Eclipse MicroProfile Interoperable JWT RBAC

Scott Stark; David Blevins; Pedro Igor Silva

1.1-RC1, May 19, 2018

Table of Contents

Specification: Eclipse MicroProfile Interoperable JWT RBAC

Version: 1.1-RC1

Status: Draft

Release: May 19, 2018

Chapter 1. Introduction

This specification outlines a proposal for using OpenID Connect(OIDC) based JSON Web Tokens(JWT) for role based access control(RBAC) of microservice endpoints.

Chapter 2. Motivation

MicroProfile is a baseline platform definition that optimizes Enterprise Java for a microservices architecture and delivers application portability across multiple MicroProfile runtimes. While Java EE is a very feature rich platform and is like a toolbox that can be used to to address a wide variety of application architectures, MicroProfile focuses on defining a small and a minimum set of Java EE standards that can be used to deliver applications based on a microservice architecture, they are:

- JAX-RS
- CDI
- JSON-P

The security requirements that involve microservice architectures are strongly related with RESTful Security. In a RESTful architecture style, services are usually stateless and any security state associated with a client is sent to the target service on every request in order to allow services to re-create a security context for the caller and perform both authentication and authorization checks.

One of the main strategies to propagate the security state from clients to services or even from services to services involves the use of security tokens. In fact, the main security protocols in use today are based on security tokens such as OAuth2, OpenID Connect, SAML, WS-Trust, WS-Federation and others. While some of these standards are more related with identity federation, they share a common concept regarding security tokens and token based authentication.

For RESTful based microservices, security tokens offer a very lightweight and interoperable way to propagate identities across different services, where:

- Services don't need to store any state about clients or users
- Services can verify the token validity if token follows a well known format. Otherwise, services may invoke a separated service.
- Services can identify the caller by introspecting the token. If the token follows a well known format, services are capable to introspect the token by themselves, locally. Otherwise, services may invoke a separated service.
- Services can enforce authorization policies based on any information within a security token
- Support for both delegation and impersonation of identities

Today, the most common solutions involving RESTful and microservices security are based on OAuth2, OpenID Connect(OIDC) and JSON Web Tokens(JWT) standards.

2.1. Token Based Authentication

Token Based Authentication mechanisms allow systems to authenticate, authorize and verify identities based on a security token. Usually, the following entities are involved:

- Issuer
    - Responsible for issuing security tokens as a result of successfully asserting an identity

(authentication). Issuers are usually related with Identity Providers.

- Client
  - Represented by an application to which the token was issued for. Clients are usually related with Service Providers. A client may also act as an intermediary between a subject and a target service (delegation).
- Subject
  - The entity to which the information in a token refers to.
- Resource Server
  - Represented by an application that is going to actually consume the token in order to check if a token gives access or not to a protected resource.

Independent of the token format or protocol in use, from a service perspective, token based authentication is based on the following steps:

- Extract security token from the request
  - For RESTful services, this is usually achieved by obtaining the token from the Authorization header.
- Perform validation checks against the token
  - This step usually depends on the token format and security protocol in use. The objective is make sure the token is valid and can be consumed by the application. It may involve signature, encryption and expiration checks.
- Introspect the token and extract information about the subject
  - This step usually depends on the token format and security protocol in use. The objective is to obtain all the necessary information about the subject from the token.
- Create a security context for the subject
  - Based on the information extracted from the token, the application creates a security context for the subject in order to use the information wherever necessary when serving protected resources.

Chapter 3. Using JWT Bearer Tokens to Protect Services

For now, use cases are based on a scenario where services belong to the same security domain. This is an important note in order to avoid dealing with all complexities when you need to access services across different security domains. With that in mind, we assume that any information carried along with a token could be understood and processed (without any security breaches) by the different services involved.

The use case can be described as follows:

A client sends a HTTP request to Service A including the JWT as a bearer token:

```
GET /resource/1 HTTP/1.1
Host: example.com
Authorization: Bearer mF_9.B5f-4.1JqM
```

On the server, a token-based authentication mechanism in front of Service A perform all steps described on the Token Based Authentication section. As part of the security context creation, the server establishes role and group mappings for the subject based on the JWT claims. The role to group mapping is fully configurable by the server along the lines of the Java EE RBAC security model.

JWT tokens follow a well defined and known standard that is becoming the most common token format to protect services. It not only provides a token format but additional security aspects like signature and encryption based on another set of standards like JSON Web Signature (JWS), JSON Web Encryption (JWE) and others.

There are few reasons why JWT is becoming so widely adopted:

- Token validation doesn't require an additional trip and can be validated locally by each service
- Given its JSON nature, it is solely based on claims or attributes to carry authentication and authorization information about a subject.
- Makes easier to support different types of access control mechanisms such as ABAC, RBAC, Context-Based Access Control, etc.
- Message-level security using signature and encryption as defined by both JWS and JWE standards
- Given its JSON nature, processing JWT tokens becomes trivial and lightweight. Especially if considering Java EE standards such as JSON-P or the different third-party libraries out there such as Nimbus, Jackson, etc.
- Parties can easily agree on a specific set of claims in order to exchange both authentication and authorization information. Defining this along with the Java API and mapping to JAX-RS APIs are the primary tasks of the MP-JWT specification.
- Widely adopted by different Single Sign-On solutions and well known standards such as OpenID

Connect given its small overhead and ability to be used across different different security domains (federation)

Chapter 4. Recommendations for Interoperability

The maximum utility of the MicroProfile JWT(MP-JWT) as a token format depends on the agreement between both identity providers and service providers. This means identity providers - responsible for issuing tokens - should be able to issue tokens using the MP-JWT format in a way that service providers can understand in order to introspect the token and gather information about a subject. To that end, the requirements for the MicroProfile JWT are:

1. Be usable as an authentication token.
2. Be usable as an authorization token that contains Java EE application level roles indirectly granted via a groups claim.
3. Can be mapped to IdentityStore in JSR375.
4. Can support additional standard claims described in IANA JWT Assignments as well as non-standard claims.

To meet those requirements, we introduce 2 new claims to the MP-JWT:

- "upn": A human readable claim that uniquely identifies the subject or user principal of the token, across the MicroProfile services the token will be accessed with.
- "groups": The token subject's group memberships that will be mapped to Java EE style application level roles in the MicroProfile service container.

4.1. Minimum MP-JWT Required Claims

The required minimum set of MP-JWT claims is then:

typ

This JOSE header parameter identifies the token as an RFC7519 and must be "JWT" RFC7519, Section 5.1

alg

This JOSE header parameter identifies the cryptographic algorithm used to secure the JWT. MP-JWT requires the use of the RSASSA-PKCS1-v1_5 SHA-256 algorithm and must be specified as "RS256", RFC7515, Section 4.1.1

kid

This JOSE header parameter is a hint indicating which key was used to secure the JWT. RFC7515, Section-4.1.4

iss

The MP-JWT issuer. RFC7519, Section 4.1.1

sub

Identifies the principal that is the subject of the JWT. See the "upn" claim for how this relates to

the container java.security.Principal. RFC7519, Section 4.1.2

exp

Identifies the expiration time on or after which the JWT MUST NOT be accepted for processing. The processing of the "exp" claim requires that the current date/time MUST be before the expiration date/time listed in the "exp" claim. Implementers MAY provide for some small leeway, usually no more than a few minutes, to account for clock skew. Its value MUST be a number containing a NumericDate value. RFC7519, Section 4.1.4

iat

Identifies the time at which the JWT was issued. This claim can be used to determine the age of the JWT. Its value MUST be a number containing a NumericDate value. RFC7519, Section 4.1.6

jti

Provides a unique identifier for the JWT. The identifier value MUST be assigned in a manner that ensures that there is a negligible probability that the same value will be accidentally assigned to a different data object; if the application uses multiple issuers, collisions MUST be prevented among values produced by different issuers as well. The "jti" claim can be used to prevent the JWT from being replayed. The "jti" value is a case-sensitive string. RFC7519, Section 4.1.7

upn

This MP-JWT custom claim is the user principal name in the java.security.Principal interface, and is the caller principal name in javax.security.enterprise.identitystore.IdentityStore. If this claim is missing, fallback to the "preferred_username", OIDC Section 5.1 should be attempted, and if that claim is missing, fallback to the "sub" claim should be used.

groups

This MP-JWT custom claim is the list of group names that have been assigned to the principal of the MP-JWT. This typically will required a mapping at the application container level to application deployment roles, but a a one-to-one between group names and application role names is required to be performed in addition to any other mapping.

NOTE	NumericDate used by `exp`, `iat`, and other date related claims is a JSON numeric value representing the number of seconds from 1970-01-01T00:00:00Z UTC until the specified UTC date/time, ignoring leap seconds

An example minimal MP-JWT in JSON would be:

```
{
     "typ": "JWT",
    "alg": "RS256",
    "kid": "abc-1234567890"
}
{
       "iss": "https://server.example.com",
       "jti": "a-123",
       "exp": 1311281970,
       "iat": 1311280970,
       "sub": "24400320",
       "upn": "jdoe@server.example.com",
       "groups": ["red-group", "green-group", "admin-group", "admin"],
}
```

This specification defines a JsonWebToken java.security.Principal interface extension that makes this set of required claims available via get style accessors. The JsonWebToken interface definition is:

```
package org.eclipse.microprofile.jwt;
public interface JsonWebToken extends Principal {

    /**
     * Returns the unique name of this principal. This either comes from the upn
     * claim, or if that is missing, the preferred_username claim. Note that for
     * guaranteed interoperability a upn claim should be used.
     *
     * @return the unique name of this principal.
     */
    @Override
    String getName();

    /**
     * Get the raw bearer token string originally passed in the authentication
     * header
     * @return raw bear token string
     */
    default String getRawToken() {
        return getClaim(Claims.raw_token.name());
    }

    /**
     * The iss(Issuer) claim identifies the principal that issued the JWT
     * @return the iss claim.
     */
    default String getIssuer() {
        return getClaim(Claims.iss.name());
    }
```

```
    /**
     * The aud(Audience) claim identifies the recipients that the JWT is
     * intended for.
     * @return the aud claim.
     */
    default Set<String> getAudience() {
        return getClaim(Claims.aud.name());
    }

    /**
     * The sub(Subject) claim identifies the principal that is the subject of
     * the JWT. This is the token issuing
     * IDP subject, not the
     *
     * @return the sub claim.
     */
    default String getSubject() {
        return getClaim(Claims.sub.name());
    }

    /**
     * The jti(JWT ID) claim provides a unique identifier for the JWT.
     The identifier value MUST be assigned in a manner that ensures that
     there is a negligible probability that the same value will be
     accidentally assigned to a different data object; if the application
     uses multiple issuers, collisions MUST be prevented among values
     produced by different issuers as well.  The "jti" claim can be used
     to prevent the JWT from being replayed.
     * @return the jti claim.
     */
    default String getTokenID() {
        return getClaim(Claims.jti.name());
    }

    /**
     * The exp (Expiration time) claim identifies the expiration time on or
     * after which the JWT MUST NOT be accepted
     * for processing in seconds since 1970-01-01T00:00:00Z UTC
     * @return the exp claim.
     */
    default long getExpirationTime() {
        return getClaim(Claims.exp.name());
    }

    /**
     * The iat(Issued at time) claim identifies the time at which the JWT was
     * issued in seconds since 1970-01-01T00:00:00Z UTC
     * @return the iat claim
     */
    default long getIssuedAtTime() {
        return getClaim(Claims.iat.name());
```

```
    }

    /**
     * The groups claim provides the group names the JWT principal has been
     * granted.
     *
     * This is a MicroProfile specific claim.
     * @return a possibly empty set of group names.
     */
    default Set<String> getGroups() {
        return getClaim(Claims.groups.name());
    }

    /**
     * Access the names of all claims are associated with this token.
     * @return non-standard claim names in the token
     */
    Set<String> getClaimNames();

    /**
     * Verify is a given claim exists
     * @param claimName - the name of the claim
     * @return true if the JsonWebToken contains the claim, false otherwise
     */
    default boolean containsClaim(String claimName) {
        return claim(claimName).isPresent();
    }

    /**
     * Access the value of the indicated claim.
     * @param claimName - the name of the claim
     * @return the value of the indicated claim if it exists, null otherwise.
     */
    <T> T getClaim(String claimName);

    /**
     * A utility method to access a claim value in an {@linkplain Optional}
     * wrapper
     * @param claimName - the name of the claim
     * @param <T> - the type of the claim value to return
     * @return an Optional wrapper of the claim value
     */
    default <T> Optional<T> claim(String claimName) {
        return Optional.ofNullable(getClaim(claimName));
    }
}
```

4.2. Additional Claims

The JWT can contain any number of other custom and standard claims, and these are made

available from the JsonWebToken getOtherClaim(String) method. An example MP-JWT that contains additional "auth_time", "preferred_username", "acr", "nbf", "aud" and "roles" claims is:

```
{
     "typ": "JWT",
    "alg": "RS256",
    "kid": "abc-1234567890"
}
{
   "iss": "https://server.example.com",
   "aud": ["s6BhdRkqt3"],
   "exp": 1311281970,
   "iat": 1311280970,
   "sub": "24400320",
   "upn": "jdoe@server.example.com",
   "groups: ["red-group", "green-group", "admin-group"],
   "roles": ["auditor", "administrator"],
   "jti": "a-123",
   "auth_time": 1311280969,
   "preferred_username": "jdoe",
   "acr": "phr",
   "nbf":  1311288970
}
```

4.3. The `Claims` Enumeration Utility Class, and the Set of Claim Value Types

The `org.eclipse.microprofile.jwt.Claims` utility class encapsulate an enumeration of all the standard JWT related claims along with a description and the required Java type for the claim as returned from the `JsonWebToken#getClaim(String)` method.

```
public enum Claims {
    // The base set of required claims that MUST have non-null values in the
JsonWebToken
    iss("Issuer", String.class),
    sub("Subject", String.class),
    exp("Expiration Time", Long.class),
    iat("Issued At Time", Long.class),
    jti("JWT ID", String.class),
    upn("MP-JWT specific unique principal name", String.class),
    groups("MP-JWT specific groups permission grant", Set.class),
    raw_token("MP-JWT specific original bearer token", String.class),

    // The IANA registered, but MP-JWT optional claims
    aud("Audience", Set.class),
    nbf("Not Before", Long.class),
    auth_time("Time when the authentication occurred", Long.class),
    updated_at("Time the information was last updated", Long.class),
```

```
    azp("Authorized party - the party to which the ID Token was issued", String.class
),
    nonce("Value used to associate a Client session with an ID Token", String.class),
    at_hash("Access Token hash value", Long.class),
    c_hash("Code hash value", Long.class),

    full_name("Full name", String.class),
    family_name("Surname(s) or last name(s)", String.class),
    middle_name("Middle name(s)", String.class),
    nickname("Casual name", String.class),
    given_name("Given name(s) or first name(s)", String.class),
    preferred_username("Shorthand name by which the End-User wishes to be referred to
", String.class),
    email("Preferred e-mail address", String.class),
    email_verified("True if the e-mail address has been verified; otherwise false",
Boolean.class),

    gender("Gender", String.class),
    birthdate("Birthday", String.class),
    zoneinfo("Time zone", String.class),
    locale("Locale", String.class),
    phone_number("Preferred telephone number", String.class),
    phone_number_verified("True if the phone number has been verified; otherwise
false", Boolean.class),
    address("Preferred postal address", JsonObject.class),
    acr("Authentication Context Class Reference", String.class),
    amr("Authentication Methods References", String.class),
    sub_jwk("Public key used to check the signature of an ID Token", JsonObject.class
),
    cnf("Confirmation", String.class),
    sip_from_tag("SIP From tag header field parameter value", String.class),
    sip_date("SIP Date header field value", String.class),
    sip_callid("SIP Call-Id header field value", String.class),
    sip_cseq_num("SIP CSeq numeric header field parameter value", String.class),
    sip_via_branch("SIP Via branch header field parameter value", String.class),
    orig("Originating Identity String", String.class),
    dest("Destination Identity String", String.class),
    mky("Media Key Fingerprint String", String.class),

    jwk("JSON Web Key Representing Public Key", JsonObject.class),
    jwe("Encrypted JSON Web Key", String.class),
    kid("Key identifier", String.class),
    jku("JWK Set URL", String.class),

    UNKNOWN("A catch all for any unknown claim", Object.class)
    ;
...
    /**
     * @return A desccription for the claim
     */
    public String getDescription() {
```

```
        return description;
    }

    /**
     * The required type of the claim
     * @return type of the claim
     */
    public Class<?> getType() {
        return type;
    }
}
```

Custom claims not handled by the Claims enum are required to be valid JSON-P `javax.json.JsonValue` subtypes. The current complete set of valid claim types is therefore, (excluding the invalid Claims.UNKNOWN Void type):

- java.lang.String
- java.lang.Long
- java.lang.Boolean
- java.util.Set<java.lang.String>
- javax.json.JsonValue.TRUE/FALSE
- javax.json.JsonString
- javax.json.JsonNumber
- javax.json.JsonArray
- javax.json.JsonObject

4.4. Service Specific Authorization Claims

An extended form of authorization on a per service basis using a "resource_access" claim has been postponed to a future release. See Future Directions for more information.

Chapter 5. Marking a JAX-RS Application as Requiring MP-JWT Access Control

Since the MicroProfile does not specify a deployment format, and currently does not rely on servlet metadata descriptors, we have added an `org.eclipse.microprofile.jwt.LoginConfig` annotation that provides the same information as the web.xml login-config element. It's intended usage is to mark a JAX-RS `Application` as requiring MicroProfile JWT RBAC as shown in the following sample:

```
import org.eclipse.microprofile.annotation.LoginConfig;

import javax.ws.rs.ApplicationPath;
import javax.ws.rs.core.Application;

@LoginConfig(authMethod = "MP-JWT", realmName = "TCK-MP-JWT")
@ApplicationPath("/")
public class TCKApplication extends Application {
}
```

The MicroProfile JWT implementation is responsible for either directly processing this annotation, or mapping it to an equivalent form of metadata for the underlying implementation container.

Chapter 6. Requirements for Rejecting MP-JWT Tokens

The MP-JWT specification requires that an MP-JWT implementation reject a bearer token as an invalid MP-JWT token if any of the following conditions are not met:

1. The JWT must have a JOSE header that indicates the token was signed using the RS256 algorithm.
2. The JWT must have an iss claim representing the token issuer that maps to an MP-JWT implementation container runtime configured value. Any issuer other than those issuers that have been whitelisted by the container configuration must be rejected with an HTTP_UNUATHENTICATED(401) error.
3. The JWT signer must have a public key that that maps to an MP-JWT implementation container runtime configured value. Any public key other than those that have been whitelisted by the container configuration must be rejected with an HTTP_UNUATHENTICATED(401) error.

NOTE	A future MP-JWT specification may define how an MP-JWT implementation makes use of the MicroProfile Config specification to allow for configuration of the issuer, issuer public key and expiration clock skew. Additional requirements for validation of the required MP-JWT claims may also be defined.

Chapter 7. Mapping MP-JWT Tokens to Java EE Container APIs

The requirements of how a JWT should be exposed via the various Java EE container APIs is discussed in this section. For the 1.0 release, the only mandatory container integration is with the JAX-RS container, and injection of the MP-JWT types.

7.1. CDI Injection Requirements

This section describes the requirements for MP-JWT implementations with regard to the injection of MP-JWT tokens and their associated claim values.

7.1.1. Injection of `JsonWebToken`

An MP-JWT implementation must support the injection of the currently authenticated caller as a `JsonWebToken` with `@RequestScoped` scoping:

```
@Path("/endp")
@DenyAll
@ApplicationScoped
public class RolesEndpoint {

    @Inject
    private JsonWebToken callerPrincipal;
```

7.1.2. Injection of `JsonWebToken` claims via Raw Type, `ClaimValue`, `javax.enterprise.inject.Instance` and JSON-P Types

This specification requires support for injection of claims from the current `JsonWebToken` using the `org.eclipse.microprofile.jwt.Claim` qualifier:

```
/**
 * Annotation used to signify an injection point for a {@link ClaimValue} from
 * a {@link JsonWebToken}
 */
@Qualifier
@Retention(RetentionPolicy.RUNTIME)
@Target({ElementType.FIELD, ElementType.METHOD, ElementType.PARAMETER, ElementType
.TYPE})
public @interface Claim {
    /**
     * The value specifies the id name the claim to inject
     * @return the claim name
     * @see JsonWebToken#getClaim(String)
     */
    @Nonbinding
    String value() default "";

    /**
     * An alternate way of specifying a claim name using the {@linkplain Claims}
     * enum
     * @return the claim enum
     */
    @Nonbinding
    Claims standard() default Claims.UNKNOWN;
}
```

with `@Dependent` scoping.

MP-JWT implementations are required to throw a `DeploymentException` when detecting the ambiguous use of a `@Claim` qualifier that includes inconsistent non-default values for both the value and standard elements as is the case shown here:

```
@ApplicationScoped
public class MyEndpoint {
    @Inject
    @Claim(value="exp", standard=Claims.iat)
    private Long timeClaim;
...
}
```

The set of types one my use for a claim value injection is:

- java.lang.String
- java.util.Set<java.lang.String>
- java.lang.Long
- java.lang.Boolean
- javax.json.JsonValue subtypes

- java.util.Optional wrapper of the above types.
- org.eclipse.microprofile.jwt.ClaimValue wrapper of the above types.

MP-JWT implementations are required to support injection of the claim values using any of these types.

The `org.eclipse.microprofile.jwt.ClaimValue` interface is:

```
/**
 * A representation of a claim in a {@link JsonWebToken}
 * @param <T> the expected type of the claim
 */
public interface ClaimValue<T> extends Principal {

    /**
     * Access the name of the claim.
     * @return The name of the claim as seen in the JsonWebToken content
     */
    @Override
    public String getName();

    /**
     * Access the value of the claim.
     * @return the value of the claim.
     */
    public T getValue();
}
```

The following example code fragment illustrates various examples of injecting different types of claims using a range of generic forms of the `ClaimValue`, `JsonValue` as well as the raw claim types:

```
import org.eclipse.microprofile.jwt.Claim;
import org.eclipse.microprofile.jwt.ClaimValue;
import org.eclipse.microprofile.jwt.Claims;

@Path("/endp")
@DenyAll
@RequestScoped
public class RolesEndpoint {
...

    // Raw types
    @Inject
    @Claim(standard = Claims.raw_token)
    private String rawToken;
    @Inject ①
    @Claim(standard=Claims.iat)
    private Long issuedAt;
```

```
    // ClaimValue wrappers
    @Inject ②
    @Claim(standard = Claims.raw_token)
    private ClaimValue<String> rawTokenCV;
    @Inject
    @Claim(standard = Claims.iss)
    private ClaimValue<String> issuer;
    @Inject
    @Claim(standard = Claims.jti)
    private ClaimValue<String> jti;
    @Inject ③
    @Claim("jti")
    private ClaimValue<Optional<String>> optJTI;
    @Inject
    @Claim("jti")
    private ClaimValue objJTI;
    @Inject
    @Claim("groups")
    private ClaimValue<Set<String>> groups;
    @Inject ④
    @Claim(standard=Claims.iat)
    private ClaimValue<Long> issuedAtCV;
    @Inject
    @Claim("iat")
    private ClaimValue<Long> dupIssuedAt;
    @Inject
    @Claim("sub")
    private ClaimValue<Optional<String>> optSubject;
    @Inject
    @Claim("auth_time")
    private ClaimValue<Optional<Long>> authTime;
    @Inject ⑤
    @Claim("custom-missing")
    private ClaimValue<Optional<Long>> custom;
    //
    @Inject
    @Claim(standard = Claims.jti)
    private Instance<String> providerJTI;
    @Inject ⑥
    @Claim(standard = Claims.iat)
    private Instance<Long> providerIAT;
    @Inject
    @Claim("groups")
    private Instance<Set<String>> providerGroups;
    //
    @Inject
    @Claim(standard = Claims.jti)
    private JsonString jsonJTI;
    @Inject
    @Claim(standard = Claims.iat)
    private JsonNumber jsonIAT;
```

```
    @Inject ⑦
    @Claim("roles")
    private JsonArray jsonRoles;
    @Inject
    @Claim("customObject")
    private JsonObject jsonCustomObject;
```

① Injection of a non-proxyable raw type like java.lang.Long must happen in a RequestScoped bean as the producer will have dependendent scope.

② Injection of the raw MP-JWT token string.

③ Injection of the jti token id as an `Optional<String>` wapper.

④ Injection of the issued at time claim using an `@Claim` that references the claim name using the Claims.iat enum value.

⑤ Injection of a custom claim that does exist will result in an Optional<Long> value for which isPresent() will return false.

⑥ Another injection of a non-proxyable raw type like java.lang.Long, but the use of the javax.enterprise.inject.Instance interface allows for injection to occur in non-RequestScoped contexts.

⑦ Injection of a JsonArray of role names via a custom "roles" claim.

The example shows that one may specify the name of the claim using a string or a `Claims` enum value. The string form would allow for specifying non-standard claims while the `Claims` enum approach guards against typos.

7.1.3. Handling of Non-RequestScoped Injection of Claim Values

MP-JWT implementations are required to validate the use of claim value injection into contexts that do not match @RequestScoped. When the target context has @ApplicationScoped or @SessionScoped scope, implementations are required to generate a `javax.enterprise.inject.spi.DeploymentException`. For any other context, implementations should issue a warning, that may be suppressed by an implementation specific configuration setting.

NOTE	If one needs to inject a claim value into a scope with a lifetime greater than @RequestScoped, such as @ApplicationScoped or @SessionScoped, one can use the javax.enterprise.inject.Instance interface to do so.

7.2. JAX-RS Container API Integration

The behavior of the following JAX-RS security related methods is required for MP-JWT implementations.

7.2.1. `javax.ws.rs.core.SecurityContext.getUserPrincipal()`

The `java.security.Principal` returned from these methods MUST be an instance of `org.eclipse.microprofile.jwt.JsonWebToken`.

7.2.2. `javax.ws.rs.core.SecurityContext#isUserInRole(String)`

This method MUST return true for any name that is included in the MP-JWT "groups" claim, as well as for any role name that has been mapped to a group name in the MP-JWT "groups" claim.

7.3. Using the Common Security Annotations for the Java Platform (JSR-250)

The expectations for use of the various security annotations described in sections 2.9 - 2.12 of JSR-250 (@RolesAllowed, @PermitAll, @DenyAll), is that MP-JWT containers support the behavior as described in those sections. In particular, the interaction between the annotations should be as described in section 2.12 of JSR-250.

7.3.1. Mapping the `@RolesAllowed` to the MP-JWT group claim

In terms of mapping between the MP-JWT claims and role names used in @RolesAllowed, the role names that have been mapped to group names in the MP-JWT "groups" claim, MUST result in an allowing authorization decision wherever the security constraint has been applied.

7.4. Recommendations for Optional Container Integration

This section describes the expected behaviors for Java EE container APIs other than JAX-RS.

7.4.1. javax.security.enterprise.identitystore.IdentityStore.getCallerGroups(CredentialValidationResult)

This method should return the set of names found in the "groups" claim in the JWT if it exists, an empty set otherwise.

7.4.2. javax.ejb.SessionContext.getCallerPrincipal()

The java.security.Principal returned from this method MUST be an instance of `org.eclipse.microprofile.jwt.JsonWebToken`.

7.4.3. javax.ejb.SessionContext#isCallerInRole(String)

This method MUST return true for any name that is included in the MP-JWT "groups" claim, as well as for any role name that has been mapped to a group name in the MP-JWT "groups" claim.

7.4.4. Overriding @LoginConfig from web.xml login-config

If a deployment with a web.xml descriptor contains a login-config element, an MP-JWT implementation should view the web.xml metadata as an override to the deployment annotation.

7.4.5. javax.servlet.http.HttpServletRequest.getUserPrincipal()

The java.security.Principal returned from this method MUST be an instance of org.eclipse.microprofile.jwt.JsonWebToken.

7.4.6. javax.servlet.http.HttpServletRequest#isUserInRole(String)

This method MUST return true for any name that is included in the MP-JWT "groups" claim, as well as for any role name that has been mapped to a group name in the MP-JWT "groups" claim.

7.4.7. javax.security.jacc.PolicyContext.getContext("javax.security.auth.Subject.container")

The javax.security.auth.Subject returned by the PolicyContext.getContext(String key) method with the standard "javax.security.auth.Subject.container" key, MUST return a Subject that has a `java.security.Principal` of type `org.eclipse.microprofile.jwt.JsonWebToken` amongst it's set of `Principal`s returned by `getPrincipals()`. Similarly, `Subject#getPrincipals(JsonWebToken.class)` must return a set with at least one value. This means that following code snipet must not throw an AssertionError:

```
    Subject subject = (Subject) PolicyContext.getContext(
"javax.security.auth.Subject.container");
    Set<? extends Principal> principalSet = subject.getPrincipals(JsonWebToken.class);
    assert principalSet.size() > 0;
```

Chapter 8. Mapping MP-JWT Token to Other Container APIs

For non-Java EE containers that provide access to some form of `java.security.Principal` representation of an authenticated caller, the caller principal MUST be compatible with the `org.eclipse.microprofile.jwt.JsonWebToken` interface.

Chapter 9. Configuration

Verification of JSon Web Tokens (JWT) passed to the Microservice in HTTP requests at runtime is done with the RSA Public Key corresponding to the RSA Private Key held by the JWT Issuer.

At the time of JWT creation, the Issuer will sign the JWT with its Private Key before passing it to the user. Upon receiving the JWT in future HTTP requests, Microservices can then use the matching Public Key to verify the JWT and trust the user information (claims) it contains.

The goal of this chapter is to detail means of passing the Public Key from the JWT Issuer to the MicroProfile JWT implementation as well as any standard configuration options for the verification itself.

MicroProfile JWT leverages the MicroProfile Config specification to provide a consistent means of passing all supported configuration options. Prior to MicroProfile JWT 1.1 all configuration options for the Public Key and verification were vendor-specific. Any vendor-specific methods of configuration are still valid and shall be considered to override any standard configuration mechanisms.

9.1. Obtaining the Public Key

In practice, the Public Key is often obtained manually from the JWT Issuer and stored in or passed to the binary of the Microservice. If your public Keys do not rotate frequently, then storing them in the binary image or on disk is a realistic option for many environments. For reference, SSL/TLS Certificates to support HTTPS, which are also Public Key based, are usually configured in the JVM itself and last for up to two years.

Alternatively, Public Keys may be obtained by the Microservice at runtime, directly from the JWT Issuer via HTTPS request. MicroProfile JWT implementations are required to support this method of fetching the Public Key from the JWT Issuer via means defined here. It should be noted, however, not all JWT Issuers support downloading of the Public Key via HTTPS request.

9.2. Supported Public Key Formats

Support for RSA Public Keys of 1024 or 2048 bits in length is required. Other key sizes are allowed, but should be considered vendor-specific.

Other asymmetric signature algorithms are allowed, but should be considered vendor-specific. This includes Digital Signature Algorithm (DSA), Diffie-Hellman (DS), Elliptical curve Digital Signature Algorithm (ECDSA), Edwards-curve Digital Signature Algorithm (EdDSA, aka ed25519)

NOTE	Symmetrically signed JWTs such as HMAC-SHA256 (hs256) are explicitly not supported, deemed insecure for a distributed Microservice architecture where JWTs are expected to be passed around freely. Use of symmetric signatures would require all microservices to share a secret, eliminating the ability to determine who created the JWT.

Public Keys may be formatted in any of the following formats, specified in order of precedence:

- Public Key Cryptography Standards #8 (PKCS#8) PEM
- JSON Web Key (JWK)
- JSON Web Key Set (JWKS)
- JSON Web Key (JWK) Base64 URL encoded
- JSON Web Key Set (JWKS) Base64 URL encoded

Attempts to parse the Public Key text will proceed in the order specified above until a valid Public Key can be derived.

Support for other Public Key formats such as PKCS#1, SSH2, or OpenSSH Public Key format is considered optional.

MicroProfile JWT implementations are required to throw a `DeploymentException` when given a public key that cannot be parsed using either the standardly supported or vendor-specific key formats.

MicroProfile JWT implementations are required to throw a `DeploymentException` when given a Private Key in any format.

9.2.1. PCKS#8

Public Key Cryptography Standards #8 (PKCS#8) PEM format is a plain text format and is the default format for OpenSSL, many public/private key tools and is natively supported in Java.

The format consists of a Base64 URL encoded value wrapped in a standard `-----BEGIN PUBLIC KEY-----` header and footer. The Base64 URL encoded data can be decoded and the resulting byte array passed directly to `java.security.spec.PKCS8EncodedKeySpec`.

The following is an example of a valid RSA 2048 bit Public Key in PKCS#8 PEM format.

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0440JtmhlywtkMvR6tTM
s0U6e9Ja4xXj5+q+joWdT2xCHt91Ck9+5C5WOaRTco4CPFMBxoUPi1jktW5c+Oyk
nOIACXu6grXexarFQLjsREE+dkDVrMu75f7Gb9/lC7mrVM73118wnMP2u5MOQIoX
OqqC1y1gaoJaLp/OjTiJGCm4uxzubzUPN5IDAFaTfK+QErhtcGeBDwWjvikGfUfX
+WVq74DOoggLiGbB4jsT8iVXEm53JcoEY8nVr2ygr92TuU1+xLAGisjRSYJVe7V1
tpdRG1CiyCIkqhDFfFBGhFnWlu4gKMiT0KToA9GJfOuCz67XZEAhQYizcXbn1uxa
OQIDAQAB
-----END PUBLIC KEY-----
```

MicroProfile JWT implementations must inspect the supplied Public Key body for the `-----BEGIN PUBLIC KEY-----` header and parse the key as PCKS#8 if found.

Support for the legacy PKCS#1 format is not required and should be considered vendor-specific. PKCS#1 formatted keys can be identified by the use of the `-----BEGIN RSA PUBLIC KEY-----` header and footer.

MicroProfile JWT implementations are required to throw a `DeploymentException` if given a Private

Key in any format such as `-----BEGIN PRIVATE KEY-----` or `-----BEGIN RSA PRIVATE KEY-----`

9.2.2. JSON Web Key (JWK)

JSON Web Key (JWK) allows for a Public Key to be formatted in json and optionally Base64 encoded.

At minimum JWK formatted Public Keys must contain the `kty` field. RSA Public Keys must contain the `n` and `e` fields.

The following example is the previously shown PKCS#8 PEM formatted Public Key converted to JWK format.

```
{
  "kty": "RSA",
  "n": "sszbq1NfZap2IceUCO9rCF9ZYfHE3oU5m6Avgyxu1LmlB6rNPejO-
eB7T9iIhxXCEKsGDcx4Cpo5nxnW5PSQZM_wzXg1bAOZ3O6k57EoFC108cB0hdvOiCXXKOZGrGiZuF7q5Zt1ftq
Ik7oK2gbItSdB7dDrR4CSJSGhsSu5mP0",
  "e": "AQAB"
}
```

MicroProfile JWT implementations are required to throw a `DeploymentException` if the JWK `kty` field is missing or JSON text is found, but does not follow either JWK or JWKS format.

The JWK may be supplied in plain JSON or Base64 URL encoded JSON format.

See RFC-7517 for further details on JWK format and optional fields.

9.2.3. JSON Web Key Set (JWKS)

The JSON Web Key Set (JWKS) format allows for multiple keys to supplied, which can be useful for either key rotation or supporting environments that have multiple JWT Issuers and therefore multiple Public Keys.

An example of a valid JWKS:

```
{
  "keys": [
    {
      "kid": "orange-1234",
      "kty": "RSA",
      "n": "sszbq1NfZap2IceUCO9rCF9ZYfHE3oU5m6Avgyxu1LmlB6rNPejO-
eB7T9iIhxXCEKsGDcx4Cpo5nxnW5PSQZM_wzXg1bAOZ3O6k57EoFC108cB0hdvOiCXXKOZGrGiZuF7q5Zt1ftq
Ik7oK2gbItSdB7dDrR4CSJSGhsSu5mP0",
      "e": "AQAB"
    },
    {
      "kid": "orange-5678",
      "kty": "RSA",
      "n":
"xC7RfPpTo7362rzATBu45Jv0updEZcr3IqymjbZRkpgTR8B19b_rS4dIficnyyU0plefkE2nJJyJbeW3Fon9B
Le4_srfXtqiBKcyqINeg0GrzIqoztZBmmmdo13lELSrGP91oHL-
UtCd1u5C1HoJc4bLpjUYxqOrJI4mmRC3Ksk5DV2OS1L5P4nBWIcR1oi6RQaFXy3zam3j1TbCD5urkE1CfUATFw
fXfFSPTGo7shNqsgaWgy6B205l5Lq5UmMUBG0prK79ymjJemODwrB445z-lk3CTtlMN7bcQ3nC8xh-
Mb2XmRB0uoU4K3kHTsofXG4dUHWJ8wGXEXgJNOPzOQ",
      "e": "AQAB"
    }
  ]
}
```


If the incoming JWT uses the `kid` header field and there is a key in the supplied JWK set with the same `kid`, only that key is considered for verification of the JWT's digital signature.

For example, the following decoded JWT would involve a check on only the `orange-5678` key.


```
{
  "alg": "RS256",
  "typ": "JWT",
  "kid": "orange-5678"
}.
{
  "sub": "1234567890",
  "name": "John Doe",
  "admin": true,
  "iat": 1516239022
}
```


The JWKS may be supplied in plain JSON or Base64 URL encoded JSON format.

9.3. Configuration Parameters

Parameters are passed using the MicroProfile Config specification. This specification allows at minimum configuration options to be specified in the microservice binary itself or via command-line via -D properties as follows:

```
java -jar movieservice.jar -Dmp.jwt.verify.publickey.location=orange.pem
```

By convention of the MicroProfile JWT specification, property names are always lowercase and begin with `mp.jwt.`

9.3.1. `mp.jwt.verify.publickey`

The `mp.jwt.verify.publickey` config property allows the Public Key text itself to be supplied as a string. The Public Key will be parsed from the supplied string in the order defined in section Supported Public Key Formats.

The following example shows a Base 64 URL encoded JWK passed via system property.

```
java -jar movieservice.jar -Dmp.jwt.verify.publickey=eyJrdHkiOiJSU0EiLCJuI\
joieEM3UmZQcFRvNzM2MnJ6QVRCdTQ1SnYwdXBkRVpjcjNJcXltamJaUmtwZ1RSOEIxOWJfclM\
0ZElmaWNueXlVMHBsZWZrRTJuSkp5SmJlVzNGb245QkxlNF9zcmZYdHFpQktjeXFJTmVnMEdye\
klxb3p0WkJtbW1kbzEzbEVMU3JHUDkxb0hMLVV0Q2QxdTVDMUhvSmM0YkxwalVZeHFPckpJNG1\
tUkMzS3NrNURWMk9TMUw1UDRuQldJY1Ixb2k2UlFhRlh5M3phbTNqMVRiQ0Q1dXJrRTFDZlVBV\
EZ3ZlhmRlNQVEdvN3NoTnFzZ2FXZ3k2QjIwNWw1THE1VW1NVUJHMHBySzc5eW1qSmVtT0R3ckI\
0NDV6LWxrM0NUdGxNTjdiY1EzbkM4eGgtTWIyWG1SQjB1b1U0SzNrSFRzb2ZYRzRkVUhXSjh3R\
1hFWGdKTk9Qek9RIiwiZSI6IkFRQUIifQo
```

When supplied, `mp.jwt.verify.publickey` will override other standard means to supply the Public Key such as `mp.jwt.verify.publickey.location`. Vendor-specific options for supplying the key will always take precedence.

If neither the `mp.jwt.verify.publickey` nor `mp.jwt.verify.publickey.location` are supplied configuration are supplied, the MP-JWT signer configuration will default to a vendor specific behavior as was the case for MP-JWT 1.0.

MicroProfile JWT implementations are required to throw a `DeploymentException` if both `mp.jwt.verify.publickey` and `mp.jwt.verify.publickey.location` are supplied.

9.3.2. `mp.jwt.verify.publickey.location`

The `mp.jwt.verify.publickey` config property allows for an external or internal location of Public Key to be specified. The value may be a relative path or a URL.

MicroProfile JWT implementations are required to check the path at startup or deploy time. Reloading the Public Key from the location at runtime as well as the frequency of any such reloading is beyond the scope of this specification and any such feature should be considered vendor-specific.

9.3.2.1. Relative Path

Relative or non-URL paths supplied as the location are resolved in the following order:

- `new File(location)`

- `Thread.currentThread().getContextClassLoader().getResource(location)`

The following example shows the file `orange.pem` supplied as either a file in the Microservice's binary or locally on disk.

```
java -jar movieservice.jar -Dmp.jwt.verify.publickey.location=orange.pem
```

Any non-URL is treated identically and may be a path inside or outside the archive.

```
java -jar movieservice.jar -Dmp.jwt.verify.publickey.location=/META-INF/orange.pem
```

Parsing of the file contents occurs as defined in Supported Public Key Formats

9.3.2.2. `file:` URL Scheme

File URL paths supplied as the location allow for explicit externalization of the file via full url.

```
java -jar movieservice.jar
-Dmp.jwt.verify.publickey.location=file:///opt/keys/orange.pem
```

Parsing of the file contents occurs as defined in Supported Public Key Formats

9.3.2.3. `http:` URL Scheme

HTTP and HTTPS URL paths allow for the Public Key to be fetched from a remote host, which may be the JWT Issuer or some other trusted internet or intranet location.

The location supplied must respond to an HTTP GET. Parsing of the HTTP message body occurs as defined in Supported Public Key Formats

```
java -jar movieservice.jar
-Dmp.jwt.verify.publickey.location=https://location.dev/widget/issuer
```

Other forms of HTTP requests and responses may be supported, but should be considered vendor-specific.

9.3.2.4. Other URL Schemes

All other locations containing a colon will be considered as URLs and be resolved using the following method:

- `new URL(location).openStream()`

Thus additional vendor-specific or user-defined options can easily be added.

Example custom "smb:" location

```
java -jar movieservice.jar -Dmp.jwt.verify.publickey.location=smb://Host/orange.pem
-Djava.protocol.handler.pkgs=org.foo
```

Example stub for custom "smb:" URL Handler

```
package org.foo.smb;

import java.io.IOException;
import java.net.URL;
import java.net.URLConnection;
import java.net.URLStreamHandler;

/**
 * The smb: URL protocol handler
 */
public class Handler extends URLStreamHandler {
    @Override
    protected URLConnection openConnection(URL u) throws IOException {
        return // your URLConnection implementation
    }
}
```

See java.net.URL javadoc for more details.

Parsing of the `InputStream` occurs as defined in Supported Public Key Formats and must return Public Key text in one of the supported formats.

Chapter 10. Future Directions

Not all considerations discussed during the specification process make it into the specification. This section serves as an abridged version for the purposes of soliciting feedback and interest. By convention we will leave items in the Future Direction for at most two revisions.

10.1. "resource_access" claim

In future versions of the API we would like to address service specific group claims. The "resource_access" claim originally targeted for the 1.0 release of the specification has been postponed as addition work to determine the format of the claim key as well as how these claims would be surface through the standard Java EE APIs needs more work than the 1.0 release timeline will allow.

For reference, a somewhat related extension to the OAuth 2.0 spec Resource Indicators for OAuth 2.0 has not gained much traction. The key point it makes that seems relevant to our investigation is that the service specific grants most likely need to be specified using URIs for the service endpoints. How these endpoints map to deployment virtual hosts and partial, wildcard, etc. URIs needs to be determined.

10.2. "roles" claim

A "roles" claim was considered in addition to the "groups" claim that made it into the final specification. The "groups" claim is intended to be mapped to specific roles on the target resource server. The "roles" claim was intended to explicitly state roles inside the JWT that would not be subject to any mappings and are made available to directly to the application for `@RolesAllowed` and similar RBAC checks. The roles in the JWT should be exposed to the app in addition to any roles that result from group-to-role mapping provided by the target resource server. The intended JWT datatype for "roles" should be a JSON string array.

Though a "roles" claim is not required, implementations that support it and applications that use it should do so as detailed in this section to ensure alignment for any future standardization.

10.3. "aud" claim

The "aud" claim defined in RFC 7519 section 4.1.3 was considered for addition. The intended JWT datatype for "aud" should be a JSON string array or a single string as defined in RFC 7519.

Though a "aud" claim is not required, implementations that support it and applications that use it should do so as detailed in this section to ensure alignment for any future standardization.

10.4. `mp.jwt.verify.issuer` configuration option

Discussion of a standard configuration option for enabling the explicit checking of the issuer was discussed. Discussion is still ongoing as to what the default behavior of the property should be if no explicit value is supplied. The definition as last phrased is below.

The `mp.jwt.verify.issuer` config property allows for the expected value of the `iss` claim to be optionally specified. When specified, the MicroProfile JWT implementation must verify the `iss` claim of incoming JWTs is present and matches the configured value of `mp.jwt.verify.issuer`.

If the `mp.jwt.verify.issuer` config property has not been set, any issuer or none at all is allowed.

NOTE	In most cases relying on the digital signature check via the Public Key alone is sufficient to establish trust.

10.5. `classpath:` URL Scheme

The option to have a built-in `classpath:` URL Scheme was discussed with the intended benefit of providing some way to explicitly state a Public Key file is inside the archive and to remove potential a similarly named file existed on disk.

For the moment this was deemed an edge-case that could be solved with a custom URL Scheme and consensus that this would add to the complexity of the specification. In practice, this may be very useful so those who find themselves with this scenario are encouraged to contact the MicroProfile discussion lists.

10.6. Expiration tolerance

Relaxing or potentially ignoring the expiration time of a JWT was discussed and deemed an attractive option for future standardization. It was omitted in efforts to keep the first revision of the configuration as simple as possible.

Users who find themselves with this need are encouraged to both request support from their respective implementation and to detail their use case the MicroProfile discussion lists, so any future standardization work accounts for all scenarios.

10.7. Passing JWTs as Cookies

Semantics for passing JWTs via HTTP `Cookie` headers instead of the HTTP `Authorization` header were discussed and deemed a valuable addition for interoperability purposes.

It is likely to be a future recommendation that MicroProfile JWT implementation supporting the transport of MP-JWT tokens using cookies SHOULD recognize the cookie name `Bearer`, and the cookie value format being the JWS Compact Serialization as described in section 7.1 of JSON Web Signature (RFC-7515).

There are a number of security considerations when using cookies to transfer security information such as tokens in cookies. Issues related to CSRF, XSS, and storage need to be considered. The following links present material on these issues:

- Cookie Storage
- XSS
- CSRF

The motivation for using `Bearer` as the Cookie name is to establish a pattern of using the `Authorization` scheme as the cookie name. Bearer token example would look as follows:

- `Authorization: Bearer as14efgscd31qrewtadg`
- `Cookie: Bearer=as14efgscd31qrewtadg`

Basic auth would look as follows:

- `Authorization: Basic gasdqwe198abg313ffd`
- `Cookie: Basic=gasdqwe198abg313ffd`

Chapter 11. Sample Implementations

This sections references known sample implementations of the Eclise MicroProfile JWT RBAC authorization specification.

11.1. General Java EE/SE based Implementations

A baseline sample implementation that is available under the Apache License, Version 2.0 can be found at https://github.com/MicroProfileJWT/microprofile-jwt-auth-prototype. The purpose of this prototype is to offer reusable code for integration of the JWT RBAC authenticaiton and authorization spec in various container environments. This particular implementation contains:

- a default implementation of the JsonWebToken interface
- a JAX-RS ContainerRequestFilter prototype
- JSR-375 IdentityStore and Credential prototypes

11.2. Wildfly Swarm Implementations

A sample implementation for a custom auth-method of MP-JWT with the Wildfly/Wildfly-Swarm Undertow web container, as a Wildfly-Swarm fraction, available under the Apache License, Version 2.0 can be found at: https://github.com/MicroProfileJWT/wfswarm-jwt-auth-fraction.