Problematyka bezpieczeństwa usług Web Services

Witold Andrzejewski

Plan prezentacji

- Co to jest bezpieczeństwo? Podstawowe terminy.
- Dlaczego bezpieczeństwo jest ważne?
- Dotychczasowe rozwiązania.
- Nowe rozwiązania w dziedzinie bezpieczeństwa.
- Rozwiązania wspomagające.
- Podsumowanie.

Plan prezentacji

- Co to jest bezpieczeństwo? Podstawowe terminy.
- Dlaczego bezpieczeństwo jest ważne?
- Dotychczasowe rozwiązania.
- Nowe rozwiązania w dziedzinie bezpieczeństwa.
- Rozwiązania wspomagające.
- Podsumowanie.

Co to jest bezpieczeństwo?

- Na bezpieczeństwo składają się:
  - **Uwierzytelnianie** – usługa musi mieć możliwość sprawdzenia od kogo przyszło żądanie.
  - **Poufność** – przesyłanych danych nie może podsłuchać strona trzecia.
  - **Integralność** – dane nie mogą dotrzeć zmienione.
  - **Niezaprzeczalność** – nadawca nie może się wyprzeć faktu nadania wiadomości
  - **Autoryzacja** – stwierdzenie czy dany podmiot ma dostęp do danych zasobów

Podstawowe terminy

- **Kryptografia symetryczna** – komunikat szyfrowany i odszyfrowywany tym samym kluczem.
- **Kryptografia asymetryczna** – komunikat szyfrowany **kluczem publicznym** a odszyfrowywany **kluczem prywatnym**.
- **Skrót wiadomości** – wynik działania funkcji haszującej na wiadomości. Ma stałą długość. Trudno znaleźć **kolizję**.

Podstawowe terminy

- **Żeton bezpieczeństwa** – Zbiór twierdzeń o jakimś podmiocie (np. nazwa, rola, hasło)
- **Podpis elektroniczny** – jedno z zastosowań kryptografii asymetrycznej. Wiadomości można podpisać za pomocą klucza prywatnego, a sprawdzić podpis za pomocą klucza publicznego. Zapewnia integralność, uwierzytelnianie i niezaprzeczalność

Podstawowe terminy

- **Podpisany żeton bezpieczeństwa –** żeton bezpieczeństwa podpisany cyfrowo.
- **Certyfikat** – żeton bezpieczeństwa zawierający klucz publiczny podmiotu podpisany przez zaufaną stronę trzecią.
- **Infrastuktura klucza publicznego –** układ, w którym trzecia strona może poświadczać bądź zaprzeczać tożsamości podmiotów oraz wystawiać certyfikaty.

Plan prezentacji

- Co to jest bezpieczeństwo? Podstawowe terminy.
- Dlaczego bezpieczeństwo jest ważne?
- Dotychczasowe rozwiązania.
- Nowe rozwiązania w dziedzinie bezpieczeństwa.
- Rozwiązania wspomagające.
- Podsumowanie.

Dlaczego bezpieczeństwo jest ważne?

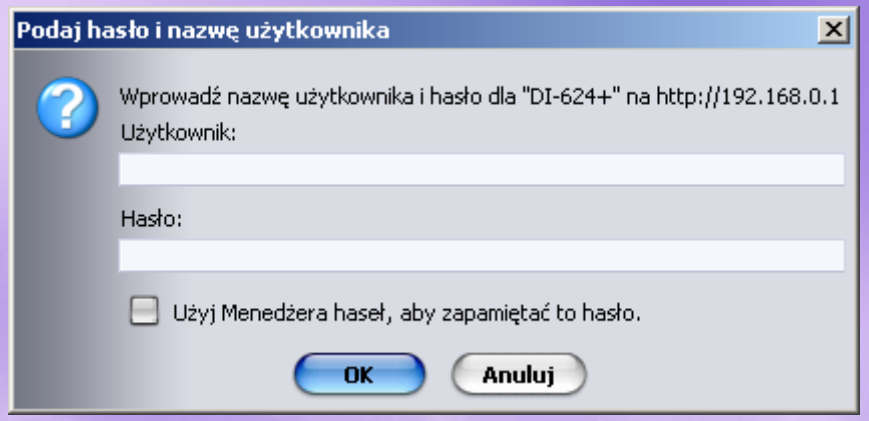
- Sekrety handlowe.
- Zaufanie klientów i partnerów handlowych.
- Prawna gwarancja ochrony danych osobowych klientów.
- Możliwość wykorzystania dziur w systemie do popełnienia przestępstw.

Plan prezentacji

- Co to jest bezpieczeństwo? Podstawowe terminy.
- Dlaczego bezpieczeństwo jest ważne?
- Dotychczasowe rozwiązania.
- Nowe rozwiązania w dziedzinie bezpieczeństwa.
- Rozwiązania wspomagające.
- Podsumowanie.

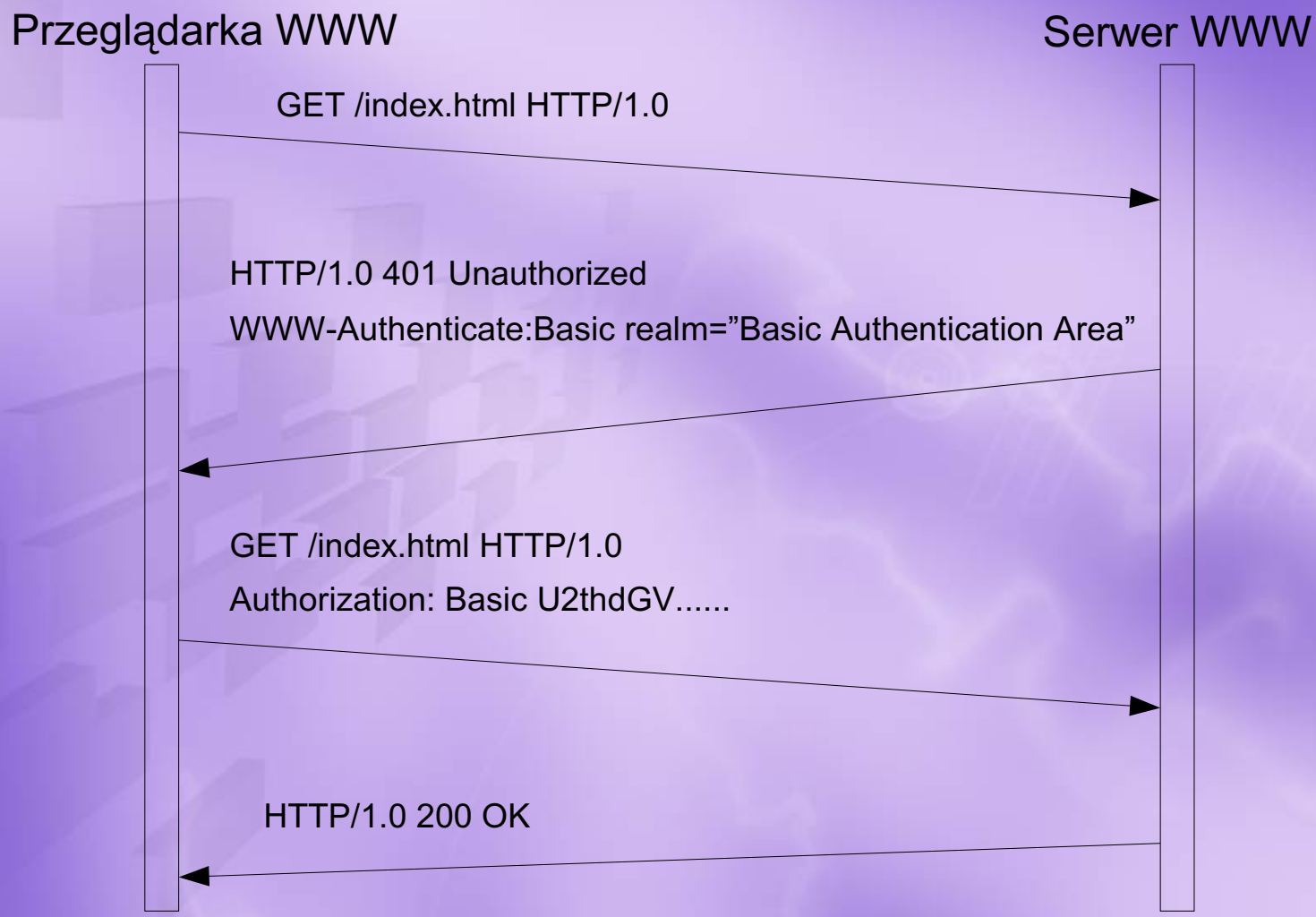
Dotychczasowe rozwiązania

- **BASIC-AUTH**
  - Uwierzytelnienie przez podanie hasła (RFC 2617).

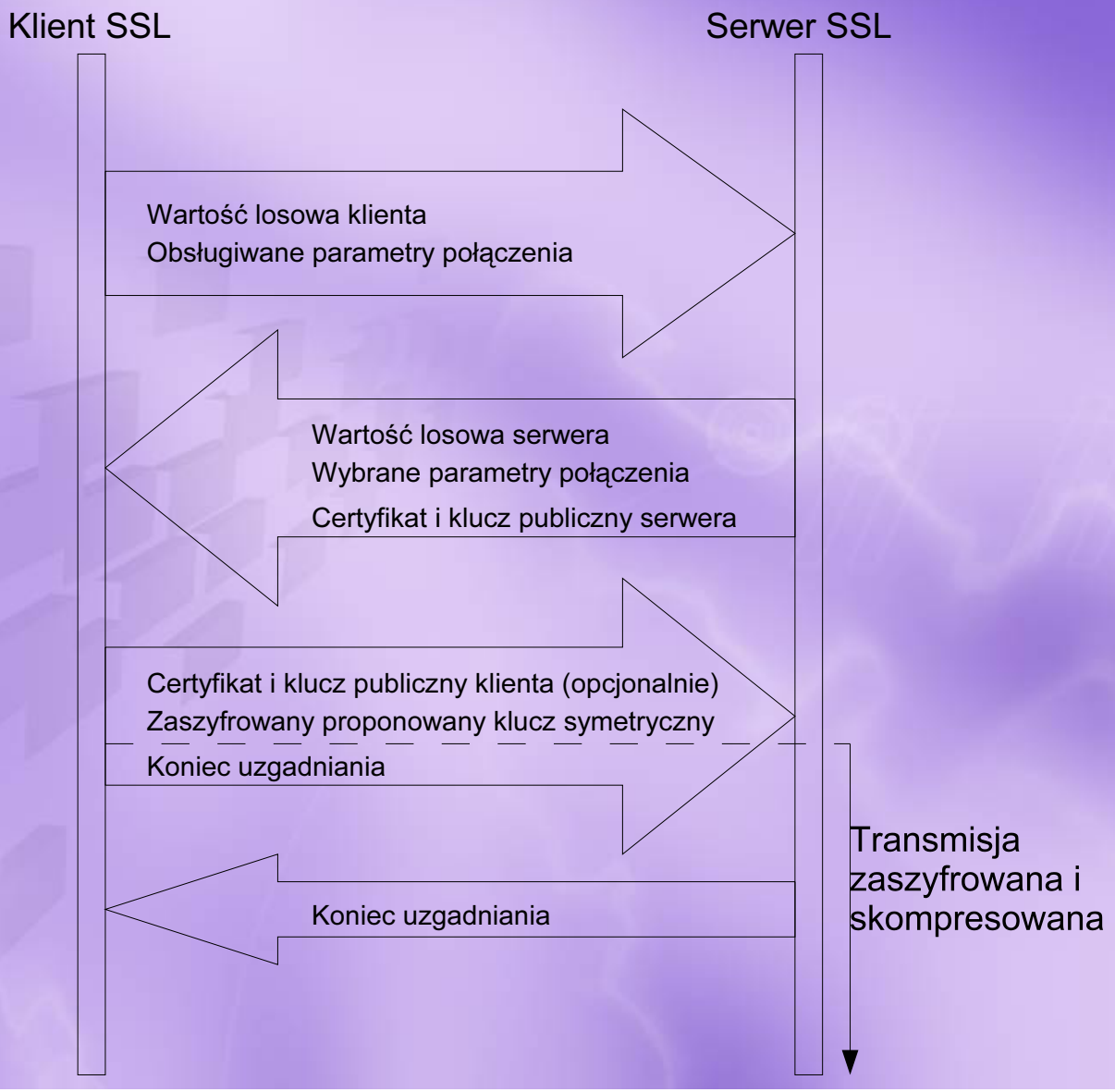


- **SSL/TLS**
  - Protokół szyfrujący transmisję (RFC 2246). Znajduje się pomiędzy warstwą transportową (TCP) a warstwą aplikacji. Przykłady zastosowania: HTTPS, SSH.

BASIC-AUTH


Przeglądarka WWW
Serwer WWW
GET /index.html HTTP/1.0
HTTP/1.0 401 Unauthorized
WWW-Authenticate:Basic realm=”Basic Authentication Area”
GET /index.html HTTP/1.0
Authorization: Basic U2thdGV.....
HTTP/1.0 200 OK

SSL/TLS

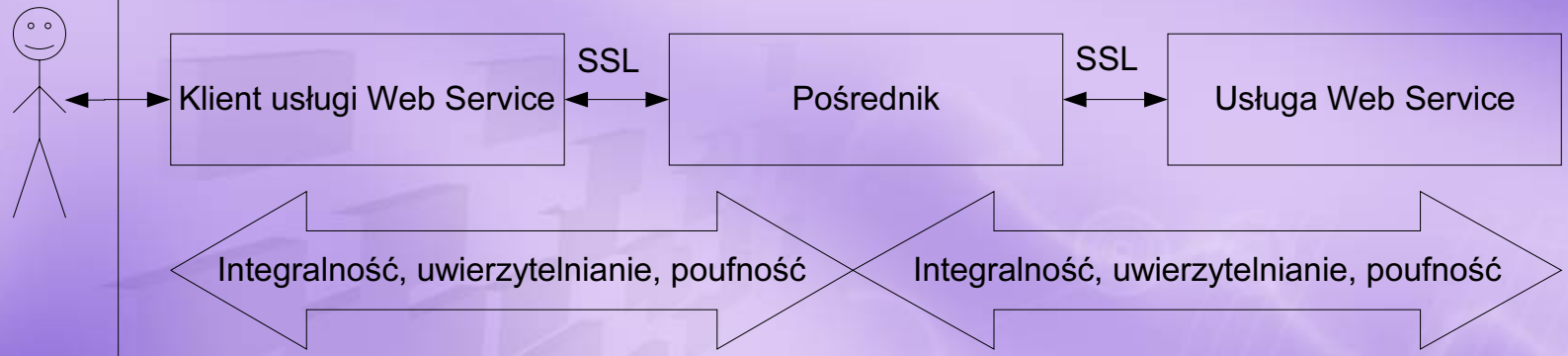

Klient SSL
Serwer SSL
Wartość losowa klienta
Obsługiwane parametry połączenia
Wartość losowa serwera
Wybrane parametry połączenia
Certyfikat i klucz publiczny serwera
Certyfikat i klucz publiczny klienta (opcjonalnie)
Zaszyfrowany proponowany klucz symetryczny
Koniec uzgadniania
Koniec uzgadniania
Transmisja zaszyfrowana i skompresowana

Dlaczego BASIC-AUTH i SSL nie wystarczają?

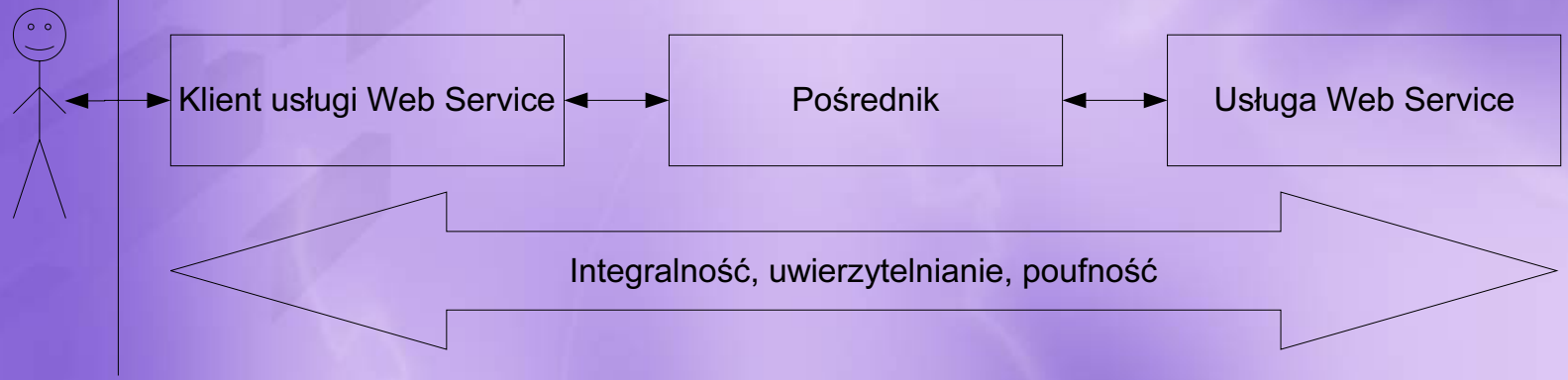
- SSL zapewnia uwierzytelnianie, poufność, integralność i potencjalnie niezaprzeczalność, a BASIC-AUTH uwierzytelnianie i autoryzację, ale jedynie pomiędzy dwoma węzłami.
- W transmisji komunikatów SOAP mogą wystąpić pośrednicy, z których każdy może potrzebować przeczytać kawałek komunikatu.

Dlaczego BASIC-AUTH i SSL nie wystarczają?

- Co mamy w tej chwili?



- Czego potrzebujemy ?



Plan prezentacji

- Co to jest bezpieczeństwo? Podstawowe terminy.
- Dlaczego bezpieczeństwo jest ważne?
- Dotychczasowe rozwiązania.
- Nowe rozwiązania w dziedzinie bezpieczeństwa.
- Rozwiązania wspomagające.
- Podsumowanie.

Nowe rozwiązania

- W celu zabezpieczenia transmisji komunikatów SOAP stosuje się następujące standardy:
  - XML Digital Signature (W3C),
  - XML Encryption (W3C),
  - WS-Security (OASIS).

XML Digital Signature

- Od 12 lutego 2002 rekomendacja (standard) W3C.
- Opracowany przez W3C i Internet Engineering Task Force (IETF).
- Specyfikuje jak można użyć dowolnego algorytmu kryptografii symetrycznej lub asymetrycznej do podpisania dowolnego dokumentu XML.

XML Digital Signature

- Umożliwia umieszczenie wielu różnych podpisów w jednym dokumencie.
- Pozwala na podpisanie zarówno dowolnego fragmentu dokumentu XML jak i całości.
- Zapewnia uwierzytelnianie, integralność i niezaprzeczalność.

XML Encryption

- Od 10 grudnia 2002 jest rekomendacją W3C.
- Nie jest związany z komunikatami SOAP – nadaje się do szyfrowania dowolnego dokumentu XML.
- Nie określa żadnego konkretnego algorytmu szyfrowania, ale pozwala na zastosowanie dowolnego algorytmu kryptografii symetrycznej i asymetrycznej.

XML Encryption

- Specyfikuje w jaki sposób można utworzyć dokument XML zawierający zaszyfrowane:
  - dokument XML,
  - znacznik XML,
  - zawartość znacznika XML,
  - dowolne dane nie będące dokumentem XML,
  - zaszyfrowany dokument XML.

WS-Security

- XML Digital Signature i XML Encryption nie są rozwiązaniami przeznaczonymi specyficznie dla SOAP.
- Standardem, który określa sposób wykorzystania dwóch powyższych do podpisywania i szyfrowania wiadomości SOAP jest WS-Security.

WS-Security

- WS-Security doczekał się dwóch wersji zatwierdzonych przez OASIS:
  - 1.0 zatwierdzona w marcu 2004
  - 1.1 zatwierdzona w lutym 2006
- WS-Security nie definiuje jednego protokołu bezpiecznej komunikacji usług Web Services, ale stanowi raczej szkielet, na bazie którego, takie protokoły można budować.

Nowe rozwiązania

- WS-I (Web Services Interoperability) – Basic Security Profile:
  - HTTP over TLS
  - XML Digital Signature (certyfikaty X.509)
  - XML Encryption
  - WS-Security

Firewall XML

- Normalne urządzenia albo aplikacje typu firewall działają w warstwie transportowej, a zatem mogą blokować ruch pakietów w zależności od ich źródła i celu.
- Firewall XML w przeciwieństwie do firewalli warstwy transportowej, działa w warstwie aplikacji, a zatem może zaglądać do środka przesyłanych komunikatów.

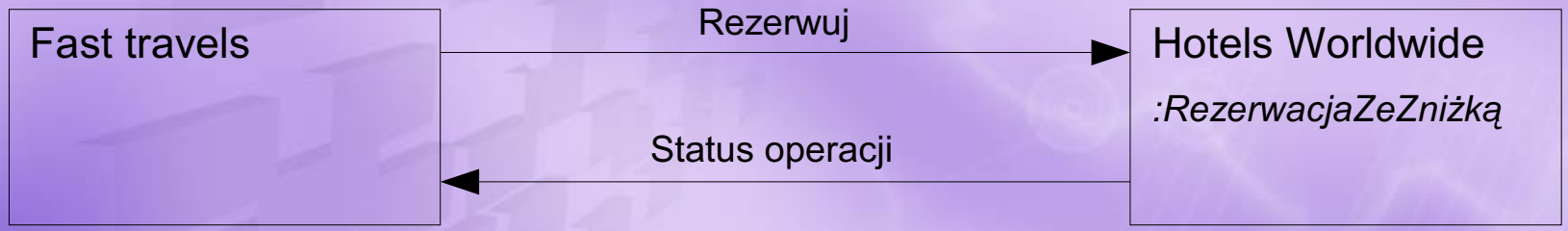
Firewall XML

- Firewall XML jest specyficznym rozwiązaniem służącym do zabezpieczania przesyłania wiadomości opartego na XML (w tym SOAP).
- Taki firewall może sprawdzić poprawność podpisu przesyłanego komunikatu SOAP, odszyfrować ten komunikat, i przesłać go dalej do usługi Web Service.

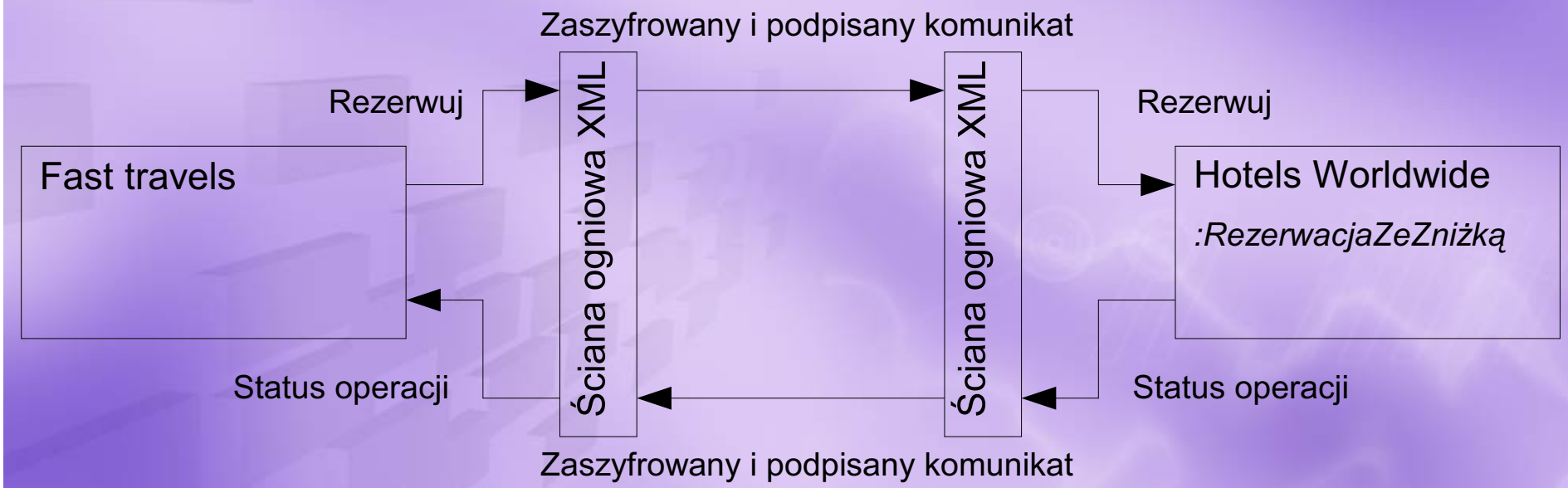
Firewall XML

- Firewall XML może być:
  - osobnym urządzeniem,
  - osobnym programem działającym na serwerze,
  - częścią platformy na której została zaimplementowana usługa.
- Przykładowe firewalle XML to:
  - XML Message Server firmy Westbridge Technology,
  - SOAP Content Inspector firmy Quadrasis,

Nowe rozwiązania, przykład 1



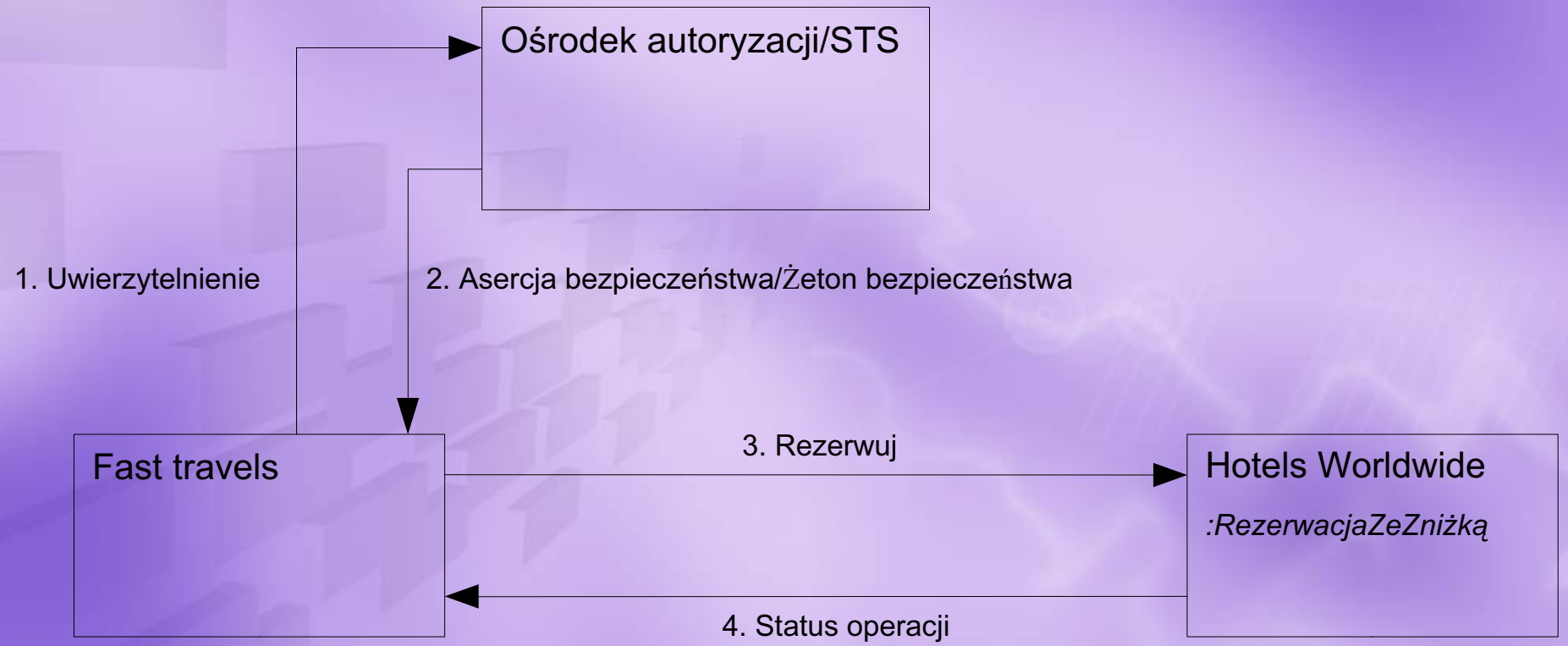
Nowe rozwiązania, przykład 2



Problem

- Rozwiązanie przedstawione na przykładzie 2 jest mało realistyczne.
- Usługa nie powinna zajmować się autoryzacją dostępu do niej.
  - Nadmierna rozbudowa funkcjonalności usługi.
  - Zarządzanie uprawnieniami.
- Konieczny 3 podmiot, zaufany zarówno przez klienta, jak usługę, który zajmowałby się uwierzytelnianiem i autoryzacją.

Nowe rozwiązania, przykład 3



SAML 1.0-2.0, WS-Trust

- Problemem autoryzacji i uwierzytelniania przez osobny ośrodek zajmują się dwie specyfikacje:
  - SAML 1.0, 1.1 i 2.0. Standard OASIS:
    - 1.0 – 5 listopad 2002
    - 1.1 – 2 wrzesień 2003
    - 2.0 – 15 marzec 2005
  - WS-Trust – najnowsza wersja – luty 2005
- Rozwiązania pokrywające się i sprzeczne

SAML vs WS-Trust

- SAML – 3 rodzaje żetonów bezpieczeństwa, tzw. asercji:
  - asercja dotycząca uwierzytelnienia,
  - asercja dotycząca atrybutów,
  - asercja dotycząca decyzji.
- WS-Trust dowolne rodzaje żetonów bezpieczeństwa.
- SAML jest znacznie bogatszy niż WS-Trust, rozwiązuje więcej różnych problemów
- SAML jest standardem OASIS, a WS-Trust jest tylko specyfikacją.

Problem

- SAML i WS-Trust opisują metody uwierzytelniania i autoryzacji dostępu do zasobów.
- Problemem jest opisanie polityki dostępu do zasobów.
- Listy dostępu (*access control lists*) są mało elastyczne.

Nowe rozwiązania

- Problematyką opisu polityki dostępu do zasobów zajmują się trzy specyfikacje:
  - XACML, standard OASIS
    - 1.0 – 18 luty 2003,
    - 1.1 – 7 lipiec 2003,
    - 2.0 – 1 luty 2005,
  - XrML - ogłoszona 26 listopada 2001
  - WS-Authorization – jeszcze nie opracowana

XACML

- Definiuje sposób opisu metod autoryzacji dostępu do zasobów.
- Warunki dostępu można zdefiniować w oparciu między innymi o:
  - datę i godzinę,
  - lokalizację zasobu,
  - przynależność podmiotu żądającego autoryzacji do ról albo grup.
- Niezależna od SAML, ale definiuje również funkcjonalność dostępną jedynie przy współpracy z tym standardem.

XrML

- Zarządzanie dostępem do danych w kontekście DRM (D*igital Rights Management*)
- Uprawnienia definiowane w oparciu o 4 koncepcje:
  - Zasób
  - Żądane uprawnienie
  - Podmiot żądający uprawnienia
  - Warunek, który musi być spełniony, aby uprawnienie uzyskać.

XACML vs XrML

- XACML jest ogólny
- XrML skupia się przede wszystkim na DRM, chociaż nadaje się również do innych zastosowań.
- XACML jest standardem, XrML został zgłoszony do OASIS, ale standardem jeszcze nie został.

Problem

- W przypadku prowadzenia dłuższej wymiany komunikatów wielokrotna autoryzacja i uwierzytelnianie mocno obniża wydajność.
- Potrzebny mechanizm podobny do stosowanego w SSL/TLS polegający na ustaleniu bezpiecznego kontekstu w którym mogłaby się odbywać wydajna wymiana komunikatów.

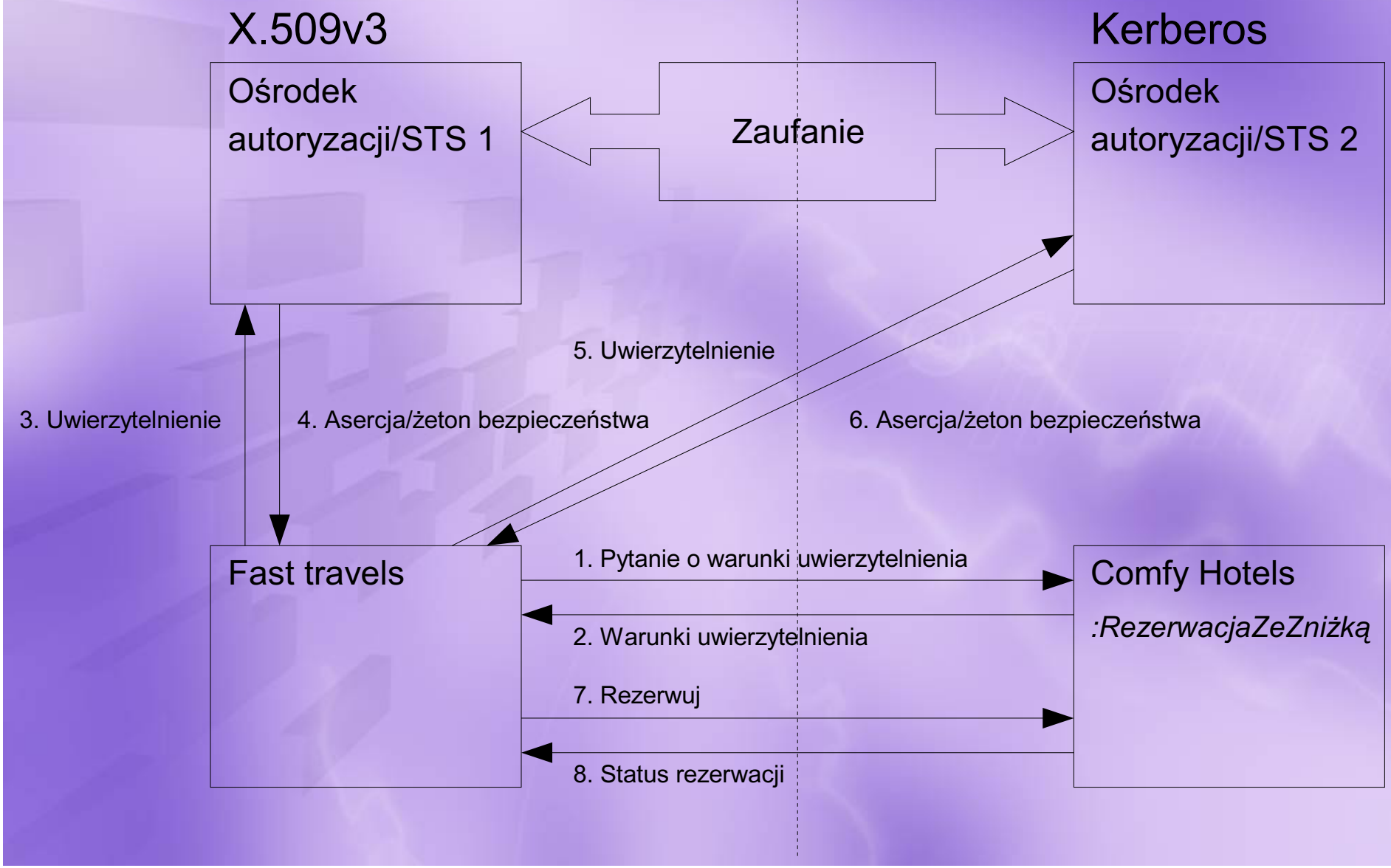
WS-SecureConversation

- Zabezpieczeniem dłuższej wymiany komunikatów zajmuje się specyfikacja WS-SecureConversation.
- Najnowsza wersja pochodzi z lutego 2005.
- Nie jest standardem, ale jest na dobrej drodze:
  - OASIS, 17 październik 2005, *Call for Participation* w komitecie technicznym WS-SX (Web Services Secure Exchange)

Problem

- Rozwiązanie z jednym ośrodkiem autoryzacji implikuje jeden sposób uwierzytelniania i autoryzacji.
- W praktyce jednak stosuje się różne żetony bezpieczeństwa.
- Istnieje potrzeba zapewnienia sposobu tłumaczenia żetonów bezpieczeństwa pomiędzy systemami.

Nowe rozwiązania, przykład 4



Nowe rozwiązania

- Tworzeniem federacji systemów informatycznych zajmują się dwie specyfikacje:
  - WS-Federation – ostatnia wersja lipiec 2003
  - ID-FF – Standard Liberty Aliance
- Specyfikacje sprzeczne oparte na różnych podstawach.

WS-Federation vs ID-FF

- ID-FF to dojrzały standard, WS-Federation jest jedynie specyfikacją.
- ID-FF istnieje wiele implementacji, WS-Federation jak na razie żadnej.
- ID-FF oparty na SAML, WS-Federation na WS-Trust
- ID-FF jest darmowy do przeglądania i implementacji, WS-Federation – można przeglądać za darmo, licencja na implementację nieznana

Plan prezentacji

- Co to jest bezpieczeństwo? Podstawowe terminy.
- Dlaczego bezpieczeństwo jest ważne?
- Dotychczasowe rozwiązania.
- Nowe rozwiązania w dziedzinie bezpieczeństwa.
- Rozwiązania wspomagające.
- Podsumowanie.

Rozwiązania wspomagające

- Wcześniej wymienione specyfikacje zajmują się zapewnieniem bezpieczeństwa w heterogenicznych środowiskach.
- Istnieją również specyfikacje, które nie są bezpośrednio związane z zapewnieniem bezpieczeństwa przekazywania danych, ale wspomagają wcześniej wymienione specyfikacje.

Problem

- Usługi Web Services powinny mieć możliwość komunikowania klientom o swoich wymaganiach i preferencjach, np:
  - Kodowanie przesyłanych komunikatów
  - Wersje specyfikacji na jakich została oparta
  - Wspierane algorytmy zapewniające
    - Integralność
    - Poufność
    - Uwierzytelnianie
    - .....

Nowe rozwiązania

- Problemem komunikowania przez usługi o swoich możliwościach, wymaganiach i preferencjach zajmują się dwie specyfikacje:
  - WS-Policy, we współpracy z, m. in.:
    - WS-PolicyAttachments
    - WS-PolicyAssertions
    - WS-SecurityPolicy
  - WSPL - podzbiór XACML
- Obie specyfikacje nie są standardami.

Nowe rozwiązania

- Specyficzną grupą komunikowanych wymagań przez usługi Web Services jest ich polityka względem danych osobowych.
- Problemem tym ma zajmować się nieukończona jeszcze specyfikacja WS-Privacy, oparta o WS-Trust, WS-Security i WS-Policy.

Nowe rozwiązania

- DSS – *Digital Signature Service*. Nie ukończony jeszcze standard OASIS, który opisuje jak można tworzyć usługi wspomagające tworzenie podpisu elektronicznego.
- XKMS – *XML Key Management Specification*.
  - X-KISS - *XML Key Information Service Specification*
  - X-KRSS - *XML Key Registration Service Specification*

Nowe rozwiązania

- XCBF – XML Common Biometric Format. Standard OASIS pozwalający m. in. na tworzenie żetonów bezpieczeństwa w oparciu o pomiary biometryczne.
- AVDL – *Application Vurnerability Description Language*, oparty na XMLu język pozwalający opisywać zagrożenia bezpieczeństwa w aplikacjach.

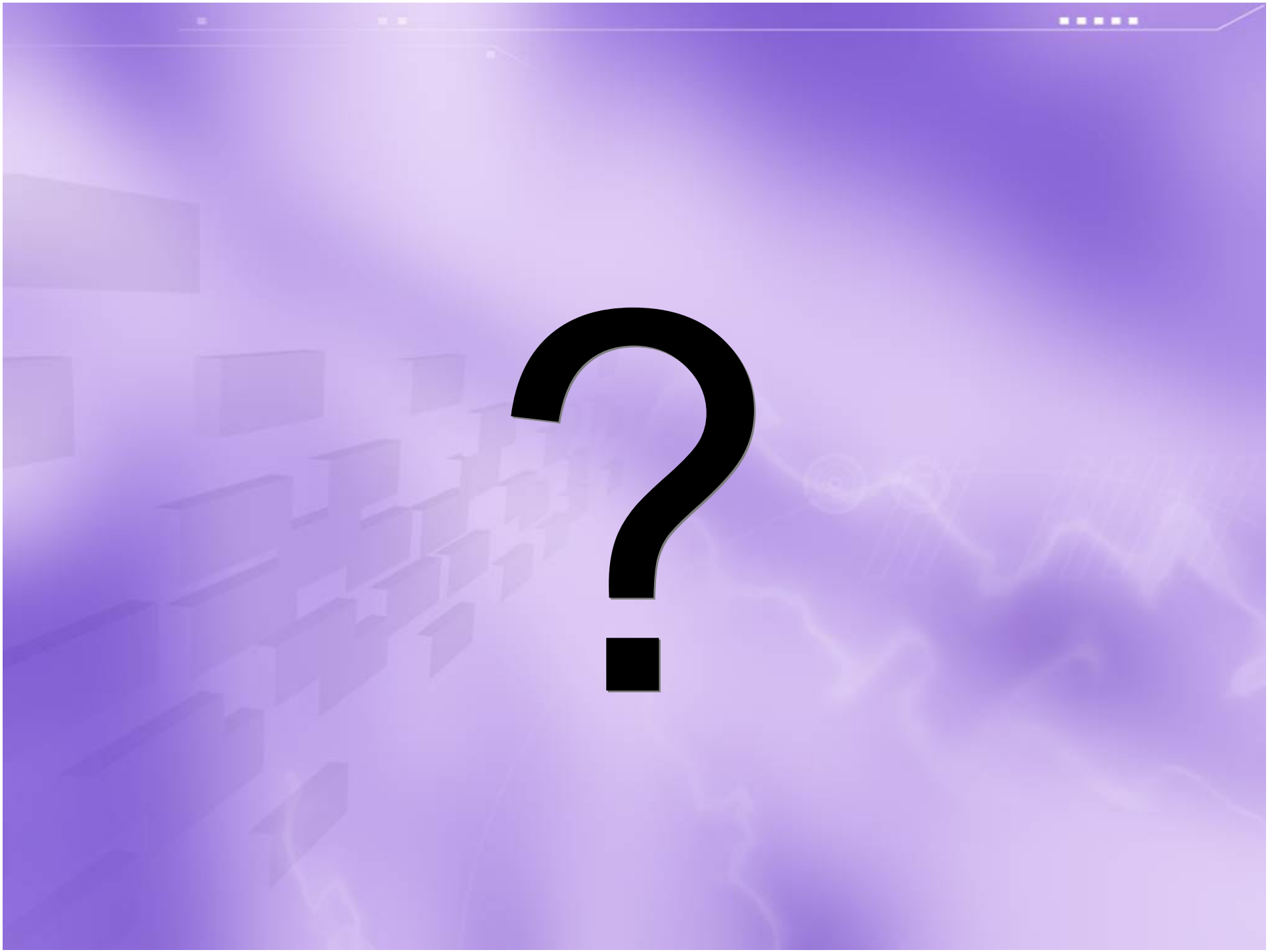
Plan prezentacji

- Co to jest bezpieczeństwo? Podstawowe terminy.
- Dlaczego bezpieczeństwo jest ważne?
- Dotychczasowe rozwiązania.
- Nowe rozwiązania w dziedzinie bezpieczeństwa.
- Rozwiązania wspomagające.
- Podsumowanie.

Podsumowanie

- Istnieje wiele rozwiązań dotyczących różnych aspektów zapewnienia bezpieczeństwa.
- Część rozwiązań dotyczy podobnego zbioru problemów i jest ze sobą sprzecznych.
- Które rozwiązania wybrać?

Dziękuję



XML Digital Signature, przykład

```
<?xml version=”1.0”?>
<SOAP-ENV:Envelope
 xmlns:SOAPENV=”http://schemas.xmlsoap.org/
  soap/envelope/”>
 <SOAP-ENV:Body>
  <s:RezerwacjaZeZnizka
   xmlns:s=
    “http://www.FastTravels.com/partnerservice/”>
   <!—Parametry metody-->
  </s:RezerwacjaZeZnizka >
 </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

XML Digital Signature, przykład

```
<?xml version="1.0"?>
<SOAP-ENV:Envelope
 xmlns:SOAPENV="http://schemas.xmlsoap.org/
  soap/envelope/"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
 <SOAP-ENV:Header>
  <ds:Signature>
   <ds:SignedInfo/><ds:SignatureValue/><ds:KeyInfo/>
   </ds:Signature>
 </SOAP-ENV:Header>
 <SOAP-ENV:Body>
   <s:RezerwacjaZeZnizka ID=„RezerwacjaZeZnizka"
    xmlns:s=
     "http://www.FastTravels.com/partnerservice/">
    <!—Parametry metody-->
   </s:RezerwacjaZeZnizka >
 </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

XML Digital Signature, przykład

```
<ds:SignedInfo>
 <ds:CanonicalizationMethod
  Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
 <ds:SignatureMethod Algorithm="http://www.w3.org/2000
  /09/xmldsig#rsa-sha1"/>
 <ds:Reference URI="#RezerwacjaZeZnizka">
  <ds:Transforms>
   <ds:Transform Algorithm="http://www.w3.org/2001/
    10/xml-exc-c14n#"/>
  </ds:Transforms>
  <ds:DigestMethod
     Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
  <ds:DigestValue>BIUddkjKKo2...</ds:DigestValue>
 </ds:Reference>
</ds:SignedInfo>
```

XML Digital Signature, przykład

```
<ds:SignatureValue>
 halHJghyf765....
</ds:SignatureValue>
<ds:KeyInfo>
 <ds:KeyName>MyKeyIdentifier</ds:KeyName>
</ds:KeyInfo>
```

XML Encryption, przykład

```
<SOAP-ENV:Body>
 <xenc:EncryptedData
  xmlns:xenc="http://www.w3.org/2001/04/xmlenc#„
  Type="http://www.w3.org/2001/04/xmlenc#Element">
  <xenc:EncryptionMethod
   Algorithm="http://www.w3.org/2001/
    04/xmlenc#aes128-cbc"/>
   <ds:KeyInfo xmlns:ds="http://www.w3.org/
    2000/09/xmldsig#”
    <ds:KeyName>MyKeyIdentifier</ds:KeyName>
   </ds:KeyInfo>
   <xenc:CipherData>
    <xenc:CipherValue>B457V645B45......</xenc:CipherValue>
   </xenc:CipherData>
 </xenc:EncryptedData>
</SOAP-ENV:Body>
```