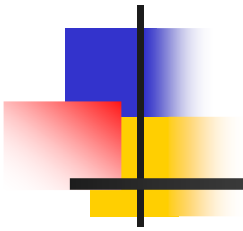


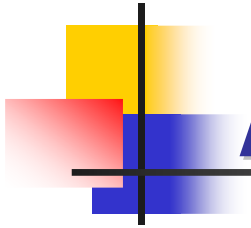
Podpis Grupowy

w zastosowaniach systemów anonimowości

Krystian Baniak

Seminarium Doktoranckie

03.03.2010



Agenda

- Wprowadzenie
- Definicja podpisu grupowego
- Typy podpisu grupowego
- Przegląd schematów podpisu grupowego
- Obszary zastosowań podpisu grupowego
- Podpis grupowy w schematach anonimowości
- Q&A

Podpis grupowy

Definicja problemu:

- *Jak przekazać informację w sposób wiarygodny, przekonywujący odbiorcę o autentyczności wiadomości, a zarazem nie ujawniając tożsamości wysyłającego.*

- Podpis grupowy jest jednym z mechanizmów kryptograficznych mających zastosowanie w tej dziedzinie
  - Podpis Grupowy *Group Signature*
  - *Ring Signatures*
  - *Threshold Signatures (t,k)*

Podpis Grupowy

- Mechanizm kryptograficzny zaproponowany przez Davida Chaum i Eugene van Heijst [CvH91] w 1991

Schemat podpisu grupowego definiujemy jako zbiór podmiotów, gdzie każdy podmiot posiada własny klucz prywatny, i każdy zdolny jest generować podpis w imieniu całej grupy. Podpis jest weryfikowalny z użyciem klucza publicznego grupy. Schemat zawiera także arbitra GM w postaci centrum certyfikującego i weryfikującego tożsamość podmiotu podpisującego w razie potrzeby odwołania jego anonimowości.

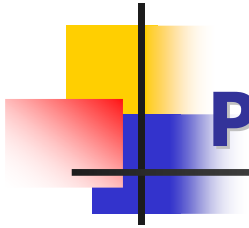
E_i – zbiór podmiotów, i <= n

sk_i – klucz prywatny E_i

gpsk – klucz publiczny grupy

gmsk – klucz prywatny GM

W szczególności Schemat może zawierać dodatkowego arbitra będącego centrum weryfikacji podpisu w celu ustalenia tożsamości podpisującego.



Podpis grupowy

- Cechy Schematu Popisu Grupowego

  - **Correctness** – poprawny podpis jest zawsze weryfikowalny a sfałszowany podpis nigdy nie weryfikuje się pozytywnie (soundness, completeness)
  - **Unforgeable** – tylko należący do grupy mogą podpisywać w jej imieniu
  - **Anonymity** – nie można skojarzyć podpisu z podpisującym (weak conditional anonymity)
  - **Unlinkability** – mając m1 i m2 oraz s1,s2 nie można stwierdzić że pochodzą od tego samego podpisującego
  - **Exculpability** – nikt nie może podszyć się pod dany podmiot
  - **Traceability** – GM może ustalić tożsamość podpisującego w operacji OPEN
  - **Coalition-resistant** – podmioty nie mogą stworzyć układu pozwalającego na fałszowanie lub otworzenie podpisu (no framing)
  - **unforgeable tracing** – GM nie może fałszywie oskarżyć członka grupy o podpisanie danej wiadomości

Pokrewne mechanizmy

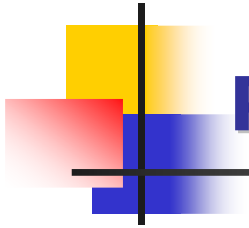
- Ring Signature

  Rivest,Shamir,Tauman ASIACRYPT 2001

  - Zapewnia w odróżnieniu od podpisu grupowego bezwarunkową anonimowość
  - Brak Group Managera
  - Rozmiar grupy może być dowolny i nie wymaga przygotowania schematu jak w przypadku podpisu grupowego
  - Schemat podpisu :

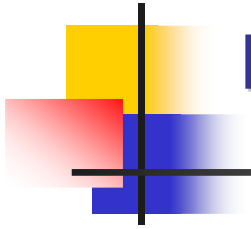
    C <= SIGN(M,SKi,PK1,PK2,…,PKi,…PKn)

- Threshold Signature (n,k)
  - Podpis jest ważny w wyniku podpisania wiadomości przez k z N członków grupy.
  - Quorum k członków pozostaje anonimowe bezwarunkowo



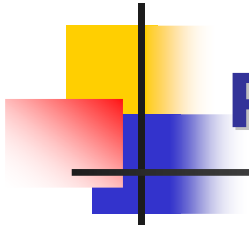
Podpis grupowy

- **Zestaw właściwości akceptowalnego systemu podpisu grupowego można zredukować do postaci pary z której wynikają inne pożądane właściwości:**
  - **Pełna Anonimowość** (full-anonymity)
    - Anonymity; unlinakability
    - Należy pamiętać, że jest to anonimowość warunkowa
  - **Pełna Rozliczalność** (full-traceability)
    - Unforgeability; (Weak) exculpability; Nonframing;
    - Traceability; Coalition-resistance
- Inne właściwości
  - **Revocation of members**
    - Wymiana klucza gpsk
    - CRL
    - Ograniczenia czasowe i schematu
  - **Dynamiczność** – możliwość rozszerzania schematu podpisu grupowego o nowych członków
    - Operacje: JOIN



Podpis grupowy

- Inne Problemy
- Forward security
  - Co zrobić aby w dynamicznym systemie nowy członek grupy nie mógł podpisywać wiadomości datowanych czasem z przed operacji JOIN
    - Signing key rekeying for time intervals
- Schematy dynamiczne – implikacje
  - Operacja revoke a ważność podpisu
    - Podpis ważny gdy członek grupy należał do grupy w momencie podpisywania wiadomości – podpis wykonany w czasie kadencji jest zawsze wazny
    - Podpis ważny wtedy gdy weryfikacja odbywa się w czasie gdy wystawca należy do grupy – podpis wykonany w czasie kadencji nie jest już ważny po jej zakończeniu – anulowanie decyzji podjętych w czasie kadencji!
      - Wymusza wymianę klucza publicznego grupy
      - Powoduje zagrożenia dla anonimowości – klucz zmienia się gdy podpisujący odchodzi



Podpis grupowy

- Operacje podstawowe w ramach schematu

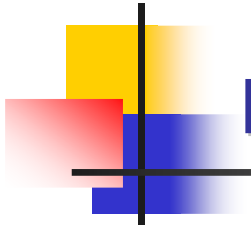
SETUP – inicjalizacja schematu; generacja kluczy *sk,gpsk,gmsk*

JOIN – dołączenie podmiotu do schematu

SIGN – podpisanie przez podmiot w imieniu grupy wiadomości *m*

VERIFY – weryfikacja podpisu grupy w oparciu o *gpsk*

OPEN – sprawdzenie tożsamości podpisującego (deanonymizacja podmiotu podpisującego)



Podpis grupowy

- Schematy Statyczne
  - Zamknięte ze względu na liczbę członków grupy
  - Materiał kryptograficzny tworzony w fazie inicjalizacji schematu
  - BMW ‘2003
  - Klucze powstałe w czasie inicjalizacji są znane przez GM!

- Schematy dynamiczne
  - Bardziej praktyczne, umożliwiają rozszerzanie (join) lub zmniejszanie(! revoke) schematu o daną liczbę członków
  - ACJT ‘2000
  - Klucz prywatny członka nie jest znany GM. Procedura JOIN może być wywołana w dowolnej chwili

Podpis grupowy

- Przykład schematu statycznego BMW ’03 (Bellare, Micciano, Wanrinshi)

Setup(L,n), n – rozmiar grupy
→ gpk, gmsk, sk_1 … sk_i
Sign(sk_i,M) → S
Verify(gpk,S) → {yes; no}
Open(gmsk,S) → i, i <=n || :fail

- Przykład schematu dynamicznego ADJT ’00 + revocation ’03

Setup() → gpk, gmsk
Join(G(sk_i)) → (cert[Ai,ei])
Sign(cert, M) → S
Verify(gpk, S) → {true,false}
Open(gmsk,S) → Ai
Revoke(cert) → gmsk, gpk, cert

Podpis grupowy

- Mechanizmy kryptograficzne używane do realizacji podpisu grupowego
  - DDH (rozróżnienie g^a g^b, g^{ab} od 3 losowych elementów grupy),
  - CDH (problem obliczenia g^{ab} znajac g^a i g^b)
  - Strong RSA ($y = u^e \bmod n$, znając n,y nie można poznać u,e)
  - Bilinear maps (2004, BB04, BBS04)

    G, G_T grupy cykliczne Zp równego rzędu, a,b należą do Zp

    e: G x G → G_T => $e(g^a,g^b) = e(g,g)^{ab}$

    <e(g,g)> = G_T - mapa nie jest zdegenerowana

    DDH jest słaby w BM, CDH jest równie mocny

    G typowo grupa abelowa nad jakimś ciałem skończonym

    umożliwia tworzenie podpisów o wielkości nieznacznie większej od RSA (do 50%)

    wykorzystuje mocny problem jak BDHP (bilinear DHP) jako podstawę bezpieczeństwa schematu: given P, *a*P, *b*P, *c*P in **G**, compute $e(P,P)^{abc}$

- ZNK, NIZNK, zero knowledge proof
  - Goldwasser
  - Protokół QR

Podpis grupowy

- Procedura JOIN jest dowodem „zero knowledge” dla GM na znajomość dyskretnego logarytmu pewnej liczby p – klucza prywatnego danego członka grupy.
- Procedura SIGN jest dowodem „zero knowledge” na posiadanie certyfikatu uprawniającego do podpisu w imieniu grupy

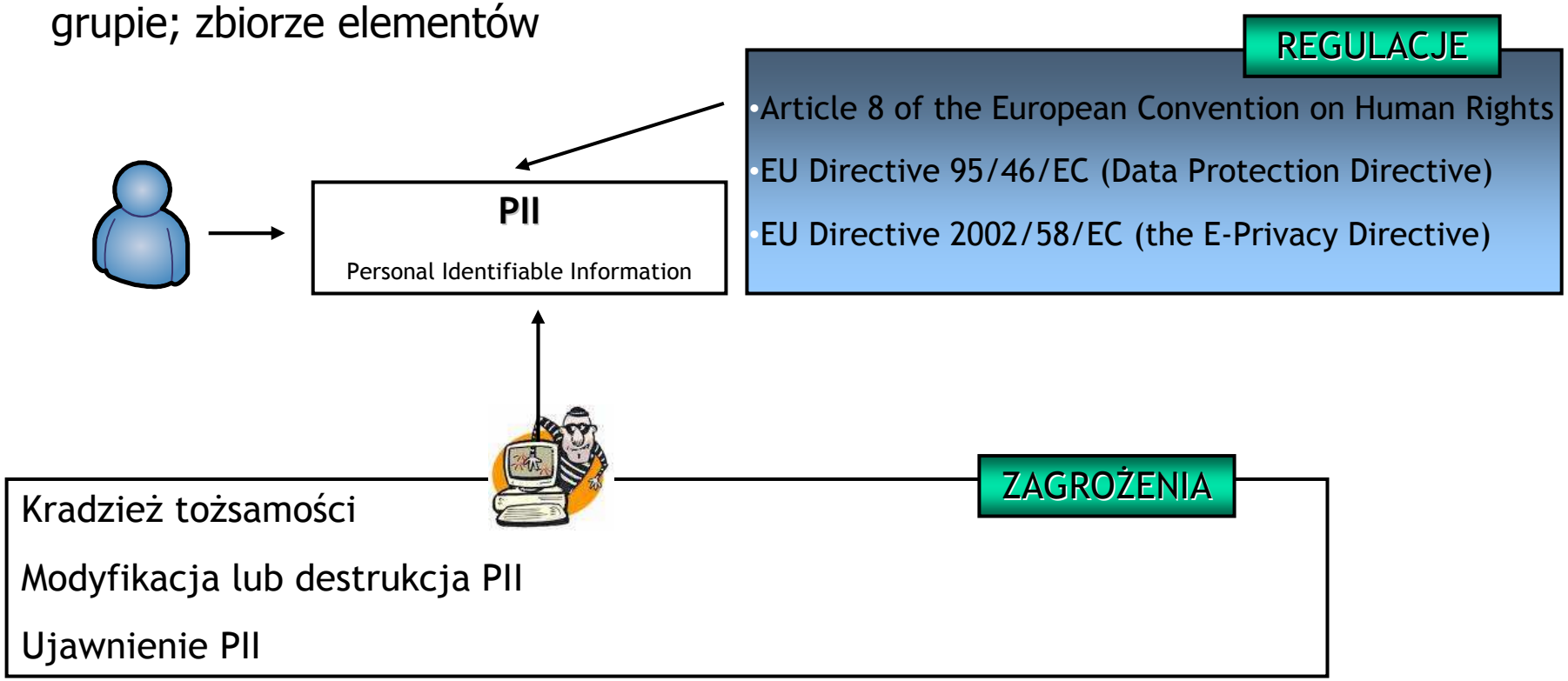
Podpis (H(m||T1,T2,..TN,R1,R2,…RN),T1,T2..TN,s1,s2…sN)

Weryfikacja (w uproszczeniu):

- odtworz R1,…Rn z T1..TN oraz s1…sN
- oblicz H’
- przyjmij podpis o ile H = H’

Prywatność i Anonimowość

- Prywatność – możliwość utrzymania poufności odnośnie szczegółów z życia osobistego i kontroli nad zakresem, czasem oraz metodą dysponowania tego typu informacjami.
- Anonimowość – stan w którym dany obiekt pozostaje nierozpoznany w danej grupie; zbiorze elementów



Anonimowość a rozliczalność

- Anonimowość nie zawsze jest pożądana zwłaszcza w systemach on-line
- Agencje bezpieczeństwa i konsultanci ds. bezpieczeństwa często traktują anonimowość jako niepożądaną z punktu widzenia rozliczalności
- EU Working Party od spraw związanych z przetwarzaniem danych osobowych stwierdza, że w wielu wypadkach należy posługiwać się rozwiązaniami kompromisowymi – słabszymi rozwiązaniami anonimowości

Regulacje zagrażające prywatności

- Nowe przywileje służb specjalnych
  - **USA PATRIOT Act** umożliwia łatwiejszy dostęp, bez nakazu sądowego, do danych dotyczących komunikacji elektronicznej przechowywanych przez operatorów
- EU data retention directive 2006/24/EC (Styczeń 2010 w Polsce)
  - Dane przechowywane pozwalają identyfikować źródło które wykonywało akcje w sieci operatora
- USA: The Internet Stopping Adults Facilitating the Exploitation of Today's Youth (SAFETY) Act of 2009 also known as H.R. 1076 and S.436

retain for a period of at least two years all records or other information pertaining to the identity of a user of a temporarily assigned network address the service assigns to that use

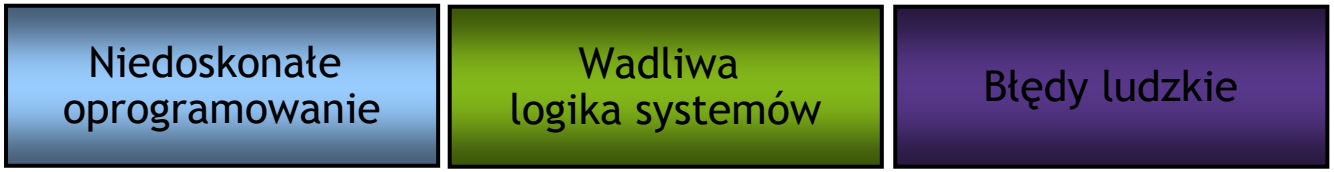
Polska:

Rejestr Stron i Usług Niedozwolonych zaakceptowany przez Radę Ministrów

Systemy kontroli i monitorowania zagrożeniem dla prywatności

- Technologia jest zagrożeniem dla prywatności
  - Technologiczne środki potwierdzania tożsamości oraz środki płatnicze
  - Bazy danych osobowych oraz komercyjnych
  - Systemy kontroli dostępu oraz wykrywania nadużyć

Obszary występowania zagrożeń



- Systemy profilowania użytkowników bazują na PII w celu identyfikacji potencjalnych problemowych podmiotów

Wprowadzenie

Przykłady praktycznych problemów

- System sprawdzania legalności oprogramowania, gdzie OS należąc do schematu podpisu grupowego może poinformować o fakcie posiadania licencji, bez ujawniania informacji o użytkowniku aplikacji
- Elektroniczny pieniądz

- System nadzoru ruchu sieciowego, który zbiera informacje o profilach użytkowników i informuje centralę podpisując komunikaty w sposób anonimowy zapewniając w ten sposób anonimowość (na pewnym poziomie) obserwowanemu internaucie
- Sieci sensorów w środowiskach sieci bezprzewodowych
- Smart metering

Jak pogodzić potrzebę kontroli oraz anonimowość użytkowników?

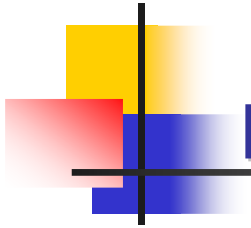
Jakie cechy powinien mieć dobry system monitorowania?

- Anonimowość obiektu należy zachować do momentu uzyskania pewności że zbieranie PII jest uzasadnione jako proces identyfikacji oraz wstęp do wyciągnięcia konsekwencji wobec obiektu
- Dane uzyskane w ramach zbierania PII muszą być wystarczające do identyfikacji obiektu i zapewnienia rozliczalności

Odwoływalna Anonimowość

"…unless the Internet Service Provider is in a position to distinguish with absolute certainty that the data correspond to users that cannot be identified, it will have to treat all IP information as personal data to be on the safe side…"

Opinion of WP136, April 2007



Podpis grupowy a anonimowość

- Umożliwia wysłanie komunikatu wiarygodnego z punktu widzenia odbiorcy (poprzez weryfikację względem dostępnego kryptograficznego materiału publicznego dla podpisu komunikatu)
- Umożliwia pozostanie anonimowym względem weryfikującego a nawet wobec zaufanego centrum certyfikującego grupę w przypadku posiadania odrębnego centrum zajmującego się „otwieraniem” podpisu
- Dojrzałość zagadnienia podpisu grupowego – istnieją poprawne i dające się zaimplementować schematy takie jak BBS04, BMW03

Podpis grupowy a anonimowość

Zagadnienie anonimowości w podpisie grupowym

- Akceptowalny podpis grupowy zapewnia pełną rozliczalność i pełną anonimowość
- Podpisujący jest nieznany do momentu dokonania na sygnaturze operacji OPEN przez GM
- Inni członkowie grupy nie mogą wskazać autora podpisu

Problemy:

- Większość schematów ma wydzieloną jednostkę GM (Group Manager), która ma uprawnienia do identyfikacji podpisującego.
- Poziom zaufania do zachowania anonimowości zależy od bezpieczeństwa GM czyli sprowadza się to do kontroli klucza prywatnego **gmsk.**
- Operacja usuwania członków grupy jest słabym punktem schematu gdyż zazwyczaj wymaga wymiany klucza publicznego i certyfikatów.
  - Problem weryfikacji podpisu uzależnia się od znajomości kluczy historycznych i czasu
  - Powstaje problem przechowywania kluczy historycznych dla potrzeb odwoływania anonimowości

Podpis grupowy

- Praktyczne metody poprawy ochrony anonimowości
  - Wydzielenie osobnej jednostki służącej do weryfikacji tożsamości (GOA Group Opening Authority)
  - Zabezpieczenie klucza prywatnego grupy (GM) lub klucza otwierającego GOA przez mechanizmy kontroli dostępu
    - Podział sekretu dla odblokowania funkcji JOIN oraz OPEN
    - PKI
    - Ochrona bazy certyfikatów członków grupy – Procedura OPEN zazwyczaj musi przeszukać bazę certyfikatów w celu dopasowania wartości otrzymanej w wyniku działania procedury

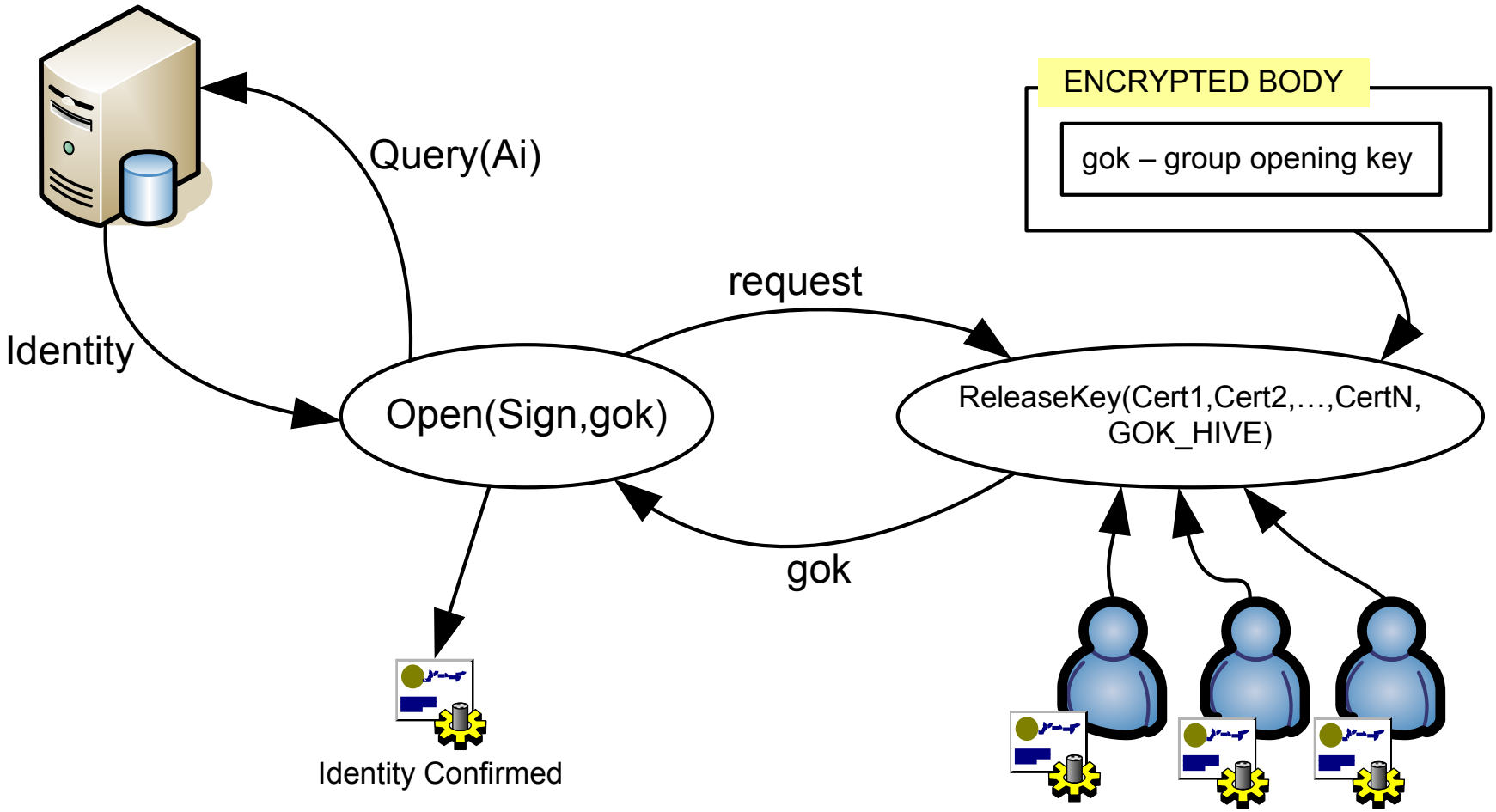
Przykład::

Podpis w schemacie ACJT ($c, s1, s2, s3, s4, T1, T2, T3$), klucz prywatny grupy: x

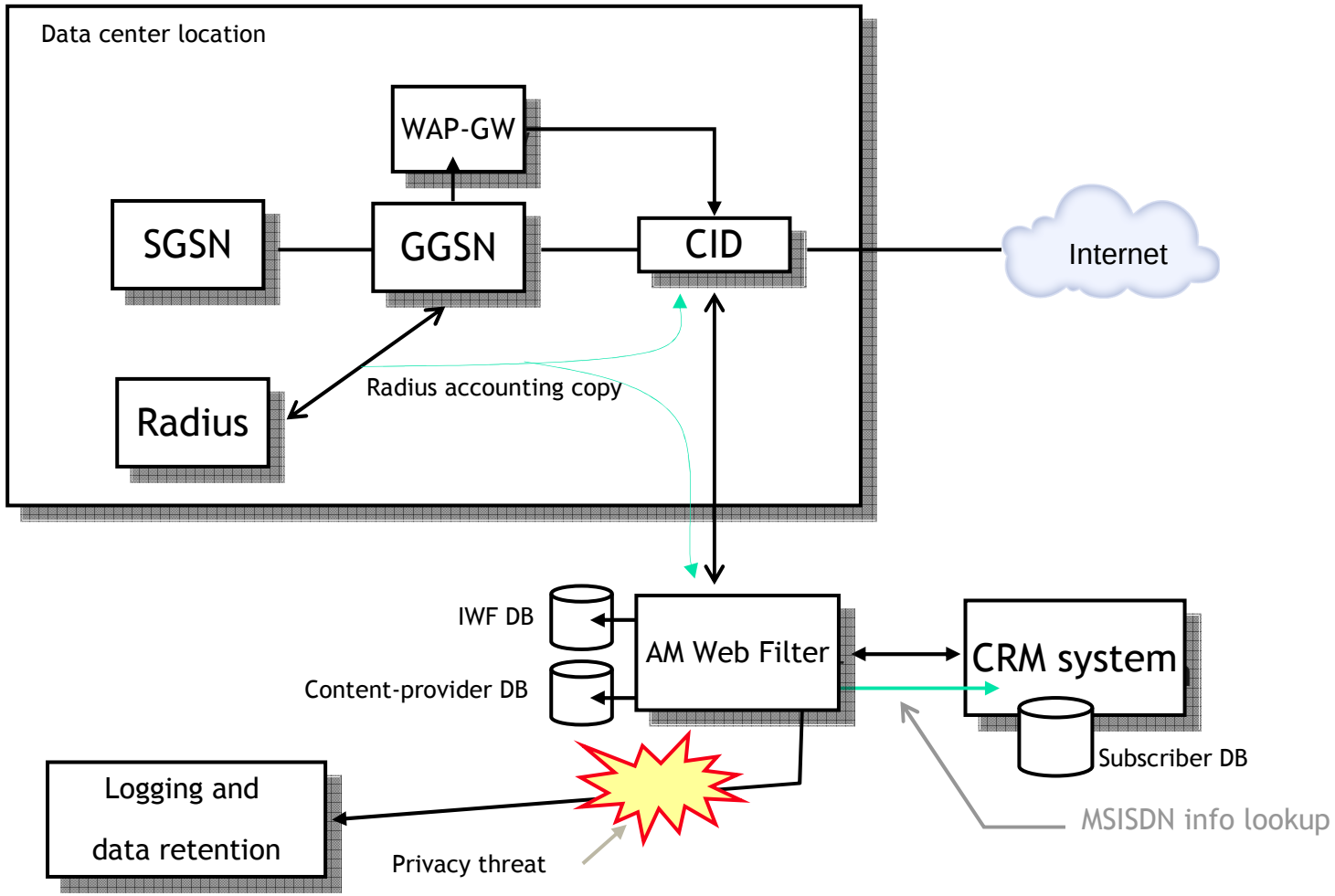
Weryfikacja w ramach procedury OPEN:

1. $A_i = T1/T2^x \pmod n$
2. Przeszukaj bazę certyfikatów i podaj tożsamość I gdzie I(Ai)

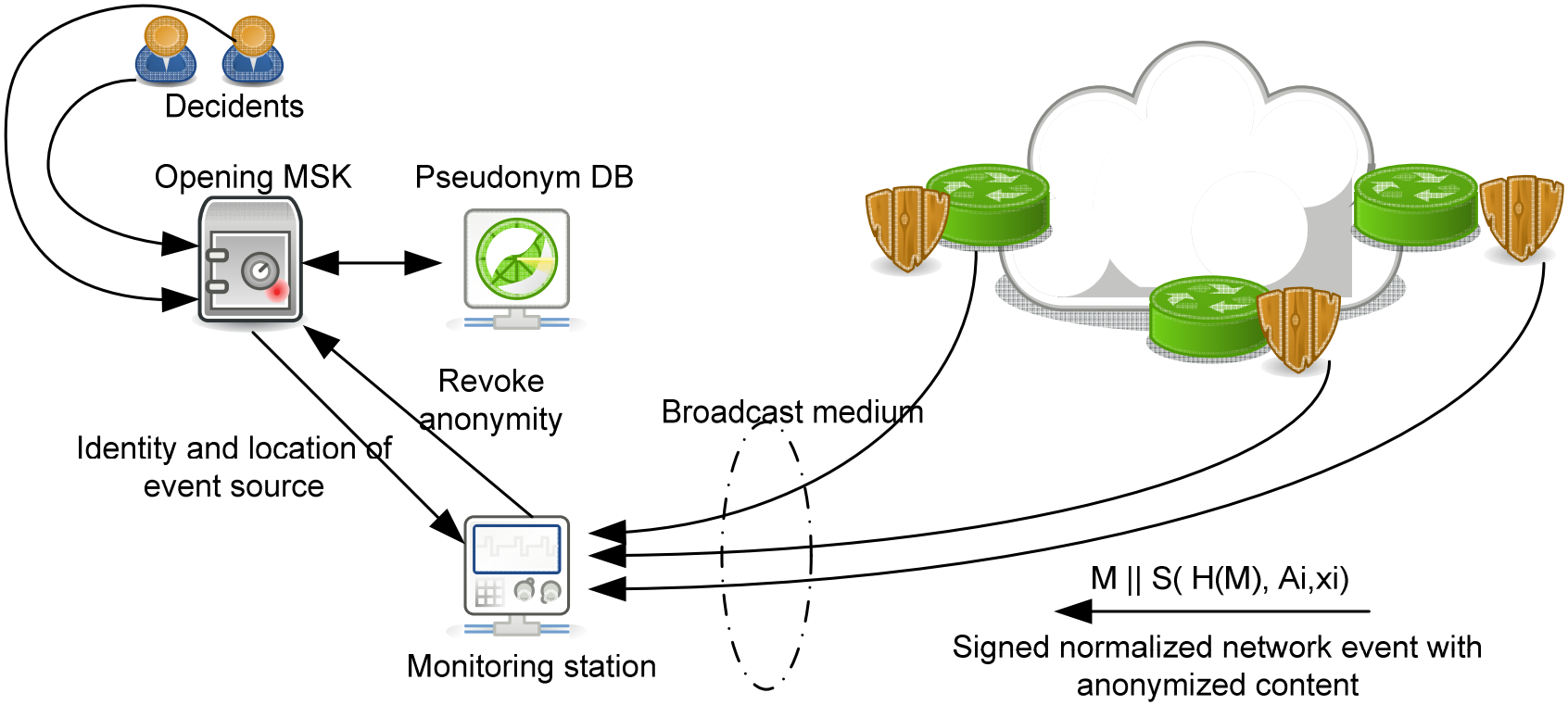
Propozycja schematu odwoływalnej anonimowości podpisującego



Przykład zastosowania
Filtrowanie URL u operatora mobilnego



Przykład zastosowania
Filtrowanie URL u operatora mobilnego



Bibliography

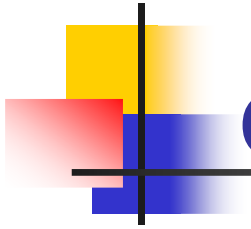
The beginning:

- D. Chaum and E. van Heyst "Group signatures". Advances in Cryptology — EUROCRYPT '91, volume 547 in LCNS, Springer

Online resources:

- http://www.larc.usp.br/~pbarreto/pblounge.html pairing-based crypto resources
- http://cseweb.ucsd.edu/users/mihir/papers/gs.html
- http://www.cs.bham.ac.uk/~gzw/bible/group-sign.htm !! Very good bobliography

- [BMW03] M. Bellare, D. Micciancio, and B. Warinschi. Foundations of Group Signatures: Formal Definitions, Simplified Requirements, and a Construction Based on General Assumptions. In: *EUROCRYPT 2003,* LNCS 2656, pp. 614-629. Berlin: Springer-Verlag, 2003.
- [ACJT2000] G. Ateniese, J. Camenisch , M. Joye, and G. Tsudik. A practical and provably secure coalition-resistant group signature scheme. In: Crypto'2000, LNCS 1880,. Springer Verlag, 2000.
- [BB04] Dan Boneh, Hovav Shacham. Group signatures with verifier-local revocation. In: *Proc. of the 11th ACM Conference on Computer and Communications Security (CCS 2004)*, pp. 168-177. ACM, 2004.
- [BBS04] Dan Boneh, Xavier Boyen, Hovav Shacham. Short Group Signatures. In: *CRYPTO 2004,* LNCS 3152, pp. 41-55. Springer-Verlag, 2004



Q&A

- dyskusja

Dziękuję za uwagę