notitie

FORUM STANDAARDISATIE 10 juni 2015
Agendapunt 2. Open standaarden, lijsten
Stuk 2E Intake-advies voor Kerberos, versie 5

Advies

Het Forum Standaardisatie wordt geadviseerd om de aangemelde standaard Kerberos niet in behandeling te nemen voor opname op de lijst.

Daarnaast is het advies om de toelichting op het functioneel toepassingsgebied van SAML (dat op de 'pas toe of leg uit'-lijst staat) aan te vullen om zodoende het verschil tussen Keberos en SAML te verduidelijken.

Toelichting
Kerberos is een standaard voor single-sign-on (hierna: SSO) op besloten netwerken (zoals een LAN binnen een organisatie). Kerberos wordt breed gebruikt bij overheidsorganisaties binnen de eigen (kantoorautomatiserings-) netwerken. Bijvoorbeeld RDW en Servicecentrum Drechtsteden gebruiken de standaard. De standaard is echter niet van toepassing bij gegevensuitwisseling tussen overheidsorganisaties en voldoet daarom niet aan de criteria voor inbehandelname.

Op de lijst staat ook de Single Sign On standaard SAML. SAML richt zich echter, kort gezegd, op SSO bij webapplicaties. Het advies is om in de toelichting op het functioneel toepassingsgebied van SAML deze aan te vullen met een toelichting waarin Kerberos meer voor de hand liggend is.

Toelichting

1. Aanmelding, intakegesprek en toetsingsprocedure

Op 16 april 2015 is door Mike van Dijk van Greenvalley de standaard Kerberos versie 5 release 1.13.1 aangemeld voor de lijst met open

standaarden. De aanmelder heeft als doel de standaard een aanbevolen standaard te maken.

Op 30 april 2015 heeft een intakegesprek plaatsgevonden met de aanmelder. In dit gesprek is de aanmelding besproken. Hierbij is gekeken of alle basisinformatie aanwezig is en of de standaard voldoet aan de criteria voor inbehandelname. Daarnaast is vooruitgeblikt op de procedure.

Experts, betrokken bij de adoptie-evaluatie van SAML, zijn naar aanleiding van het intakegesprek gevraagd naar hun kennis over Kerberos en de relatie tot SAML. Het intakegesprek gaf hier niet voldoende duidelijkheid over. De reacties hebben inhoudelijk inzicht gegeven over de twee standaarden, maar onvoldoende over de relatie tussen de standaarden. De feitelijke kennis van de experts is gebundeld en indien mogelijk opgenomen in dit intakeadvies.

2. Korte beschrijving standaard

Waar gaat de standaard over?
De standaard is een single-sign-on (hierna: SSO) authenticatieprotocol voor besloten netwerkomgevingen, oftewel binnen een organisatie. Gebruikers kunnen zich door verificatie van hun identiteit binnen de netwerkomgeving eenmalig aanmelden, in plaats van meerdere keren, om toegang te krijgen tot verschillende client/server-applicaties.

Onder andere het veelgebruikte Active Directory van Microsoft gebruikt Kerberos. Active Directory zorgt voor het beheer van gebruikersrechten en instellingen binnen Windows-omgevingen in een netwerk. Dit betekent dat sprake is van gebruik van de standaard binnen organisaties. Web-authenticatie wordt niet ondersteund door deze standaard.

Wie beheert de standaard?
De standaard wordt beheerd door het Amerikaanse Massachusetts Institute of Technology (hierna: MIT, web.mit.edu/Kerberos). MIT heeft de standaard ontwikkeld als een oplossing voor beveiligingsproblemen binnen een netwerkomgeving. De belangrijkste beveiligingsproblemen volgens MIT waren het niet hebben van zekerheid over veilige toegang met SSO, gebrek aan flexibiliteit en het gebruik van de mogelijkheid om andere veiligheidsraamwerken en wachtwoord-verminderende authenticatiemechanismen te kunnen integreren.

Waarom is de standaard aangemeld voor aanbevolen?
De standaard wordt door organisaties vaak gebruikt naast standaarden die al op de lijst staan, zoals Security Assertion Markup Language (hierna: SAML). Door de standaard op de aanbevolen lijst te plaatsen verwacht de aanmelder dat de standaard sneller in overweging wordt genomen. Door de interne toepassing van de standaard, valt plaatsing op de lijst van het Forum Standaardisatie buiten de scope van de lijst. (zie ook: 7*. Functionele use case*)

3. Criteria voor inbehandelname

Om een standaard in behandeling te nemen moet de standaard vallen binnen de scope van de lijst. Hiervoor gelden drie criteria:

1. Is de standaard toepasbaar voor elektronische gegevensuitwisseling tussen (semi-)overheidsorganisaties en bedrijven, tussen (semi-)overheidsorganisaties en burgers of tussen (semi-)overheidsorganisaties onderling?

Nee, doordat de standaard binnen een besloten netwerkomgeving wordt gebruikt zullen andere partijen dan de organisatie zelf hier geen onderdeel van zijn. Wel zal het eenmalig uitvragen van gebruikersgegevens binnen de organisatie bevorderd worden.

2. Is het beoogde functioneel toepassingsgebied en het organisatorisch werkingsgebied van de standaard, voldoende breed om substantieel bij te dragen aan de interoperabiliteit van de (semi-)overheid?

Ja in de zin dat een eventuele toepassing van de standaard, client/server-authenticaties omvat. Dit betekent dat organisaties die kiezen voor deze standaard vrijwel alle client/server-authenticaties kunnen uitvoeren met deze standaard, mits de applicatie daartoe geschikt is. Dat maakt de standaard geschikt voor iedere organisatie.

Nee in de zin dat er geen sprake is van een éénduidig interoperabiliteitsprobleem. Ook na navraag bij de experts betrokken bij de adoptie-evaluatie van SAML was er geen duidelijke casus aan te wijzen waar uit blijkt dat er interoperabiliteitsconflicten zijn.

3. Is het zinvol de standaard op te nemen, gezien het feit dat deze niet al wettelijk verplicht is voor het beoogde functioneel toepassingsgebied en organisatorisch werkingsgebied?

Ja, de standaard is niet wettelijk verplicht.

<u>Conclusie</u>
De standaard voldoet *niet* aan de criteria voor inbehandelname. De experts die de standaard SAML bij de adoptie-evaluatie getoetst hebben aan de inhoudelijke criteria. Zij geven aan dat Kerberos mogelijk wel op de lijst met aanbevolen standaarden kan worden geplaatst om zodoende het onderscheid met SAML helderder te maken.

4. Toetsing kansrijkheid procedure

Het Forum Standaardisatie wil voorkomen dat er standaarden in procedure worden genomen, waarvan bij voorbaat al bekend is dat deze in de expertronde of consultatieronde zullen stranden op één van de inhoudelijke criteria. Daarom heeft de procedurebegeleider de beantwoording van de criteriavragen nagelopen, waar mogelijk zelf aangevuld en vervolgens besproken met de indiener.

1. Open standaardisatieproces

De ontwikkeling en het beheer van de standaard moeten op een open, onafhankelijke, toegankelijke, inzichtelijke, zorgvuldige en duurzame wijze zijn ingericht.

Het standaardisatieproces is voldoende open. Het specificatiedocument en het ontwikkel- en beheerproces is kosteloos toegankelijk (http://web.mit.edu/kerberos/krb5-1.13/).

MIT is een non-profit organisatie en heeft een neutrale positie als universiteit. De continuïteit van MIT als beheerder staat niet ter discussie. De Amerikaanse origine kan ervoor zorgen dat belangen van de Nederlandse overheid niet specifiek vertegenwoordigd zijn, tot op heden is dit geen belemmering geweest.

2. Toegevoegde waarde
De interoperabiliteitswinst en andere voordelen van adoptie van de standaard wegen overheidsbreed en maatschappelijk op tegen de kosten, de risico's en nadelen. Voor elk van de te onderscheiden stakeholders (overheid, bedrijven en burgers) afzonderlijk zouden de baten voor de informatievoorziening en de bedrijfsvoering op moeten wegen tegen de kosten. Verder moeten de risico's aan overheidsbrede adoptie van de standaard (beveiliging, privacy) acceptabel zijn.

Er is binnen organisaties behoefte aan SSO-oplossingen. De keuze dat Kerberos naast andere vergelijkbare standaarden gebruikt wordt is herkenbaar bij organisaties. Het verplichtende karakter van SAML kan er voor zorgen dat om die reden Kerberos onterecht niet gekozen wordt, terwijl SAML niet met dit toepassingsgebied op de lijst is geplaatst. Er bestaat behoefte bij de indiener en bij de bevraagde experts aan duiding van het onderscheid tussen SAML en Kerberos. Het verplichtend voorschrijven van de standaard is niet nodig daarom zou aan Kerberos of de 'aanbevolen' status toegekend kunnen worden en/of de toelichting op het functioneel toepassingsgebied van SAML aangevuld kunnen worden. Gezien de criteria voor inbehandelname wordt het laatste geadviseerd.

De implementatiekosten en -tijd zijn laag (vergelijkbaar met DNSSEC) indien client/server-applicaties reeds geschikt zijn (geïntegreerd in de broncode) voor gebruik van Kerberos versie 5. Deze implementatiekosten zijn van toepassing op het reeds beschreven functioneel toepassingsgebied bij 3.2. De implementatietijd betreft een aantal dagen.

De standaard is op uitzondering van een zevental landen voor iedereen te gebruiken. Er zijn open source en gesloten broncode implementaties, wat bijdraagt aan leveranciersonafhankelijkheid. Kerberos is gericht op veiligheid van gebruikersgegevens bij authenticatie en SSO. Er zijn geen beveiligings- en privacyissues bekend.

3. Draagvlak
Aanbieders en gebruikers moeten voldoende ervaring hebben met de implementatie en het gebruik van de standaard.

De aanbieders zijn de grote leveranciers van operating systemen (o.a. Apple, Microsoft, Oracle, Red Hat en Google).

Na rondvraag bestaat het beeld dat de toepassing van de standaard met name internationaal maar ook binnen het beschreven organisatorisch werkgebied redelijk gangbaar is. Zo maakt de RDW, binnen de eigen besloten netwerkomgeving gebruik van Kerberos 5 als SSO-toepassing voor Windows-gerelateerde toepassingen. Voor andere interne diensten is dit SAML 2.0. Naar buiten toe maakt de RDW voor diensten ook gebruik van SAML.

Daarnaast zijn er verschillende leveranciers zoals (Funatic en Greenvalley) die als marktpartij ondersteuning leveren bij implementatie van SSO-toepassingen. Binnen de zorg zetten zij Kerberos 5 soms in binnen intranetomgevingen. Bijvoorbeeld waar voorheen Microsoft's NTLM werd gebruikt.

Een voorziening voor toetsing van de conformiteit van een implementatie is niet voorhanden.

4. Opname bevordert adoptie
De opname op de lijst moet een geschikt middel zijn om de adoptie van de standaard te bevorderen.

De standaard is aangemeld voor de aanbevolen en 'pas toe of leg uit' lijst. Tijdens het intakegesprek kwam de aanvrager zelf tot de conclusie de aanbevolen lijst aannemelijker te vinden, door het ontbreken van het verplichtende karakter. Het doel van de aanmelding is om te informeren en daarmee onbedoelde afwijkende keuzes te voorkomen.

<u>Conclusie</u>
Het struikelblok is het toepassingsgebied van de standaard. Kerberos richt zich op SSO binnen een besloten netwerk. SSO bij web-applicaties vindt onder andere plaats met SAML. Over toepassing van Kerberos buiten een besloten netwerk is onvoldoende informatie bekend geworden tijdens de intake.

5. Samenhang

Forum Standaardisatie wil weten of de aangemelde standaard samenhangt met standaarden die reeds op de lijst zijn opgenomen, of standaarden die voor toetsing in aanmerking komen. Uit de intake moet duidelijk worden of dit gevolgen heeft voor de toetsing en eventuele opname van de aangemelde standaard.

1. Bestaat er samenhang tussen de aangemelde standaard en de verplichte ('pas-toe-of-leg-uit') standaarden die reeds op de lijst zijn opgenomen en wat betekent dit voor de toetsing en eventuele opname van de standaard?

   Er zijn raakvlakken met SAML 2.0. SAML wordt gebruikt voor SSO bij web-applicaties en buiten besloten netwerken. Dat wil zeggen dat een gebruiker na eenmalig inloggen via zijn browser toegang krijgt tot verschillende diensten van verschillende partijen. Ook is

zoals in het eerder genoemde voorbeeld te zien dat sommige diensten binnen een besloten netwerk ook worden opgelost met SAML. Het is gebruikelijk dat organisaties binnen een netwerkomgeving kiezen voor Kerberos als het gaat om Active Directory van Windows.

De expertgroep, die verantwoordelijk was voor het toetsen op inhoudelijke criteria van SAML, kon het onderscheid tussen toepassing van Kerberos 5 of SAML buiten een besloten netwerk onvoldoende duiden. Mocht alsnog besloten worden om Kerberos in behandeling te nemen, is het advies in de toetsing te laten duiden of conflicten tussen deze standaarden wel of niet bestaan en wat dat betekent. De gevolgen van eventuele opname van de standaard op toepassing buiten het eigen netwerk zijn nu niet bekend.

Daarnaast heeft Transport Security Layer (hierna: TLS) een relatie met Kerberos als het gaat om encryptie. TLS zorgt voor het met behulp van certificaten beveiligen van de verbinding (op de transportlaag) tussen client- en serversystemen en tussen serversystemen onderling, voor zover deze gerealiseerd wordt met internettechnologie. De voornaamste verschillen met Kerberos zijn dat TLS niet gericht is op single-sign-on, maar op datazekerheid.

2. Bestaat er samenhang tussen de aangemelde standaard en de aanbevolen standaarden die reeds op de lijst zijn opgenomen en wat betekent dit voor de toetsing en eventuele opname van de standaard?

   Niet voor zover bekend.

3. Bestaat er samenhang tussen de aangemelde standaard en standaarden die in aanmerking komen voor opname op de lijst en wat betekent dit voor de toetsing van de standaard(en)? (Denk bijvoorbeeld ook aan een gezamenlijke toetsing met (een deel van) deze aanvullende standaarden)

   Niet voor zover bekend.

6. Sponsorschap

De aanmelding van standaarden voor de lijst van het Forum en het Nationaal Beraad dient ondersteund of gesponsord te worden door overheids- en/of (semi)publieke organisaties die de standaard reeds in gebruik hebben (of voornemens zijn dit te doen) en die de beoogde opname op de lijsten ondersteunen. Dit draagt bij aan het draagvlak voor de standaard, geeft zicht op de functionele usecase voor de overheid en helpt bovendien om tijdens de toetsing de juiste experts te benaderen.

1. Welke overheden en/of (semi) publieke organiasties ondersteunen de aanmelding van de standaard?

   De aanmelding van de standaard wordt (nog) niet ondersteund door een overheidsorganisatie. RDW en Servicecentrum Drechtsteden

passen de standaard toe en de aanmelder verwacht dat deze organisaties de aanmelding ondersteunen.

2. Hebben deze organisaties de standaard geïmplementeerd?

   De RDW heeft de standaard geïmplementeerd, Servicecentrum Drechtsteden is bezig met de implementatie. Funatics heeft binnen de zorg klanten die de standaard hebben geïmplementeerd.

7. Functionele use case

Voor de standaard dient een duidelijke use case beschikbaar te zijn op basis waarvan overheden en/of instellingen uit de (semi) publieke sector kunnen bepalen of de aangemelde standaard voor hen relevant is en wie eventueel moet deelnemen aan de experttoetsing van de standaard.

De RDW maakt binnen de eigen besloten netwerkomgeving voor Windows altijd gebruik van Kerberos als SSO-toepassing. Voor andere interne diensten is dit SAML 2.0. Naar buiten toe maken zij voor diensten ook gebruik van SAML.

Funatics biedt ondersteuning bij implementatie van SSO-toepassingen. Binnen de zorg zetten zij Kerberos soms in binnen intranet omgevingen, bijvoorbeeld waar voorheen Microsoft's NTLM werd gebruikt.