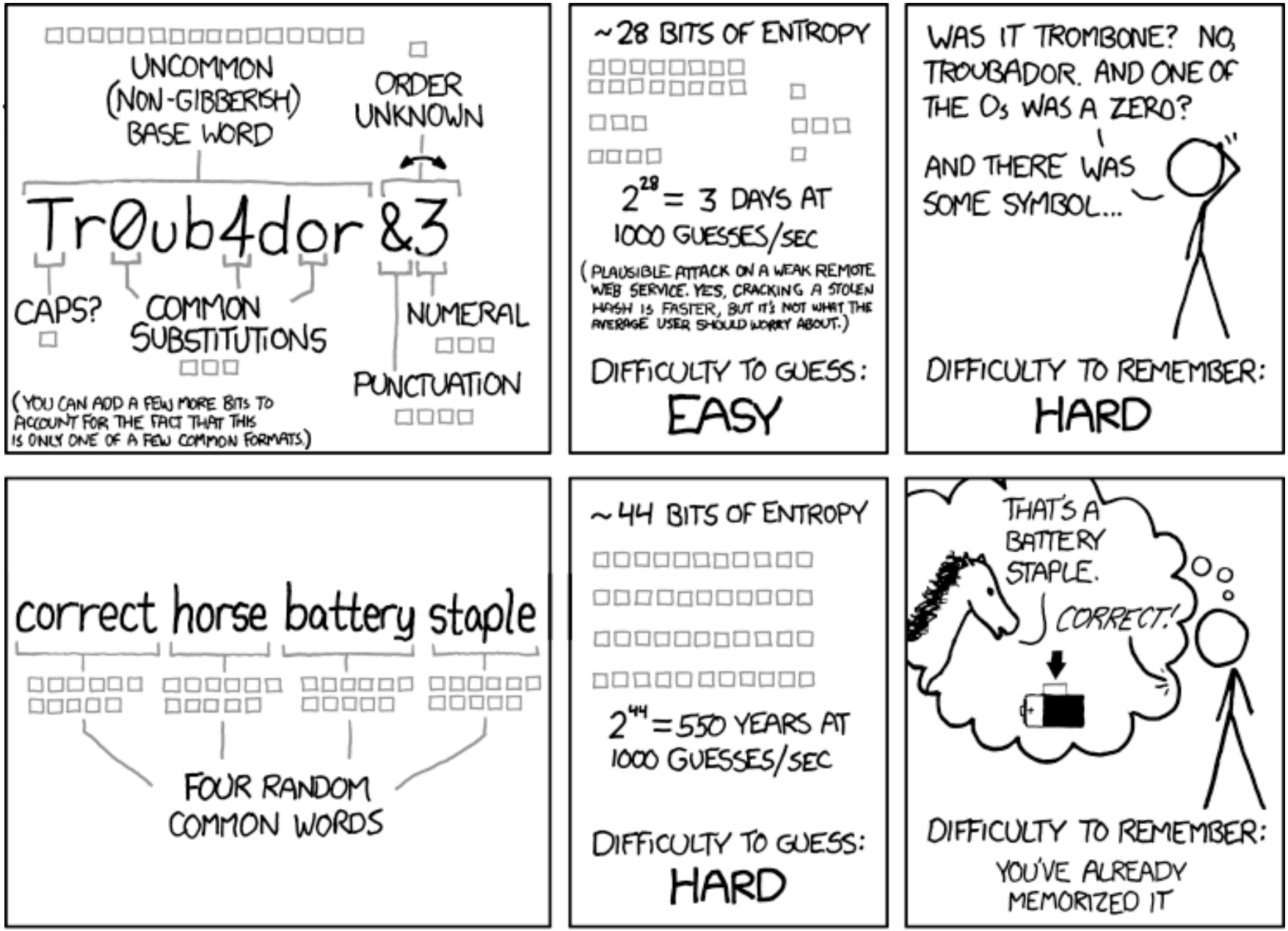
- scrypt (RFC7914)
  - PBKDF2, HMAC-SHA256, Salsa20
  - Dąży do maksymalizacji zarówno potrzebnej mocy obliczeniowej jak i pamięci.

GDAŃSK UNIVERSITY OF TECHNOLOGY

Unix password encryption – crypt()

- Ciąg 64 bitów o wartości 0 jest 25-krotnie szyfrowany algorytmem DES – wartość końcowa jest zapamiętywana i używana przy uwierzytelnianiu.
  - DES szyfruje 64-bitowe bloki danych z użyciem 56-bitowego klucza.
  - Brak jest metod pozwalających na znaczące uproszczenie ataku na algorytm DES.
- Celem powyższego sposobu przetwarzania hasła jest uczynienie ataku typu brute force kosztownym obliczeniowo.
- Jako klucz wykorzystywane jest zmodyfikowane hasło użytkownika.
  - Modyfikacja polega na wykorzystywaniu 12-bitowej wartości *salt* wraz z hasłem użytkownika.
  - Takie same hasła nie dają tej samej wartości wynikowej.
  - Przygotowanie gotowych słowników haseł staje się mniej efektywne.
  - Użycie popularnych koderów sprzętowych staje się niemożliwe.





THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

xkcd.com

GDAŃSK UNIVERSITY OF TECHNOLOGY

Explained

- Words: ~65000 dictionary words (16 bits), ~2000 common words (11 bits),
- Digits: $\log_2(10) = 3.3$ bits,
- Punctuation: 16 common punctuation marks (4 bits).

If you're confused, don't worry; you're in good company; even security "experts" don't understand the comic:

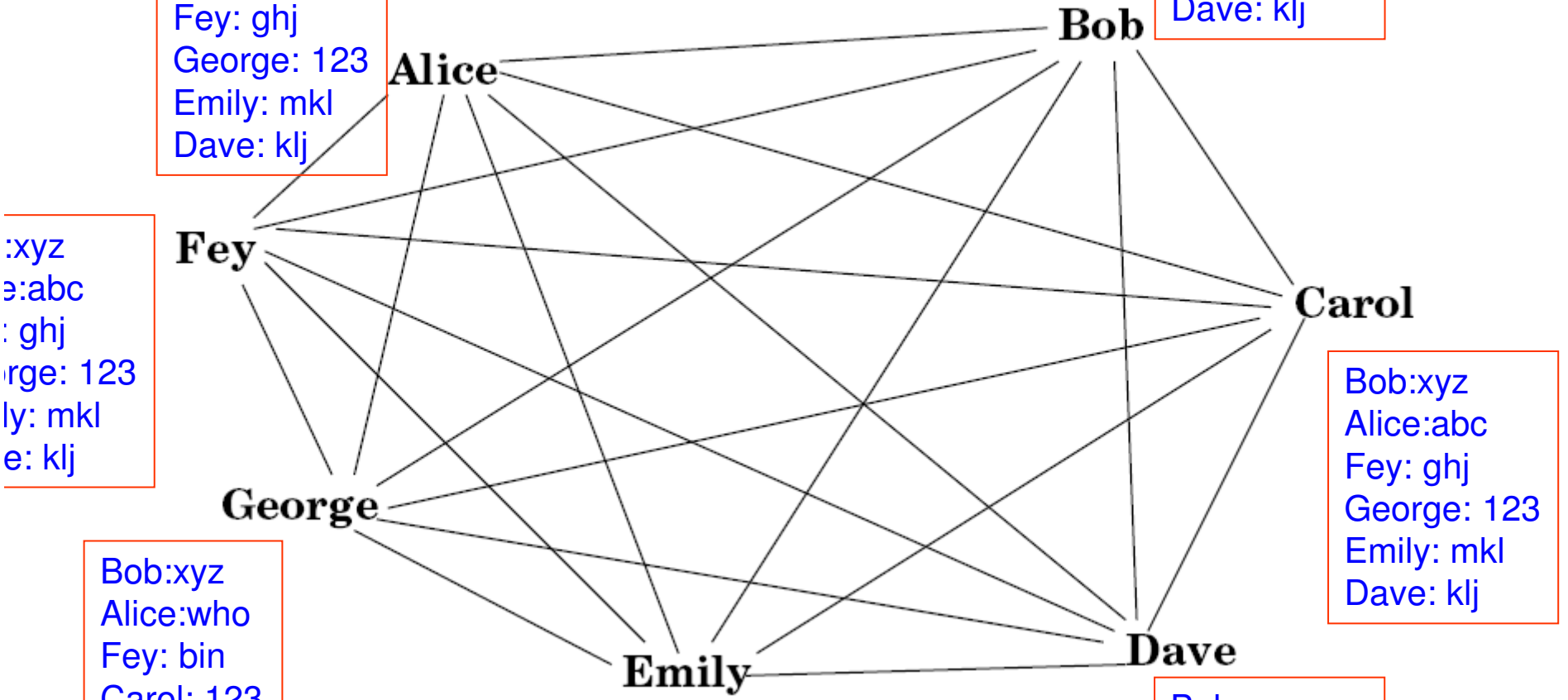
- „A” thinks that dictionary attacks make this method "obsolete", despite the comic *assuming* perfect knowledge of the user's dictionary from the get-go. He advocates his own low-entropy "first letters of common plain English phrases" method instead: „A”'s original article and rebuttals: 1 2 3 4 5 6
- „B” basically gets it, but calculates entropy incorrectly in order to promote his own method and upper-bound password-checking tool: „B” Security Now transcript and rebuttal
- Computer security consultant „C” *almost* understands the comic, but then advocates adding numerals and other crud to make passphrases less memorable, missing the point: Analyzing the XKCD Passphrase Comic
- „D” incorrectly thinks that user-selected sentences like "I have really bright children" have the same entropy as randomly-selected words: Is Your Password Policy Stupid?
- „E” doesn't understand that the words have to be truly random, not user-selected, like "let me in facebook": Password Security: Why the horse battery staple is not correct

Sigh.

Mediated authentication

GDAŃSK UNIVERSITY OF TECHNOLOGY

Direct authentication (1-to-1)



Bob:xyz
Alice:abc
Fey: ghj
George: 123
Emily: mkl
Dave: klj

Bob:xyz
Alice:abc
Fey: ghj
George: 123
Emily: mkl
Dave: klj

:xyz
e:abc
: ghj
rge: 123
ly: mkl
e: klj

Bob:xyz
Alice:abc
Fey: ghj
George: 123
Emily: mkl
Dave: klj

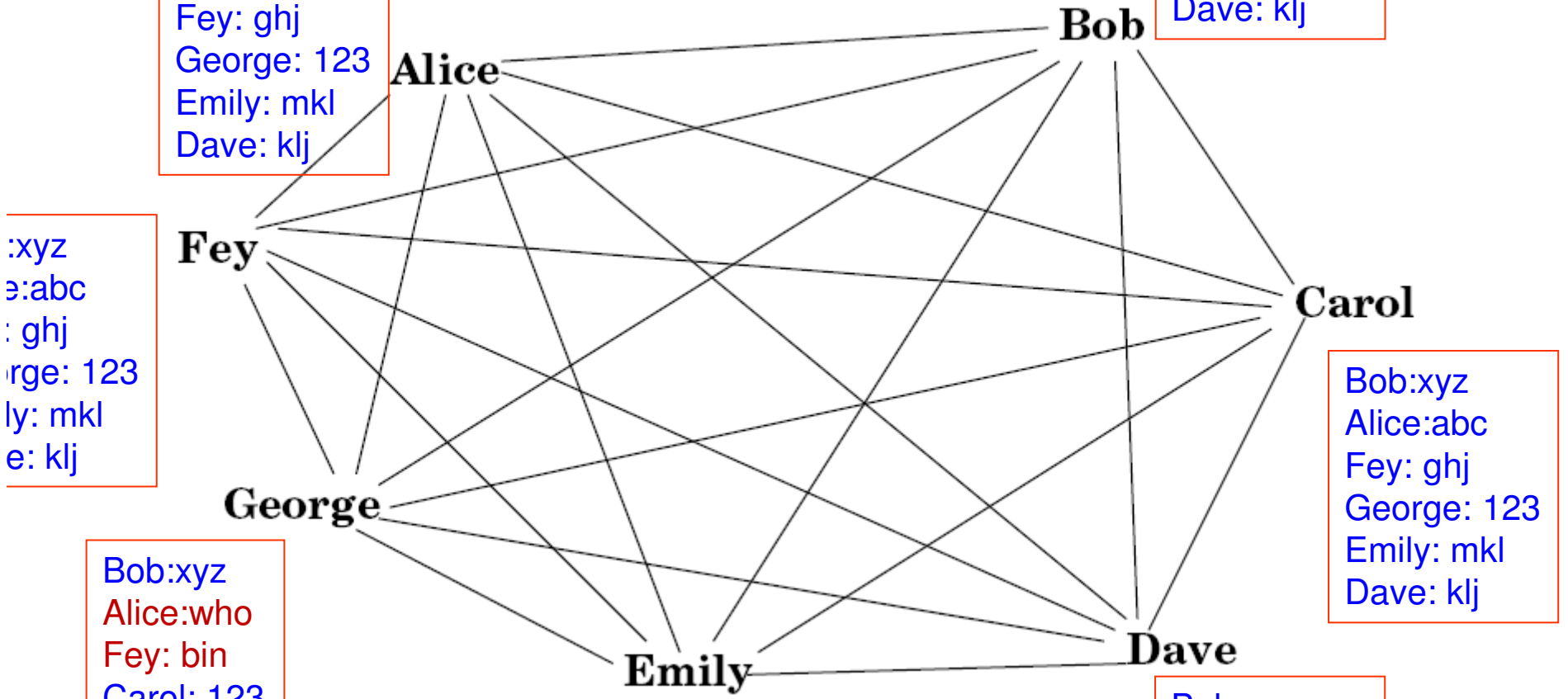
Bob:xyz
Alice:who
Fey: bin
Carol: 123
Emily: dog
Dave: cat

Bob:xyz
Alice:abc
Fey: ghj
George: 123

Bob:xyz
Alice:abc
Fey: ghj
George: 123
Emily: mkl

GDAŃSK UNIVERSITY OF TECHNOLOGY

Direct authentication (1-to-1)



Bob:xyz
Alice:abc
Fey: ghj
George: 123
Emily: mkl
Dave: klj

Bob:xyz
Alice:abc
Fey: ghj
George: 123
Emily: mkl
Dave: klj

:xyz
e:abc
: ghj
rge: 123
ly: mkl
e: klj

Bob:xyz
Alice:abc
Fey: ghj
George: 123
Emily: mkl
Dave: klj

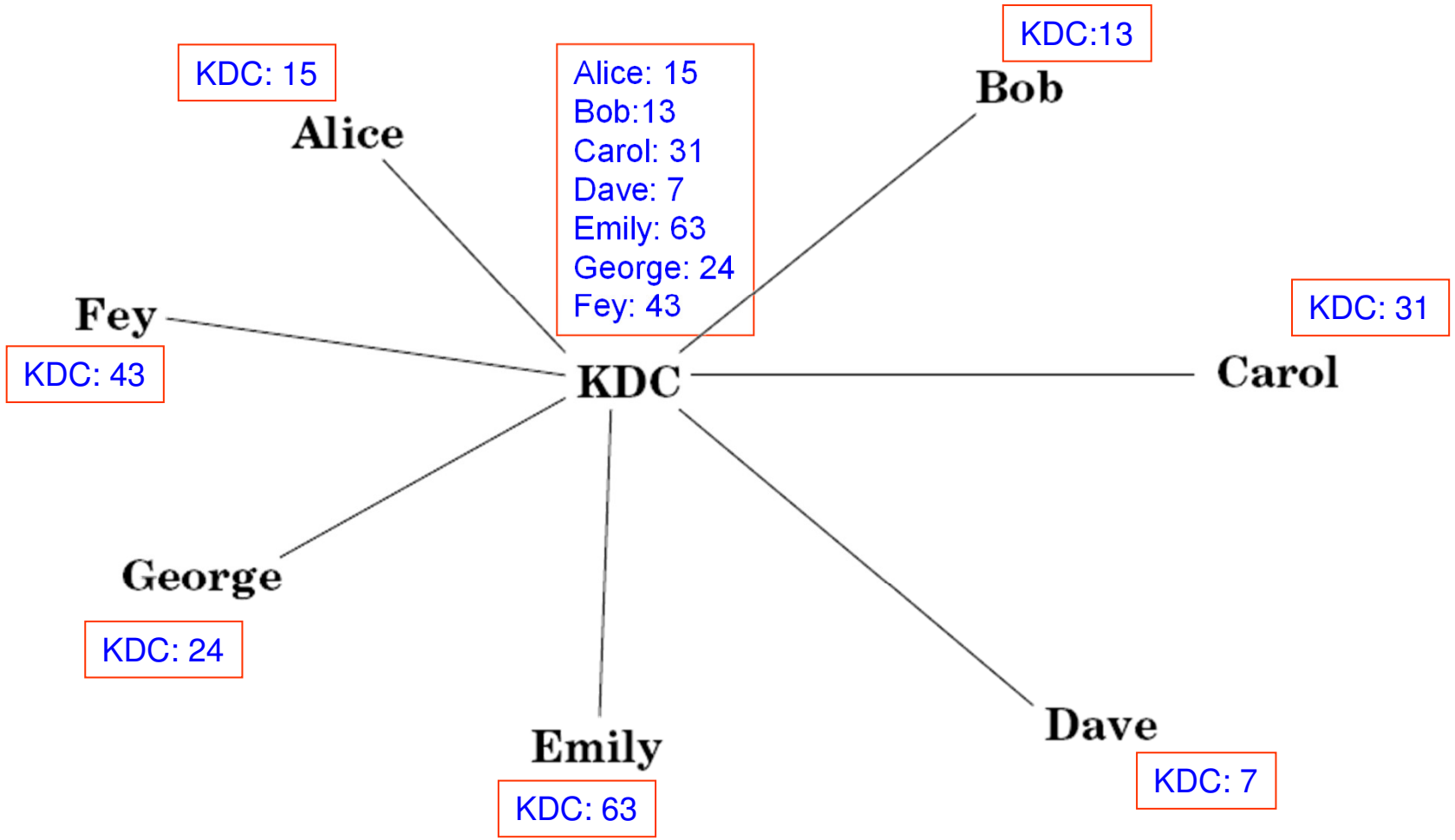
Bob:xyz
Alice:who
Fey: bin
Carol: 123
Emily: dog
Dave: cat

Bob:xyz
Alice:abc
Fey: ghj
George: 123

Bob:xyz
Alice:abc
Fey: ghj
George: 123
Emily: mkl

GDAŃSK UNIVERSITY OF TECHNOLOGY

Trusted intermediary (KDC)



GDAŃSK UNIVERSITY OF TECHNOLOGY

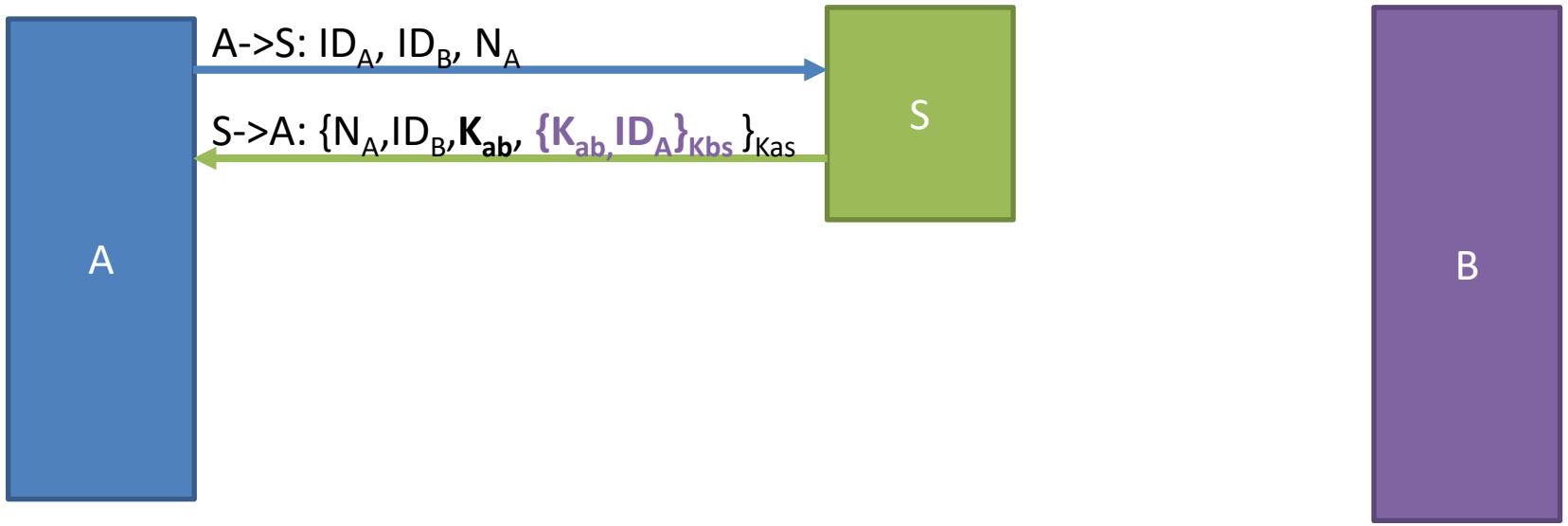
Mediated Authentication

- Zakłada istnienie zaufanej trzeciej strony procesu:
  - centrum dystrybucji kluczy (Key Distribution Center, KDC),
  - serwer uwierzytelniania (Authentication Server),
  - …
- Każdy z użytkowników posiada tajny klucz, znany KDC.
  - Znajomość powyższego klucza umożliwia KDC uwierzytelnienie użytkownika.

- W razie konieczności nawiązania komunikacji pomiędzy użytkownikami KDC generuje w tym celu klucze sesyjne, dostarczane następnie zaangażowanym użytkownikom.
  - Znajomość klucza sesyjnego potwierdza tożsamość użytkownika, przy założeniu, że KDC jest zaufane.
  - W celu finalizacji procesu uwierzytelnienia, strona musi udowodnić drugiej, że faktycznie zna klucz sesyjny.

GDAŃSK UNIVERSITY OF TECHNOLOGY

Needham-Schroeder Protocol

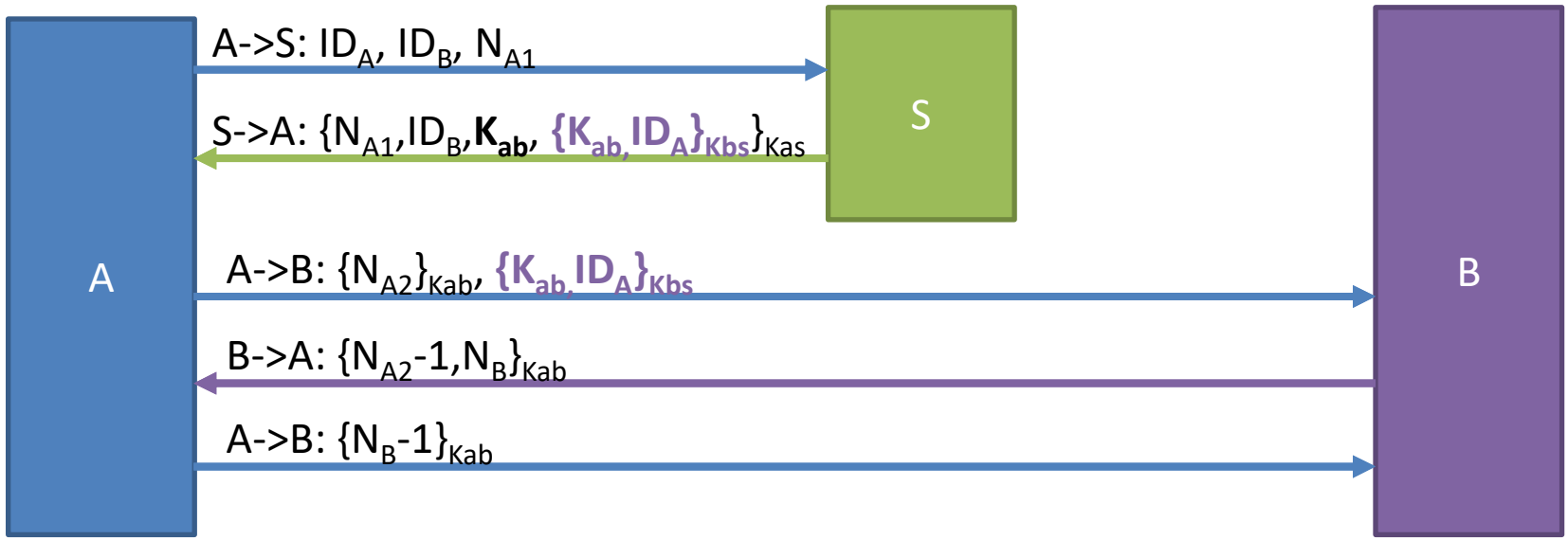


- S zna klucze $K_{?s}$ wszystkich stron chcących się komunikować.
  - Są one używane jako informacja uwierzytelniająca.
  - Są używane wyłącznie do komunikacji z S.

- A zgłasza chęć komunikacji z B.
- A otrzymuje - zaszyfrowane kluczem $K_{as:}$
  - klucz sesyjny K_{ab}, który ma wykorzystać do komunikacji z B,
  - pakiet danych zaszyfrowanych kluczem K_{bs} do przekazania B.

GDAŃSK UNIVERSITY OF TECHNOLOGY

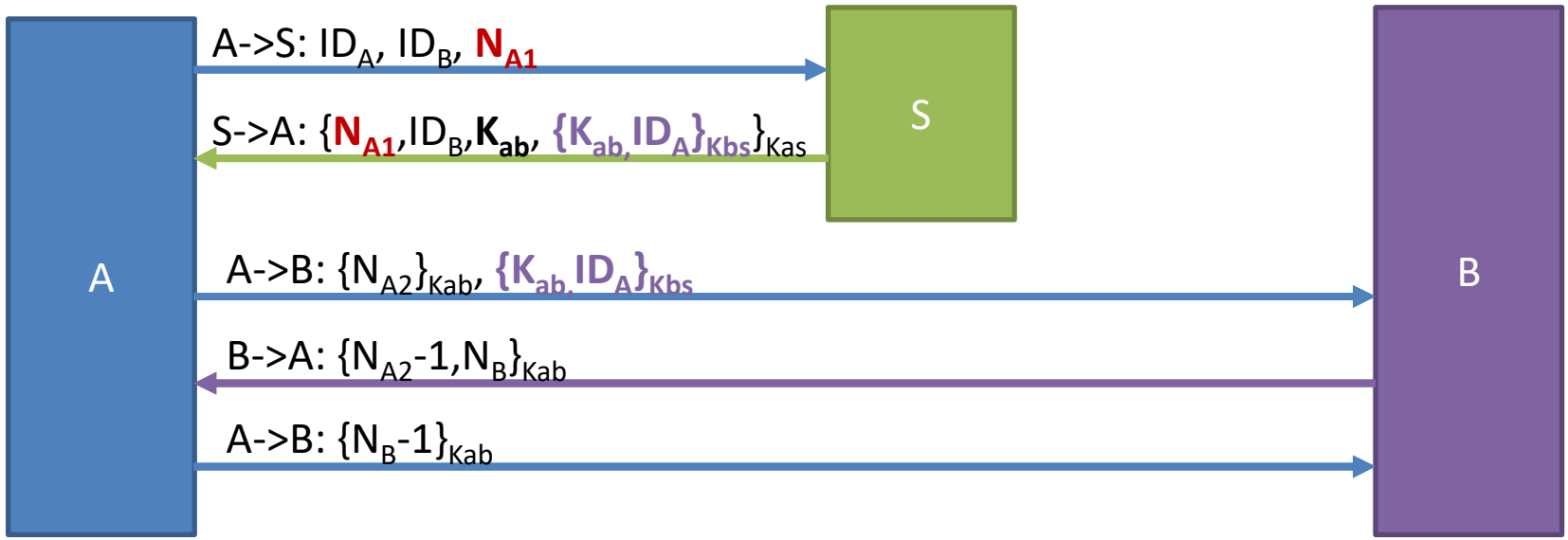
Needham-Schroeder Protocol



- A przekazuje B powyższy pakiet danych zawierający klucz sesyjny K_{ab}.
  - B rozszyfrowuje go i uzyskuje klucz K_{ab}.
  - Utworzony został kanał łączności A-B zabezpieczony kluczem sesyjnym K_{ab}.
- Uwierzytelnienie:
  - wraz z powyższym pakietem zostaje przesłana wartość N_{A2},
  - B udowadnia znajomość prawidłowego klucza K_{ab}, odszyfrowując N_{A2} i odsyłając je po odpowiednim przekształceniu i ponownym zaszyfrowaniu kluczem sesyjnym,
  - B generuje wartość nonce N_B. i przesyła do A po zaszyfrowaniu kluczem sesyjnym,
  - A udowadnia znajomość prawidłowego klucza K_{ab} w podobny sposób jak wcześniej B – przekształcając i odsyłając N_B.

GDAŃSK UNIVERSITY OF TECHNOLOGY

Needham-Schroeder Protocol

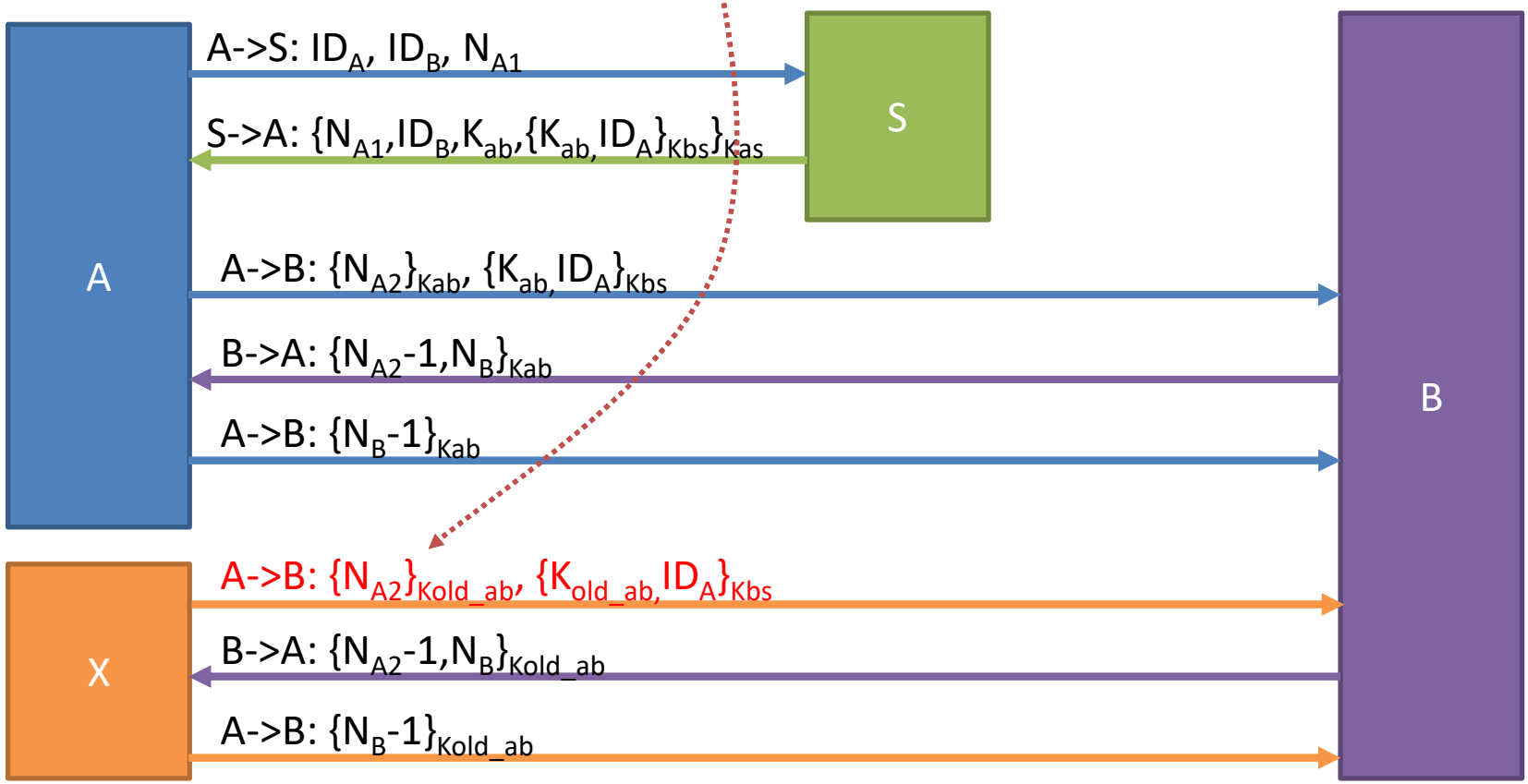


- Bez N_{A1} atakujący mógłby (podszywając się pod S) odtworzyć starą odpowiedź z S->A i wymusić użycie skompromitowanego klucza K_{ab}.
- Tym samym mógłby podszyć się pod B – atak na A.

GDAŃSK UNIVERSITY OF TECHNOLOGY

Odtworzenie wiadomości z wcześniejszego uwierzytelnienia.
Klucz K_{old_ab} został już złamany.

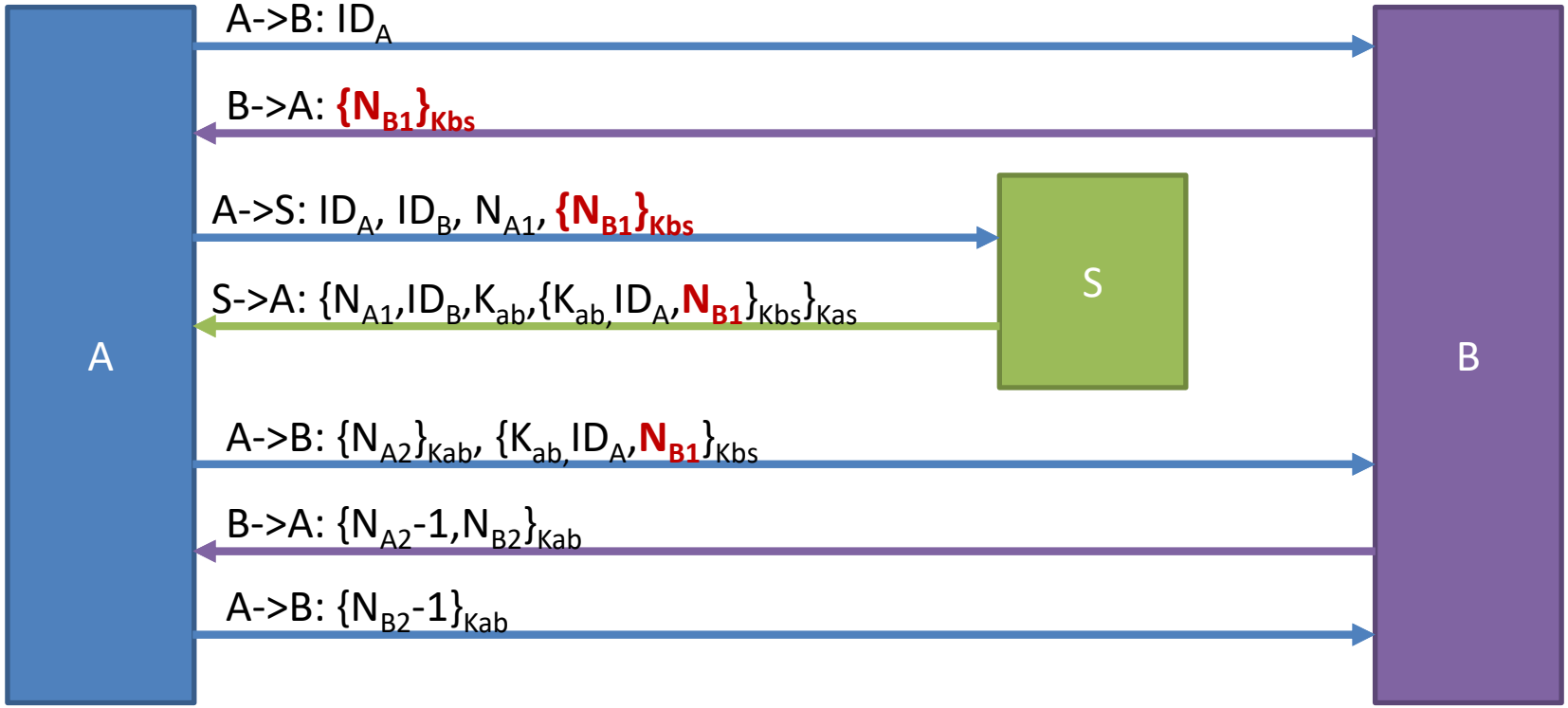
Needham-Schroeder Protocol



X zna nieaktualny już K_{old_ab}. Może się uwierzytelnić odtwarzając wiadomość A->B: $\{K_{old\_ab}, ID_A\}_{Kbs}$

GDAŃSK UNIVERSITY OF TECHNOLOGY

Extended Needham-Schroeder

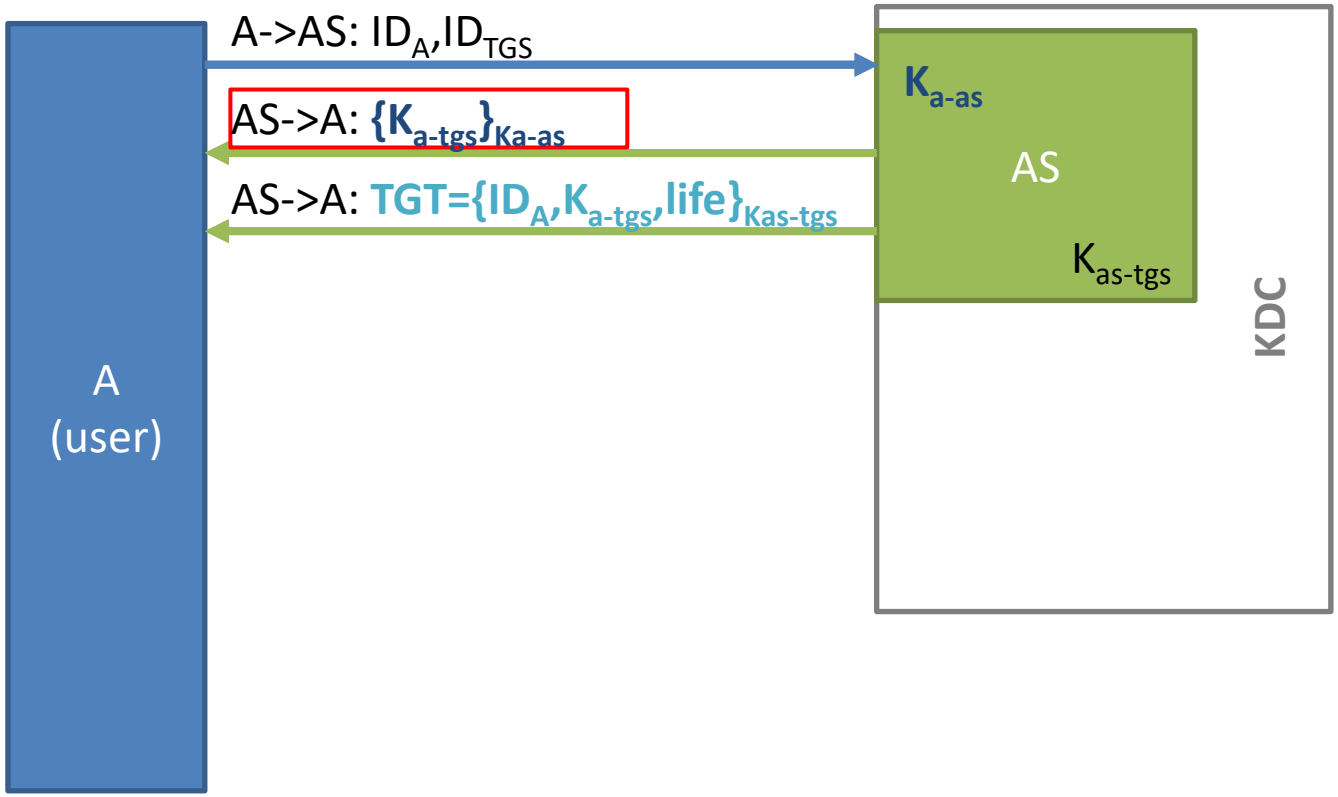


- Wprowadzenie unikalnej wartości nonce (N_{B1}), ustalanej przez B i wymaganej przez B w odpowiedzi od S przekazywanej przez A.

Kerberos

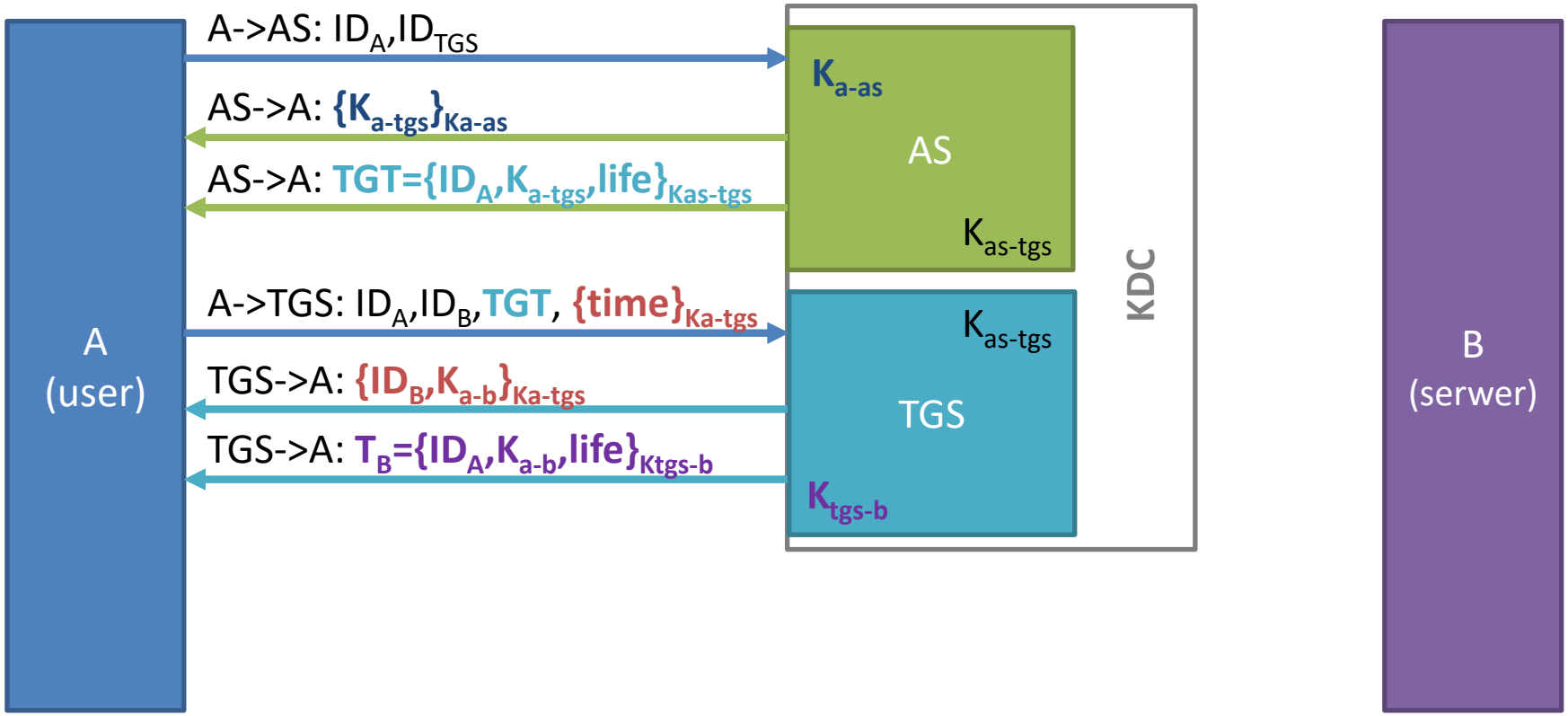
- Advantages:
  - No password communicated on the network.
  - Authenticating password is used rarely (single sign-on).
  - No authenticating passwords (even encrypted) exchanged across the network.
  - Limited period of validity. Each ticket is issued for a limited period of time.
    - Long attacks, such brute force cryptanalysis, are usually neutralized because the attacker does not have time to complete the attack.
  - Time stamps to prevent reply attacks. Each user request to a server is stamped with the time of the request. The request is accepted only if the time is reasonably close to the current time.
- Drawbacks:
  - Single point of failure: requires continuous availability of the central server. When the Kerberos server is down, no one can log on (multiple Kerberos servers).
  - Kerberos requires the clocks of the involved hosts to be synchronized.
  - Since all authentication is controlled by a centralized KDC, compromise of this authentication infrastructure will allow an attacker to impersonate any user.

Kerberos – client authentication



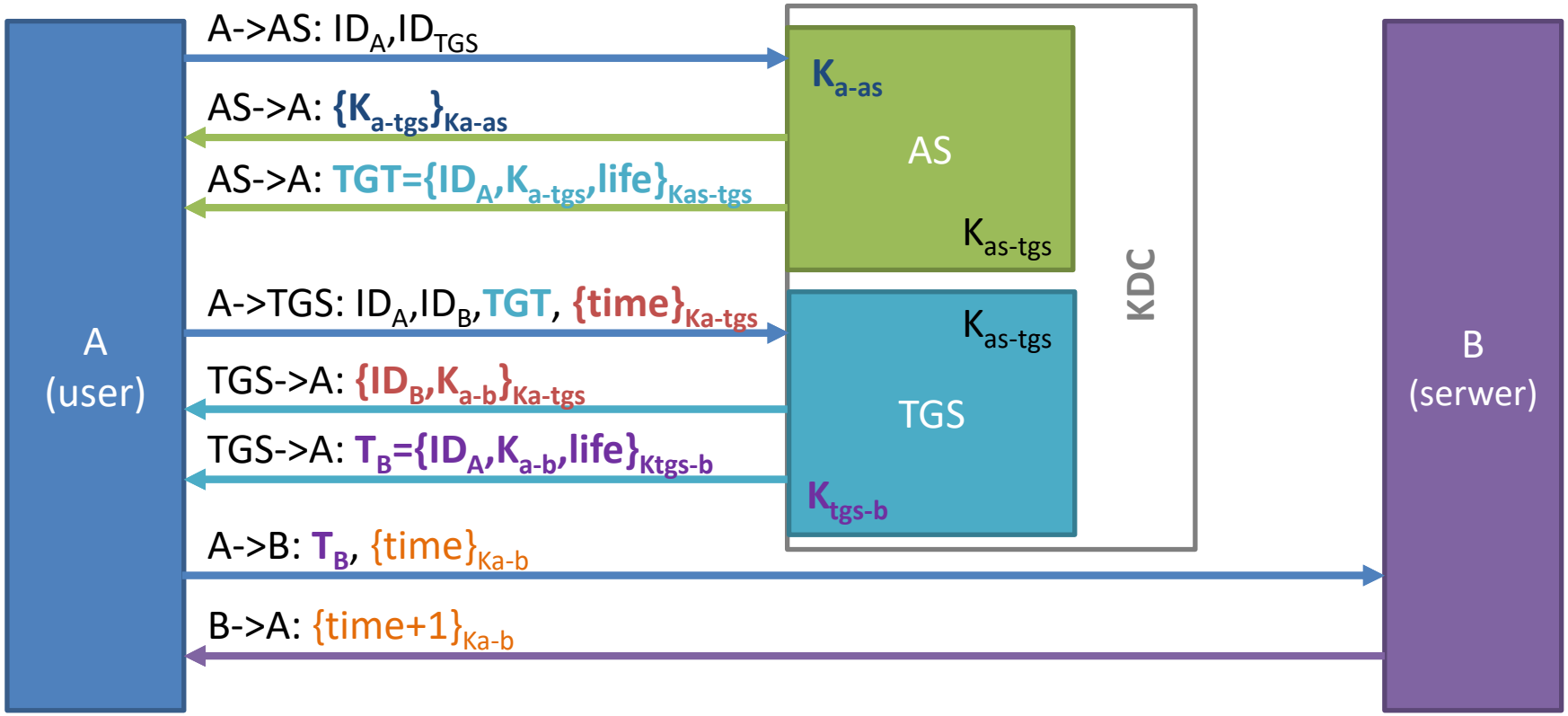
GDAŃSK UNIVERSITY OF TECHNOLOGY

Kerberos – service authorization



GDAŃSK UNIVERSITY OF TECHNOLOGY

Kerberos – service request



GDAŃSK UNIVERSITY OF TECHNOLOGY

Smart Cards

- **Memory cards** – oferują możliwość przechowywania i odczytywania informacji.
  - Straight Memory Cards – brak zabezpieczeń, dostęp np. I^2C,
  - Protected / Segmented Memory Cards – dostęp do zapisu (czasem również do odczytu) kontrolowany hasłem/PINem,
  - Stored Value Memory Cards – przechowują wartości o specyficznym przeznaczeniu i sposobie dostępu, np. liczniki, wartości o jednorazowym dostępie, itp. Funkcjonalność (a czasem także zawartość) określana ma etapie produkcji.

- **Microprocessor cards** – oferują możliwość zarówno przechowywania jak i przetwarzania informacji.
  - Wykorzystują dedykowany system operacyjny, np.:
    - JavaCard Runtime Environment,
    - MULTOS Card Operating System.

GDAŃSK UNIVERSITY OF TECHNOLOGY

Microprocessor Smart Cards

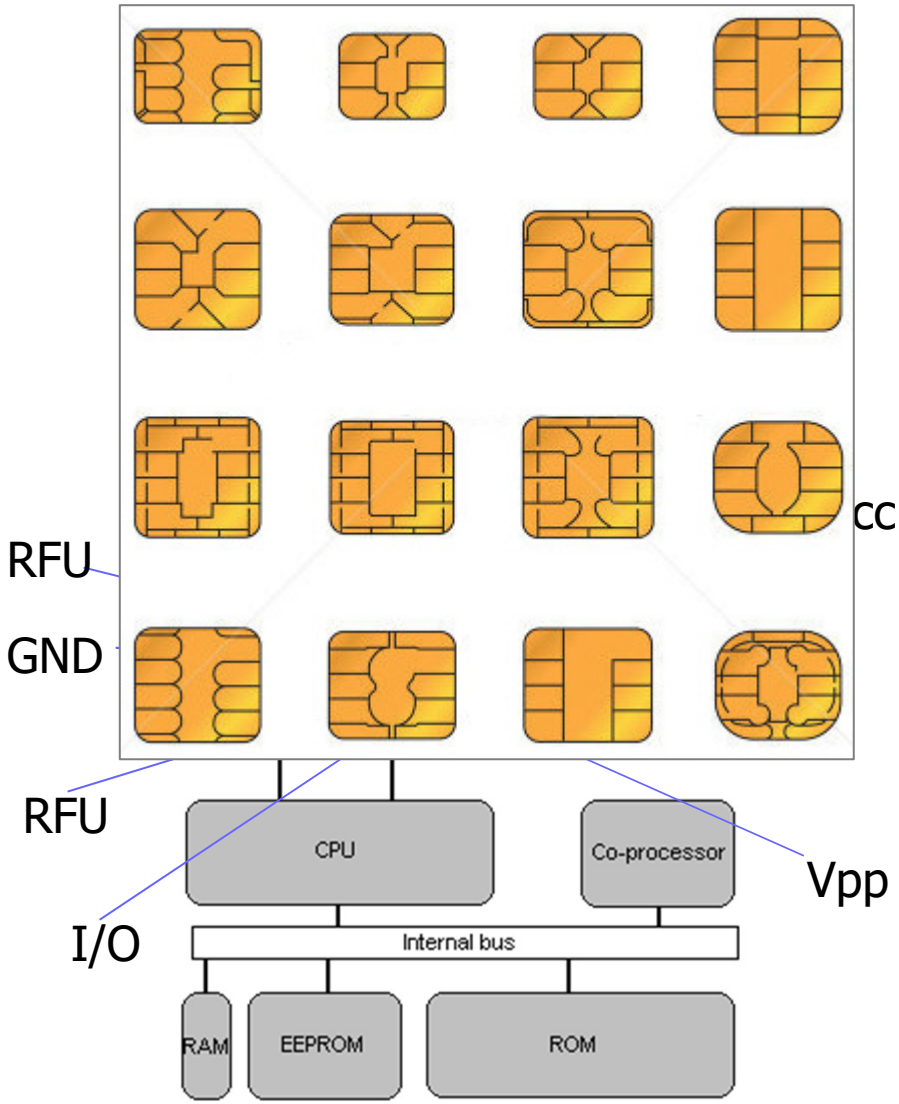
- The terminal/PC sends commands to the card (through the serial line).
- The card executes the command and sends back the reply.
- The terminal/PC cannot directly access memory of the card
  - Data in the card is protected from unauthorized access by OS.

- Standardization:
  - ISO 7810 standard – physical characteristics, RF frequencies,
  - ISO 7816 standard – logical structure, programming, biometric verification, memory usage for services, communication.
  - ISO 14443 standard – contactless cards.
- Commands are initiated by the terminal:
  - Interpreted by the card OS.
  - Card state is updated.
  - Response is given by the card.

GDAŃSK UNIVERSITY OF TECHNOLOGY

Ogólna architektura

- Typowe parametry:
  - 256 bytes to 8KB RAM.
  - 4KB to 32KB ROM.
  - 1KB to 32KB EEPROM.
  - Opcjonalnie: Crypto-coprocessors (3DES, RSA, RSA etc.).
  - CPU: 8-bit,16-bit, rzadko 32-bit.
- Karta bez co-processor'a kryptograficznego nie obsługuje funkcji kryptograficznych.
- Istnieją standardy złączy – i to dość sporo…



GDAŃSK UNIVERSITY OF TECHNOLOGY

Smart card usage

- Password verification
  - Terminal asks the user to provide a password.
  - Password is sent to Card for verification.
  - Scheme can be used to permit user authentication.
- Biometric techniques
  - Fingerprint identification – Features of fingerprints can be kept on the card or even verified on the card.
  - Photograph/IRIS pattern etc. – Such information is to be verified by external mechanisms or a person. The information can be only be stored on the card (securely).
- Certificate/private key operations
  - Personal Identity Verification (PIV) – generation of keys, digital signatures, authentication, …

GDAŃSK UNIVERSITY OF TECHNOLOGY

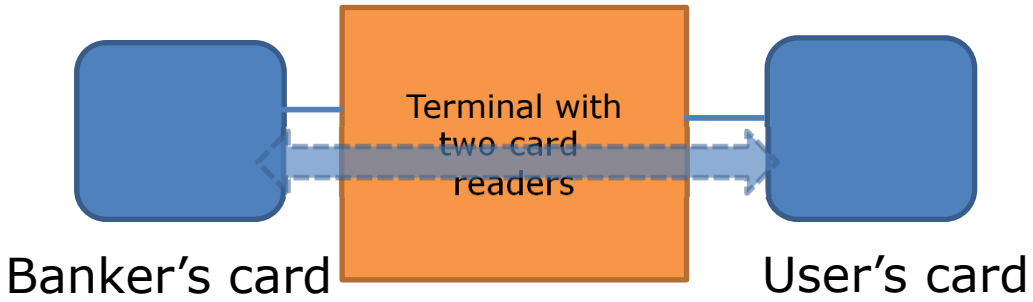
Smart card cryptographic verification

- Terminal verifies card (INTERNAL AUTH)
  - Terminal sends a random number to card to be hashed or encrypted using a key.
  - Card provides the hash or cyphertext.
  - Terminal can know that the card is authentic.

- Card verifies terminal (EXTERNAL AUTH)
  - Terminal asks for a challenge and sends the response to card to verify.
  - Card thus know that terminal is authentic.

GDAŃSK UNIVERSITY OF TECHNOLOGY

Two-card scenario



1. Authenticate user to bank officer card:
    1. Get challenge from banker card.
    2. Obtain response for the challenge from passport (IAUTH).
    3. Validate response with officer card (EAUTH)
2. Authenticate officer card to passport.
    1. ...
3. Transfer money to the user's card

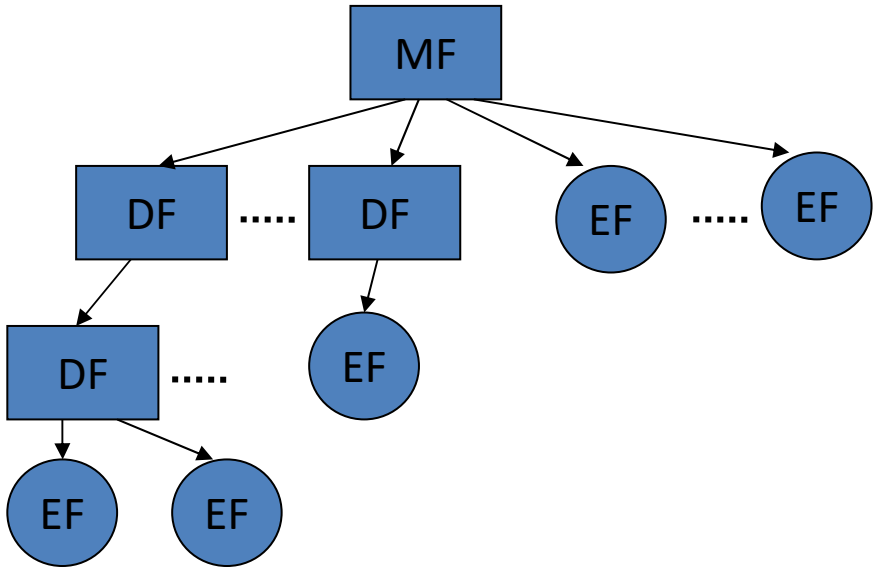
The terminal itself does not store any keys, it's the two cards that really authenticate each other. The terminal just facilitates the process.

GDAŃSK UNIVERSITY OF TECHNOLOGY

Smart card filesystem

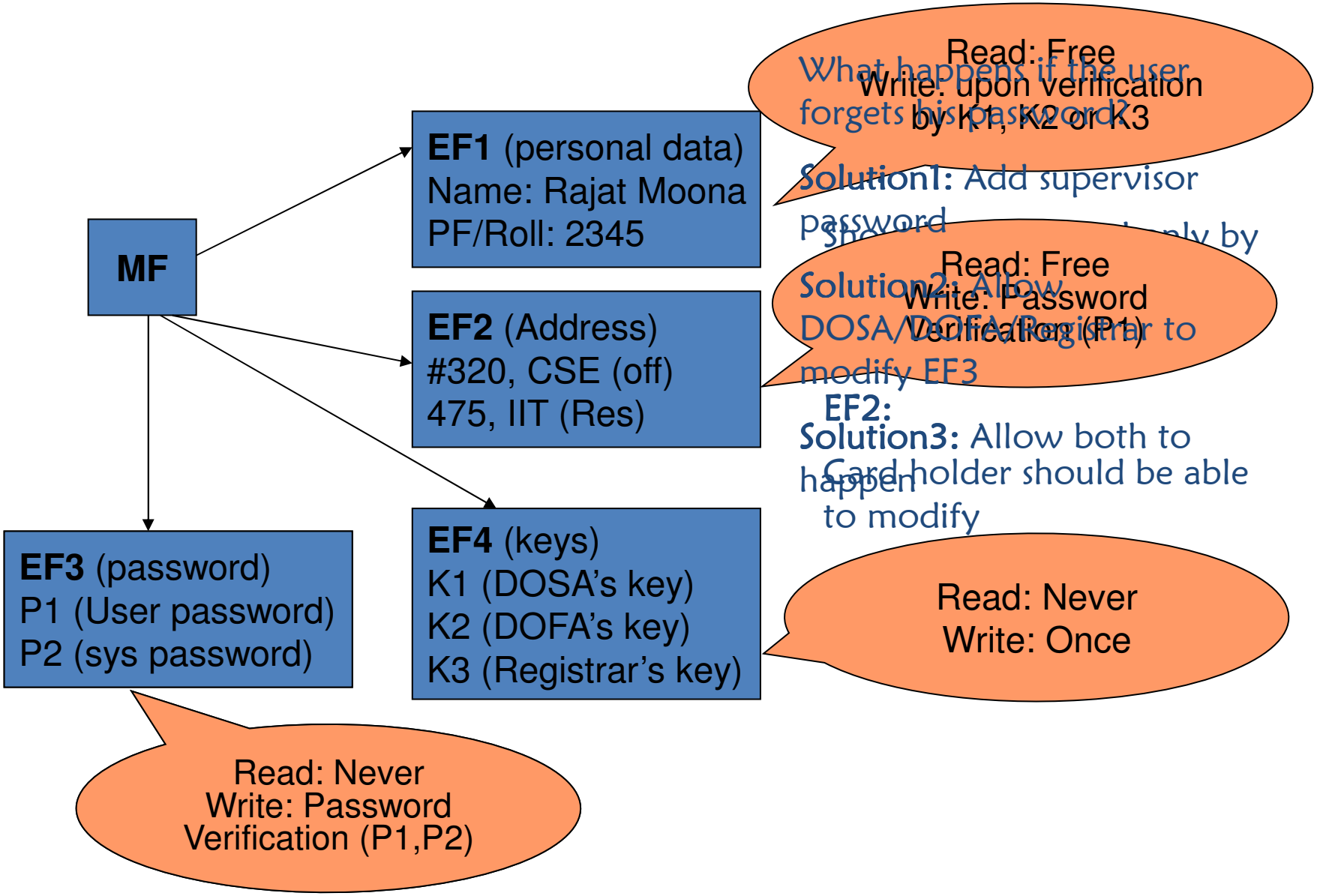
- Elementy systemu plików:
  - Master File (MF) – „folder główny”,
  - Dedicated File (DF) –„folder”,
  - Elementry File (EF) – „plik”.

- Każdy z powyższych elementów może zawierać dane.
- Dostęp realizowany jest z użyciem systemu operacyjnego karty.
- Obsługiwana jest kontrola dostępu do elementów systemu plików.



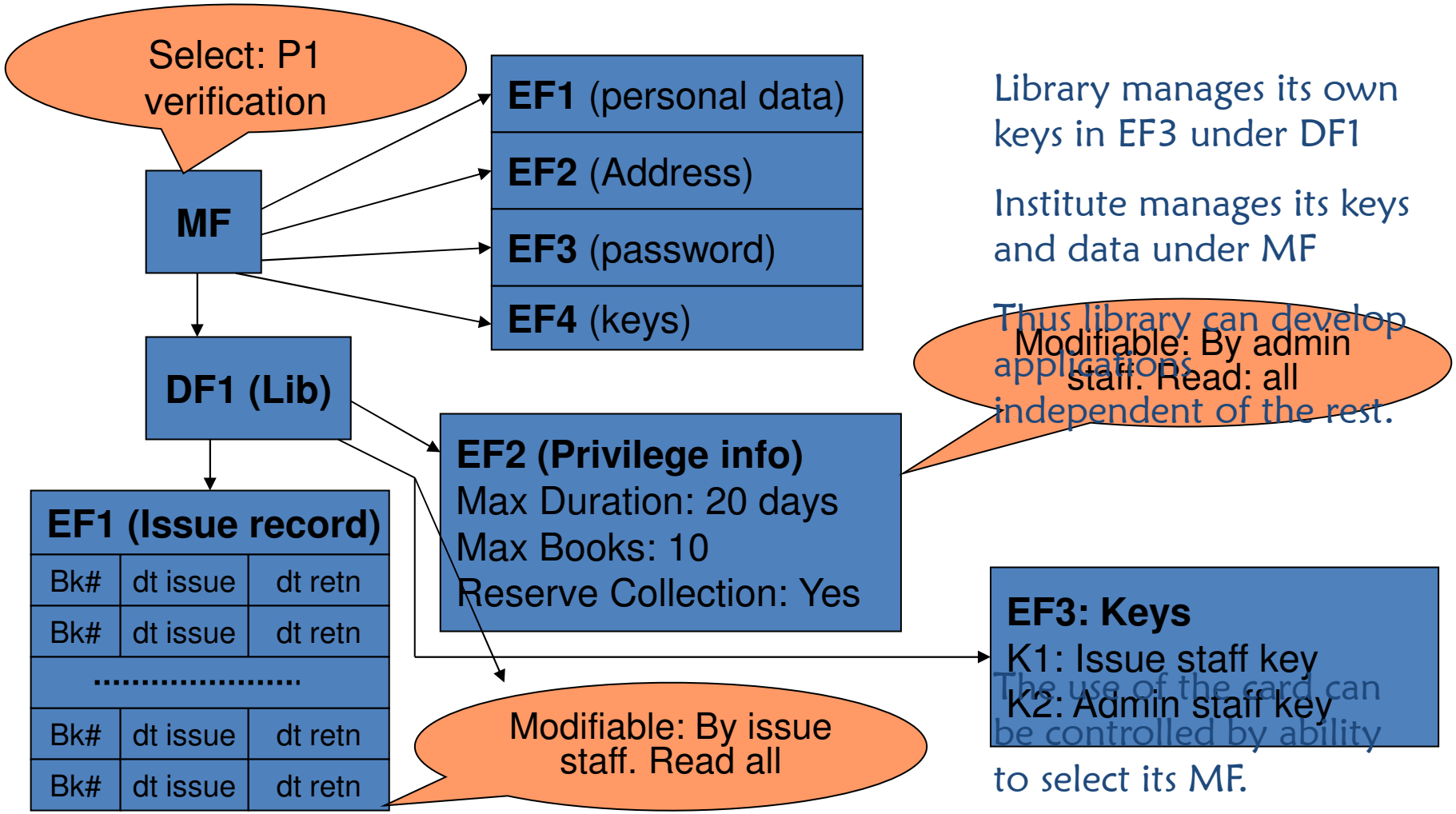
GDAŃSK UNIVERSITY OF TECHNOLOGY

An example scenario



GDAŃSK UNIVERSITY OF TECHNOLOGY

An example scenario



Library manages its own keys in EF3 under DF1

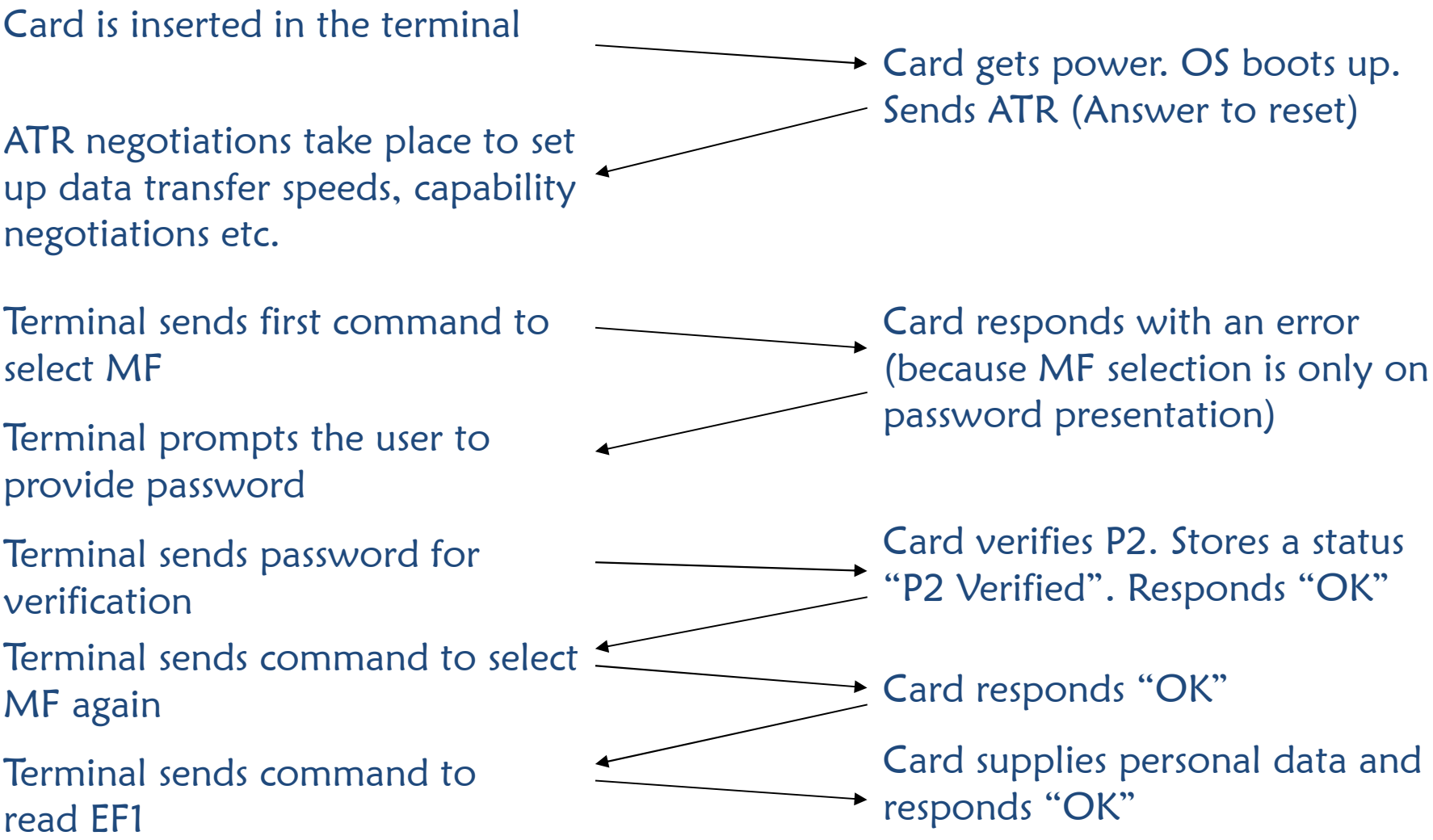
Institute manages its keys and data under MF

Thus library can develop applications independent of the rest.

The use of the card can be controlled by ability to select its MF.

GDAŃSK UNIVERSITY OF TECHNOLOGY

Example card access procedure



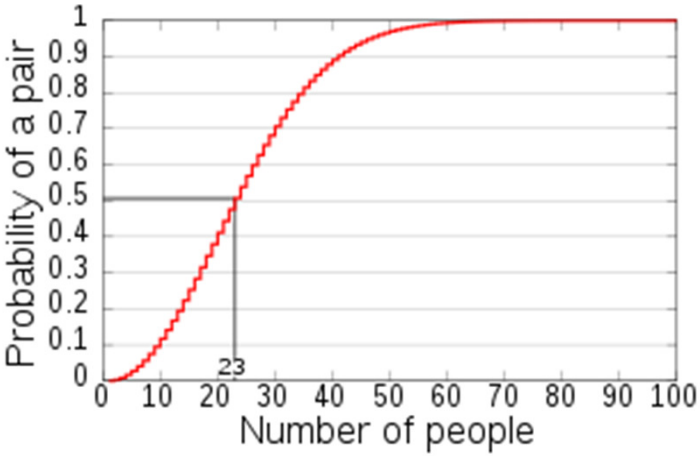
Uwierzytelnianie biometryczne

GDAŃSK UNIVERSITY OF TECHNOLOGY

Najpopularniejsze rodzaje

- Fizyczne:
  - odciski palców,
  - twarz,
  - tęczówka,
  - źrenica,
  - układ naczyń krwionośnych,
  - geometria dłoni.
- Behawioralne:
  - dynamika pisania na klawiaturze,
  - głos,
  - chód,
  - dynamika pisania odręcznego.

GDAŃSK UNIVERSITY OF TECHNOLOGY



Podstawowe rodzaje zastosowań

- Weryfikacja
  - 1-do-1: dla danej próby uwierzytelnienia, potwierdzić zgodność z określonym profilem w czasie zbliżonym do rzeczywistego,
  - Wymaga dodatkowej metody identyfikacji, np.: login, token, karta, …

- Identyfikacja
  - 1-do-wielu: dla danej próby uwierzytelnienia znaleźć profil zgodny, w czasie zbliżonym do rzeczywistego,
  - Problem z uzyskaniem próbek pozwalających na uzyskanie wystarczającej separacji (birthday paradox),
  - Zalecana do wykorzystania jedynie w przypadkach gdy weryfikacja nie jest wystarczająca.

GDAŃSK UNIVERSITY OF TECHNOLOGY

Kryteria oceny systemu biometrycznego

- Uniqueness – zdolność do rozróżniania użytkowników,
- Universality – dostępność mierzonej cechy u użytkowników,
- Permanence – zdolność do zachowania aktualności wzorców wraz z upływem czasu i prawdopodobnymi zmianami mierzonych parametrów,
- Collectability – łatwość dokonania pomiarów,
- Performance – szybkość i dokładność wykorzystywanych rozwiązań technicznych,
- Acceptability – łatwość zaakceptowania przez użytkowników,
- Circumvention – łatwość ominięcia/sfałszowania wyników.

GDAŃSK UNIVERSITY OF TECHNOLOGY

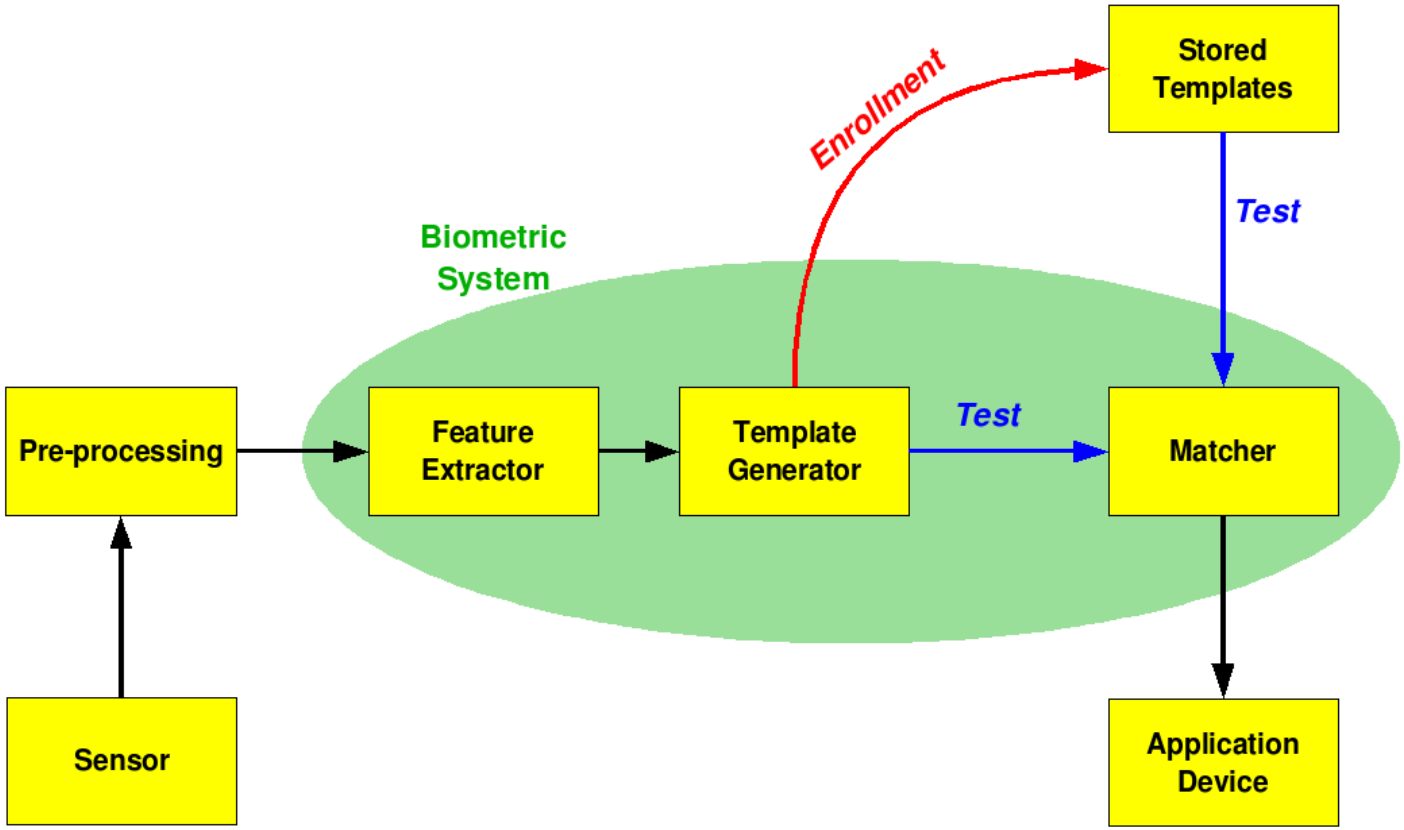
Proces uwierzytelniania biometrycznego

- Rejestracja:
  - Pobranie danych biometrycznych (Acquisition)
  - Stworzenie profilu (Creation of master characteristics)
  - Przechowywanie profilu (Storage of master characteristics)

- Weryfikacja:
  - Pobranie danych biometrycznych (Acquisition)
  - Porównanie z profilem (Comparison)
  - Decyzja (Decision)

GDAŃSK UNIVERSITY OF TECHNOLOGY

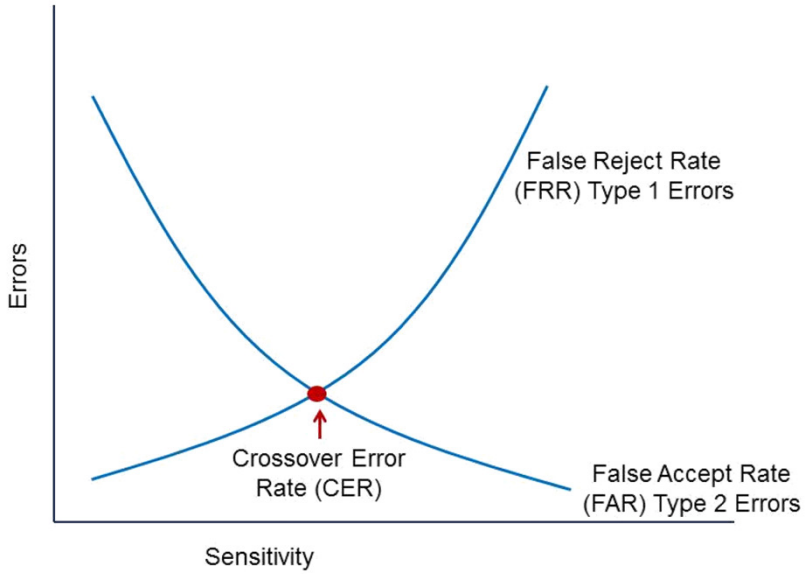
Ogólna architektura systemu biometrycznego



GDAŃSK UNIVERSITY OF TECHNOLOGY

Parametry technik biometrycznych

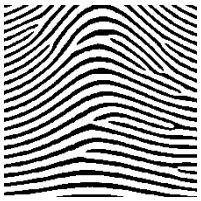
- Podstawowe metryki:
  - FTA – Failure To Acquire,
  - FTE – Failure To Enroll,
  - FAR – False Acceptance Rate,
  - FRR – False Reject Rate.
- Crossover Error Rate (CER) – wartość często używana w szacowaniu poprawności działania systemu.
- Inne wymogi implementacyjne:
  - Weryfikacja oryginalności odczytu (Liveness testing).
  - Odporność na próby oszustwa (Tamper resistance).
  - Bezpieczeństwo komunikacji (Secure communication).
  - Konfigurowalny poziom bezpieczeństwa.
  - Dostępność metody alternatywnej.



GDAŃSK UNIVERSITY OF TECHNOLOGY

Odciski palców

Kształty:



ARCH

WHORL

LOOP

Szczegóły:

END

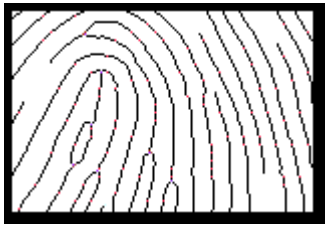
BIFURCATION

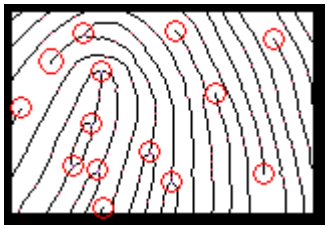
ISLAND

LAKE

DOT

- Minutiae based - Wyróżnikiem jest unikalny układ szczegółów.
- Correlation based – analizowany jest całościowy obraz złożony z pikseli.





- Metoda nieinwazyjna, niezawodna i tania.
- Czujniki optyczne, pojemnościowe, termiczne, ultradźwiękowe, …
- Wykorzystywana popularnie do weryfikacji, w specjalizowanych zastosowaniach także do identyfikacji.
- Problemy:
  - zabrudzenia, zranienia,
  - sposób przyłożenia palca,
  - łatwość ataku odtworzeniowego – w zależności od rodzaju czujnika.

GDAŃSK UNIVERSITY OF TECHNOLOGY

Geometria dłoni

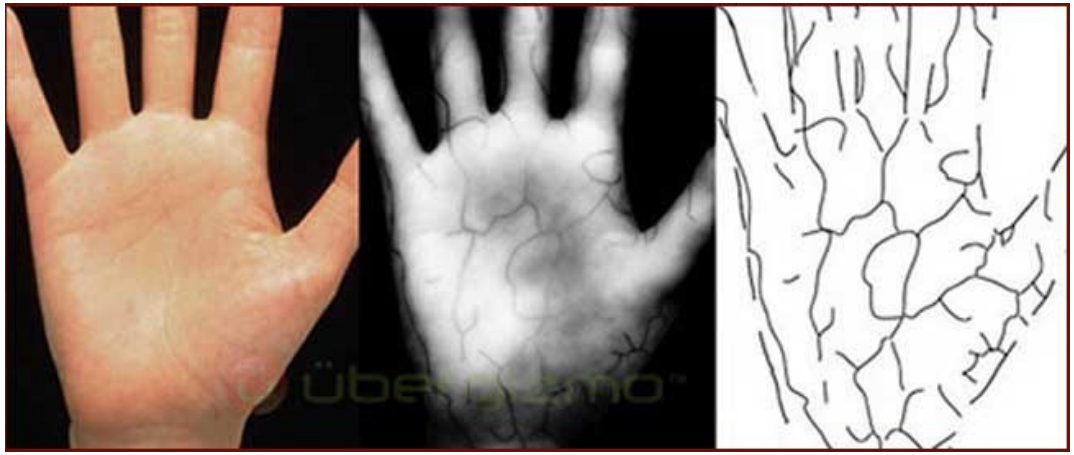
- Jedna z najwcześniej zaimplementowanych technik biometrycznych
  - kontrola dostępu do pomieszczeń,
  - rejestracja obecności, czasu pracy, itp.
- Czytnik wykorzystuje kamerę CCD i zestaw luster do wykonania pomiarów kształtu, najczęściej w < 1 s.
  - Długości, szerokości, grubości, powierzchni, itp.
- Wykorzystywana najczęściej do weryfikacji.
  - Identyfikacja realizowana inną metodą (np. kartą).
- Łatwa w użyciu i nieinwazyjna,
  - Duże gabaryty czytników.

GDAŃSK UNIVERSITY OF TECHNOLOGY

Układ naczyń krwionośnych

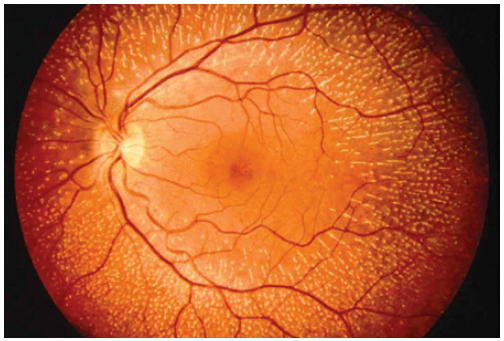
- Vein patterns are unique to an individual (even twins)
- Scanned with infrared rays, using reflective photography

- **High Safety** - palm vein is an internal biometric, therefore difficult to defeat compared to other external body biometrics such as fingerprint, face and iris.
- **High Accuracy** - it has a false acceptance rate under 0.00001% when the false rejection rate is 0.01% (with 1 retry) which makes it one of the most accurate biometric authentication system currently available in the market.
- **High Acceptance** – Contactless, easy and hygiene operation with virtually 0% fail to enroll rate.



GDAŃSK UNIVERSITY OF TECHNOLOGY

Skanowanie siatkówki (retinal scan)

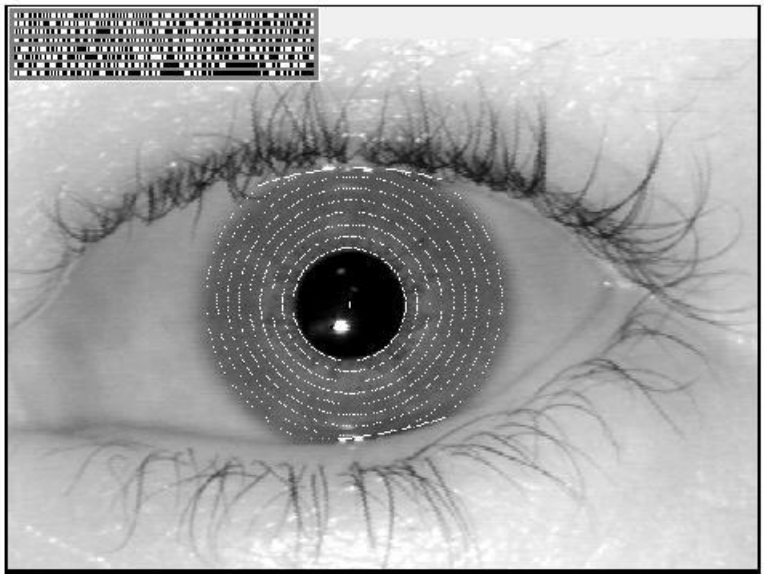


- Bazuje na analizie układu naczyń krwionośnych siatkówki.
- Pomiar około 400 parametrów, poddawanych następnie analizie w celu ustalenia 96-bajtowego wzorca.
- Wprowadzenie tej metody poprzedza skanowanie tęczówki, lecz problemy wdrożenia sprawiają, iż jest mniej popularne.
- Problemy:
  - konieczność precyzyjnego „spojrzenia” w czytnik skanera,
  - konieczność zdjęcia okularów,
  - stosunkowo wysoki poziom FTE,
  - odczyt uważany za „inwazyjny”.

GDAŃSK UNIVERSITY OF TECHNOLOGY

Skanowanie tęczówki (iris scan)

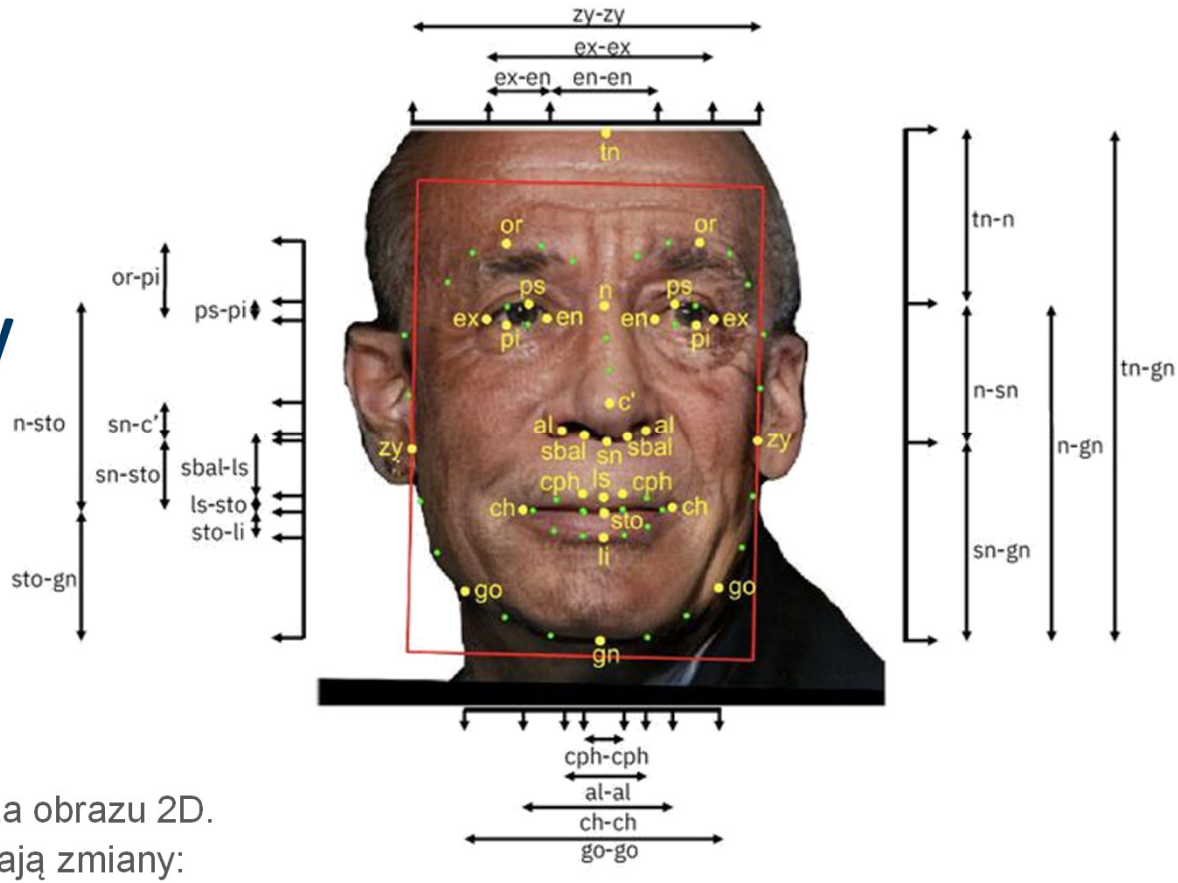
- Zawartość informacyjna: 3.4 bits/mm^2
- Wysoka dokładność: prawdopodobieństwo wystąpienia identycznego profilu różnych użytkowników (włączając bliźniaki) $< 10^{-72}$
- Szybkie przeszukiwanie: ~2 s. dla bazy 100 000 wzorców.
- Metoda stosunkowo rzadko uznawana z inwazyjną lub niebezpieczną.
- Nie posiada większości problemów wdrożeniowych mechanizmów skanowania siatkówki.
  - Dobra widoczność tęczówki.



GDAŃSK UNIVERSITY OF TECHNOLOGY

Rozpoznawanie twarzy

- Appearance based – analiza całości obrazu twarzy lub obrazów jej części poprzez porównywanie do obrazów wzorcowych.
- Feature based – odszukanie charakterystycznych punktów twarzy i opis zależności geometrycznych pomiędzy nimi.
- Knowledge based – dodatkowo wykorzystujące informacje, na temat budowy anatomicznej ludzkiej twarzy.



- W zdecydowanej większości analiza obrazu 2D.
- Na efektywność negatywnie wpływają zmiany:
  - Sposobu obserwacji: oświetlenie, kąt obserwacji,
  - Wyglądu, krótkoterminowe: nastrój, zarost, fryzury, okulary, itp.
  - Wyglądu, długoterminowe: wiek.
- W kontrolowanym środowisku stosunkowo łatwe,
  - Widok frontalny, określona odległość, dobre oświetlenie,
  - Najczęściej występuje w przypadku kontroli dostępu, w postaci mechanizmu weryfikacji (identyfikacja dodatkowymi mechanizmami),
  - Wystarczające są proste podejścia appearance based.
- Trudne w zmiennym środowisku,
  - Występuje większość elementów utrudniających.
- Mechanizmy feature-based są odporniejsze od appearance-based.

GDAŃSK UNIVERSITY OF TECHNOLOGY

Analiza głosu

- Analiza głosu i rozpoznawanie mowy to zupełnie inne zadania.

- Charakterystyka głosu zależy od cech fizycznych układu mowy i oddechowego.
- Rozwiązania:
  - Zależne od treści – analiza możliwa dla fraz określonych w procesie uczenia:
    - Statyczne – analizie podlegają ściśle określone frazy,
    - Dynamiczne – próbki zebrane w procesie uczenia służą do generowania losowych fraz.
  - Niezależne od treści – analiza możliwa dla dowolnej treści wypowiedzi.

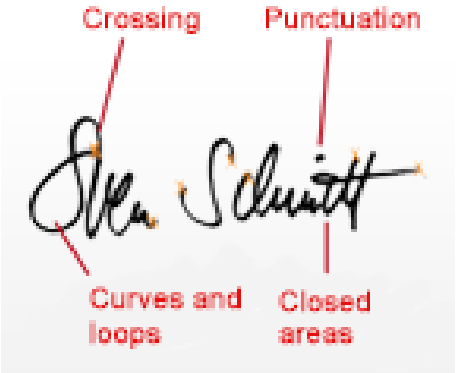
- Duża liczba możliwych technik:
  - frequency estimation, hidden Markov models, Gaussian mixture models, pattern matching algorithms, neural networks, matrix representation, vector quantization, decision trees.

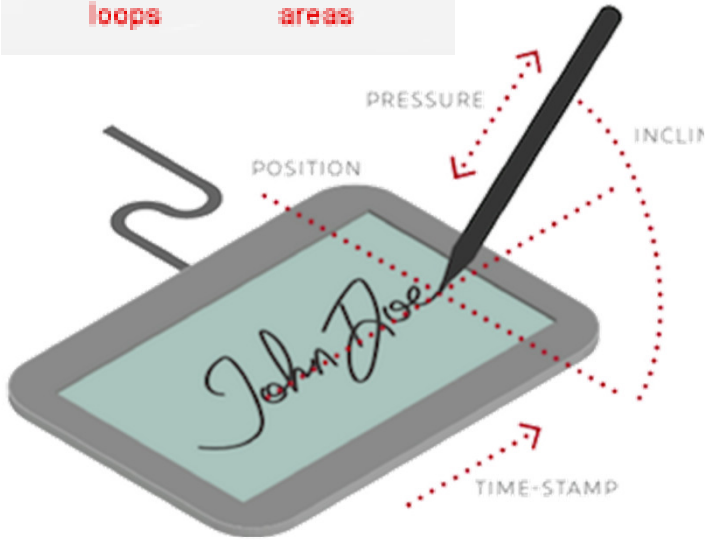
- Wygodna w użyciu lecz mniej niezawodna od innych technik biometrycznych.
  - Możliwość łatwego zastosowania w systemach komunikacji zdalnej.
- Słabości: podatność na atak odtworzeniowy, zakłócenia z otoczenia, zmiany głosu związane z szeroką gamą przyczyn (od zmian nastroju do chorób).

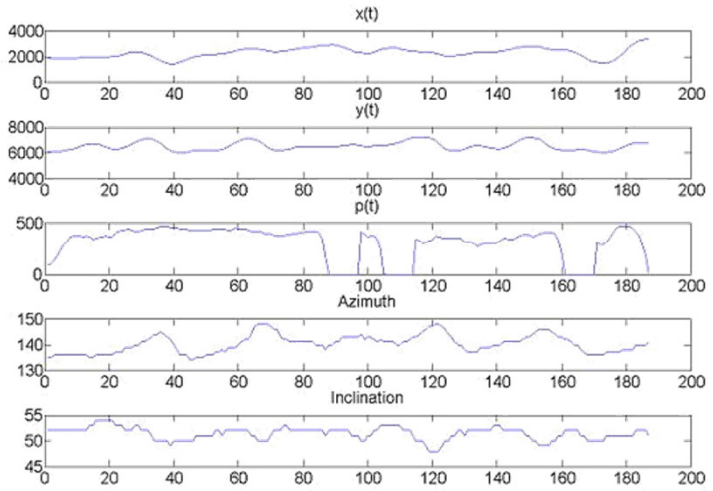
GDAŃSK UNIVERSITY OF TECHNOLOGY

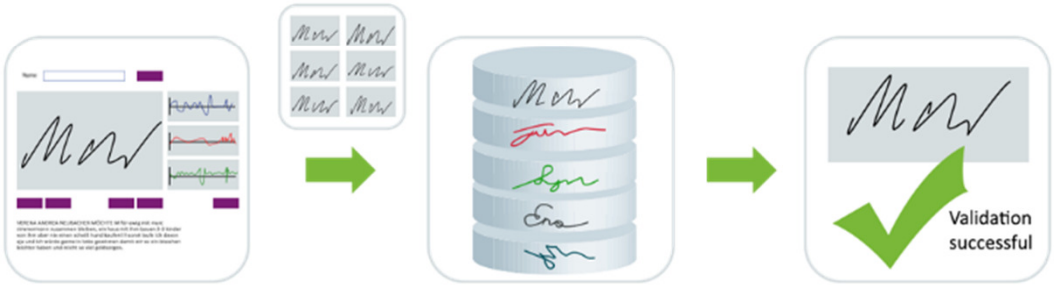
Sprawdzenie podpisu odręcznego

- Charakterystyki statyczne
  - Dotyczące kształtu podpisu.
  - Nieco podobne do szczegółów odcisku palca:
    - Przecięcia, łuki, punkty, obszary.
- Charakterystyki dynamiczne
  - Gromadzone w funkcji czasu.
  - Pozycja punktu, przyspieszenie, nacisk (oraz obecność/brak kontaktu z powierzchnią), pochylenie pióra.
- Wzorzec najczęściej generowany na podstawie wielu próbek podpisu.







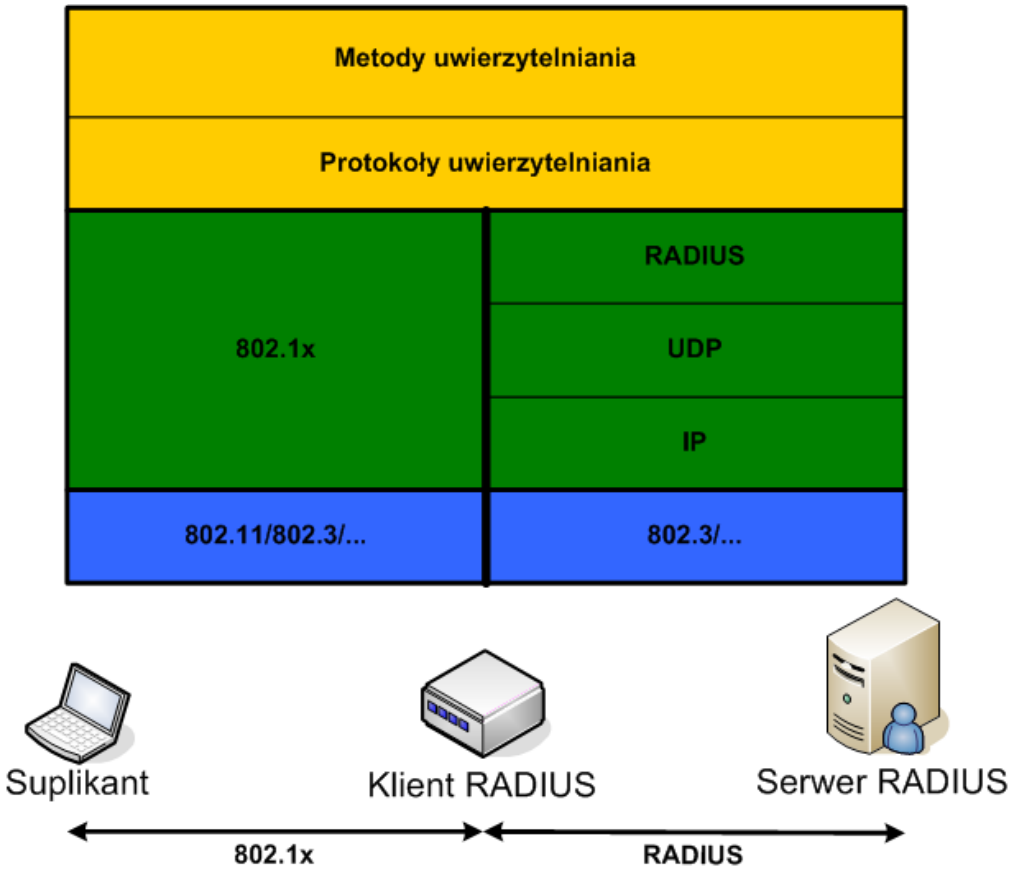


Extensible Authentication Protocol (EAP)

GDAŃSK UNIVERSITY OF TECHNOLOGY

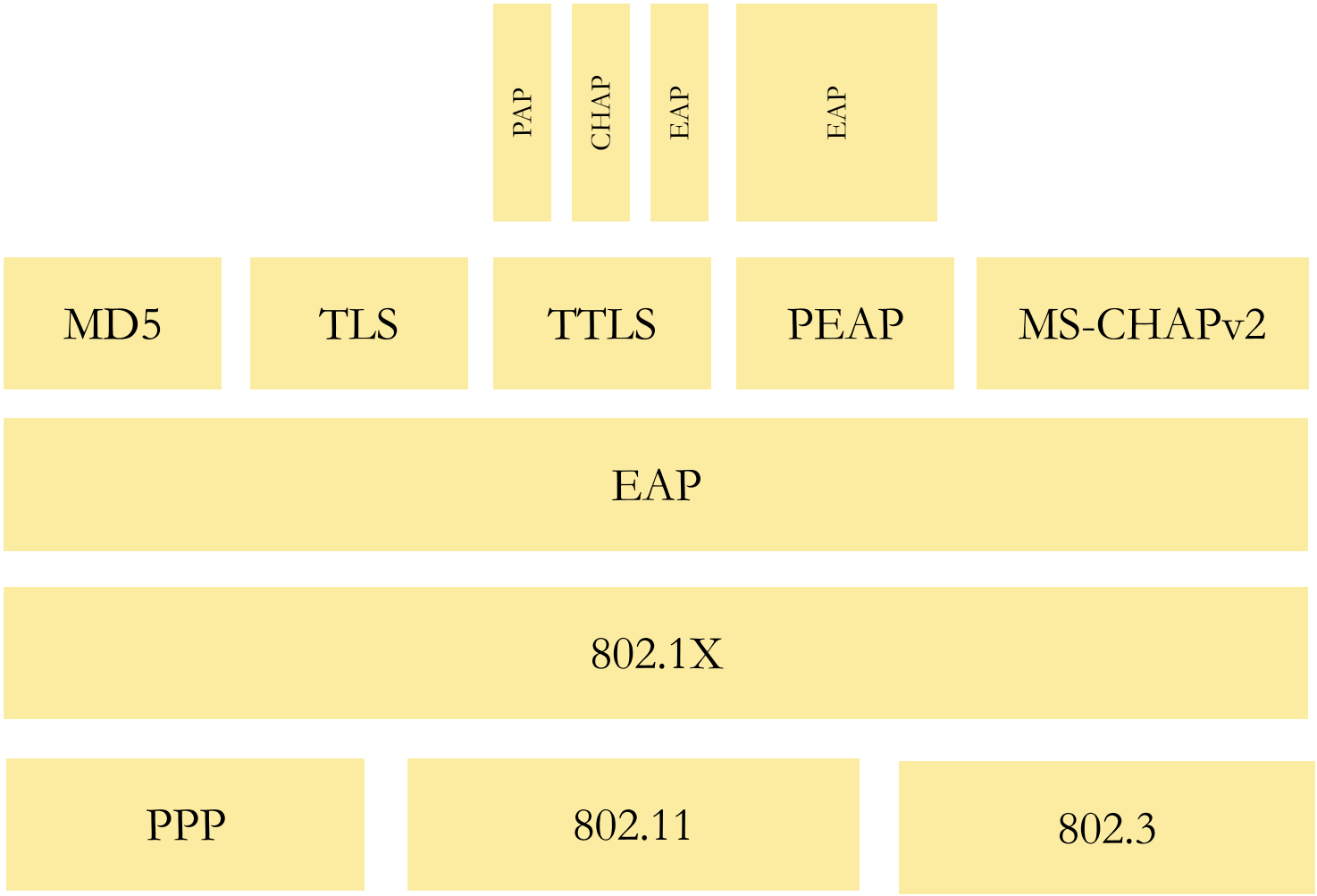
Extensible Authentication Protocol (EAP)

- Jest to protokół transportowy, a nie metoda uwierzytelniania.
- Istnieje wiele odmian stosujących różne mechanizmy komunikacji (EAP-TTLS, PEAP, ...).
- Wspiera różne metody uwierzytelniania, np.: PAP, CHAP, MSCHAP2, GTC...



GDAŃSK UNIVERSITY OF TECHNOLOGY

Odmiany i metody EAP



GDAŃSK UNIVERSITY OF TECHNOLOGY

Odmiany EAP

- **EAP** – podstawowa wersja protokołu. Metody uwierzytelniania takie jak MD5 MS_CHAPv2 itp. wymieniają wiadomości bezpośrednio, korzystając z platformy komunikacyjnej udostępnionej przez protokół EAP.
- **Lightweight EAP (LEAP)** – opracowana przez Cisco wersja EAP z wzajemnym uwierzytelnianiem przez funkcje skrótów z długimi kluczami;
- **EAP-TLS/EAP-TTLS** – na platformie komunikacyjnej udostępnianej przez protokół EAP, zestawiany jest szyfrowany tunel TLS pomiędzy suplikantem i NAS. Metody uwierzytelniania wymieniają dane korzystając z tego tunelu.
- **PEAP (Protected EAP)** – podobnie jak w TTLS, ale w zestawionym tunelu TLS uruchamiana jest kolejna warstwa protokołu EAP i to z jej pomocą komunikują się metody uwierzytelniania.

GDAŃSK UNIVERSITY OF TECHNOLOGY

Metody EAP

- **MD5** – nazwa użytkownika i hasło szyfrowane funkcją skrótu MD5; nadaje się głównie do środowisk przewodowych - w warunkach sieci WLAN jest zbyt podatny na podsłuch i łamanie haseł offline oraz ataki typu man-in-the-middle.
- **TLS** – metoda oparta na certyfikatach klientów i tunelowaniu TLS/SSL; daje wystarczający poziom bezpieczeństwa w sieciach WLAN i jest powszechnie wspierana przez producentów urządzeń
- **MS-CHAPv2** – technologia opracowana przez Microsoft zbliżona w ogólnych zarysach do MD5, lecz stosująca inną funkcję skrótu - MD4.
- **PAP** – uwierzytelnianie z użyciem stałych haseł przesyłanych otwartym tekstem,
- **OTP (One-time Password)** – uwierzytelnianie z użyciem haseł jednorazowych,

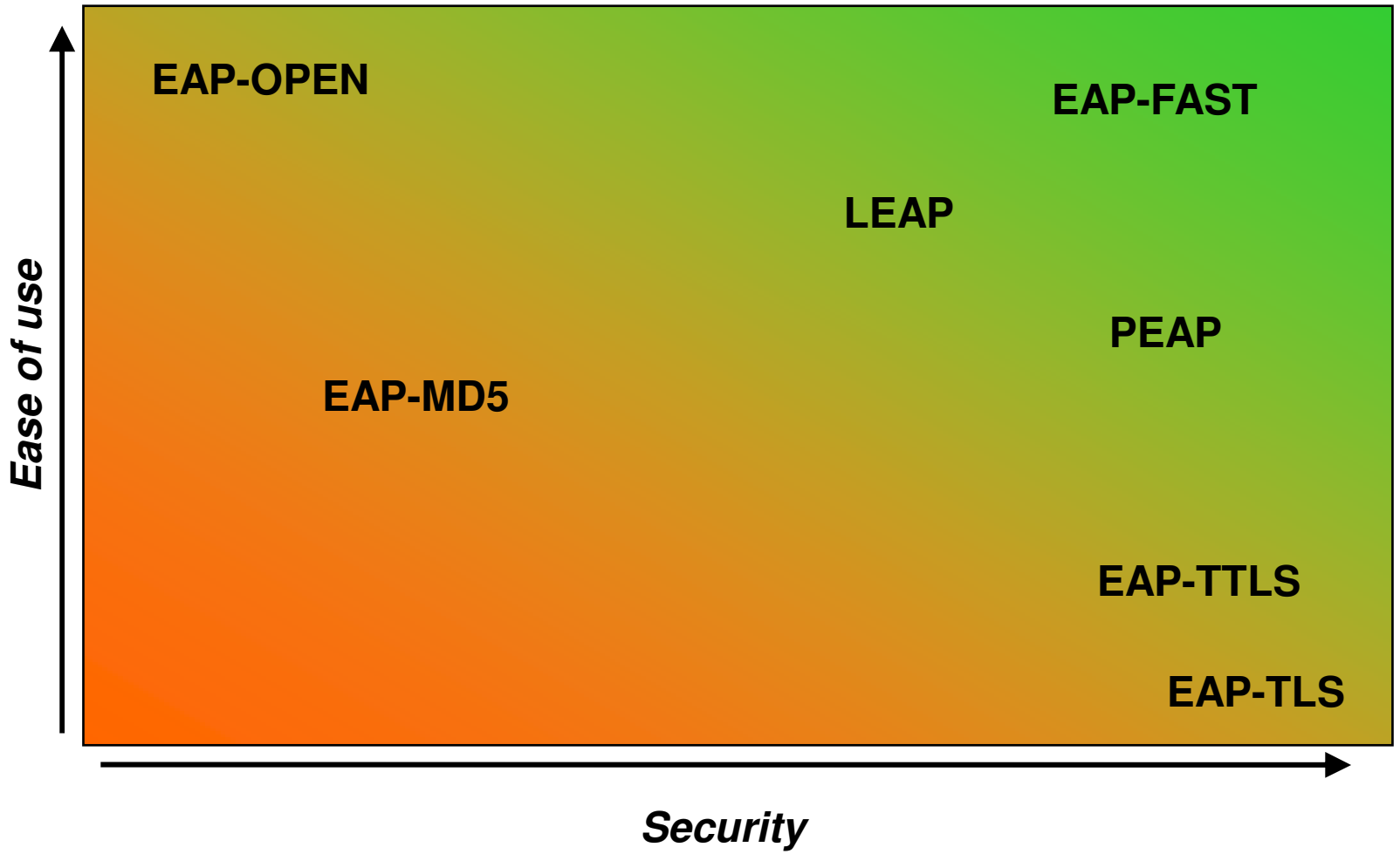
GDAŃSK UNIVERSITY OF TECHNOLOGY

Metody EAP

- **GTC (Generic Token Card)** – uwierzytelnianie z użyciem kart chipowych,
- **SIM (Subscriber Identity Module)/AKA (UMTS Authentication and Key Agreement)** – uwierzytelnianie z użyciem kart SIM i architektury uwierzytelniania właściwej dla sieci telefonii komórkowej.
- **SecurID** – nie wymaga udostępniania danych uwierzytelniających suplikantowi.
- **SRP (Secure Remote Password)** – nie wymaga przechowywania hasła na serwerze uwierzytelniającym.

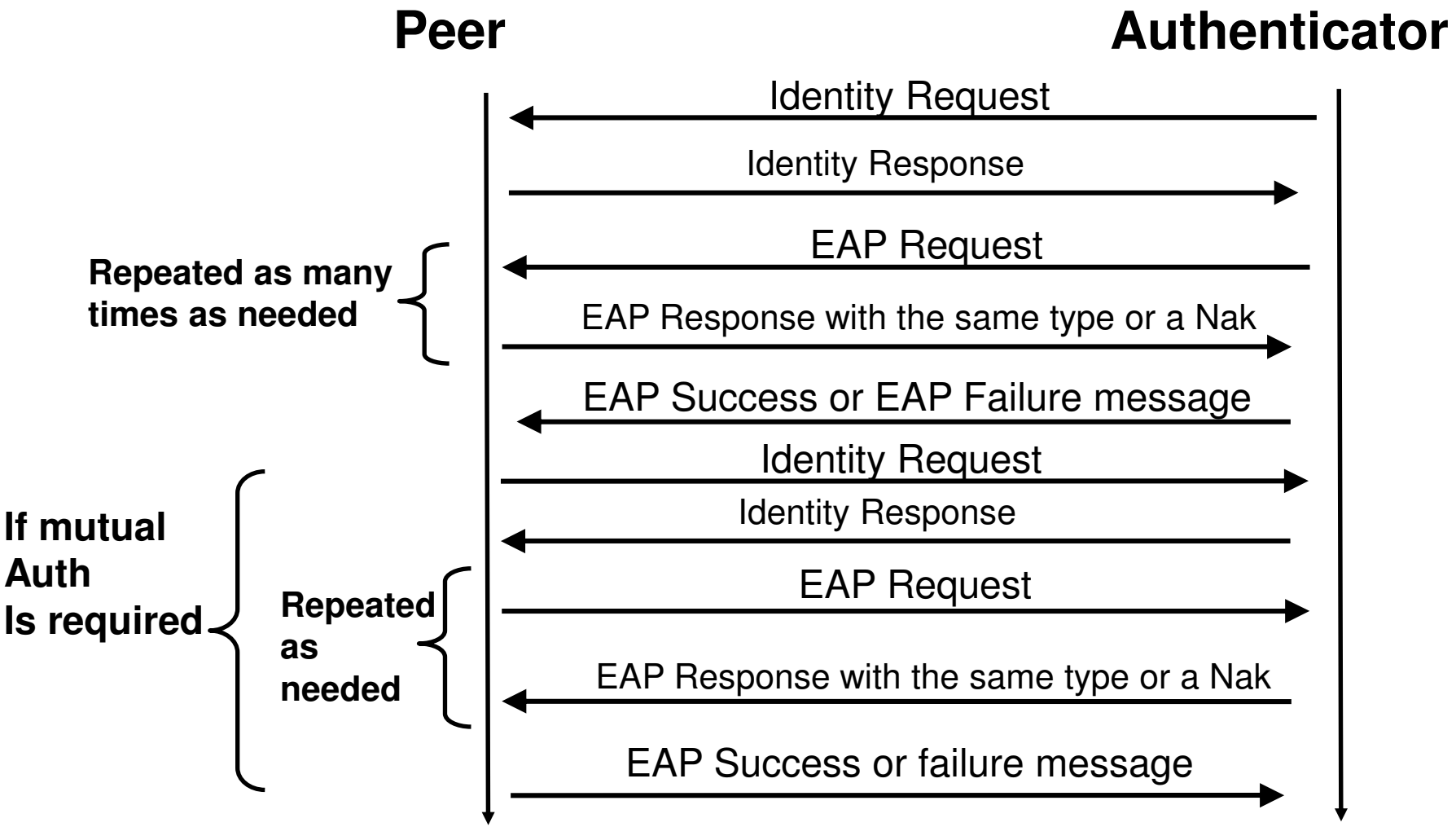
GDAŃSK UNIVERSITY OF TECHNOLOGY

EAP mechanisms



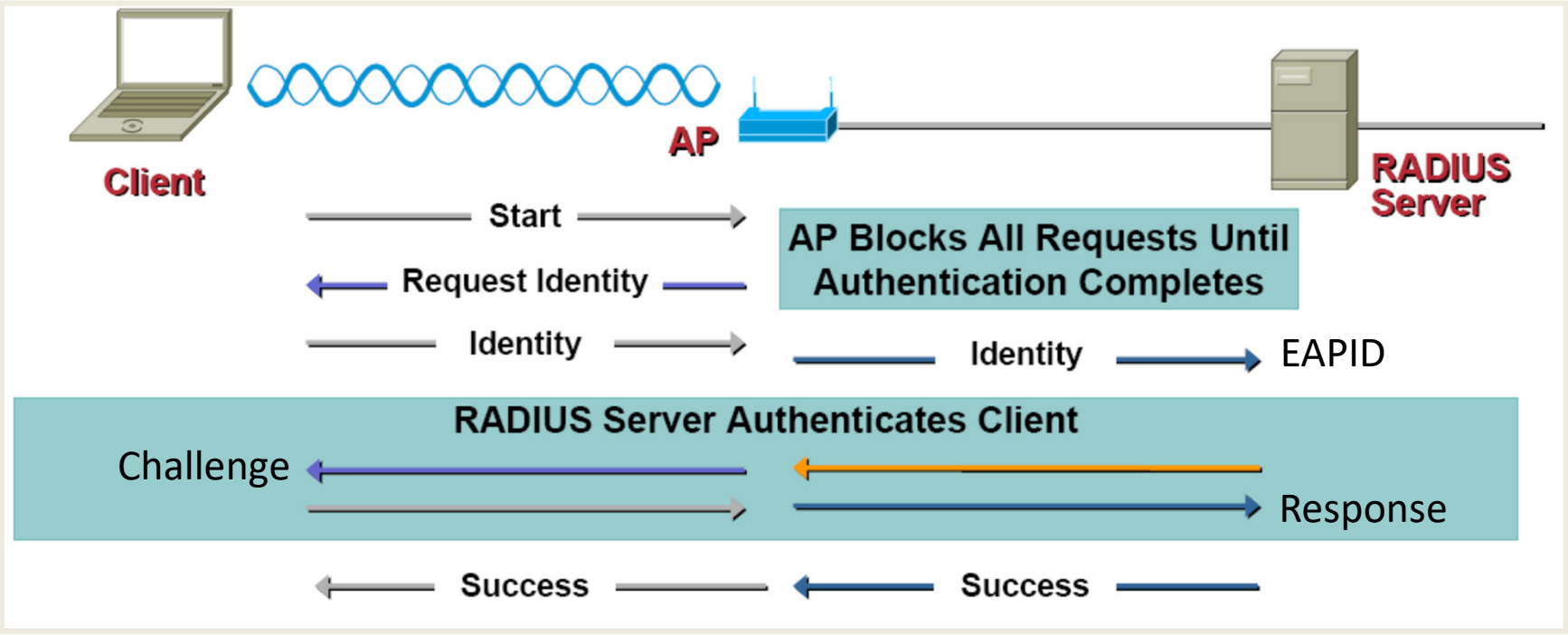
GDAŃSK UNIVERSITY OF TECHNOLOGY

Generic EAP Authentication Flow



GDAŃSK UNIVERSITY OF TECHNOLOGY

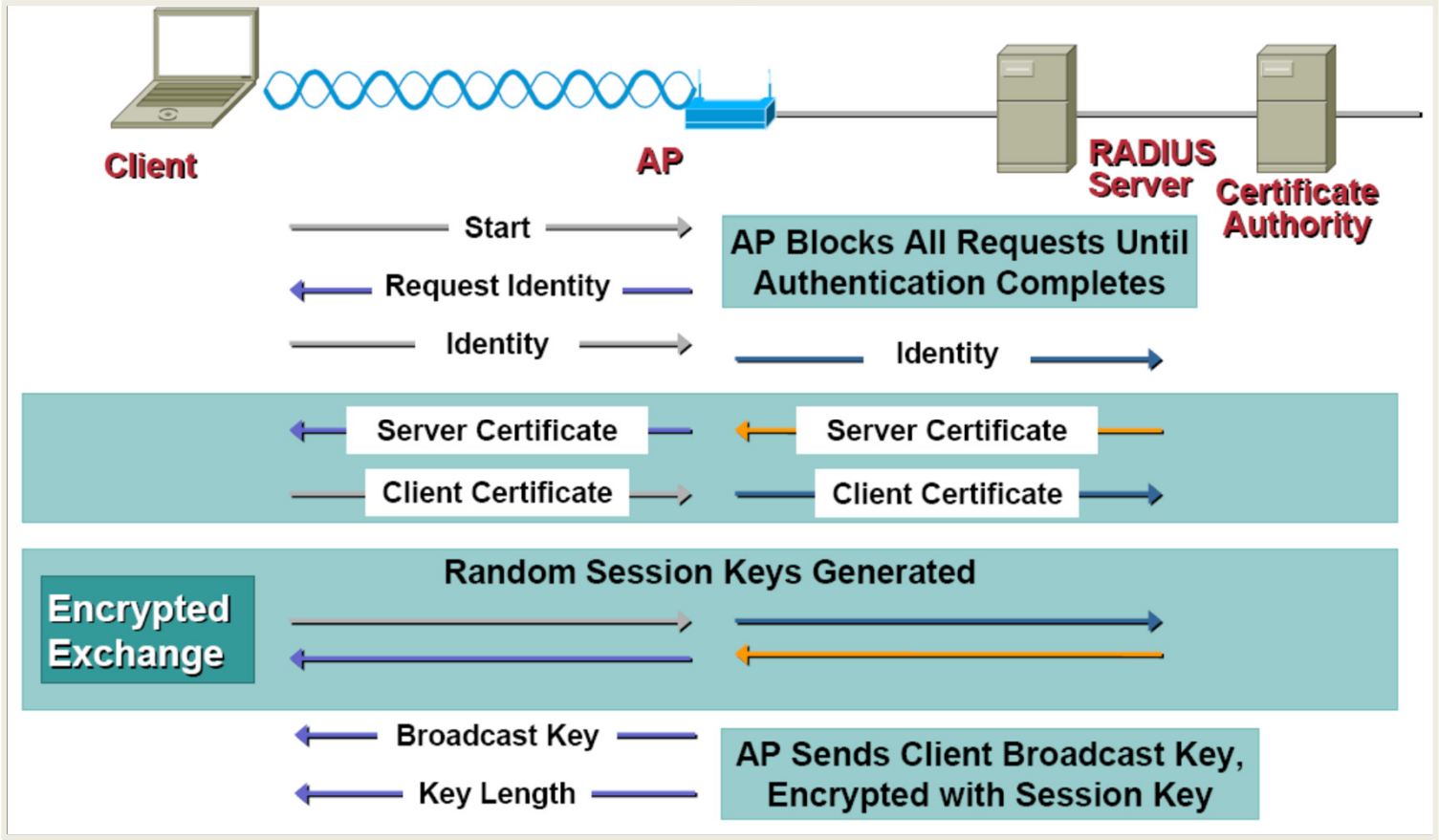
EAP-MD5



Response = MD5(EAPID || Password || Challenge)

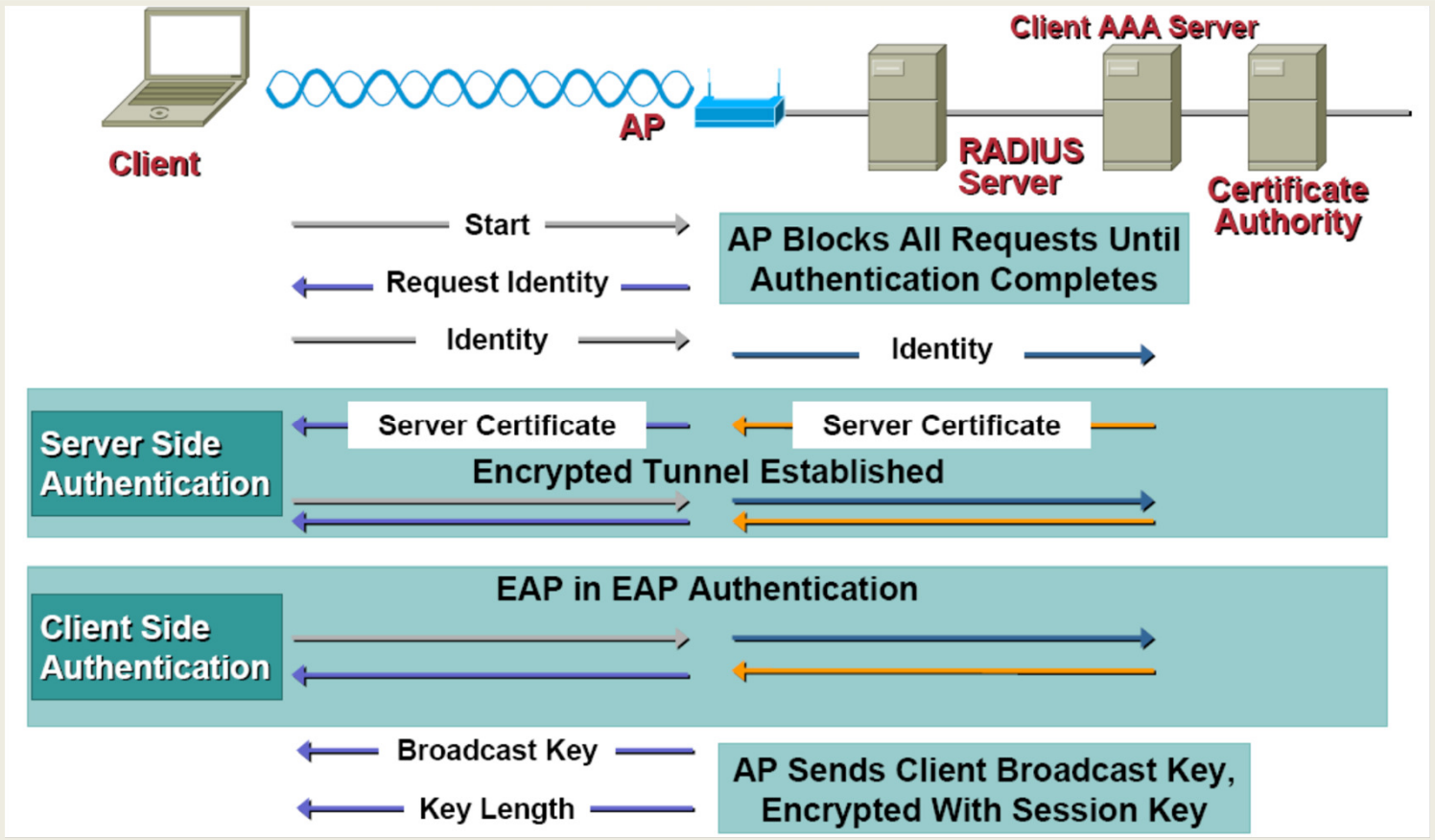
GDAŃSK UNIVERSITY OF TECHNOLOGY

EAP-TLS



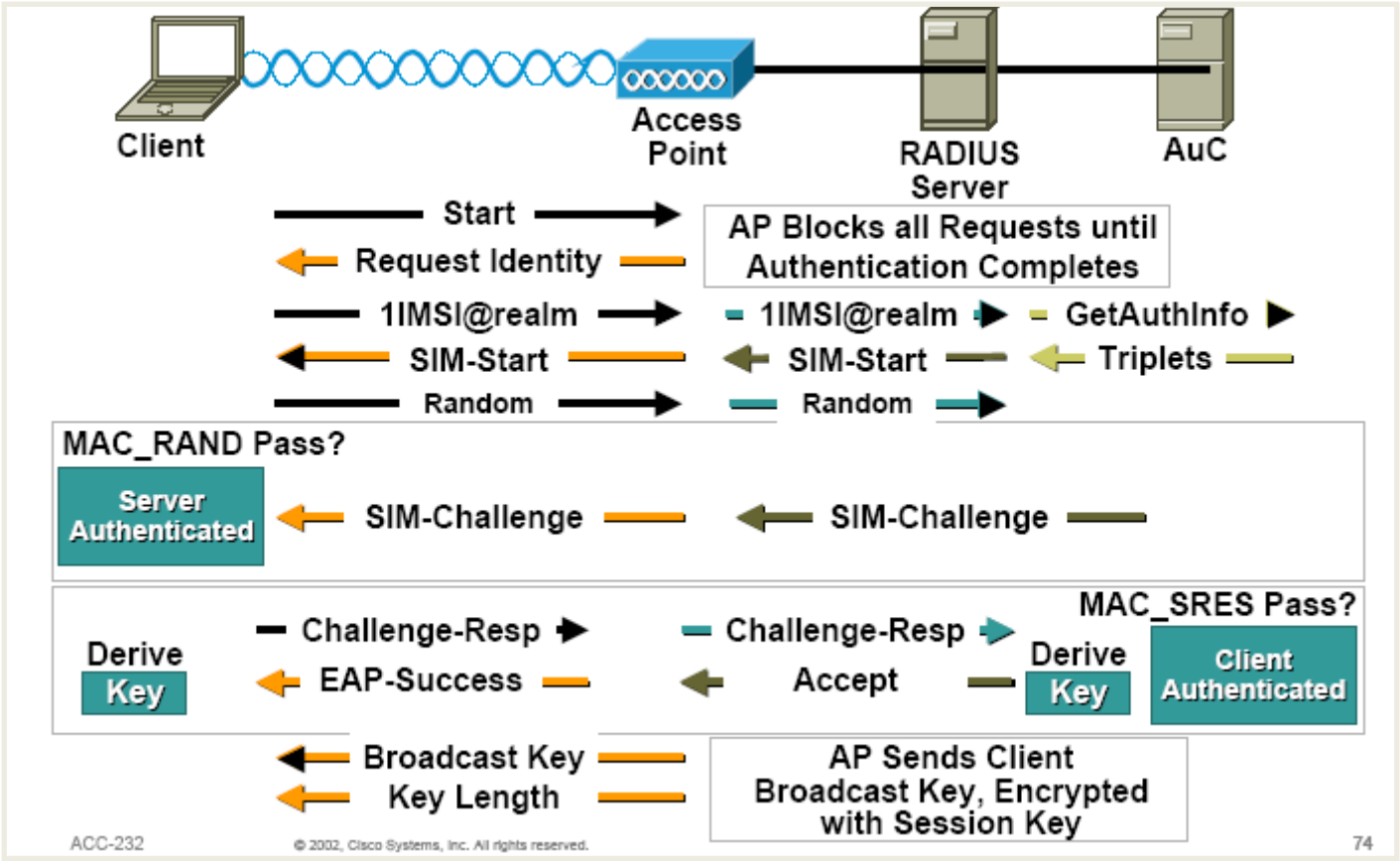
GDAŃSK UNIVERSITY OF TECHNOLOGY

Protected EAP



GDAŃSK UNIVERSITY OF TECHNOLOGY

EAP-SIM



Protokół Diameter

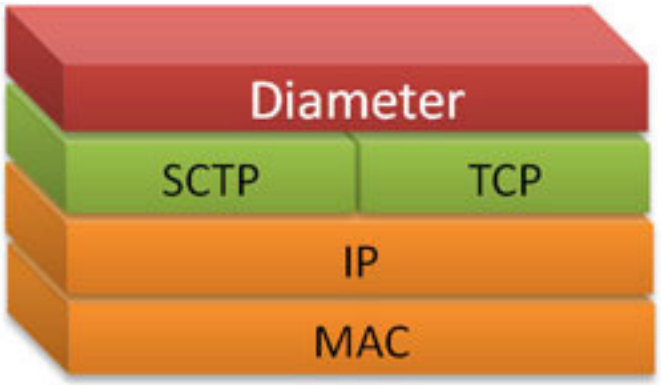
GDAŃSK UNIVERSITY OF TECHNOLOGY

Protokół Diameter

- Protokół służący obsłudze AAA (Authentication, Authorization, Accounting), mający zastąpić popularny obecnie protokół RADIUS (Remote Authentication Dial In User Service).
- Diameter został opracowany w związku z szeregiem nowych potrzeb w stosunku do protokołu AAA, związanych np. z:
  - Koniecznością obsługi użytkowników mobilnych
  - Rozwojem sieci 4G i rozwiązań IMS
  - Trendem w kierunku integracji systemów sieciowych – w szczególności systemów dostępowych.
- Protokół RADIUS, wziąwszy pod uwagę wiele wprowadzonych rozszerzeń, jest w stanie zrealizować większość obecnych wymagań, lecz mało efektywnie.
  - Słabym elementem protokołu RADIUS jest w szczególności obsługa błędów i niezawodność.

GDAŃSK UNIVERSITY OF TECHNOLOGY

Protokół Diameter



- Wymagania względem protokołów AAA będące przyczyną powstania protokołu Diameter:
  - **Failover** – zdolność do wykrycia niedostępności elementu architektury AAA i użycia elementu zastępczego,
  - **Transmission-level security** – zabezpieczenie komunikacji realizowanej z użyciem protokołu AAA,
  - **Reliable transport** – zastosowanie do celów komunikacji AAA protokołu wykorzystującego mechanizmy niezawodnego dostarczania danych (np. retransmisje, ochrona przed powtórzeniami),
  - **Agent suport** – konieczność zastosowania architektury elementów bardziej złożonej niż podstawowa klient-serwer,
  - **Server-initiated messages** – potrzeba wprowadzenia możliwości inicjowania przez serwer działań związanych z procesem AAA,
  - **Capability negotiation** – potrzeba rozszerzalności przy jednoczesnym zachowaniu kompatybilności elementów architektury,
  - **Peer discovery and configuration** – potrzeba zmniejszenia nakładów pracy związanych z ręczną konfigurację elementów architektury AAA.

GDAŃSK UNIVERSITY OF TECHNOLOGY

Diameter – podstawowa architektura

- Protokół Diameter składa się z:
  - **Protokołu bazowego (Base Protocol)** – definiuje podstawową funkcjonalność protokołu, umożliwia rozliczanie (Accounting),
  - **Aplikacji** – definiują funkcjonalność niezbędną do realizacji innych funkcji (np. uwierzytelniania) przy użyciu protokołu Diameter.
- W chwili obecnej najpopularniejsze zdefiniowane aplikacje to np.:
  - Network Access Server Application
  - Extensible Authentication Protocol Application
  - Credit-Control Application
  - Aplikacje 3GPP IMS

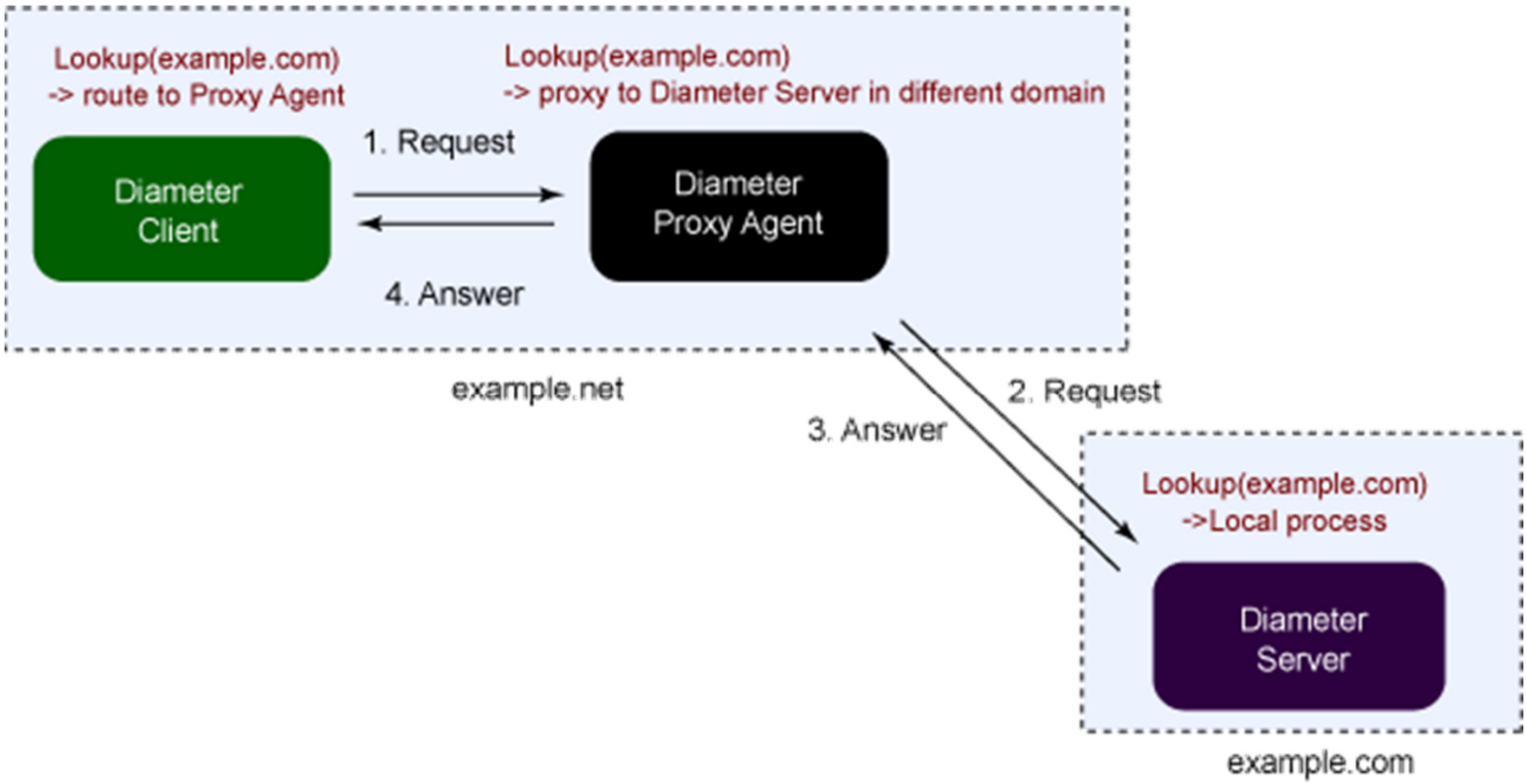
GDAŃSK UNIVERSITY OF TECHNOLOGY

Diameter – podstawowa architektura

- Protokół Diameter nosi cechy protokołu peer-to-peer – każdy z elementów może zainicjować komunikację.
  - W odróżnieniu od protokołu RADIUS, gdzie możliwość tę posiadał wyłącznie klient.
- Rodzaje węzłów (nodes) protokołu Diameter:
  - **Relay agent** – umożliwia przekazywanie wiadomości protokołu wg zadanych kryteriów.
  - **Proxy agent** – podobnie jak Relay agent, lecz posiada możliwość modyfikowania przekazywanych wiadomości.
  - **Redirect agent** – zwraca informację do jakiego węzła należy przekazać określoną wiadomość protokołu.
  - **Translation agent** – umożliwia translację i wymianę wiadomości pomiędzy protokołem Diameter i innym protokołem AAA.

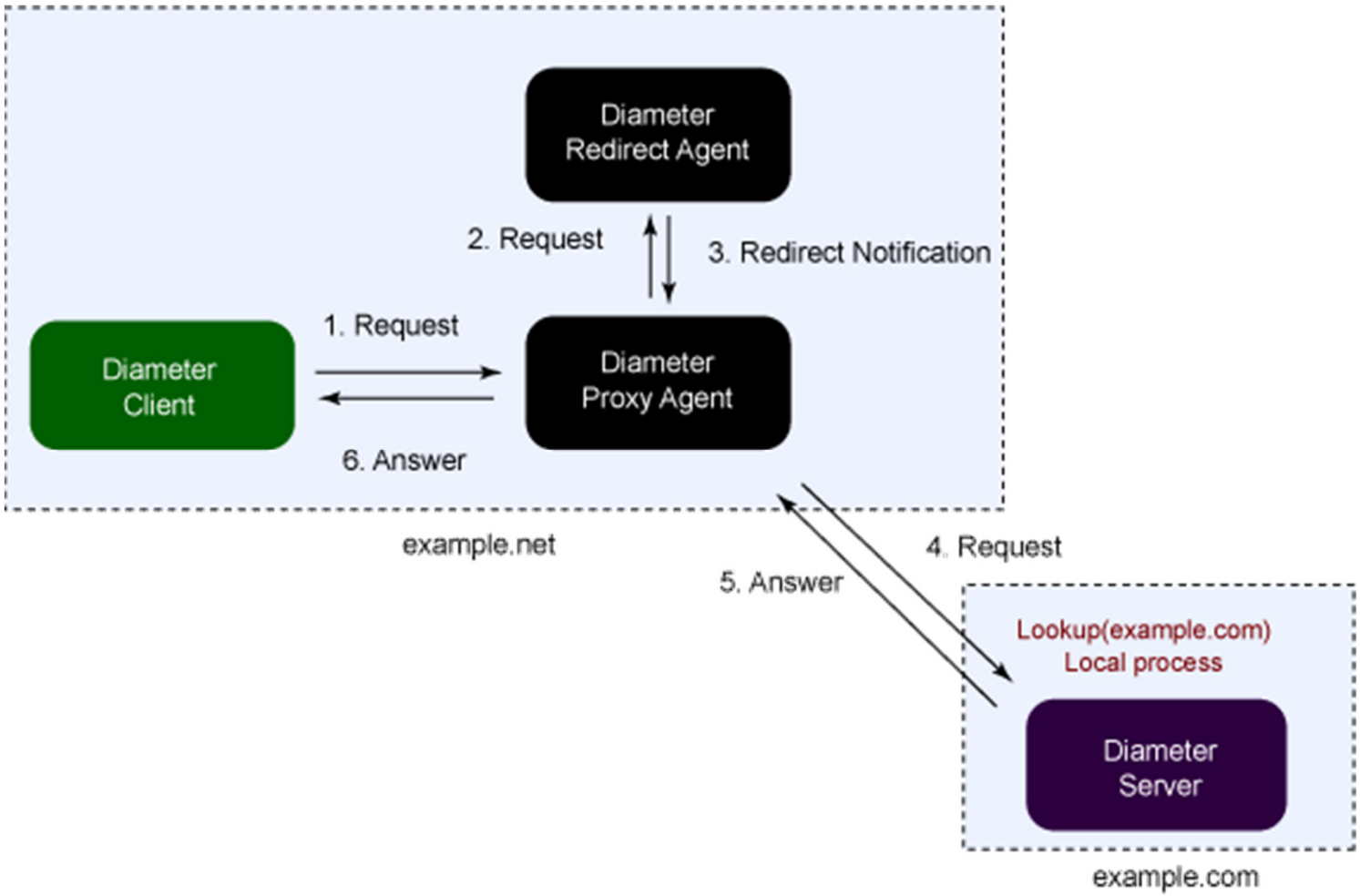
GDAŃSK UNIVERSITY OF TECHNOLOGY

Diameter Relay / Proxy Agent



GDAŃSK UNIVERSITY OF TECHNOLOGY

Diameter Redirect Agent



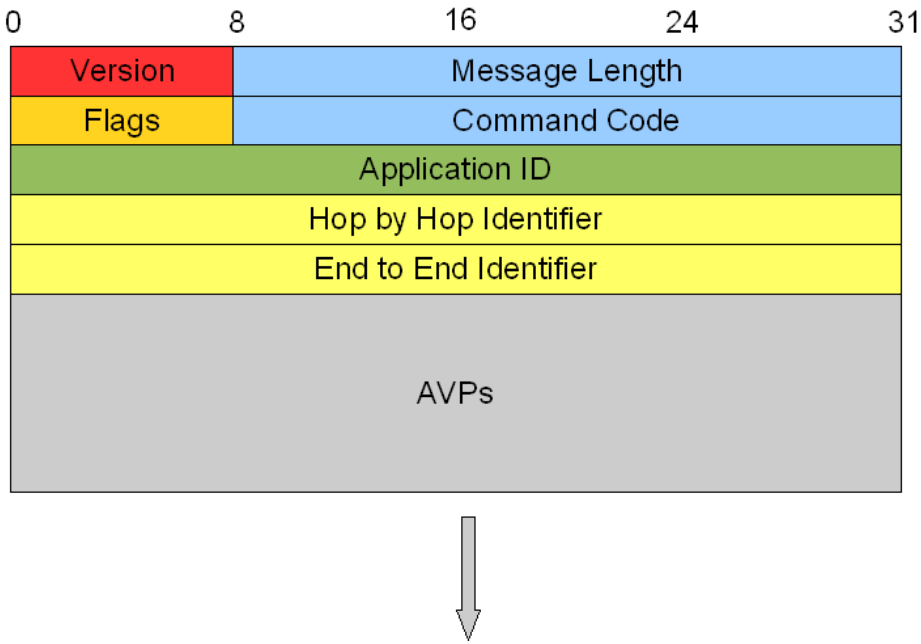
GDAŃSK UNIVERSITY OF TECHNOLOGY

Diameter Translation Agent

GDAŃSK UNIVERSITY OF TECHNOLOGY

Format wiadomości protokołu Diameter

- **Version:** wersja protokołu Diameter.
- **Message Length:** długość wiadomości (z nagłówkiem).
- **Command Flags:** określają pożądany sposób przetwarzania wiadomość przez protokół Diameter.
  - R = The message is a request (1) or an answer (0).
  - P = The message is proxiable (1) and may be proxied, relayed or redirected, or it must be processed locally (0).
  - E = The message is an error message (1) or a regular message (0).
  - T = The message is potentially being re-transmitted (1) or being sent for the first time (0).
- **Command-Code:** określa konkretne przeznaczenie wiadomości.
- **Application-ID:** określa aplikację Diameter, dla której przeznaczona jest wiadomość.
- **Hop by Hop ID**: Unikalny identyfikator pozwalający powiązać żądanie z odpowiedzią. Używany podczas routingu wiadomości.
- **End to End ID:** unikalny w okresie kilku minut identyfikator wiadomości. Używany w celu uniknięcia powtórzeń.



GDAŃSK UNIVERSITY OF TECHNOLOGY

Diamater Command Codes

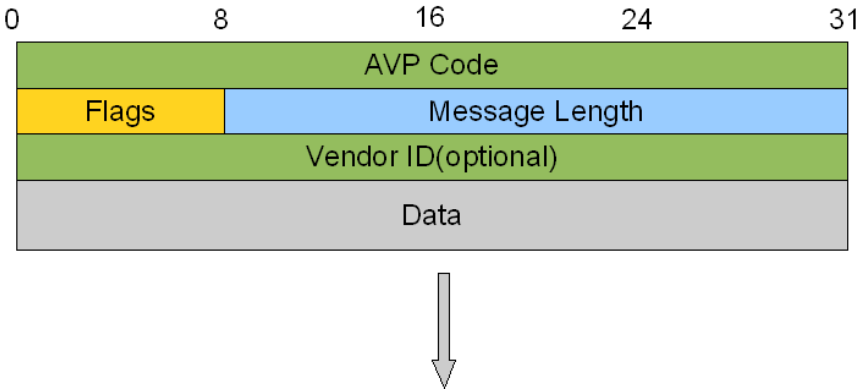
Nazwa	Skrót	Wartość pola
Abort-Session-Request	ASR	274
Abort-Session-Answer	ASA	274
Accounting-Request	ACR	271
Accounting-Answer	ACA	271
Capabilities-Exchanging-Request	CER	257
Capabilities-Exchanging-Answer	CEA	257
Device-Watchdog-Request	DWR	280
Device-Watchdog-Answer	DWA	280
Disconnect-Peer-Request	DPR	282
Disconnect-Peer-Answer	DPA	282
Re-Auth-Request	RAR	258
Re-Auth-Answer	RAA	258
Session-Termination-Request	STR	275
Session-Termination-Answer	STA	275

- Określają ogólne przeznaczenie wiadomości, lecz konkretne znaczenie nadają jej dane zawarte w elementach Attribute-Value Pairs (AVP).
- Pierwszych 255 wartości zarezerwowanych jest dla zgodności z protokołem RADIUS.

GDAŃSK UNIVERSITY OF TECHNOLOGY

Attribute-Value pairs

- Informacje przekazywane są z wykorzystaniem elementów Attribute-Value Pair (AVP)
  - AVP code i AVP Vendor-ID jednoznacznie identyfikują typ wiadomości.
  - Flags – określają żądany sposób przetwarzania AVP:
    - V = oznacza obecność pola Vendor ID,
    - M = powoduje, że odbiorca musi wygenerować wiadomość o błędzie, jeśli nie jest w stanie przetworzyć danego AVP,
    - P = sygnalizuje żądanie ochrony poufności w trybie end-to-end.



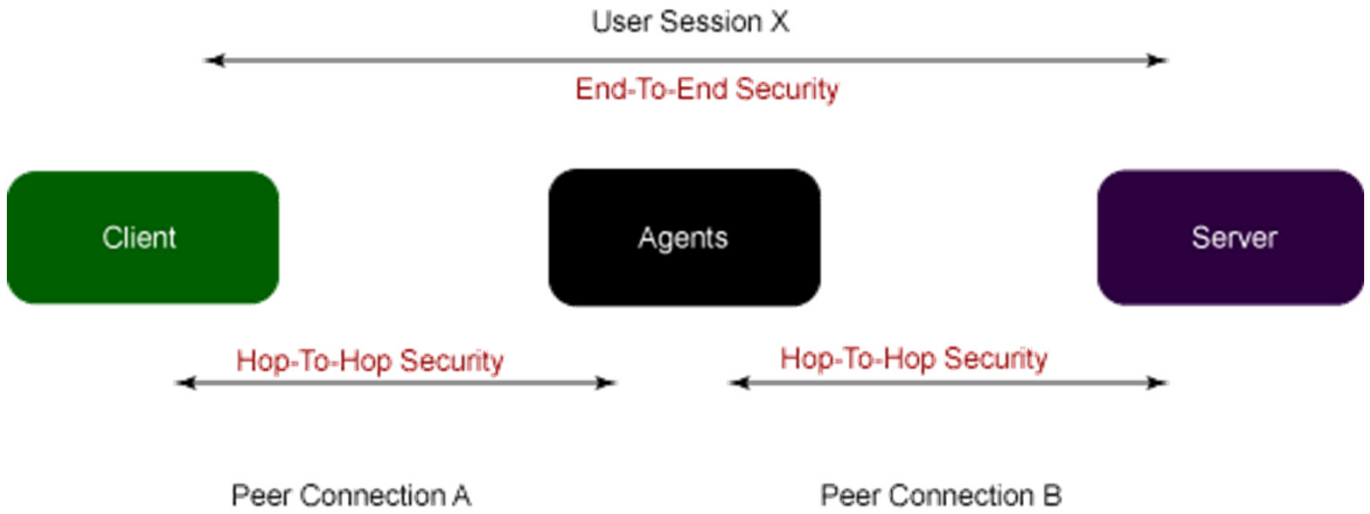
- AVP wykorzystywane są zarówno do wymiany wiadomości niezbędnych do działania samego protokołu Diameter, jak i powiązanych aplikacji.

GDAŃSK UNIVERSITY OF TECHNOLOGY

Połączenia i sesje

- Sesja (Diameter Session) – logiczne powiązanie pomiędzy dwoma węzłami umożliwiające przeprowadzenie sekwencji działań służących realizacji określonego zdania.
  - Jednoznacznie identyfikowana unikalnym Session-Id wykorzystywanym w AVP.

- Połączenie (Diameter Peer Connection) – połączenie komunikacyjne pomiędzy dwoma węzłami Diameter.



GDAŃSK UNIVERSITY OF TECHNOLOGY

Peer Discovery

- Węzeł Diameter może rozgłaszać informacje o:
  - swojej obecności i adresie,
  - obsługiwanym realm,
  - obsługiwanych aplikacjach,
  - udostępnianych mechanizmach zabezpieczeń.
- Zdefiniowano 2 metody:
  - Service Location Protocol (SRVLOC) – przeznaczona dla sieci lokalnych,
  - DNS – poprzez rejestrację rekordów SRV (_diameter._tcp.realm, _diameter._sctp.realm)
- Węzeł przechowuje informacje innych węzłach w:
  - Peer table – adresy, parametry oraz stan wykrytych węzłów Diameter,
  - Realm routing table – informacje pozwalające na właściwe kierowanie wiadomości.

Realm, AppId, Action, Next-hop Peer, isStatic, ExpireTime

- **Realm**: Primary key, matched with Destination-Realm Avp
- **AppId**: Secondary key, matched with AppId in message header
- **Action**: For each matching entry, possible actions are: LOCAL, RELAY, PROXY, REDIRECT
- **isStatic**: Indication of static or dynamic route
- **ExpireTime**: Time before dynamic route are no longer valid

GDAŃSK UNIVERSITY OF TECHNOLOGY

Obsługa błędów

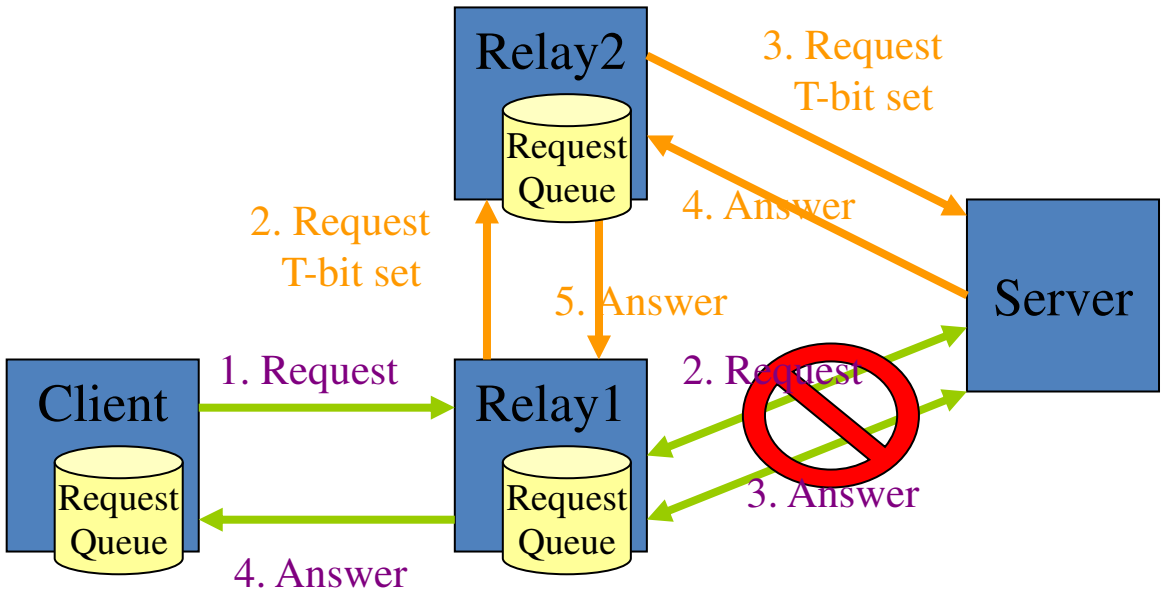
- Dwie podstawowe grupy błędów:
  - **Błędy protokołu (protocol errors)** – błędy związane z podstawowym działaniem bazowego protokołu Diameter, najczęściej związane z przenoszeniem wiadomości.
  - **Błędy aplikacji (application errors)** – błędy odnoszące się do działania aplikacji wykorzystujących protokół Diameter.
- Wartości AVP związane z obsługą błędów:
  - *Return-Code AVP* – informacja o wyniku przetwarzania otrzymanej przez węzeł wiadomości,
  - *Error-Reporting-Host AVP* – identyfikacja węzła który wygenerował Return-Code AVP,
  - *Failed-AVP* – informacja na temat grupy AVP, która spowodowała wystąpienie błędu.
  - *Error-Message AVP* – słowny opis błędu.

- Monitorowanie stanu połączeń – okresowa wymiana wiadomości *Device-Watchdog-Request / Answer.*

GDAŃSK UNIVERSITY OF TECHNOLOGY

Failover-Failback Procedure

- Failover: Attempt to re-route pending request to an alternate peer in case of transport failure
  - 'T' bit is set for re-routed requests
- Failback: Switch back to the original next hop when connection is re-established



GDAŃSK UNIVERSITY OF TECHNOLOGY

RADIUS i Diameter

	Diameter	RADIUS
Transportation Protocol	Connection-Oriented Protocols (TCP and SCTP)	Connectionless Protocol (UDP)
Security	Hop-to-Hop, End-to-End	Hop-to-Hop
Agent Support	Relay, Proxy, Redirect, Translation	Implicit support, which means the agent behaviors might be implemented in a RADIUS server
Capabilities Negotiation	Negotiate supported applications and security level	Don't support
Peer Discovery	Static configuration and dynamic lookup	Static configuration
Server Initiated Message	Supported. For example, re-authentication message, session termination, etc.	Don't support
Maximum Attribute Data Size	16,777,215 octets	255 octets
Vendor-specific Support	Support both vendor-specific messages and attributes	Support vendor-specific attributes only