KAIA-OR · TEKNİK RAPOR · GİZLİLİK

Mimari düzeyde gizlilik

KAIA-OR'un hassas kanıtları nasıl cihazda tuttuğu, her kurumun verilerini nasıl birbirinden ayrı tuttuğu ve bir aileye ya da iş yerine üyeliğin başkalarının hayatına bakmanın bir yolu hâline gelmemesini nasıl sağladığı.

BELGE KİMLİĞİ	WP-2
SÜRÜM	1.0
TARİH	3 Kasım 2026
HEDEF KİTLE	Gizlilik sorumluları, veri koruma ve hukuk ekipleri, çalışan temsilcileri, güvenlik mimarları, aile alanını yöneten kişiler ve bireyler

İçindekiler

1. Yönetici özeti 3
2. Güvenlik araçları neden gözetim aracına dönüşür ve ilkelerimiz 4
    1. Üç örüntü 4
    2. Altı ilke 4
3. Cihazda neler kalır ve bir kurum neleri görür 6
4. Kiracı yalıtımı ve üyelik 8
    1. Kurumlar arası yalıtım 8
    2. Aileler 8
    3. İş yerleri: çalışan temsilcileri ve gizlilik sorumluları için 8
5. Bulut tabanlı yapay zekâ için rıza, yetki ve verilerin bulunduğu yer 10
6. Bu özellikleri nasıl test ediyoruz ve her tedarikçiye sorulacak sorular 11
7. Bunun sizin için anlamı 12
    1. Terimler sözlüğü 12

© Kaia Technologies, Inc.

Yönetici özeti

Güvenlik ürünleri alışılmadık bir güven ister. Yerlerinizi ve seyahatlerinizi neyin etkilediğini size söyleyebilmek için bir ürünün nerede olduğunuzu bilmesi gerekiyormuş gibi görünür. Şüpheli bir mesajı kontrol edebilmek için onu okuması gerekiyormuş gibi görünür. Bir aileye ya da iş yerine hizmet verebilmek için birinin başkalarının cihazlarının içine bakmasına izin vermesi gerekiyormuş gibi görünür. Pek çok ürün bu ödünleşimleri kabul eder ve zamanla bir güvenlik aracı bir gözetim aracına dönüşür.

KAIA-OR bu ödünleşimlere gerek kalmayacak şekilde tasarlanmıştır. Gizlilik, daha sonra sessizce değiştirilebilecek bir ayar değil, mimarinin bir özelliğidir. Onu altı ilke tanımlar:

- **Önce yerel.** Kayıtlı yerler, anlık konum, kontrol edilen mesajlar ve bağlantılar ve konu tercihleri cihazda kalır. Eşleştirme ve asistan önce cihazda çalışır; sorular bulut tabanlı bir yapay zekâ hizmetine yalnızca kişinin kendi rızasıyla ulaşır.
- **Önce rıza, sonra bulut tabanlı yapay zekâ.** Bulut tabanlı bir yapay zekâ hizmetine herhangi bir şey gönderilmeden önce her kişi kendi rızasını verir. Kamu kurumlarında bulut tabanlı yapay zekâ başlangıçta kapalıdır.
- **Üyelik erişim hakkı vermez.** Roller kişileri değil, üyeliği yönetir. Üyelik, başka bir üyenin mesajlarına, cihazlarına, konumuna veya kayıtlı yerlerine asla erişim hakkı vermez.
- **Kurumlar arası yalıtım.** Kiracı (müşteri ortamı) yalıtımı uygulama katmanında sağlanır ve özel nitelikteki her işlem kiracı ve cihaz için yetkilendirilir.
- **Yapay zekâ bilgi verir, kararı insanlar verir.** Model çıktısı hiçbir yetki vermez.
- **Asgari veri.** KAIA-OR yalnızca bir özelliğin ihtiyaç duyduğu verileri toplar.

Bu rapor her ilkeyi, bunun bireyler, aileler ve kurumlar için ne anlama geldiğini ve ilkenin geçerliliğini nasıl test ettiğimizi açıklar. Rapor, herhangi bir alıcının gizlilik konusunda herhangi bir tedarikçiye sorabileceği sorularla sona erer.

> **BU RAPOR HAKKINDA**
> Bu rapor, KAIA-OR'un tasarımını ve taahhüt edilen ürün kapsamını ilkeler ve kavramsal mimari düzeyinde açıklar. Bir yeteneğin sunulup sunulmadığı pakete ve kuruluma bağlıdır. Sözleşme koşulları KAIA-OR hukuki belgelerinde yer alır ve bu belgeler bu rapora göre önceliklidir.

© Kaia Technologies, Inc.

1. Güvenlik araçları neden gözetim aracına dönüşür ve ilkelerimiz

Üç örüntü

Yaygın üç örüntü, koruma amaçlı araçları gözlem araçlarına dönüştürür.

- **Temel özellik olarak konum paylaşımı.** Pek çok aile ürünü, üyelerin nerede olduğunu görme üzerine kuruludur. Konum ürünün kendisi olduğunda her üyenin hareketleri başka biri tarafından görülebilir hâle gelir ve bundan vazgeçmek, üründen ayrılmak anlamına gelir.
- **Güvenlik modeli olarak içerik denetimi.** Bazı ürünler insanları, onlar adına mesajlarını, internette gezinmelerini veya hesaplarını inceleyerek korur. Koruma ancak başka biri görebildiği sürece işler.
- **İşverenin kişisel cihazlara uzanması.** Kurum odaklı tasarlanmış çalışan güvenliği araçları çoğu zaman çalışanların kişisel telefonlarına kadar uzanır. Seyahat edenler için işverenin programı, işverenin personelin nerede olduğunu gördüğü bir pencereye dönüşür.

Her örüntünün makul bir gerekçesi vardır: endişeli bir yakın, sorumlu bir işveren. Her biri aynı sonucu doğurur. Korunan kişi, kendisiyle ilgili bilgiler üzerindeki denetimini kaybeder. İş yerlerinde bu durum, çalışan temsilcilerinin ve gizlilik sorumlularının haklı olarak sorduğu soruları gündeme getirir. Ailelerde yetişkinler arasındaki güveni aşındırır. İşe yarar bir güvenlik sunmak için bu bedellerin hiçbiri gerekli değildir.

Alternatif, korumayı kişinin bulunduğu yere koymaktır. Olaylar yerlerle cihazda eşleştirilirse yerleri başka kimsenin bilmesi gerekmez. Bir mesaj cihazda kontrol edilirse onu başka kimsenin okuması gerekmez. Bir ailenin ya da kurumun her üyesinin kendi KAIA-OR'u olursa kimsenin başkasınınkine bakması gerekmez.

Altı ilke

İLKELER VE HER BİRİNİN DIŞARIDA BIRAKTIKLARI

İlke	Ne anlama gelir	Neyi dışarıda bırakır
Önce yerel	Hassas kanıtlar ve kesin konum varsayılan olarak cihazda kalır. Eşleştirme ve asistan önce cihazda çalışır.	İnsanların nerede olduğunun ve neleri kontrol ettiğinin merkezde toplanması
Önce rıza, sonra bulut tabanlı yapay zekâ	Bulut tabanlı bir yapay zekâ hizmetine herhangi bir şey gönderilmeden önce her kişi kendi rızasını verir. Kamu kurumlarında bulut tabanlı yapay zekâ başlangıçta kapalıdır.	Kişisel içerik üzerinde üçüncü taraf bir yapay zekâ hizmetinin sessizce kullanılması
Üyelik erişim hakkı vermez	Roller kişileri değil, üyeliği yönetir.	Sahiplerin veya Yöneticilerin üyelerin mesajlarını, cihazlarını, konumunu veya kayıtlı yerlerini görmesi
Kurumlar arası yalıtım	Kiracı yalıtımı uygulama katmanında sağlanır. Özel nitelikteki her işlem kiracı ve cihaz için yetkilendirilir.	Bir kurumun verilerinin başka bir kuruma ulaşması

© Kaia Technologies, Inc.

İlke	Ne anlama gelir	Neyi dışarıda bırakır
Yapay zekâ bilgi verir, kararı insanlar verir	Model çıktısı hiçbir yetki vermez. Tarama araçları yalnızca sizin belirlediğiniz sınırlar içinde ve sizin yetkinizle harekete geçer.	Güncelliğini yitirmiş veya bilinmeyen kanıtlara dayanılarak alınan otomatik kararlar veya yapılan otomatik işlemler
Asgari veri	KAIA-OR yalnızca bir özelliğin ihtiyaç duyduğu verileri toplar.	Verilerin bir gün işe yarar diye toplanması

İlkeler bilerek basit tutulmuştur. Her biri tek bir cümleyle ifade edilip test edilebilir ve kişi Bireysel paketinden Kamu paketine kadar hangi paketi kullanırsa kullansın her biri geçerlidir.

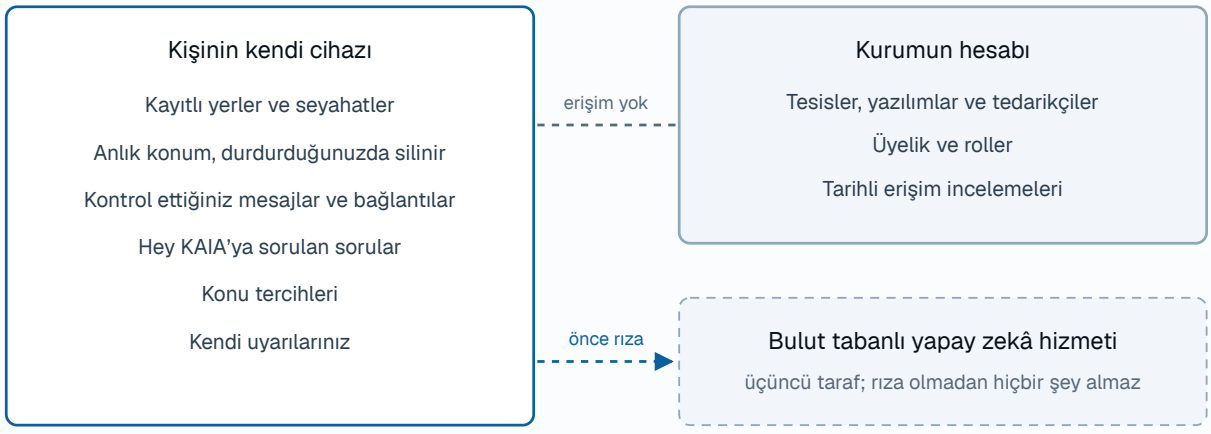
© Kaia Technologies, Inc.

2. Cihazda neler kalır ve bir kurum neleri görür

En işe yarar gizlilik açıklaması somut olanıdır. Aşağıdaki tablo, bilgilerin nerede kaldığını ve onları kimin görebildiğini madde madde listeler.

BİLGİLERİN KALDIĞI YER

Bilgi	Nerede kalır	Kim görebilir
Kayıtlı yerler ve seyahatler	Cihazınızda	Siz
Anlık konum	Cihazınızda; çevre kontrolü için kullanılır ve durdurduğunuzda silinir	Siz
Kontrol ettiğiniz mesajlar ve bağlantılar	Cihazınızda	Siz
Hey KAIA'ya sorulan sorular	Cihazınızda; bulut tabanlı bir yapay zekâ hizmetine yalnızca rızanızla gönderilir	Siz
Konu tercihleri	Cihazınızda	Siz
Uyarılarınız	Cihazınızda; cihaz bildirimleri yeri veya olayı asla belirtmez	Siz
Kurumun tesisleri, yazılımları ve tedarikçileri	Kurumun ortak tablosunda	Kurumun rollerinin izin verdiği kişiler
Üyelik ve erişim kayıtları	Kurumun hesabında	Kurumun Sahip ve Yöneticileri; indirebilecekleri tarihli erişim incelemeleri ve görebilecekleri yetki etkinliği aracılığıyla



Şekil 1. Bilgilerin kaldığı yer. Şekil kavramsaldır; hiçbir hizmetin, tedarikçinin veya altyapının adını vermez.

© Kaia Technologies, Inc.

Bir kurumun gördükleri. Kendi tesisleri, yazılımları ve tedarikçileri, bunları ilgilendiren olaylar ve kendi hesabının üyeliği. **Görmedikleri.** Üyelerinin yerleri, seyahatleri, nerede oldukları, mesajları, bağlantıları, asistana sordukları sorular veya cihazları. Kurum, kişilerin nerede olduğunu değil, kendi tesislerini görür.

Paylaşım üyenin tercihidir. Bir üye, cihazının güvenlik durumunu aile Sahibiyle veya bir kurum Yöneticisiyle paylaşmayı seçebilir. Bu seçimi üye, kendi cihazında yapar.

© Kaia Technologies, Inc.

3. Kiracı yalıtımı ve üyelik

Kurumlar arası yalıtım

KAIA-OR'daki her kurum ayrı bir kiracıdır. Kiracı yalıtımı uygulama katmanında sağlanır. Yetkilendirme yalnızca girişte değil, özel nitelikteki her işlemde zorunludur: herhangi bir özel veri okunmadan veya değiştirilmeden önce talebin, geldiği kiracı ve cihaz için yetkilendirilmiş olması gerekir. Doğru kiracıya ve cihaza bağlanamayan bir talep reddedilir. Yapılandırılmamış bir entegrasyon, izin verici bir varsayılana geri dönmek yerine kapalı kalır ve gerçek durumunu gösterir.

İki kural daha yetkiyi dar tutar. Bilinmeyen veya güncelliğini yitirmiş kanıt bir müdahaleye yetki veremez. Bir yapay zekâ modelinin hiçbir çıktısı da bir kişinin, bir rolün veya bir otomatik aracın yapmasına izin verilenleri genişletemez. Dolayısıyla yalıtım yalnızca kurumlar arasında bir sınır değildir; bir talebin iddia ettiği ile yapmasına izin verilen arasında da bir sınırdır.

Aileler

Davet ettiğiniz her yetişkin, ayrı yaşasa bile kendi KAIA-OR'unu alır: kendi yerleri ve seyahatleri, kendi uyarıları ve İngilizce, Fransızca, Türkçe veya İbranice mesajlara ve bağlantılara kendi ikinci bakışı. Kimin üye olduğunu aile Sahibi yönetir. Üyelik, başka bir üyenin mesajlarına, cihazlarına, konumuna veya kayıtlı yerlerine asla erişim hakkı vermez. Hiç kimse başka bir üye adına yer eklemez.

Bu, bir aile ürününün ne işe yaradığına dair bilinçli bir tercihtir. Bir aileye, yetişkinlerden birinin diğerlerinin nerede olduğunu görmesiyle değil, her yetişkinin kendi cihazında, kendi dilinde kendi yardımına sahip olmasıyla hizmet edilir. Roller kişileri değil, üyeliği yönetir.

İş yerleri: çalışan temsilcileri ve gizlilik sorumluları için

İşverenlerin tesislerine ve çalışanlarına karşı meşru sorumlulukları vardır. Çalışanların da bir iş yeri güvenlik ürününün kişisel hayatlarına açılan bir pencereye dönüşmemesine ilişkin meşru bir beklentisi vardır. KAIA-OR bu sınırı mimaride çizer; böylece sınır, değiştirilebilecek bir politikaya bağlı kalmaz.

BİR İŞVERENİN GÖREBİLDİKLERİ VE GÖREMEDİKLERİ

İşveren şunları yapabilir	İşveren şunları yapamaz
Kendi tesislerini, yazılımlarını ve tedarikçilerini ve bunları ilgilendiren olayları görmek	Çalışanların iş yerinde veya yurt dışında nerede olduğunu görmek
Üyeliği roller aracılığıyla yönetmek	Çalışanların kişisel yerlerini veya seyahatlerini görmek
Bir hesaba bağlı tek kullanımlık davetler oluşturmak	Çalışanların kontrol ettiği mesajları veya bağlantıları okumak
Tarihli erişim incelemeleri yapmak ve indirmek, yetki etkinliğini görmek	Çalışanların Hey KAIA'ya sorduğu soruları okumak
Olayları API ve webhook'lar aracılığıyla kendi araçlarına göndermek	Çalışanların cihazlarını incelemek; bir çalışan cihazının güvenlik durumunu paylaşmayı kendisi seçebilir

© Kaia Technologies, Inc.

Seyahat edenler. Seyahat eden her çalışan kendi seyahatleri için kendi uyarılarını alır ve varış noktasının resmî seyahat tavsiyesinde nelerin değiştiğini görür. Kuruma çalışanların nerede olduğu bildirilmez ve kurum onların hareketlerini takip etmez.

Çalışan temsilcilerinin sorabileceği sorular. İşveren nerede olduğumu görebilir mi? Hayır. Kontrol ettiklerimi okuyabilir mi? Hayır. Bir yönetici KAIA-OR'uma yer ekleyebilir ya da benim yerlerimi görebilir mi? Hayır. Yapay zekâ benim hakkımda bir karar verebilir mi? Hayır: model çıktısı hiçbir yetki vermez ve kararlar insanlarda kalır.

© Kaia Technologies, Inc.

4. Bulut tabanlı yapay zekâ için rıza, yetki ve verilerin bulunduğu yer

Bulut tabanlı yapay zekâ yalnızca rızayla. Hey KAIA önce cihazda çalışır. Bazı sorular daha büyük bir bulut tabanlı yapay zekâ hizmetinden yarar sağlar. KAIA-OR açık rıza olmadan bulut tabanlı bir yapay zekâ hizmetine hiçbir zaman hiçbir şey göndermez. Böyle bir hizmet kullanıldığında bu, üçüncü taraf bir yapay zekâ hizmetidir ve herhangi bir şey gönderilmeden önce kişinin kendi rızası, özellik bazında istenir. Bu rızayı yalnızca o kişi verebilir. Kamu kurumlarında bulut tabanlı yapay zekâ başlangıçta kapalıdır.

Kendine yetki veremeyen yapay zekâ. Kendine erişim yetkisi verebilen bir asistan, bu rapordaki diğer ilkeleri dolanmanın bir yolu olurdu. KAIA-OR'da model çıktısı hiçbir yetki vermez. Bir modelin ürettiği hiçbir şey bir işlemi onaylayamaz, bir izni değiştiremez ya da bir otomatik aracın yapabileceklerini genişletemez. Tarama araçları yalnızca kişinin veya kurumun belirlediği sınırlar içinde ve yalnızca yetkiyle harekete geçer. Hiçbir otomatik araç açık yetki olmadan yıkıcı bir işlem yapmaz, mesaj göndermez veya satın alma yapmaz. Asistan, okuduğu içeriğe gizlenmiş talimatlara ve doğrudan yapay zekâyı hedef alan sosyal mühendisliğe direnecek şekilde tasarlanmıştır.

Verilerin bulunduğu yer: sizin yaptığınız seçimler. Bireyler ve aileler için verilerin nerede bulunacağına ilişkin en önemli seçimi mimari yapar: hassas kişisel kanıtlar varsayılan olarak cihazda kalır. Geri kalan seçimler açıktır ve kişiye aittir: bulut tabanlı yapay zekânın kullanılıp kullanılmayacağı ve cihaz durumunun paylaşılıp paylaşılmayacağı. Kurumlar için ortak tablo, kurumun kendisinin girdiklerini (tesislerini, yazılımlarını ve tedarikçilerini) ve üyelik kayıtlarını içerir. Kurum, paylaşılan verilerinin tutulduğu bölgeyi kendisi seçer. Barındırmaya ilişkin diğer gereksinimler değerlendirme sırasında ekibimizle görüşülür ve sözleşmede yer alır.

> **UYGULAMADA ASGARİ VERİ**
>
> KAIA-OR'un yerlerinizi neyin etkilediğini size söylemek için nerede olduğunuzu bilmesi gerekmez; çünkü eşleştirme cihazınızda yapılır. Size ikinci bir bakış sunmak için mesajlarınızı merkezde okuması gerekmez; çünkü kontrol, mesajın zaten bulunduğu yerde yapılır. Merkezî bir hizmet ne kadar az veri tutarsa açığa çıkabilecek veri de o kadar az olur.

© Kaia Technologies, Inc.

5. Bu özellikleri nasıl test ediyoruz ve her tedarikçiye sorulacak sorular

Gizlilik ilkeleri ancak uygulamada geçerli olduklarında işe yarar. Güvencemizi iç ayrıntılar düzeyinde değil, uygulama düzeyinde açıklıyoruz.

- **Güvenli yazılım geliştirme uygulamaları;** her sürümün bir parçası olarak tür denetimi ve güvenlik testleriyle.
- **Sabitlenmiş bağımlılıklar ve tedarik zinciri kontrolleri;** yazılım derlenip yayımlanmadan önce.
- **Yalıtım testleri.** Kiracı ve cihaz yetkilendirmesi her derlemede otomatik yalıtım testleriyle sınanır ve bağımsız incelemeye tabidir.
- **İddia değil, kanıt.** Başarılı bir derleme bir güvenlik sonucu değildir. Testler bir özelliğin test edilen durumlarda geçerli olduğunu gösterir; biz de onları bu şekilde anlatırız.
- **Güvenlik açığı bildirimi.** Güvenlik araştırmacıları bir güvenlik açığını KAIA-OR Güven sayfasındaki iletişim adresi aracılığıyla bildirebilir.

Aşağıdaki sorular, biz dâhil, aile, çalışan veya kişisel güvenlik yazılımı sunan her tedarikçiye yöneltilebilir.

GİZLİLİK KONUSUNDA HER TEDARİKÇİYE SORULACAK SORULAR

Sorun	Güçlü bir yanıt
Kesin konumum ve kayıtlı yerlerim nerede işleniyor ve saklanıyor?	Cihazımda; konum, durdurduğumda siliniyor.
Bir aile Sahibi veya bir işveren üyelerin mesajlarını, cihazlarını, konumunu veya yerlerini görebilir mi?	Hayır. Üyelik erişim hakkı vermez.
Bulut tabanlı yapay zekâ kullanılıyor mu ve herhangi bir şey gönderilmeden önce rıza isteniyor mu?	Yalnızca her kişinin kendi açık rızasıyla ve özellik bazında.
Yapay zekâ çıktısı izinleri değiştirebilir veya işlem başlatabilir mi?	Hayır. Yetki yalnızca doğru role sahip kişilerden gelir.
Bir kurumun verileri diğerininkinden nasıl ayrı tutuluyor?	Kiracı yalıtımıyla; özel nitelikteki her işlemde yetkilendirmeyle ve bunu gösteren testlerle.
Kurum seyahat eden çalışanlar hakkında neleri görüyor?	Seyahat edenlerin nerede olduğunu değil, kendi tesislerini ve bunları ilgilendiren olayları.
Testlerinizin sınırlarını nasıl anlatıyorsunuz?	Açıkça; bir vaat olarak değil, test edilen durumlar için kanıt olarak.

© Kaia Technologies, Inc.

Bunun sizin için anlamı

Bireyler. Yerleriniz, konumunuz ve kontrol ettikleriniz cihazınızda kalır. Siz önce kabul etmedikçe hiçbir şey bulut tabanlı bir yapay zekâ hizmetine gitmez.

Aileler. Her yetişkin kendi KAIA-OR'unu korur. Üyeliği aile Sahibi yönetir ve üyelik, başka bir üyenin mesajlarına, cihazlarına, konumuna veya kayıtlı yerlerine asla erişim hakkı vermez.

Kurumlar, çalışan temsilcileri ve gizlilik sorumluları. Kurum, kişilerin nerede olduğunu değil, kendi tesislerini görür. Erişimin hesabı tek kullanımlık davetler, indirilebilen tarihli erişim incelemeleri ve yetki etkinliği aracılığıyla verilir. Kiracı yalıtımı uygulama katmanında sağlanır.

Kamu kurumları. Bulut tabanlı yapay zekâ başlangıçta kapalıdır ve her kişi kendi rızasını verir. Model çıktısı hiçbir yetki vermez; tarama araçları yalnızca sizin yetkinizle harekete geçer. KAIA-OR'u değerlendirmek için KAIA-OR web sitesinden erken erişim talep edin ya da "Bize ulaşın" seçeneğini kullanın.

Terimler sözlüğü

Terim	Bu rapordaki anlamı
Kiracı	Bir kurumun KAIA-OR'daki ayrı alanı (müşteri ortamı): tesisleri, yazılımları, tedarikçileri ve üyeliği.
Kiracı yalıtımı	Her kiracının verilerinin ayrı tutulması; özel nitelikteki her işlemin yetkilendirilmesiyle uygulama katmanında sağlanır.
Önce yerel	Hassas kanıtların varsayılan olarak kişinin kendi cihazında işlenmesi ve tutulması.
Üyelik	KAIA-OR'da bir aileye veya kuruma ait olmak. Başka bir üyenin verilerine asla erişim hakkı vermez.
Bulut tabanlı yapay zekâ hizmeti	Açık rıza olmadan hiçbir şey almayan üçüncü taraf bir yapay zekâ hizmeti.
Erişim incelemesi	Bir kurumun hesabına kimin hangi rolle erişimi olduğunun tarihli kaydı.

© Kaia Technologies, Inc.

WP-2 · Sürüm 1.0 · 3 Kasım 2026

Bir yeteneğin sunulup sunulmadığı pakete ve kuruluma bağlıdır. Yetenekler, KAIA-OR'un taahhüt edilen ürün kapsamı olarak açıklanmıştır.