

YETKİM

Üstveri Kayıt Uygulama Bildirgesi (ÜKUB)

Yazarlar	Gökhan ERYOL, Neşe KAPTAN KOÇ, Mehmet Uğur YILMAZ
Son Güncelleme	2019-04-01
Sürüm	1.0

Lisans



Bu belge Creative Commons CC BY 3.0 altında lisanslıdır. Atfedildiği sürece, bu belgeyi paylaşabilir, yeniden kullanabilir ve uyarlayabilirsiniz. Bu belge, UK Access Management Federation ve ACOnet Identity Federation'un yapmış olduğu gayretli çalışmalardan yararlanılarak yazılmıştır.

İçindekiler

1 Tanımlar ve Terimler	3
2 Giriş ve Uygulanabilirlik	3
3 Üye Uygunluğu ve Mülkiyet	3
4 Üstveri Biçimi	4
5 Varlığın Uygunluğu ve Onayı	4
5.1 Varlık Kaydı	4
5.2 Varlık Kimliği Biçimi	5
5.3 Varlık Doğrulama	5
6 Varlık Yönetimi	5
6.1 Varlık Değişim Talepleri	5
6.2 Talep Edilmemiş Varlık Değişiklikleri	5
7 Kaynakça	6

1 Tanımlar ve Terimler

Bu belgede aşağıdaki tanımlar kullanılmıştır:

Federasyon	Kimlik Federasyonu, farklı kurumların bir araya gelerek kullanıcıları ve kaynakları ile ilgili bilgi paylaşımını sağlayarak işbirliği ve işlem kolaylığı sağlayan birlik.
Federasyon Üyesi	Federasyon politikasını imzalayarak kabul eden ve federasyona katılan kurum. Bu kurum federasyon çerçevesinde ev kurumu, servis sağlayıcı ve/veya Nitelik yetkilisi olarak faaliyet gösterebilir.
Federasyon İşletmecisi	Federasyon üyelerine kimlik doğrulama ve yetkilendirme altyapısı sağlayan kurum.
Federasyon Politikası	Federasyon üyelerinin ve federasyon İşletmecisinin yükümlülüklerini, haklarını ve beklentilerini açıklayan belge.
Varlık	Bir üyenin kaydettirmek istediği ve üstveride tanımladığı ayrık bileşen. Genellikle bir Kimlik Sağlayıcı veya Servis Sağlayıcıdır..
Kayıtlı Temsilciler	Üye adına hareket etmeye yetkili kişiler. Bu kişiler, farklı haklara sahip farklı roller üstlenebilirler..
ULAKNET	TÜBİTAK ULAKBİM tarafından işletilen Ulusal Akademik Ağ

2 Giriş ve Uygulanabilirlik

Bu belge, Federasyon İşletmecisinin üstveri kayıt uygulamasını açıklamaktadır ve yayın tarihinden itibaren geçerli olur. Yayın tarihinden sonra yapılan tüm yeni varlık kayıtları, belgenin yenisi yayınlanıncaya kadar, burada açıklandığı şekilde işleme alınır.

Bu belge Federasyon web sitesinde, aşağıdaki adresten yayınlanır:

<https://yetkim.ulakbim.gov.tr/katilim/>

Belgedeki güncellemeler, varlık üstverilerinde uygun biçimde atıf edilmelidir.

3 Üye Uygunluğu ve Mülkiyet

Federasyon üyesi olma prosedürü aşağıdaki adreste yayınlanmıştır:

<https://yetkim.ulakbim.gov.tr/katilim/>

Üyelik prosedürü, üye adayının tüzel kişiliğe sahip olduğunu doğrulamayı ve tüm üyelerin Federasyon politikasını kabul ederek, Federasyon İşletmecisi ile sözleşme yapmasını gerektirir. İşletmeci, bildirilen yasal adı temel alarak kontroller yapar. Kontroller için

- ULAKNET üye listesi
- Yükseköğretim Kurulu, üniversiteler listesi
- Türkiye Cumhuriyeti Resmi Gazete

gibi kaynaklar kullanılır.

Üyelik süreci, Federasyon İşletmecisi ile ilişkilerde kurum adına hareket etmesine izin verilen Kayıtlı Temsilcileri de belirler ve doğrular. Doğrulama, doğrudan temas (e-posta veya telefon yoluyla) ile sağlanır.

Üyelik süreci aynı zamanda, Federasyon üyesi için kanonik bir isim belirler. Bir üyenin kanonik ismi, üyelik süresi boyunca, kurum ismi değişikliği veya birleşmeler gibi gerekçelerle değişebilir. Üyenin kanonik ismi, varlığın <md:OrganizationName> ögesinde ilan edilir [SAML-Metadata-OS].

4 Üstveri Biçimi

Federasyon İşletmecisi tarafından kaydedilen tüm varlıkların üstverileri [SAML-Metadata-RPI-V1.0] üstveri eklentisini içermelidir. Bu eklenti, Federasyon İşletmecisinin, bu varlığın kayıt kuruluşu olduğunu belirtir, ayrıca bu varlık için geçerli olan ÜKUB sürümünü gösterir.

Aşağıda genel bir örnek verilmiştir:

```
<mdrpi:RegistrationInfo
registrationAuthority="https://yetkim.ulakbim.gov.tr"
registrationInstant="2018-12-29T13:39:41Z">
<mdrpi:RegistrationPolicy xml:lang="en">
https://yetkim.ulakbim.gov.tr/doc/YETKIM-MRPS-EN-v1.0.pdf</mdrpi:
RegistrationPolicy> </mdrpi:RegistrationInfo>
```

5 Varlığın Uygunluğu ve Onayı

5.1 Varlık Kaydı

Bir Federasyon üyesinin, bir varlığını kayıt ettirme süreci aşağıdaki adreste açıklanmaktadır:

<https://yetkim.ulakbim.gov.tr/katilim/>

Federasyon İşletmecisi, üyenin, varlık kimliği niteliklerine ilişkin, kullanacağı alan adlarını tasdik eder.

Alan adı aşağıdaki yollardan biriyle tasdik edilir:

- Üyenin kanonik adı, DNS tescil bilgileri ile eşleşmelidir.
- Üye, alan adı sahibinden alınmış izin yazısıyla, belirli bir alan adını kullanma hakkını almış olmalıdır. Bu izin yazısı varlık bazında olmalıdır ve alt alan adlarının kullanım izni olarak kabul edilemez.

5.2 Varlık Kimliđi Biçimi

Kayıtlı varlık kimliđi niteliđinin deđeri, http ve https şemalarını kullanan mutlak bir URI olmalıdır.

https-şema URI'lerin kullanımı TAVSİYE EDİLİR.

Varlık kimliđi deđerleri için kullanılan http-şema ve https-şema URI'lerinin, host bölümü bir DNS alanı olmalıdır.

5.3 Varlık Doğrulama

Varlık kaydı sırasında, Federasyon İşletmecisi varlık doğrulama kontrollerini gerçekleştirir. Bu kontroller şunları içerir:

- Gerekli tüm bilginin üstverilerde mevcut olmasını sağlamak.
- Üstverinin doğru biçimde biçimlendirilmesini sağlamak.
- Protokol uç noktalarının TLS / SSL sertifikalarıyla uygun şekilde korunmasını sağlamak.

6 Varlık Yönetimi

Üye Federasyona katıldıktan sonra, dilediđi kadar varlık ekleyebilir, deđiştirebilir veya kaldırabilir.

6.1 Varlık Deđişim Talepleri

Federasyon üyelerinden varlık eklenmesi, deđiştirilmesi veya kaldırılması için yapılan talepler ilgili Kayıtlı Temsilcileri tarafından iletilmeli veya onaylanmalıdır.

Deđişim ile ilgili iletişim e-posta yoluyla gerçekleşir..

6.2 Talep Edilmemiş Varlık Deđişiklikleri

Federasyon İşletmecisi, aşağıdaki amaçlar için, Federasyon üstverisini istediđi zaman iyileştirebilir veya deđiştirebilir:

- Üstverinin güvenliđini ve bütünlüğünü sağlamak;
- Federasyonlararası anlaşmalara uymak;
- Birlikte çalışabilirliđi artırmak;
- Üstverilere deđer katmak.

Deđişiklikler, varlığın Kayıtlı Temsilcilerine bildirilecektir.

7 Kaynakça

[SAML-Metadata-RPI-V1.0]	SAML V2.0 Metadata Extensions for Registration and Publication Information Version 1.0. 03 April 2012. OASIS Committee Specification 01. http://docs.oasis-open.org/security/saml/Post2.0/saml-metadata-rpi/v1.0/cs01/saml-metadata-rpi-v1.0-cs01.html .
[SAML-Metadata-OS]	OASIS Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0: http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf .