ISSN 1879-9523
journal of chain-computerisation
information exchange for chain co-operation
Universiteit Utrecht

Professioneel artikel

Ketens en identiteit

J.H.A.M. Grijpink

Journal of Chain-computerisation
Information Exchange for Chain Co-operation

2012 – Volume 3, Art. #7

Ontvangen: 8 november 2012
Geaccepteerd: 1 december 2012
Gepubliceerd: 19 december 2012

2012 – Volume 3, Art. #7
URN:NBN:NL:UI:10-1-113980
ISSN: 1879-9523
URL: http://jcc.library.uu.nl/
Uitgever: Igitur publishing, in samenwerking met het Department of Information and Computing Sciences, Universiteit Utrecht

Ketens en identiteit

J.H.A.M. (Jan) Grijpink
Universiteit Utrecht, Nederland
grijpink.jham@gmail.com

Samenvatting: Handreikingen worden gepresenteerd voor het bestrijden van identiteitsproblemen in ketens. Een keten is een samenwerkingsverband van een groot aantal autonome organisaties en professionals om samen een dominant ketenprobleem aan te pakken waar men alleen geen grip op krijgt. In veel ketens vormen identiteitsproblemen een aspect van het dominante ketenprobleem. Identiteitsfraude is het met kwade bedoelingen gebruiken van de identiteit van iemand anders, om zo goederen of rechten te verwerven waarop men geen recht heeft. Sporen wijzen automatisch naar het slachtoffer, de schuldige verschuilt zich achter de misbruikte identiteit en blijft buiten schot. Daarom kan alleen preventie identiteitsfraude effectief verminderen door een fraudeur af te schrikken of hem op heterdaad te laten betrappen. Preventie in een ketenproces kan worden bereikt door gelijktijdige multifactor identiteitscontroles (token, PIN, transactiecode, enz.), omdat een identiteitsfraudeur ze niet allemaal tegelijk consistent kan manipuleren. Multifactor identiteitsverificatie in een gesloten interactieve communicatielus levert ook metadata (bijvoorbeeld de uitkomst van een berekening of een telefoonnummer) die ook kunnen worden gebruikt voor consistentiecontrole.

Trefwoorden: identiteit, identiteitsfraude, keten, ID protocol, multifactor identiteitscontrole, interactieve communicatielus

---

1 Hoofdlijnen

1. Veel ketens blijken een dominant ketenprobleem te hebben met **identiteit** als component. Het dominante ketenprobleem bepaalt welke **mate van eenduidigheid** bij aanduiding of herkenning noodzakelijk is.
2. **Identiteitsfraude** – met kwade bedoelingen bewust de schijn oproepen van een identiteit die niet bij je hoort – kan overal en op velerlei manieren plaatsvinden. Als een identiteitsfraude eenmaal is geslaagd op een zwakke plek in een bepaalde keten, verspreidt die zich ongemerkt naar andere ketens. De gevolgen zijn afhankelijk van de situatie waarin identiteitsfraude plaatsvindt.
3. Als identiteitsfraude slaagt, wijzen de **sporen** naar het **slachtoffer**, de dader blijft onzichtbaar en vaak onvindbaar. Daarom is alleen **preventie** effectief.
4. De voortschrijdende digitalisering geeft aan identiteitsfraude/identiteitsdiefstal minstens **drie nieuwe dimensies**, die de impact van identiteitsfraude vergroten en de bestrijding ervan frustreren: méér sporen, minder bewijs; olievlekwerking van identiteitsfraude; machtsverschuiving in een gedigitaliseer-de omgeving.

2 Toelichting

Ketens zijn tijdelijke patronen van samenwerking tussen grote aantallen min of meer autonome organisaties en professionals, afgedwongen door een dominant ketenprobleem. Omdat grootschalige stelsels zich anders gedragen dan kleinschalige, zoals organisaties, maken we niveauvergissingen. Daardoor kloppen

aannames bij systeemontwikkeling en informatiemanagement vaak niet en komen verwachtingen niet uit.

Waar we spreken van identiteit bedoelen we de maatschappelijke identiteit, een aantal officiële kenmerken waarmee we een persoon of object kunnen aanduiden. Veel ketens blijken een dominant ketenprobleem te hebben met identiteit als component. Welke mate van eenduidigheid bij aanduiding of herkenning noodzakelijk is, hangt af van het dominante ketenprobleem.

In onbeheersbare ketenprocessen is meer aandacht nodig voor identiteitsfraude/identiteitsdiefstal, d.i. met kwade bedoelingen bewust de schijn oproepen van een identiteit die niet bij je hoort. Afhankelijk van het dominante ketenprobleem kan dit die keten in opspraak brengen. In de strafrechtketen heeft aliasmisbruik (identiteitsfraude) in de loop van de tijd geleid tot ondermijning van de strafrechttoepassing (verkeerde dader, verkeerde straf) en ernstige vervuiling van het strafbladregister waardoor verkeerde personen worden aangehouden of gearresteerd. In medische ketens worden gegevens van de ID-fraudeur vastgelegd in het dossier van de officiële BSN-houder, met soms ernstige gevolgen.

Meeliften op een andere identiteit is meestal niet moeilijk, levert bij slagen veel voordeel en bij mislukken vrijwel geen nadeel. De voortschrijdende digitalisering in een mobieler en anoniemer wordende samenleving geeft aan identiteitsfraude/identiteitsdiefstal minstens drie nieuwe dimensies die de impact vergroten en de bestrijding ervan frustreren:

Méér sporen, minder bewijs. Bij een geslaagde identiteitsfraude leiden sporen naar het slachtoffer, de dader blijft vaak onvindbaar. Alleen preventie is effectief, maar veel procedures bevatten nauwelijks preventieve onderdelen.

Olievlekwerking van identiteitsfraude. Identiteitsfraude verspreidt zich als een olievlek tot in de kleinste administratieve haarvaten van allerlei maatschappelijke processen waar men de geslaagde primaire identiteitsfraude vaak niet meer kan doorzien.

Machtsverschuiving in een gedigitaliseerde omgeving. Traditioneel is de controleur de baas, de gecontroleerde moet reageren. In digitale procedures of bij gebruik van digitale hulpmiddelen is de gecontroleerde de baas. Hij kan bijvoorbeeld een noodprocedure uitlokken met een kapotgemaakte chip.

Preventie moet gelegenheid tot identiteitsfraude beperken en identiteitsfraudeurs afschrikken of tegen de lamp laten lopen. Dit is o.a. te bereiken door 'vaker te laten kloppen' (meerdere controle-instrumenten tegelijk gebruiken (pincode, transactiecode, etc.), omdat een identiteitsfraudeur niet in staat is ze allemaal tegelijkertijd en consistent naar zijn hand te zetten. Als men 'vaker kloppen' toepast in een gesloten interactieve communicatielus, kan men met de retourgegevens (bijvoorbeeld het resultaat van een berekening of een telefoonnummer) weer de consistentie bewaken.

3 Handreikingen

1. Werk bij ontwikkeling en exploitatie van grootschalige stelsels vanuit de vooronderstelling van massaal gebruik en moeilijk beheersbare condities. Zoek naar onverwachte risico's.
2. Ontwikkel ketenspecifieke ID-protocollen en test ze op bestendigheid tegen identiteitsfraude.

3. Zorg voor variatie en verrassingen in ID-procedures om identiteitsfraudeurs onzeker te houden over hun succes. Dat schrikt af.
4. Organiseer gesloten, interactieve communicatielussen die bestand zijn tegen identiteitsfraude. Maak daarin steeds gebruik van meerdere instrumenten tegelijk: 'vaker kloppen'.
5. Gebruik daarbij onafhankelijke gegevens. Gegevens die de te controleren persoon meebrengt zijn vaak niet (meer) bruikbaar voor controle.

Biografie: Prof. dr mr Jan Grijpink (1946) studeerde economie (1969) en rechten (1971) aan de Rijksuniversiteit Groningen. In 1976 sloot hij de postdoctorale opleiding organisatiekunde (SIOO) met succes af. De doctorsgraad werd hem in 1997 door de Technische Universiteit Eindhoven verleend, op basis van zijn proefschrift *Keteninformatisering*. In 2004 werd hij benoemd tot (parttime) bijzonder hoogleraar aan de faculteit Bètawetenschappen van de Universiteit Utrecht met als leeropdracht *Keteninformatisering in de Rechtstaat*. Hij was tot zijn pensioen/emeritaat in 2011 naast zijn hoogleraarschap werkzaam bij het ministerie van Veiligheid en Justitie (1984-2011), laatstelijk als raadadviseur verbonden aan de directie Strategie, met specialisatie in informatiestrategie. Momenteel is hij als senior adviseur verbonden aan de stichting PBLQ/HEC te Den Haag. Hij is initiatiefnemer en coördinator van het Platform Keteninformatisering en hoofdredacteur van het Journal of Chain-computerisation.

Literatuurverwijzingen

Grijpink, J. H. A. M. (2008). Checklist Identiteitsfraude. *Checklisten Informatie-management, 2008-2, 1.B.7*. Den Haag: Sdu Uitgevers.

Grijpink, J. H. A. M. (2006a). Criminal Records in the European Union, the challenge of large-scale information exchange. *European Journal of Crime, Criminal Law and Criminal Justice*, *14*(1), 1-19. Leiden: Brill Academic Publishers.

Grijpink, J. H. A. M. (2006b). Identiteitsfraude en overheid. *Justitiële Verkenningen*, *7*(6), 37-57. Den Haag: WODC/Boom Juridische Uitgevers.

Grijpink, J. H. A. M. & Plomp, M. G. A. (red.) (2009), *Kijk op ketens. Het ketenlandschap van Nederland*. Den Haag: Centrum voor Keteninformatisering BV.

Grijpink, J. H. A. M. (2011a). Public Information Infrastructures and Identity Fraud. In S. van der Hof & M. Groothuis (red.), *Innovating Government. Normative, Policy and Technological Dimensions of Modern Government*, pp. 363-381. The Hague: TMC Asser Press/Springer Verlag.

Grijpink, J. H. A. M. & Plomp, M. G. A. (2011b). Combating Identity Fraud in the Public Domain: Information Strategies for Healthcare and Criminal Justice. Proceedings of the 11th European Conference on E-Government (pp. 451-458). Reading UK: Academic Publishing Ltd.

Grijpink, J. H. A. M. (2012). Large-scale Information Exchange: Breaking Views and Challenges. In I. Snellen, M. Thaens & W. Van de Donk (red.), *Public Administration in the Information Age: Revisited,* pp. 182-204.