Close-up van Smals: een octrooiaanvraag!

Vitalink…omdat medische gegevens de grootste vertrouwelijkheid verdienen

Voor de eerste keer in haar geschiedenis heeft Smals een octrooiaanvraag ingediend om een concept te beschermen dat zij uitwerkte: de Secure Medical File Access. Dit systeem zorgt ervoor dat enkel de eindgebruikers de medische gegevens kunnen lezen die op beveiligde wijze opgeslagen liggen op het Vitalinkplatform. Johan Loeckx en Julien Cathalo van het team Onderzoek beschrijven het ontstaan van deze vondst…

Foto's: Nancy Boodts

Gehurkt van links naar rechts: Koen Vanderkimpen en Johan Loeckx (Onderzoek), Evelyne De Busschere en Denis Vandersteene (UAM). Staand van links naar rechts: Grégory Ogonowski, Julien Cathalo en Dirk Deridder (Onderzoek), David Tillemans (Interne veiligheid), Ludovic Desmet (UAM).

Van links naar rechts: Bob Lanno (Teamleader Onderzoek), Johan V Klantenbeheer & Onderzoek).

De medewerkers betrokken bij de ontwikkeling van "Threshold encryptie met een sterke granulariteit".

Een schets van de context

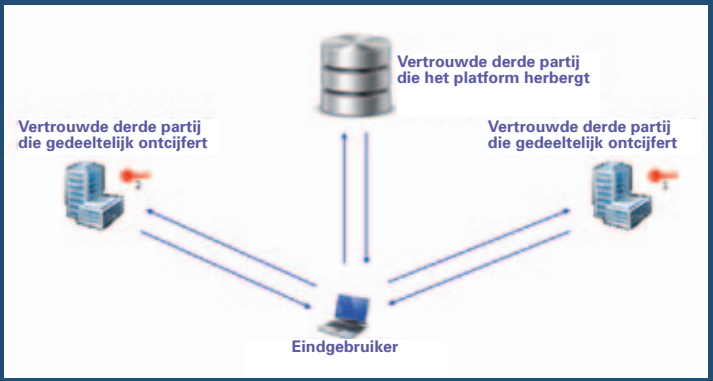
Vitalink is een initiatief van de Vlaamse regering. De coördinatie van het project werd toevertrouwd aan het Vlaams Agentschap Zorg & Gezondheid (VAZG) dat samenwerkt met partners zoals eHealth. Het Vitalinkplatform[1] heeft tot doel elektronische gegevens te delen tussen de eerstelijnsactoren in de sector van de gezondheidszorg: artsen, verplegers, apothekers, patiënten… Het einddoel is om via een vlottere samenwerking te garanderen dat de patiënt overal de beste zorgen krijgt.

Een lastige vraag...

Onze collega's van de sectie Onderzoek werden uitgenodigd een echte hersenbreker op te lossen. Hoe ervoor zorgen dat de opgeslagen gegevens op Vitalink op zo'n manier beveiligd worden dat een vertrouwde derde partij de gegevens kan encoderen, decoderen of herbergen, maar ze zelf niet kan lezen? Het was de bedoeling dat enkel de eindgebruikers de decodering konden uitvoeren en de gegevens "ongecodeerd" konden zien. Uren brainstormen, nadenken en ervaring uitwisselen hebben uiteindelijk tot een oplossing geleid…

Eureka: threshold encryptie met sterke granulariteit!

De vertrouwelijkheid van de gegevens wordt gegarandeerd door het gebruikte type encryptie: **threshold encryptie**. Concreet betekent dit dat het systeem een interventie nodig heeft van twee vertrouwde "Third Parties" (derde partijen) om de gegevens te decoderen. Men spreekt over een threshold (of drempel) van twee in dit geval. Elk van die Third Parties verschaft slechts een deel van de sleutel, wat verklaart waarom ze zelf niet in staat zijn om de gegevens te lezen. Enkel de eindgebruiker



1. Aanvankelijk heette het project Eerstelijnskluis.

Close-up van Smals: een octrooiaanvraag!

ontvangt de twee delen van de sleutel en kan de gegevens decoderen. Een derde vertrouwde Third Party herbergt het platform.

De oplossing aangereikt door onze onderzoekers kenmerkt zich ook door een **toegangscontrole met een sterke granulariteit**. Dit betekent dat de toegangsrechten van de eindgebruikers bepaald worden per gegevensveld binnen eenzelfde dossier. Dit gebeurt op een zeer verfijnde manier. Een apotheker, bijvoorbeeld, zal toegang hebben tot het dossier van een van zijn patiënten, maar zal niet evenveel gegevens kunnen lezen als de arts van de patiënt.

Goed nieuws ook voor de liefhebbers van hergebruik: het concept uitgewerkt door de onderzoekers van Smals is voldoende generiek om toegepast te worden bij andere projecten voor het opslaan van gegevens.

y (Onderzoek), Paul Stijfhals
Vercruysse (Directeur

Hoe zal dit verlopen?

Laten we een concreet voorbeeld nemen. Een arts kan dankzij de software geïnstalleerd op zijn pc een gegeven invoeren in het medisch dossier van een patiënt. Op het moment dat hij het gegeven bewaart op zijn werkstation zal de software het gegeven coderen met een publieke sleutel. Het gegeven zal via het internet overgebracht worden naar Vitalink onder een gecodeerde vorm. Wanneer een andere gebruiker dit gegeven wil decoderen, zal het systeem per gegevensveld zijn toegangsrechten tot het patiëntendossier nagaan. Als de gebruiker toegang mag hebben tot dit gegeven, dan zal de software beide vertrouwde Third Parties, die instaan voor de decodering, vragen om hun deel van de privésleutel door te geven. De software van de gebruiker zal de twee delen van de privésleutel ontvangen, ze combineren en zo het gegeven decoderen.

De talrijke voordelen van deze oplossing

Deze oplossing zal nóg meer veiligheid en vertrouwelijkheid bieden dan de oplossing van de bankensector. Het gegeven zal al geëncodeerd worden wanneer het wordt bewaard op het werkstation van de gebruiker en niet op het moment dat het wordt doorgestuurd. Bovendien zal geen enkele vertrouwde Third Party dit gegeven kunnen decoderen.

Het Vitalinkplatform zal 24 uur op 24 en 7 dagen op 7 beschikbaar zijn en over een grote "schaalbaarheid" beschikken ("scalability" in het Engels). Het platform zal met andere woorden ook bij een sterke stijging van de vraag dezelfde functionaliteiten en prestaties behouden. Om de vereiste beschikbaarheid en schaalbaarheid van het platform te garanderen, is Smals een uitdaging aangegaan door de nieuwe technologie GigaSpaces te gebruiken (zie kader).

Van idee tot concrete oplossing

In december 2010 moesten de onderzoekers het raadsel oplossen. Begin januari 2011 stelden ze een oplossing voor gebaseerd op threshold encryptie. Van half januari tot half april werkten ze het concept verder uit, legden ze de vereisten vast en werkten ze de architectuur uit. Aangezien er geen "software library"[2] bestond voor de threshold encryptie, hebben ze zelf de softwarecomponenten moeten ontwikkelen. Ze ontwikkelden een proof of concept met fictieve gegevens. Ze werkten in Java met de tool GigaSpaces. Voor de infrastructuur gebruikten ze de 6 servers van het labo van de sectie Onderzoek. De twee vertrouwde derde partijen voor de decodering werden geherbergd in de Amazon-cloud, wat ervoor zorgde dat men tests kon uitvoeren op internet.

Onze onderzoekers hebben samengewerkt met het team User Access Management (UAM) van Denis Vandersteene voor de ontwikkeling van een toegangscontrole met sterke granulariteit.

In juni 2011 kon het echte bouwproject van Vitalink beginnen met de steun van onze onderzoekers en onder de leiding van projectleider Sven Akkermans.

De oplossing uitgewerkt voor Vitalink was zo innovatief dat Smals een octrooiaanvraag indiende bij het Europees Octrooibureau. Het afronden van zo'n dossier vergt meerdere jaren.

Het platform en een pilootproject klaar in 2013

De aanmaak van Vitalink zou eind maart 2013 beëindigd moeten zijn. 400 artsen zullen toegang hebben tot een pilootproject: het medicatieschema. Laten we het voorbeeld nemen van een patiënt die medicijnen voorgeschreven krijgt door zijn arts. De verpleger die hem thuis verzorgt zal in Vitalink kunnen aanduiden hoe de patiënt reageert op de voorgeschreven medicijnen. Deze informatie zal voor de dokter nuttig zijn om eventueel de behandeling aan te passen. Elke gebruiker zal naargelang zijn profiel enkel tot bepaalde gegevensvelden toegang krijgen. De privacy van de patiënt zal gerespecteerd worden en een beter overleg tussen de zorgverleners is gegarandeerd. Andere applicaties zullen later geïntegreerd worden in het platform. Om de evolutie van het project te volgen, kijkt u naar www.vitalink.be!

Interview: **Nancy Boodts**

2. Online bibliotheek waar herbruikbare softwarecomponenten opgeslagen zijn.

Een woordje uitleg over GigaSpaces…

Ter gelegenheid van het onderzoek voor Vitalink werd het GigaSpaces Competence Center opgezet. Het Middlewareteam, onder leiding van Alain Couniot, werkt in dit kader nauw samen met de sectie Onderzoek, geleid door Paul Stijfhals.

Het Gigaspaces-platform biedt een geavanceerde support om zeer performante systemen op te stellen qua reactietijd, aantal transacties en schaalbaarheid. Het grote voordeel van GigaSpaces vergeleken met de traditionele toepassingsservers is dat het een lichte en geïntegreerde oplossing biedt. In de toekomst zal Smals applicaties kunnen ontwikkelen die een zeer hoog beschikbaarheids- en performantieniveau vereisen, alsook een elastische schaalbaarheid.

In de loop van het 2e trimester zal de sectie Onderzoek een informatiesessie houden over de XTP-platformen (eXtreme Transaction Processing). GigaSpaces zal er als praktisch voorbeeld gebruikt worden.