**TNO Informatie- en Communicatietechnologie**

*Memorandum*

ICT
Eemsgolaan 3
Postbus 1416
9701 BK Groningen

www.tno.nl

T 050 585 70 00
F 050 585 77 57
info-ict@tno.nl

**Aan**
Projectleden FAIM (Federated Authentication and Identity Management)

**Van**
L Danes

**Onderwerp**
*idemix*: een pseudoniem-systeem, wat is het en wat gaat Luuk er mee doen?

**Datum**
9 maart 2007

**Onze referentie**

**E-mail**
luuk.danes@tno.nl

# idemix
## *een pseudoniem-systeem, wat is het en wat gaat Luuk er mee doen?*

## 1 Inleiding

*idemix* is een pseudoniem-systeem ontwikkeld door IBM Research[1].
Organisaties delen credentials uit aan gebruikers die zij kennen onder pseudoniemen. De privacy van de gebruiker wordt gewaarborgd, omdat de pseudoniemen en uitgegeven credentials onderling niet te koppelen zijn.

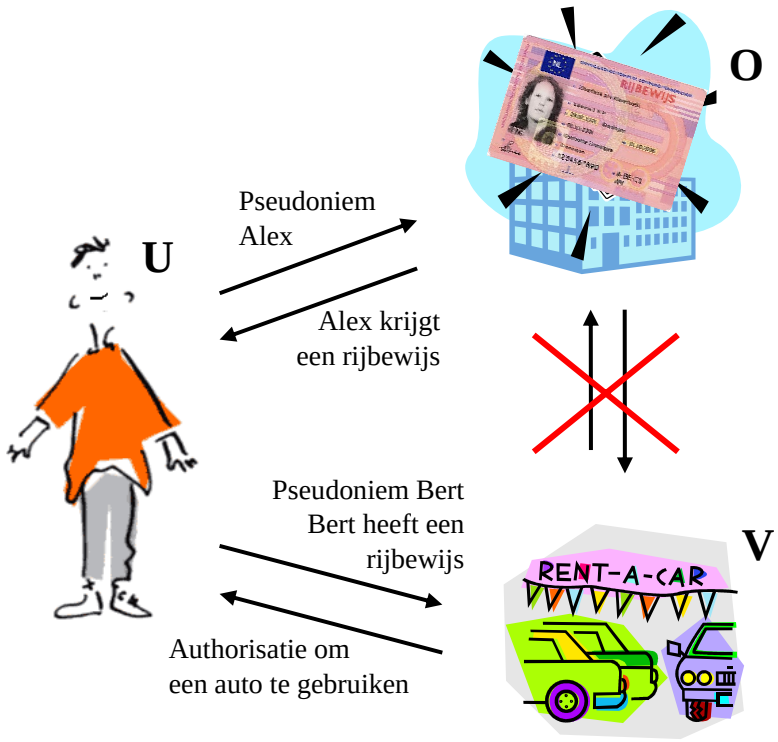
Het systeem bestaat uit gebruikers en organisaties. De organisaties geven credentials uit (een bewijs van een bepaald feit, bijvoorbeeld een rijbewijs, een bewijs van burgerschap, een bewijs van een bepaalde geldwaarde, een diploma,...) en/of controleren of een gebruiker een of meer bepaalde credentials bezit.
Voor een gebruiker is het mogelijk een credential onder een pseudoniem te verkrijgen bij een uitgevende organisatie, en dan de credential te tonen onder een ander pseudoniem aan een controlerende organisatie.
Ook al bundelen alle organisaties hun krachten, ze kunnen geen koppeling maken tussen het pseudoniem waaronder een credential is uitgegeven en het pseudoniem waaronder de credential ter controle is aangeboden.
Het is zelfs mogelijk het bezit van een credential meerdere keren aan een organisatie aan te tonen, zonder dat de organisatie weet dat het dezelfde gebruiker betreft.
Het systeem heeft bovendien eigenschappen die fraude - zoals namaken, uitlenen of doorgeven van credentials – onmogelijk maken of sterk ontmoedigen.

In dit document geef ik de eigenschappen van *idemix* en de acties binnen *idemix* weer. Daarop volgt een aantal mogelijke scenario's.
Aan het eind geef ik aan waar mijn onderzoek zich op richt.

---

[1] IBM Research heeft een website voor dit project:
http://www.zurich.ibm.com/security/idemix/
De software hiervoor geschreven wordt binnenkort als open source opgenomen in het Eclipse / Higgins Trust Framework Project: http://www.eclipse.org/higgins/

## 2 Voorbeeld




Ik heb onder pseudoniem Alex mijn rijbewijs-credential gehaald bij de rij-exameninstantie.
Als ik een auto wil huren bij een autoverhuur, dan willen ze weten dat ik een rijbewijs bezit en dat ik verzekerd ben. Ik kan er voor kiezen Bert te heten bij de autoverhuur. Met behulp van *idemix* kan ik dan aantonen dat ik een rijbewijs en een verzekeringsbewijs bezit. De autoverhuurder kan niet achterhalen onder welk pseudoniem ik het rijbewijs heb gehaald of onder welke naam ik geregistreerd sta bij de verzekering, zelfs niet als hij rechtstreeks gaat overleggen met de rij-exameninstantie of het verzekeringskantoor.

## 3 Basiseigenschappen

De basis-eigenschappen van *idemix* zijn de volgende:

1. Het is onmogelijk een credential voor een gebruiker na te maken, zelfs als gebruikers en organisaties samenwerken en een adaptieve aanval[2] uitvoeren.
   *De enige manier voor de gebruiker om een rijbewijs-credential te verkrijgen is door deze van de rij-exameninstantie aan te vragen onder het bij hen bekende pseudoniem.*
2. Het is onmogelijk een credential door te geven aan een andere gebruiker.
   Met doorgeven wordt bedoeld: een credential die een gebruiker heeft gekregen onder een eigen pseudoniem aan een pseudoniem van een andere gebruiker koppelen.
   *Ik kan de rijbewijs-credential die ik heb behaald, niet doorgeven aan een ander.*
3. Het is onmogelijk samen een credential te bemachtigen die een gebruiker alleen niet zou kunnen krijgen.
   *Ik kan niet door met anderen samen te werken een rijbewijs aanvragen en verkrijgen terwijl ik er geen recht op heb.*
4. Het systeem werkt de-centraal/peer-to-peer. Er zijn slechts enkele globale systeemparameters nodig. De gebruiker en een organisatie hebben geen andere partij nodig bij het afspreken van een pseudoniem of het afgeven van een credential, bovendien kan een gebruiker of organisatie in het systeem toetreden zonder een derde partij in te schakelen.
   *Als ik een pseudoniem afspreek met de rij-exameninstantie en mijn rijbewijs verkrijg zijn er niet meer partijen betrokken dan ikzelf en de instantie.*
5. Een organisatie kan niet meer van de gebruiker achterhalen dan het feit dat hij bepaalde credentials bezit, zelfs niet als verschillende organisaties samenwerken. Bovendien kan een organisatie later zelfs niet aantonen aan een ander dat de gebruiker een bepaalde credential bezit.
   *Nadat ik bij de autoverhuur heb aangetoond dat ik een rijbewijs-credential bezit weet de verhuurder niets meer dan dat ene feit, ook heeft hij geen gegevens waarmee hij meer informatie over mij kan achterhalen, zelfs niet door samen te werken met anderen of door de rij-exameninstantie te vragen.*
6. Het systeem is efficiënt, er is weinig communicatie nodig.
   *In mijn contact met een organisatie hoef ik weinig informatie uit te wisselen en het is ook niet nodig om ondertussen andere partijen in te schakelen.*

[2] Bij een adaptieve aanval wordt de tactiek voortdurend bijgesteld op basis van de gegevens die tijdens de aanval eerder zijn verkregen.

## 4 Extra mogelijkheden

1. Gebruikers worden ontmoedigd hun pseudoniemen en credentials uit te lenen. Met uitlenen wordt bedoeld: de getallen die nodig zijn om het bezit van een credential aan te tonen aan een ander geven, zodat hij/zij er (tijdelijk) gebruik van kan maken.
   Deze ontmoediging is op 2 manieren mogelijk in *idemix*:
   - Als je pseudoniemen en credentials uitleent, geef je de lener automatisch toegang tot een waardevolle geheime sleutel buiten het systeem.
   - Als je pseudoniemen en credentials uitleent, geef je de lener automatisch toegang tot al jouw pseudoniemen en credentials.

   *Als ik mijn pas met rijbewijscredential, of de getallen die nodig zijn om aan te tonen dat ik het rijbewijs bezit, uitleen, dan geef ik direct toegang tot meer waardevolle zaken, bijvoorbeeld mijn bankrekening.*
2. Het achterhalen van het pseudoniem waaronder de gebruiker een bepaald credential heeft gekregen. Hiervoor wordt er een door de gebruiker en controlerende organisatie vertrouwde derde partij ingeschakeld. De controlerende organisatie kan in geval van misbruik naar deze *lokale* revocatie-organisatie gaan en aan tonen dat er werkelijk sprake is van misbruik, en ontvangt dan het pseudoniem waaronder de credential is verkregen.
   *Als ik bijvoorbeeld met de auto tegen een paaltje aanrijd, dan kan het pseudoniem waaronder ik verzekerd ben achterhaald worden en de schade bij de verzekering verhaald worden.*
3. Het achterhalen van de identiteit van de gebruiker die een bepaalde credential bezit. Hiervoor wordt er een centrale vertrouwde derde partij ingeschakeld. De controlerende organisatie kan in geval van illegale activiteiten naar deze *globale* revocatie-organisatie gaan en aan tonen dat er werkelijk sprake is van illegale activiteiten, en ontvangt dan de identiteit van de bezitter van de credential.
   *Als de verhuurder van de auto te horen krijgt dat ik na een ongeluk ben doorgereden, dan kan hij mijn identiteit laten opvragen en kan ik gerechtelijk vervolgd worden.*
4. Het is mogelijk verschil te maken tussen one-show en multi-show credentials. *Een rijbewijs mag vaak getoond worden, een credential om bijvoorbeeld een artikel van een krantensite te downloaden mag maar eenmaal gebruikt worden.*
5. Met een credential kan een bepaalde getalswaarde worden meegestuurd. Er bestaan testen waarmee aangetoond kan worden dat het getal in een bepaald interval ligt, zonder dat de exacte waarde vrijgegeven hoeft te worden.
   *De verhuurder wil controleren of ik ouder dan 18 ben. Ik toon dan aan dat mijn geboortedatum-credential een datum bevat die meer dan 18 jaar geleden was, zonder de exacte geboortedatum te tonen.*

## 5 Acties

De volgende acties zijn de basis-acties in *idemix*, voor de extra mogelijkheden zijn er ook acties gedefinieerd (worden hier niet genoemd).
We bekijken de acties vanuit de gebruiker U.

**Pseudoniem maken met organisatie O**
FormNym(U,O)

het afspreken van een pseudoniem $N_O$ tussen U (user) en O (organization).

**Credential verkrijgen onder pseudoniem $N_O$, uitgegeven door O**
GrantCred($N_O$,O)

De gebruiker maakt een verbinding met organisatie O onder het pseudoniem $N_O$ en ontvangt een credential, tenzij de organisatie weigert de credential aan dit pseudoniem uit te geven.

**Aantonen van het bezitten van een pseudoniem $N_O$ en een bepaalde credential uitgegeven door O**
VerifyCred(V,$N_O$,O)

Organisatie V (verifier) controleert of de gebruiker van de huidige sessie een bepaalde credential van organisatie O bezit.
V krijgt het pseudoniem $N_O$ waaronder de credential is uitgegeven niet te weten.

**Aantonen onder pseudoniem $N_V$ van het bezitten van een pseudoniem $N_O$ met een bepaalde credential uitgegeven door O**
VerifyCredOnNym(V,$N_V$,$N_O$,O)

Organisatie V controleert of de gebruiker, waarmee hij zelf het pseudoniem $N_V$ heeft afgesproken, een bepaalde credential van organisatie O bezit. Bovendien controleert hij of het pseudoniem $N_O$ waaronder de credential is uitgegeven en het pseudoniem $N_V$ bij de zelfde gebruiker horen.
V krijgt het pseudoniem $N_O$ waaronder de credential is uitgegeven niet te weten.

## 6 Ideeën voor toepassingen van een elektronisch identiteitsbewijs binnen *idemix*

Het is een uitdaging om een elektronisch identiteitsbewijs (zoals de eNIK, de elektronische Nederlandse Identiteitskaart) de rol van de gebruiker in het *idemix*-systeem te laten vervullen.
Een elektronisch identiteitsbewijs is een pas met een chip (smartcard), deze kan binnen *idemix* de geheime sleutels voor de gebruiker bevatten.
Een aantal scenario's zijn dan mogelijk:

**Scenario A**

Ik wil een auto huren en toon mijn identiteitsbewijs bij het verhuurbedrijf. De verhuurder controleert de foto en eventuele andere gegevens en leest uit het pasje uit dat de burger een rijbewijs bezit en verhuurt de auto.
De verhuurder weet op dit moment niets meer dan het feit dat de burger een rijbewijs bezit en de gegevens die op het pasje zelf staan afgebeeld.
Als er nu met de auto een overtreding wordt begaan of de auto wordt niet teruggebracht, dan kan de verhuurder bij een aangewezen organisatie (de revocatie organisatie) alsnog de gegevens van de huurder achterhalen.

**Scenario B**

Bij de krantenkiosk (of krantenwebsite) koop ik prepaid 10 exemplaren. Ik krijg hiervoor 10 one-show credentials die ik kan tonen om een exemplaar mee te nemen of te downloaden.

**Scenario C**

Ik gebruik het elektronisch identiteitsbewijs als bankpas. Ik haal hiermee geld uit een betaalautomaat waarbij de pas met de bank mijn pseudoniem bij de bank communiceert en een credential overlegt dat ik lid ben bij de bank. Daarna doe ik boodschappen bij de supermarkt en gebruik mijn pas in een spaarsysteem, waarbij mijn pas mijn pseudoniem bij de supermarktketen aan het systeem verteld.
Als ik daarna op de bus stap gebruik ik mijn pas als OV-chipkaart.
*NB: in dit voorbeeld is de bank zowel uitgever en controleur van een credential.*

**Scenario D**

Op internet ga ik naar de website waar mijn email te lezen is. Doordat mijn pasje in een kaartlezer met de computer verbonden is, wordt ik door de website herkend en aangemeld onder mijn naam bij die emailwebsite. Als ik daarna een bericht wil plaatsen op een internetforum, wordt ik op die website ook automatisch ingelogd.
Ten slotte bestel ik bij een boekensite een boek waar ik eveneens automatisch wordt herkend. Ondertussen zorgt *idemix* ervoor dat het onmogelijk is voor de verschillende sites die ik bezoek om de verschillende aanmelding op dezelfde persoon terug te voeren.

Omdat de eNIK aan veel of alle Nederlandse burgers wordt uitgereikt en bovendien aan een identiteit gekoppeld is, waarbij de overheid aan een pasje een this-is-a-person credential kan uitreiken (en daarbij garant staat voor het bekend zijn van de eigenaar), is er potentie om deze pas te gebruiken binnen het pseudoniemsysteem van *idemix*.

## 7 Onderzoeksvraag

Afgelopen weken heb ik het systeem uitgeplozen en vooral de wiskundige principes erachter bestudeerd. Een aantal termen: strong RSA assumption, discrete log problem, decisional Diffie-Hellman assumption, zero-knowledge proofs of knowledge.

Het gebruiken van een elektronisch identiteitsbewijs binnen het systeem van *idemix* lijkt een interessante mogelijkheid. Een elektronisch identiteitsbewijs is eigenlijk niets meer dan een smartcard met beperkte kracht en opslag. *idemix* maakt daarentegen gebruik van behoorlijk zware wiskundige bewerkingen. De vraag die daaruit rolt is:

**Hoe kan het *idemix* protocol geïmplementeerd worden in een systeem waar gebruik gemaakt wordt van**

1. **een elektronisch identiteitsbewijs (smartcard) met beperkte computerkracht en geheugen**
2. **een terminal of een systeem bereikbaar via een terminal met relatief veel computerkracht en geheugen**

**waarbij het elektronisch identiteitsbewijs wel alle noodzakelijke geheime sleutels van de burger bevat en veilig afhandelt?**

Enkele concrete vragen die ik momenteel aan het bestuderen ben:

- Is het *idemix*-systeem aan te passen zodat er minder gegevens op de kaart opgeslagen hoeven te worden? Welke consequenties hebben deze aanpassingen voor de eigenschappen van het systeem?
- Is het rekenwerk dat de gebruiker moet doen op een veilige manier van de kaart naar de (krachtiger) terminal te verplaatsen, door bijvoorbeeld gebruik te maken van technieken als secure multiparty computation?
- Kan een organisatie verschillende credentials uitgeven aan een gebruiker onder steeds hetzelfde pseudoniem, omdat dit ook zal schelen in de opslag op de kaart?