

Durum

ADAXO: Otomotiv Veri Eriřimi – Geniřletilmiş ve Aık

Ara tarafından oluřturulan verilere eriřim iin VDA
konsepti



İçerik

I Özet	2
II Sınıflandırma ve bağlam	6
II.1. İnovasyonun teşviki bağlamında Avrupa ve ulusal veri stratejileri	6
II.2. Düzenleyici çerçeve	7
II.3 Otomotiv endüstrisi açısından düzenleyici yoğunluk	8
II.4. Veriye dayalı iş modellerinin ve yeniliklerin desteklenmesi	8
II.5. Araç verilerine güvenli erişim	9
III ADAXO concept - teknik detaylar	10
III.1. ADAXO konseptinde veri akışı ve sözleşme ilişkileri	10
III.2. FRAND ilkelerine göre veri erişimi	11
III.3. ADAXO'da yetkilendirme ve onay yönetimi	12
III.4. Siber Güvenlik	14
III.5. Bağlantı için önkoşullar	15
III.6. Araç kaynaklarına ücretsiz erişim	15
III.6.1 Araç kaynaklarına ayrımcı olmayan erişim	15
III.6.2 İzleme ve uygulama	16
III.6.3. Yetkisiz iş izlemenin önlenmesi	16
III.6.4. Erişim kimlik doğrulaması	17
III.6.5. Sorumluluk	18
III.6.6. Son müşteri tanımlama	19
III.7. Araçtaki çeşitli veri mimarilerinin illüstrasyonu	19
III.7.1. Yerleşik yazılımın kurulumu ve yürütülmesi	22
III.7.2 HMI (insan-makine arayüzü) üzerinden sürücü ile etkileşim	23
III.8. Yerleşik Tanılama (OBD) Arabirimi Üzerinden Erişim	25
IV Otomotiv sektörü için bütüncül bir kavramdan ilerici eylem önerisi	26
IV.1. Tesisler ve temel hedefler	26
IV.2. Otomotiv endüstrisinde veri ekonomisinin uygulanmasına yönelik eylem önerisi	27
V Ekler	29
V.1. AB Komisyonu Çalışması: TRL Çözüm Önlemleri ve İlk Değerlendirme	29
V.2. Uzaktan tanılama işlemlerinin detaylandırılması	31
V.3. Sözlük	33

I Özet

1. Veri yoluyla inovasyon – veri değer zinciri: veri üretiminden müşteriye yönelik hizmet sunumuna kadar

VDA üyesi şirketler müşteri odaklı kullanım için kapsamlı veriler hazırlıyor ve bu konuda çok çeşitli teknik erişim seçenekleri sunuyor. Bu proaktif teklif sürekli olarak genişletiliyor.

Otomotiv endüstrisinin inovasyonu ve veriye dayalı iş modellerini geliştirme taahhüdü, ileriye dönük işletim sistemlerine, elektrik / elektronik mimarilerine ve bağlantıya yatırılan milyarlarca avroya yansıyor.

Bu yatırımlar, araç verilerine dayalı tüm iş modellerinin temelini oluşturur.

2. Müşterilerimiz, mobilite ve çevre için ortak bir veri pazarı

VDA çatısı altında iş birliği yapan şirketler, verileri kullanarak ve paylaşarak yaratılabilecek katma değere inanmaktadır. Veri teklifini genişletmek ve teknik erişimi güvence altına almak için proaktif bir şekilde birlikte çalışarak bu katma değeri artırıyoruz.

Böylece müşterilerimize ilgili veri tabanlı hizmetler aracılığıyla katma değer sunabiliyoruz. Müşterilerimizin ve toplumumuzun hareketliliğini de çevre veya iklim üzerinde olumsuz etki yaratmayacak güvenli bir şekilde geliştirebiliyoruz.

Müşteriler, yürürlükteki mevzuata tabi olarak verileri üzerinde egemenliğe sahiptir. Bu, katılan herkese eşit bir oyun alanı ve gelişmekte olan veri pazarını geliştirme alanı sağlayan istikrarlı ve güvenilir bir düzenleyici çerçeveye dayanmaktadır.

Taahhüdümüz, tüm paydaşlar için yenilikçi iş modelleri sağlar. VDA'daki tüm şirketler, veri piyasasındaki herhangi bir düzenlemenin, ilgili tüm taraflar için geçerli olan adil oyun kurallarını içereceği konusunda ortak bir anlayışa sahiptir.

Veri kullanılabilirliği ve veri erişimi yalnızca araçlarla değil; servis sağlayıcılar, sigorta şirketleri, finansman şirketleri ve otomotiv ortamındaki diğer alt sektörler tarafından tutulan araçla ilgili verilerle de ilgili olacaktır.

Müşterilerin yararına yeni hizmetler geliştirmenin tek yolu budur.

3. Veri tabanlı bir iş modelinin motoru olarak büyüyen bir veri teklifi

Yalnızca tüm modellerde bütün araç üreticileri tarafından desteklenen kapsamlı bir veri teklifi; servis sağlayıcıların yeni iş modellerini başarıyla kullanıma sunmasını sağlayacaktır. Bu nedenle, VDA üyesi şirketler temel bir veri kümesinin geliştirilmesini desteklemektedir. Bu veri setini yasal gerekliliklere uygun olarak tüm araçlar için kullanılabilir hale getirmek mümkün olmalıdır. Bunun için bir ön koşul da araçların ilgili teknolojilerle donatılmasıdır.

Veri kümesi ortak bir başlangıç noktası olarak görülmelidir. Müşteri odaklı kullanım durumlarına göre sürekli olarak genişletilecektir. Bu genişleme, en büyük müşteri faydasını ve dolayısıyla en büyük talebi gösteren ve verilerin hem hızlı hem de geniş ölçekte sağlanabileceği kullanım durumları tarafından yönlendirilecektir. Kullanım durumlarının genişletilmesine ilişkin kararlar, ortaklar arasındaki diyalog çerçevesinde derneklerle birlikte verilecektir.

İlgili şirketler, genişletilmiş araç (ExVe)¹ web hizmetleri aracılığıyla sunulan tüm çevrimiçi veri teklifleriyle ilgili şeffaflık yaratmayı kabul eder. Bu veriler, birlikte çalışabilirliği garanti altına almak için uygun anlamsal işaretlemeler kullanılarak açıklanmaktadır.

4. ADAXO: Otomotiv Verilerine Erişim – Genişletilmiş ve Açık: Gizlilik Başarı İçin Çok Önemli

VDA, başarısı yeniliğe dayanan ve fikri mülkiyetin korunmasını ve buna bağlı olarak yenilikleri destekleyen şirketleri temsil eder. Veriye dayalı iş modellerinin gizliliği, VDA'nın mevcut konseptinin daha da geliştirilmesi olan ADAXO konsepti ile sağlanmaktadır.

ADAXO konsepti, erişim sağlayan şirketlerin kimliklerini veya iş modellerini birincil veri toplayıcılarına açıklama seçeneği de sunar. ADAXO tarafsızlık kavramı veri alanlarında da uygulanabilir ve bizim için tarafsız veri sağlamadaki mantıklı bir sonraki adımı temsil eder. Sonuçta veriler üzerindeki tam egemenlik araç müşterisinde kalır.

ADAXO veri teklifi, açıklanan kullanım durumu yaklaşımı ile hazırlanacak ve sürekli genişletilecek yukarıda belirtilen ilk veri setini içerir.

¹ Extended vehicle concept: Manufacturers route the data via an OEM back end.

5. FRAND - müşterilerimizin yararına iş ortakları arasındaki işbirliği kuralları

Adil, makul ve ayrımcı olmayan (FRAND); veri pazarındaki tüm katılımcılar için ortak kurallardır. VDA üyesi şirketler, FRAND ilkesine bağlı olan şirketlere veri ve işlevler için FRAND erişimi sunar.

OEM'ler, kendi hizmetlerini sağlamak için kullandıkları tüm veri ve işlevlere erişim sunar. Verilere ayrımcı olmayan erişim sırasıyla B2C veya B2B sözleşmeleri temelinde maskeli (örn. tarafsız sunucu) veya doğrudan OEM aracılığıyla sağlanır.

Her şirket için bireysel sözleşmeler hazırlanır. VDA üyesi şirketlerin bakış açısına göre, antitröst yasası uyarınca buna izin verilmesi koşuluyla standart sözleşme bileşenlerini tanımlamak için çaba gösterilmelidir. Adil veri paylaşımı da engelleyici olmayan şeffaf fiyatlandırmaya dayanmaktadır.

6. Yetkilendirme yönetimi – müşterilerimizin yararına katma değer yaratmak

Yürürlükteki yasalara uygun olarak, veriler yalnızca belirli bir amaç için yani belirli kullanım durumu için aktarılır.

- Müşteri açısından ve veri koruma yasası açısından yetkilendirme yönetimi merkezinin tutarlı ve kullanımı basit olmalıdır. Bu nedenle veri toplama için merkezi iribat noktası olarak üreticiye (OEM) dayanmalıdır.
- Müşteriler veriler üzerinde egemenliğe sahiptir. Yürürlükteki yasalara uygun olarak hangi verilerin hangi alıcılara iletileceğine karar verirler. Üreticiler müşterilerin isteklerine uymalıdır.
- Yasal, sözleşmeye dayalı veya güvenlik nedenleriyle gerekmedikçe ticari veri akışı OEM'ler tarafından izlenmez.
- Gizlilik hükümleri müşteri verilerinin analiz edilmemesini sağlayarak tersine mühendislik yapılmasını önler. Üçüncü taraf hizmetleri için yetkilendirmeler, üçüncü tarafların iş modellerinin OEM'ler tarafından bilinmemesi için şifrelenebilir.

Üreticiler, verileri, ilgili önkoşulları karşılayan OEM tarafından işletilen ve OEM tarafından işletilen olmayan veri pazarlarına erişilebilir hale getirebilir. Birincil veri toplayıcıları, uçtan uca bir yetkilendirme yönetim sistemi aracılığıyla yasal gerekliliklere uyumu sağlayacaktır.

7. Teknik erişim – müşteri odaklı ve verimli veri sağlama

VDA üye şirketleri, araç verilerinin yasal gerekliliklere uygun olarak müşteri odaklı bir şekilde sunulmasını sağlamak için halihazırda çeşitli teknik erişim yöntemleri sunmaktadır. Tüm şirketler, ortaklaşa geliştirilen temel veri seti gibi verilerin FRAND koşulları altında elde edilmesini sağlayan ADAXO konseptini desteklemektedir. Ayrıca, OEM'ler, şirketlerin B2B ve B2C sözleşmelerine dayanarak doğrudan veri edinebilecekleri kendi çevrimiçi portallarını işletmektedir.

Mobilite Veri Alanı (eski adıyla DRM "Datenraum Mobilität"), özellikle standardize veri sağlayıcılarını kullanarak birçok farklı kaynaktan hızlı, verimli ve yüksek şeffaflıkta veri elde etme imkânı sunan başka bir pazar ekleyecektir. Çok sayıda VDA üyesi zaten bu yaklaşımı destekliyor ve daha da genişlemesini teşvik ediyor.

8. Üçüncü taraf veri erişimi – önce güvenlik

Üçüncü taraflara, teknik ve yasal gereklilikleri yerine getirmeleri halinde araç verilerine ve işlevlerine doğrudan erişim izni verilebilir.

Geliştirme ilerledikçe çeşitli araç üreticileri, düzenleyici gerekliliklere (örneğin, siber güvenlik konusunda UNECE R155), sertifikasyon yönlerine ve yazılım güncelleme yönetim sistemlerine ilişkin gerekliliklere (UNECE R156) tabi olarak, araçlara üçüncü taraf sağlayıcılardan yazılım yükleme seçeneği sunacaktır. Bu amaçla, araçlara üçüncü taraf yazılımların yüklenmesi için güvenli bir temel sağlamak üzere derneklerle iş birliği içinde kılavuzlar geliştirilmelidir.

Bununla birlikte temel olarak, yalnızca aracı sertifikalandırmaktan sorumlu olan şirket yazılımı onaylayabilir ve araç kaynaklarını yönetebilir (örneğin, araçtaki veri iletimi için bant genişlikleri). Olası seçenekleri veya gelişmeleri göz önünde bulundururken, tüm şirketler tüm yol kullanıcılarının güvenliğine öncelik vermelidir.

II Sınıflandırma ve bağlam

II.1. İnovasyonun teşviki bağlamında Avrupa ve ulusal veri stratejileri

2020 Yılında AB Komisyonu, Avrupa veri stratejisi ile Avrupa'da veri ekonomisi vizyonunu yayınladı. AB, üye ülkeler ve sektörler arasında Avrupa değerleri ve standartları temelinde ve adil, pratik ve açık kurallar çerçevesinde veri akışlarıyla ortak bir veri pazarı için çalışacaktır. Amaç, Avrupa'da hem vatandaşlar hem de sanayi paydaşları için değer yaratılmasını arttırmaktır. Özellikle, eşit bir oyun alanı fikrine uygun olarak katılan herkes arasında adil bir veri paylaşımının olması sağlanmalıdır. Bu, bireysel çıkar gruplarının, sektörlerin veya şirket boyutlarının tercihli muamelesini engellemeyi amaçlamaktadır.

Bu AB stratejisinin ve ulusal veri stratejilerinin arka planına karşı, AB Komisyonu ardışık düzenlemeler yayınladı ve şu anda ek düzenleyici projeler üzerinde çalışıyor. İşte bazı örnekler:

1. Avrupa veri ekonomisini güçlendirmeyi amaçlayan Veri Yönetişimi Yasası (DGA) taslağı Kasım 2020'de sunuldu. Bu amaçla şirketler, özel kişiler ve kamu sektörü arasındaki veri paylaşımı basitleştirilmeli ve kurulan veri aktarımına güvenilmelidir.
2. Veri Yasası (DA), hem kamu hem de özel aktörlerin verilerine genişletilmiş erişimi ve bunların kullanımını ele alır. İlgili bireysel paydaşlar arasında veri piyasasında adaletin sağlanması amaçlanmıştır. DA, işletmeden işletmeye (B2B) veri ve işletmeden devlete (B2G) veri paylaşımını açıkça ele almaktadır.
3. Büyük, çevrimiçi platformları kapı bekçisi olarak nitelendirmek için dar tanımlanmış bir dizi kriter belirleyen Dijital Piyasalar Yasası (DMA), veri pazarlarındaki piyasa gücünü dengelemeyi amaçlamaktadır.
4. Dijital Hizmetler Yasası (DSA), veri pazarındaki daha küçük platformlarının, KOBİ'lerin ve girişimlerin genişlemesini kolaylaştırmayı amaçlamaktadır. Kullanıcıların temel haklarının korunduğu daha güvenli bir dijital alan yaratmayı ve işletmeler için seviyeli bir oyun alanı oluşturmayı hedeflemektedir.
5. **Yüksek Değerli Veri Kümeleri Uygulama Yasası**, verilerin sosyoekonomik potansiyelini açığa çıkarmayı amaçlamaktadır.

Atıf yapılan tüm düzenleyici projelerin ortak bir yönü var: Avrupa düzeyinde bir veri pazarına yönelik yeniliği teşvik etmenin yanı sıra müşterileri ve veri egemenliği haklarını güçlendiriyor.

² https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en.

Ancak bu çabalar Avrupa düzeyinde sınırlı değil: AB üye ülkeleri dijitalleşmeye geçişi sağlayacak ulusal düzeyde stratejiler de geliştiriyor. Örneğin Federal Alman hükümeti, Federal Alman Hükümetinin Veri Stratejisini Hazırladı. Bu, sosyal ilerleme ve sürdürülebilir büyüme için inovasyon stratejisini açıklar. Bu stratejinin temel amacı bir veri kültürü oluşturmaktır

- toplumun temel değerlerini, hak ve özgürlüklerini koruyan
- aynı zamanda, veri sunumunu önemli ölçüde artırırken, böylece yenilikçiliği teşvik etmek.

Veri stratejisinin uygulanmasının temeli, etkin ve güvenli veri altyapılarının sürdürülebilir bir şekilde genişletilmesi ve diğer şeylerin yanı sıra sanayi, Yeşil Anlaşma ve mobilite gibi sektörel veri alanlarının oluşturulmasını içermektedir.

Diğer AB üyeleri kendi ulusal veri stratejileriyle karşılaştırılabilir hedefler peşindedir.

II.2. Eşit bir oyun alanı olarak düzenleyici çerçeve

AB'nin yasal girişimleri, veri paylaşımı konusunda şirketler için iç pazarda eşit bir oyun alanı sağlamayı amaçlamaktadır. Bunun temeli, tüm katılımcılara eşit bir oyun alanı ve gelişmekte olan veri pazarlarını geliştirme alanı sağlayan istikrarlı ve güvenilir bir düzenleyici çerçevedir.

VDA'daki tüm şirketler, veri piyasasındaki herhangi bir düzenlemenin, ilgili tüm taraflar için geçerli olan adil oyun kurallarını içermesi gerektiği konusunda ortak bir anlayışa sahiptir.

Veri kullanılabilirliğini ve veri erişimini yeniden belirleyen bu kurallar yalnızca araçlarla değil, aynı zamanda servis sağlayıcılar, sigorta şirketleri, finansman şirketleri ve otomotiv ortamındaki diğer alt sektörler tarafından tutulan araçla ilgili verilerle de ilgili olacaktır.

Avrupa'daki sektörler arasında veri teklifinin stratejik olarak anlamlı bir şekilde genişletilmesi, tüm taraflar için pozisyonların paylaşılacağı ve çıkarların dengelenmesinin müzakere edilebileceği bir forum gerektirmektedir. Planlanan yönetmelikler dahilinde şu anda belirsiz veya kısıtlayıcı önkoşullara yönelik çözümler burada birlikte tartışılabilir ve geliştirilebilir.

Alman otomotiv endüstrisi birliği olarak VDA, Avrupa iç pazarındaki veri kültürünü önemli ölçüde geliştirmeye ve yönlendirmeye hazırdır.

³ Data Strategy of the Federal German Government, Cabinet Version dated 27 January 2021.

⁴ Datenstrategien: Was passiert in Deutschland und der EU? (Data strategies: What's happening in Germany and the EU?) › BASECAMP.

II.3. Otomotiv endüstrisi açısından düzenleyici yoğunluk

Giriş niteliğindeki açıklamalar, otomotiv sektörünün inovasyon kabiliyetini doğrudan ve aynı zamanda olumsuz yönde etkileyen düzenleyici yoğunluğu ve buna bağlı gereksinim karmaşıklığını göstermektedir. Şimdiye kadar, düzenleyici projeler arasında neredeyse hiçbir sinerji veya bağlantı görülmemektedir.

Ayrıca, AB Komisyonu bireysel genel müdürlükleri, araç verilerine erişim ile ilgili gereklilikleri açıklayan ve çok ayrıntılı çözümler öneren çalışmalar yaptırmıştır (bkz. Ek V.1). Çeşitli genel müdürlüklerin projelerinin daha iyi koordinasyonu sağlanmalıdır.

Ayrıca, Avrupa yasama girişimleri çerçevesinde paralel ve büyük ölçüde ayrılmış yaklaşım, araç içi verilere erişim bağlamında araç verilerinin türetilmesine ilişkin OEM'LERİN mevcut ve uygulamada test edilmiş kavram ve girişimlerine bakmaktadır.

VDA açısından, verilerle ilgili ek özel düzenlemelere gerek yoktur. Bunlar, veriye dayalı iş modellerinin teknik uygulamasında ve tasarımında ek karmaşıklık yaratır. Her ikisi de inovasyon faaliyetlerini engelliyor – sadece otomotiv endüstrisinde değil, aynı zamanda veri tabanlı hizmetler sunanlar tarafında.

Daha büyük ihtiyaç sektörler arası düzenlemelerin uyumlaştırılmasıdır. Yeni iş modellerinin oluşturulması için dijitalleşme ve sektörler arası veri paylaşımı bağlamında yenilikler ancak bu şekilde yapılabilir.

II.4. Veri odaklı iş modellerinin ve yeniliklerin desteklenmesi

VDA ve üyeleri, veri üretiminden, üreticiler arası ve sektörler arası veri pazarlarının işleyişi için gerekli koşulların oluşturulmasına kadar katma değer zincirindeki yeniliklerle veri üretimini ve veri paylaşımını proaktif olarak desteklemektedir.

Uluslararası rakiplerle başarılı bir şekilde rekabet edebilecek ve piyasaların büyük ilgisiyle karşılaşacak sürdürülebilir rekabet modellerinin geliştirilmesi ve oluşturulması için yıllardır burada büyük yatırımlar yapılmıştır.

Ayrıca, VDA ve üyeleri, uyumlaştırılmış ve sektörler arası veri paylaşımı için kamu sektörü veri alanlarına güvenli bağlantıyı uzun zamandır onaylamış ve desteklemiştir.

II.5. Araç verilerine güvenli erişim

Çeşitli veri stratejilerinin odak noktalarından biri siber suç faaliyetlerine karşı korumadır. Bu hem siyasi sektörün hem de sanayinin stratejileri için geçerlidir. Otomotiv sektöründe dijitalleşme, araçtaki teknik ara yüzlere yönelik potansiyel saldırı tehdidine ve hassas araç işlevlerine yetkisiz erişim riskine yol açmıştır. Ek güvenlik çabaları gerektiren sadece üçüncü taraflarla veri paylaşımına yönelik ara yüzlerin sağlanması değildir. Üçüncü taraf yazma erişimi için çift yönlü bağlantılar veya araçtaki yazılımın üçüncü taraflarca yüklenmesi de korunmalıdır. Arabirimlerin istenen kullanımıyla ilişkili riskler en aza indirilmelidir.

Araç üreticileri, araç mimarisi üzerinde gerekli işlemleri güvenli ve verimli bir şekilde gerçekleştirebildikleri için dış dünyaya bağlanan araçtaki tüm ara yüzlerin emniyete alınmasından büyük ölçüde sorumludur. Buradaki bir diğer önemli husus, dijitalleşmenin hızlı temposu göz önüne alındığında, bu güvencelere yönelik gereksinimlerin giderek daha karmaşık çözümler gerektirmesidir.

Bunun ışığında, araç üreticileri yıllar önce araç verilerine güvenli erişim için genişletilmiş araç konseptini (ExVe) geliştirdiler. ExVe, hücresel arayüz üzerinden araç ile üreticinin sunucusu arasındaki veri paylaşımını ele alır. ExVe web arayüzü tüm modern araçlarda mevcuttur ve araç ile üreticinin 5 sunucusu arasında güvenli iletişim sağlar. Üçüncü taraflar -ilgili B2B sözleşmelerine dayanarak- araç verilerine ISO 20078'e göre standartlaştırılmış bir arayüz üzerinden erişebilirler.

ISO belgeli ve standart arayüz ile araç mimarisine müdahale imkanı yoktur.

ExVe uzun yıllardır başarıyla kullanılmakta ve geniş bir çerçevede kendini kanıtlamıştır. Avrupa'daki milyonlarca araç şu anda bu şekilde araç üreticilerinin sunucularına bağlanmakta ve verileri üçüncü taraflara sunmaktadır. Bu kavramın temel gücü, aktarılan verilerin türüne ve miktarına ilişkin açıklıktır; bu, araç kullanıcılarına, servis sağlayıcılara ve üreticilere aynı anda yasa hükümlerine (AB GDPR) uyurken çok çeşitli yenilikçi uygulama seçenekleri sunar.

ADAXO konsepti ile VDA, araç tarafından üretilen verilerin tüm paydaşlar arasında paylaşılması için modern ve geleceğe yönelik güvenli bir model ve ayrıca araçtaki çift yönlü bağlantılar ve üçüncü taraf yazılımlar için gereklilikler sunar. Bu kavram, bu belgenin sonraki bölümlerinde daha ayrıntılı olarak sunulacaktır.

⁵ Other interfaces, such as the interface between the mobile phone and vehicle or vehicle-to-vehicle communication (V2V), are not affected by the concept. Likewise, access to vehicle data for repair and maintenance measures continues to be available via the OBD-2 diagnostic interface installed in the vehicle.

⁶ ISO 20077/20078/20080.

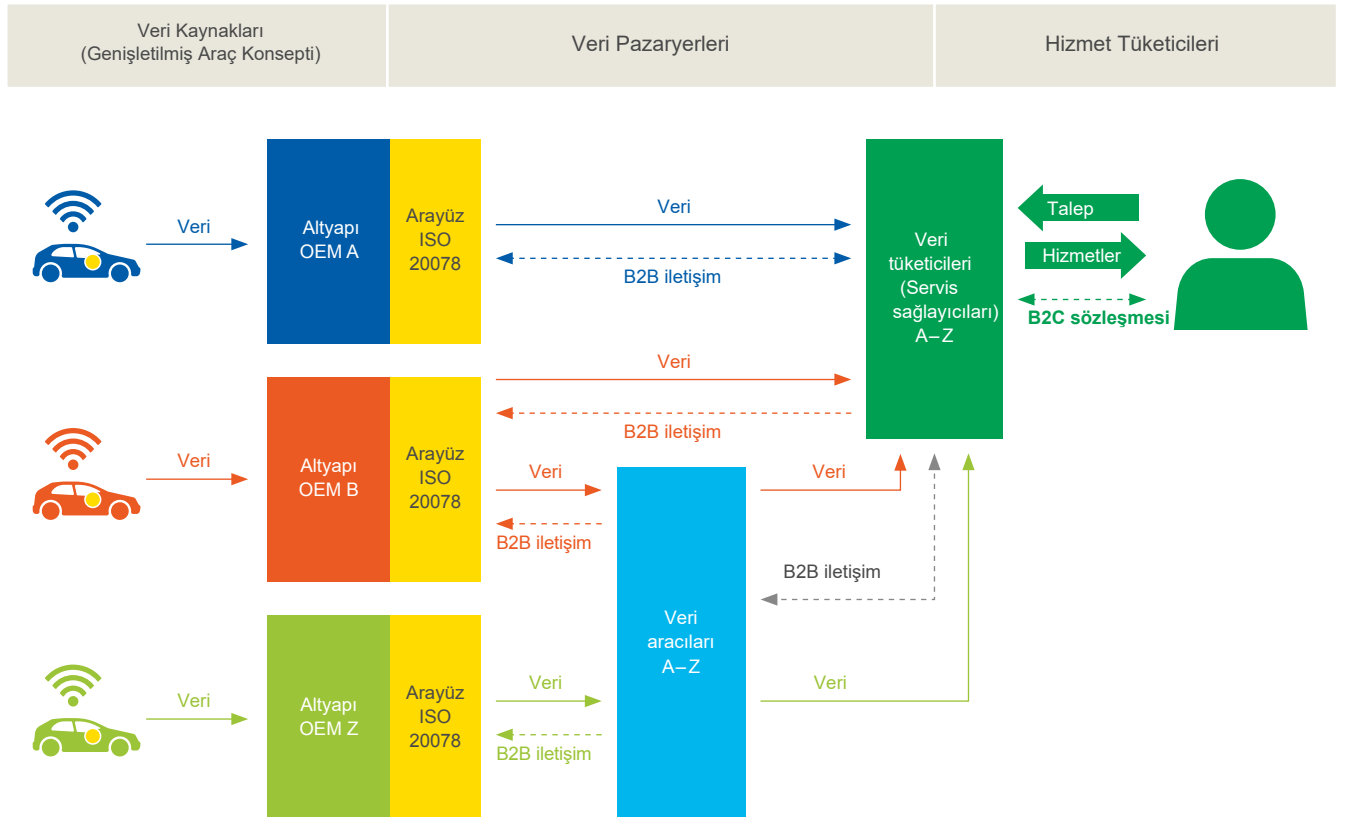
III ADAXO concept – technical details

ADAXO, siber güvenlik kapsamında ilgili yetkilendirme yönetiminin verilerine ve işlevlerine ücretsiz, ayırmacı olmayan erişim ilkelerini açıklar. Böylece ADAXO, böyle bir platform olmadan veri paylaşımı için platformların oluşturulabileceği temelleri oluşturur.

III.1. ADAXO konseptinde veri akışı ve sözleşme ilişkileri

Avrupa dijital ve veri stratejilerinin temel dayanaklarından biri, bu temelde yeni iş modellerinin oluşturulabilmesi için verilerin kullanımını ve paylaşımını basitleştirmektir. Ayrıca, üçüncü tarafların araca çift yönlü bağlantı kurma ve yazılımı araca entegre etme imkanını da açar. Alman otomotiv endüstrisi bunu memnuniyetle karşılamakta ve araç tarafından üretilen verilere dayanan hizmetlerin barındırdığı potansiyeli hesaba katmak için üçüncü taraflarla veri paylaşımını zorlamaktadır.

ADAXO'da veri akışı ve sözleşme ilişkileri



VDA üyesi şirketler, müşteri odaklı kullanım durumları için halihazırda kapsamlı verileri kullanıma sunmakta ve veri paylaşımı için çok çeşitli çözümler sunmaktadır. Üçüncü taraf yazılımların yasal gerekliliklere uygun olarak araca dahil edilmesi daha da genişletilmelidir. Ayrıca, siber güvenlik gerekliliklerine uygun olarak araç sistemlerine üçüncü taraf yazma erişimi gibi ek erişim türleri giderek daha fazla mümkün olmalıdır. Bu proaktif teklif sürekli olarak genişletiliyor.

Veriler, verileri araçtaki hücresel bir arayüz üzerinden OEM arka ucuna gönderen genişletilmiş araç konsepti aracılığıyla sağlanır. Verilere erişim ISO 20077/20078/20080'e göre standartlaştırılmış bir arayüz üzerinden yapılır.

Verilerin paylaşımı ve kullanımı ilgili kullanım durumuna veya teklife bağlıdır ve bağlı veri pazarları aracılığıyla gerçekleştirilebilir. Veri paylaşımı, OEM ile veri tüketicisi arasındaki bir B2B sözleşmesi temelinde veya isteğe bağlı olarak aralarında bir aracıyla (örn. Tarafsız sunucular, tescilli platform) yapılabilir. Bu, çeşitli iş modelleri için gerekli olan veri kaynakları ve veri tüketicileri arasındaki iş ilişkisinin ayrışmasına neden olabilir ve ayrıca OEM ile aracı / aracı ile veri tüketicisi arasındaki ilişkilerin yönetimini basitleştirebilir.

Veri aracıları verileri bir araya getirir ve bunları üçüncü taraflara (veri toplayıcıları) sunar. Böylece müşteriler için bu temelde bir ürün veya hizmet geliştirebilir ve sunabilirler. Diğer bir olasılık da OEM'in doğrudan data tüketici ile bir sözleşme imzalamasıdır. Veri paylaşımı, hangi veri sağlama biçiminin seçildiğine bağlı olarak çeşitli B2B sözleşmelerine dayanır. Bu yaklaşımın amacı, son müşterilere mümkün olan en iyi hizmeti sunmak ve çeşitli teklifler ve / veya tedarikçiler arasından seçim yapmalarını sağlamaktır.

III.2. FRAND ilkelerine göre veri erişimi

ADAXO'nun temel dayanaklarından biri üçüncü taraflar için adil, makul ve ayrımcı olmayan veri erişimidir. Verilere erişimin sağlanması / geliştirilmesi veya işletilmesi gibi çeşitli maliyet faktörleri mevcut olduğundan verilere erişim ücretsiz olmasa da fiyatlandırma her zaman adil olmalıdır. Özellikle çeşitli pazar yerleri, aracılar ve veri alanları aracılığıyla serbestçe erişilebilen veri sağlanması sayesinde fiyat, arz ve talep arasındaki etkileşimle belirlenir. Dolayısıyla veri pazarları sadece teknik bir veri paylaşım fonksiyonuna sahip olmakla kalmıyor aynı zamanda adil fiyatlandırma anlamında piyasa fiyatının doğal düzenlenmesine de hizmet ediyor. Bireysel taraflara veri vermeyi reddetme yani onlara karşı kasıtlı ayrımcılığa izin verilmez.

Gelecekteki düzenleyici projeler veri pazarlarını başlatmayı amaçlamalıdır. FRAND ilkesine göre fiyatlandırmayı ancak işleyen veri piyasaları sağlayabilir.

III.3. ADAXO'da yetkilendirme ve onay yönetimi

ADAXO'daki bir yetkili genellikle araç sahibi, araç sahibi ve / veya araç kullanıcısıdır. Yetkilendirici, veri noktasına bağlı olarak değişebilir.

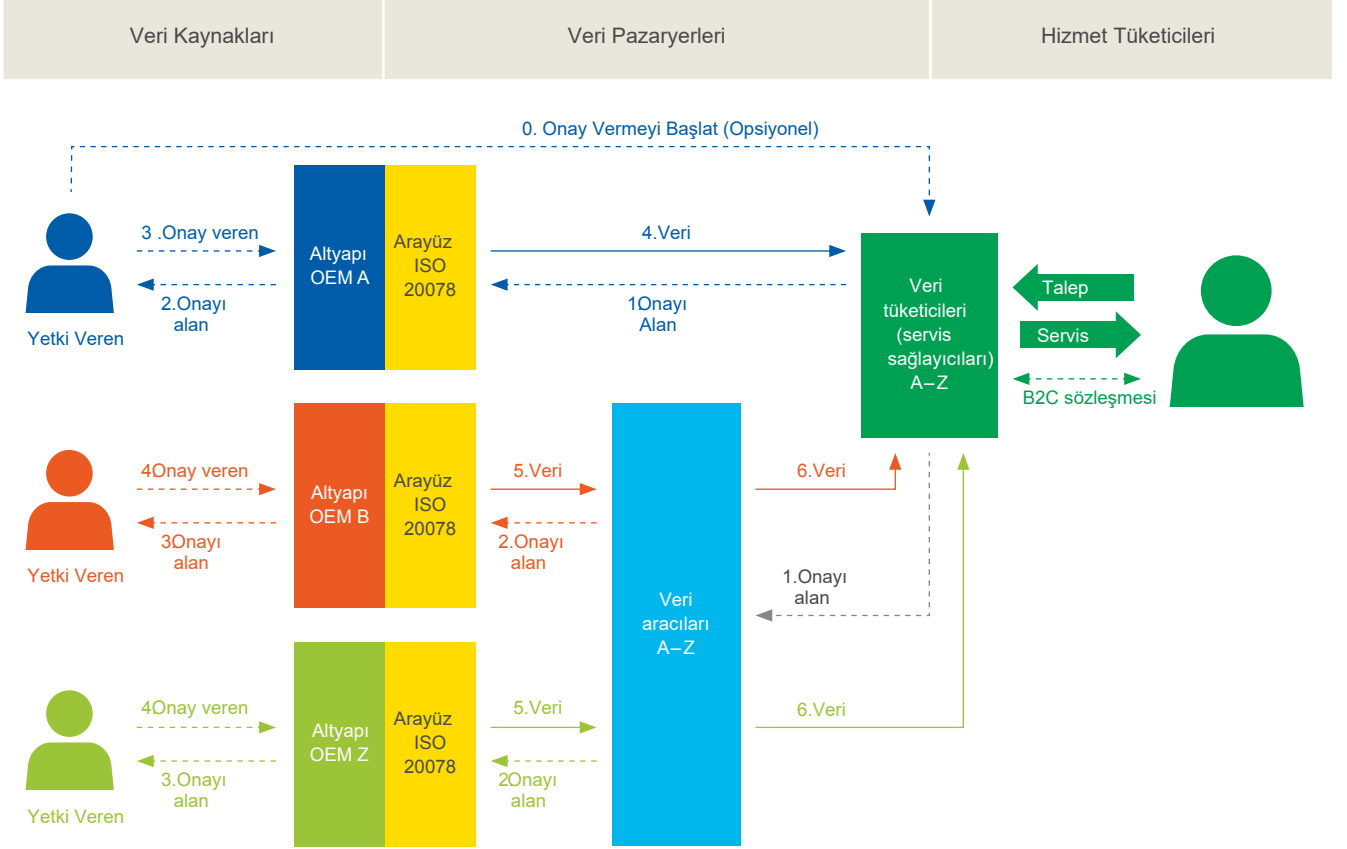
Yenilikçi iş modelleri için değerli olduğu için araçtan elde edilen verilerin önemli bir kısmı kişi ile ilgilidir. Bu veriler her zaman GDPR hükümlerine tabidir. Veriler, yalnızca yetkili tarafından amaçlanan kullanım bağlamında verilen onay temelinde kullanılabilir. Bu, etkin ve GDPR uyumlu yetkilendirme yönetiminin kurulmasını gerektirir. ADAXO konsepti bu gereksinimi tam olarak karşılar:

Yürürlükteki yasalara uygun olarak, veriler yalnızca belirli bir amaç için, yani belirli kullanım durumu için aktarılır.

- Müşteri açısından ve veri koruma yasası açısından yetkilendirme yönetimi merkezi, tutarlı ve kullanımı basit olmalı ve bu nedenle veri toplama için merkezi irtibat noktası olarak üreticiye (OEM) dayanmalıdır.
- Müşteriler veriler üzerinde egemenliğe sahiptir. Yürürlükteki yasalara uygun olarak hangi verilerin hangi alıcılara iletileceğine karar verirler. Üreticiler müşterilerin isteklerine uymalıdır.
- Yasal, sözleşmeye dayalı veya güvenlik nedenleriyle gerekmedikçe ticari veri akışı OEM'ler tarafından izlenmez.
- Gizlilik hükümleri müşteri verilerinin analiz edilmemesini sağlayarak tersine mühendislik yapılmasını önler. Üçüncü taraf hizmetleri için yetkilendirmeler, üçüncü tarafların iş modellerinin OEM'ler tarafından bilinmemesi için şifrelenebilir.

Üreticiler, verileri, ilgili önkoşulları karşılayan OEM tarafından işletilen ve OEM tarafından işletilen olmayan veri pazarlarına erişilebilir hale getirebilir. Birincil veri toplayıcıları, uçtan uca bir yetkilendirme yönetim sistemi aracılığıyla yasal gerekliliklere uyumu sağlayacaktır.

ADAXO'da yetkilendirme ve izin yönetimi



Daha önce gösterildiği gibi, ADAXO konseptindeki veriler ilk önce araçtan araç üreticisinin arka uç sunucusuna hücresel bir arayüz üzerinden akar. Veri rızası için hak sahibi için bu bir ön koşuldur. Bu normalde araç için yetkilendiricidir. Onay, başlangıçta (bir kez) araç üreticisi ile çevrimiçi olarak sözde bir sahip hesabı oluşturan yetkilendirici tarafından yönetilir. Yetkilendirici daha sonra bu hesabı şu amaçlarla kullanabilir:

Verilerinizi GDPR uyarınca yönetin. Yetkilendiren, örneğin, verilerini belirli bir amaç için üçüncü bir tarafça kullanılmak üzere serbest bırakabilir, bu onayı iptal edebilir, verilerin bir kopyasını isteyebilir vb.

Hesap sahibi ayrıca, üreticiden böyle bir üçüncü tarafça istenmesi koşuluyla, belirli bir amaç için verilerinin üçüncü bir tarafa aktarılmasına ilişkin yetkilendiricinin onayını almak için araç üreticisinin yetkilendiriciyle doğrudan iletişim kurmasını sağlar.

⁷ If the owner lends out the vehicle or if personal data of passengers are collected, it is assumed that the owner obtained the oral consent of these persons.

Başka bir deyişle, bir servis sağlayıcı OEM'e başvurur ve belirli bir müşterinin belirli verilerinin belirli bir amaç için serbest bırakılmasını ister. OEM bu isteği sahip hesabının sahibine iletir. Hesap sahibi izin verirse, OEM ilgili verileri talebi yapan veri tüketicisine iletir.

Veriler bir veri aracısından akıyorsa, yetkilendirme yönetimi elbette aracıyı da içermelidir. Bu durumda veri tüketicisi, bağlı veri kaynaklarından belirli verilerin sağlanması talebiyle aracıyla iletişim kurar. Arabulucu, önce bu talebi ilgili OEM'lere iletmelidir. Bu kez yetki isteği ile yetkilendiren ile iletişime geçer. Yetkili onay verirse, OEM ilgili verileri aracıya iletir ve daha sonra bunları veri tüketicisine devredebilir.

Özel yetkilendirme yönetimi durumu, bir yetkilendiricinin, yetkilendiricinin kişisel verilerine erişim izni verilmesi gereken belirli bir hizmeti kullanmak istediği durumdur. Bu durumda, yetkilendirici yukarıda açıklanan onay sürecini tetikler ve verilerinin iletilmesine onay vermek için OEM'DEKİ sahip hesabını kullanır.

III.4. Siber Güvenlik

Siber güvenlik, aracı yetkisiz üçüncü taraf erişimine karşı korur. Araç sistemlerine yetkisiz erişim, aktörlerin aracın kendisi dışındaki araçlara bilgi almalarını ve / veya iletmelerini ve araca fiziksel erişime gerek kalmadan aynı anda birden fazla araç arasında bir arayüz oluşturmalarını sağlar. Bu tür saldırılara karşı koymak mantıksal ve fiziksel izolasyon teknikleri gerektirir. Bu önemlidir, çünkü bir saldırganın bir aracın uzaktan kontrolünü ele geçirmesini veya performansını manipüle etmesini önlemenin en iyi yöntemi, yetkisiz bir üçüncü tarafın araç bileşenlerine erişebileceği ve onlara komut gönderebileceği güvenlik açıklarının veya bağlantıların bulunmamasını sağlamaktır.

Geliştirme ilerledikçe, çeşitli araç üreticileri, yasal düzenlemelere, sertifikasyon yönlerine ve yazılım güncelleme yönetim sistemlerine ilişkin gereksinimlere bağlı olarak araçlara üçüncü taraf sağlayıcılardan yazılım yükleme seçeneği sunacaktır. Siber güvenlik nedeniyle ve araç içi yazılımların manipülasyonuna karşı korunmak için gerekli uluslararası standartlar uygulanmıştır.

Örneğin,

UNECE R155 (Cybersecurity Management System, CSMS) Temmuz 2022'den itibaren geçerli olmak üzere tüm yeni araç tiplerinin tip onayı için başvuruda bulunuyor. Sertifikalı bir yazılım güncelleme yönetim sisteminin (SUMS) kurulmasını ve işletilmesini yöneten UNECE R156, 2020 yazında da onaylandı. Bu UNECE düzenlemeleri, diğer şeylerin yanı sıra, ürün geliştirmeden önce, sırasında ve sonrasında gerekli siber güvenlik faaliyetlerini sağlar ve her zaman ADAXO konseptine dahil edilir.

III.5. Bağlantı için önkoşullar

Çok sayıda fonksiyonun birleştirilmesi nedeniyle, veri sağlayıcıları araçların temel bağlantısını mümkün olduğunca uzun sürelerle devam ettirmede temel bir ilgiye sahiptir. Bu nedenle, aracın temel bağlantısı, bir yandan bunun için teknik önkoşullar yerine getirildiği ve diğer yandan yetkilendiricinin temel bağlantıyı rezerve ettiği sürece korunur.

Temel bağlantı sonlandırılmasına neden ve genellikle veri sağlayıcısı ve veri tüketici sahasının dışında olabilecek olası bir teknik faktörler teknolojinin eski sistemler düzeltilebilir. Güvenlik olayları, ya da ömür boyu kullanılır olmayan (2G ve 3G) büyük hücresel ağları devre dışı bırakma gibi şeyler vardır.

III.6. Araç kaynaklarına ücretsiz erişim

III.6.1. Araç kaynaklarına ayırmacı olmayan erişim

OEM'ler, kendi hizmetlerini sağlamak için kullandıkları tüm veri ve işlemlere erişim sunar. Verilere ayırmacı olmayan erişim, araçlar aracılığıyla (muhtemelen maskelenmiş, örneğin tarafsız sunucular kullanılarak) veya doğrudan OEM aracılığıyla sırasıyla B2C veya B2B sözleşmeleri temelinde sağlanır.

Arka uçta depolanan araç verilerine salt okunur erişimin aksine (yani aracın kendisini etkilemeden), araca yazma (veya okuma ve yazma) bağlantısı olduğunda araç sistemlerinin bütünlüğü ve bunların operasyonel güvenliği için ek riskler vardır. Bu nedenle, uzaktan tanılama için araç üreticisi, özellikle riskli işlemleri ve işletim durumlarını engellemek için tanıyla ilgili tüm verileri ve işlevleri bir soyutlama katmanı aracılığıyla kullanıma sunar. Buradaki geçerli ilke, yetkili üçüncü tarafların bu uzaktan kumandaya erişim sağlamasıdır.

Teşhis hizmetleri, ilgili üreticinin yetkili bayileri, atölyeleri ve servis sağlayıcıları ile aynı zamanda ve aynı ölçüde karşılıklı müdahaleyi önlemek için, uzaktan tanılama yalnızca herhangi bir zamanda tek bir tarafça gerçekleştirilebilir.

ISO 20080 (Uzaktan Tanılama Desteği) bunu içerecek şekilde değiştirilmelidir.

Yazma erişimi üzerinden yapılan uzaktan tanılama ve onarımlar genellikle güvenlik önlemlerinin (örn. pencere tutam koruması) ve aktüatörlerdeki değişikliklerin (örn. römork aksamı uzantısı) ortadan kaldırılmasını da içerdiğinden, servis sağlayıcı kullanıcı uzmanlığı ve doğru kullanım taahhüdünü sağlamalıdır.

Servis tüketicisi ile HMI üzerinden etkileşim mevcut teknik çözümleri kullanır ve bilgiler aracın HMI yansıtılır. Mevcut teknik çözümler bu gereklilikleri yerine getirebilir.

III.İzleme ve uygulama

Gerekirse teşhis mekanizmalarının izlenmesi ve uygulanması desteklenir. Bu, etkilenen tarafların “yapılandırılmış bir forumu” aracılığıyla ve muhtemelen AB Komisyonu'nun katılımıyla da olabilir.

III.6.3. Yetkisiz iş izlemenin önlenmesi

Yasal, sözleşmeye dayalı veya güvenlik nedenleriyle gerekmedikçe ticari veri akışı OEM'ler tarafından izlenmez. Gizlilik hükümleri, müşteri verilerinin analiz edilmemesini sağlayarak hizmet tekliflerinin tersine mühendislik yapılmasını engeller.

Veri erişimi kullanım durumunu oku:

- ISO 20078'in bir uzantısı olarak kesin yetkilendirme iş akışı için Bölüm III.2'ye bakın.
- Yetkili (OEM'in telematik talebi için sözleşme ortağı) OEM tarafından açıkça tanımlanmalı ve bu nedenle maskelenememelidir.
- Servis sağlayıcı ve servis sağlayıcı müşterileri bir veri aracı (ör. tarafsız sunucu) aracılığıyla maskelenebilir. Bu, yukarıdaki anlamda açıklama yapılmaması anlamına gelir.

Uzaktan teşhis desteği kullanım durumu:

- Uzaktan tanılama desteği (RDS), uzaktan tanılama ve bakım amacıyla OEM arka ucu üzerinden araç sistemlerine çevrimiçi okuma ve yazma erişimi, yani aracın elektrik / elektronik sistemi ve aktüatörler dahil bileşenleri üzerinde doğrudan etkisi olabilecek erişimi ifade eder.
- Aşağıda açıklanan konum tele-tanılama ve bakım amaçlarıyla sınırlı değildir. Aksine tüm uzaktan çevrimiçi erişim (ROA) kullanım durumlarına (uzaktan kapı kilidi açma gibi uzak hizmetlerin kullanımı dahil) uygulanabilir.

- Bir veri aracı (örn. tarafsız sunucu), çerçeve koşullarına uygun olarak ilgili OEM ile RDS için bir B2B ana sözleşmesi imzalamış olan hizmet sağlayıcısına teknik servis sağlayıcı olarak görev yapar.
- Sorumluluk servis sağlayıcıya aittir; servis sağlayıcı ile OEM arasında B2B ana sözleşmesi uyarınca bir RDS sözleşmesi imzalanır.
- Veri aracı (örn. Tarafsız sunucu), servis sağlayıcının müşterilerinin kimlik doğrulamasını ve yetkilendirmesini (iş yapan bireysel servis birimi) işler.
- Yetkilendirici, OEM tarafından açıkça tanımlanmalıdır ve bu nedenle maskelenemez.
- Düzenlenmiş sorumluluk devri nedeniyle, servis sağlayıcı OEM tarafından açıkça tanımlanmalıdır ve bu nedenle maskelenemez.
- Servis sağlayıcının müşterileri (iş yapan bireysel servis birimi) tanımlanabilir bir veri aracı (örn. tarafsız sunucu) ve tanımlanabilir servis sağlayıcı aracılığıyla maskelenebilir. Bu, iş yapan bireysel hizmet birimi için yukarıdaki anlamda açıklama yapılmaması anlamına gelir.

III.6.4. Erişim kimlik doğrulaması

OEM arka ucuna okuma veri erişimi (araç sistemlerini etkilemeden) ile OEM arka ucu üzerinden araca uzaktan tanılama desteği (RDS) gibi yazma erişimi arasında ayırım yapmak gerekir. Çünkü OEM'den servis sağlayıcıya düzenlenmiş bir sorumluluk devri sağlanmalıdır. Araca doğrudan erişim.

- Veri erişimini oku:
 - ISO 20078'in bir uzantısı olarak kesin yetkilendirme iş akışı için Bölüm III.2'ye bakın.
 - Yetkili (OEM'in telematik talebi için sözleşme ortağı) OEM tarafından açıkça tanımlanmalıdır ve bu nedenle maskelenemez.
 - Servis sağlayıcı ve servis sağlayıcı müşterileri bir veri aracı (ör. Tarafsız sunucu) aracılığıyla maskelenebilir. Bu, Bölüm III.6.3'te açıklandığı şekilde ifşa edilmemesi anlamına gelir.

- Yazma veri erişimi (örneğin, uzaktan tanılama desteği, RDS):
 - Uzaktan teşhis desteği (RDS), ISO 20080, uzaktan teşhis ve bakım için OEM arka ucu üzerinden araç sistemlerine çevrimiçi okuma ve yazma erişimini ifade eder. Yani, aracın elektrik / elektronik sistemi ve aktüatörler de dahil olmak üzere bileşenleri üzerinde doğrudan etkisi olabilecek erişim amaçları.
 - Aşağıda açıklanan pozisyon tele-teşhis ve bakım amaçları ile sınırlı değildir, aksine tüm uzaktan çevrimiçi erişim (ROA) kullanım durumlarına (uzaktan kapı kilidi açma gibi uzak servislerin kullanımı dahil) uygulanabilir.
 - Bir veri aracı, örneğin tarafsız sunucu, çerçeve koşullarına uygun olarak her OEM ile RDS için standart bir ana sözleşme imzalayarak servis sağlayıcıya teknik servis sağlayıcı olarak hareket edebilir.
 - Sorumluluk servis sağlayıcıya aittir; servis sağlayıcı ile OEM arasında standart ana sözleşmeye uygun olarak bir RDS sözleşmesi imzalanır.
 - Bir veri aracı (örn. tarafsız sunucu) kullanılıyorsa, veri aracı, hizmet sağlayıcının hizmet tüketicisinin (iş yapan bireysel hizmet birimi) kimlik doğrulama ve yetkilendirmesini işler.
 - Yetkilendirici, OEM tarafından açıkça tanımlanabilmeli ve bu nedenle maskelenememelidir.
 - Düzenlenmiş bir sorumluluk devri nedeniyle, servis sağlayıcı OEM tarafından açıkça tanımlanmalıdır ve bu nedenle maskelenemez.
 - Servis sağlayıcının müşterileri (iş yapan bireysel servis birimi) bir veri aracı (örn. tarafsız sunucu) ve tanımlanabilir servis sağlayıcı aracılığıyla maskelenebilir. Bu, Bölüm III.6.3'te açıklandığı şekilde ifşa edilmemesi anlamına gelir.

III.6.5. Yükümlülük

OEM arka ucuna (araç sistemlerini etkilemeden) okunan veri erişimi ile OEM arka ucu üzerinden araca uzaktan tanılama desteği (RDS) arasında ayırım yapmak gerekir, çünkü OEM'den servis sağlayıcıya doğrudan erişim durumunda OEM'den servis sağlayıcıya düzenlenmiş bir sorumluluk aktarımı sağlanmalıdır. Rds'nin sorumluluğu servis sağlayıcıda kalır; servis sağlayıcı ile OEM arasındaki bir RDS sözleşmesi, B2B ana sözleşmesine uygun olarak sonuçlandırılır. RDS ile servis sağlayıcının OEM tarafından açıkça tanımlanabilmesi gerekir ve bu nedenle sorumluluğun yeniden devredilmesi nedeniyle maskelenemez.

III.6.6. Son müşterinin tanımlanması

Son müşteriler hem yetkilendiriciler hem de hizmet tüketicileri olabilir.

Okuma erişimi sayesinde, servis sağlayıcının servis tüketicileri bir veri aracı (ör. tarafsız sunucu) aracılığıyla maskelenebilir.

Ancak RDS ile servis sağlayıcı OEM tarafından açıkça tanımlanabilmelidir ve bu nedenle düzenlenmiş sorumluluk devri nedeniyle maskelenemez. Bununla birlikte, tanımlanabilir servis sağlayıcının hizmet tüketicileri (iş yapan bireysel servis birimi) veri aracı (örn. tarafsız sunucu) tarafından maskelenebilir.

Yukarıdaki her iki kullanım durumunda da temel bağlantı için gerekli olan telematik sözleşme nedeniyle yetkilendirici maskelenemez.

III.7. Araçtaki çeşitli veri mimarilerinin illüstrasyonu

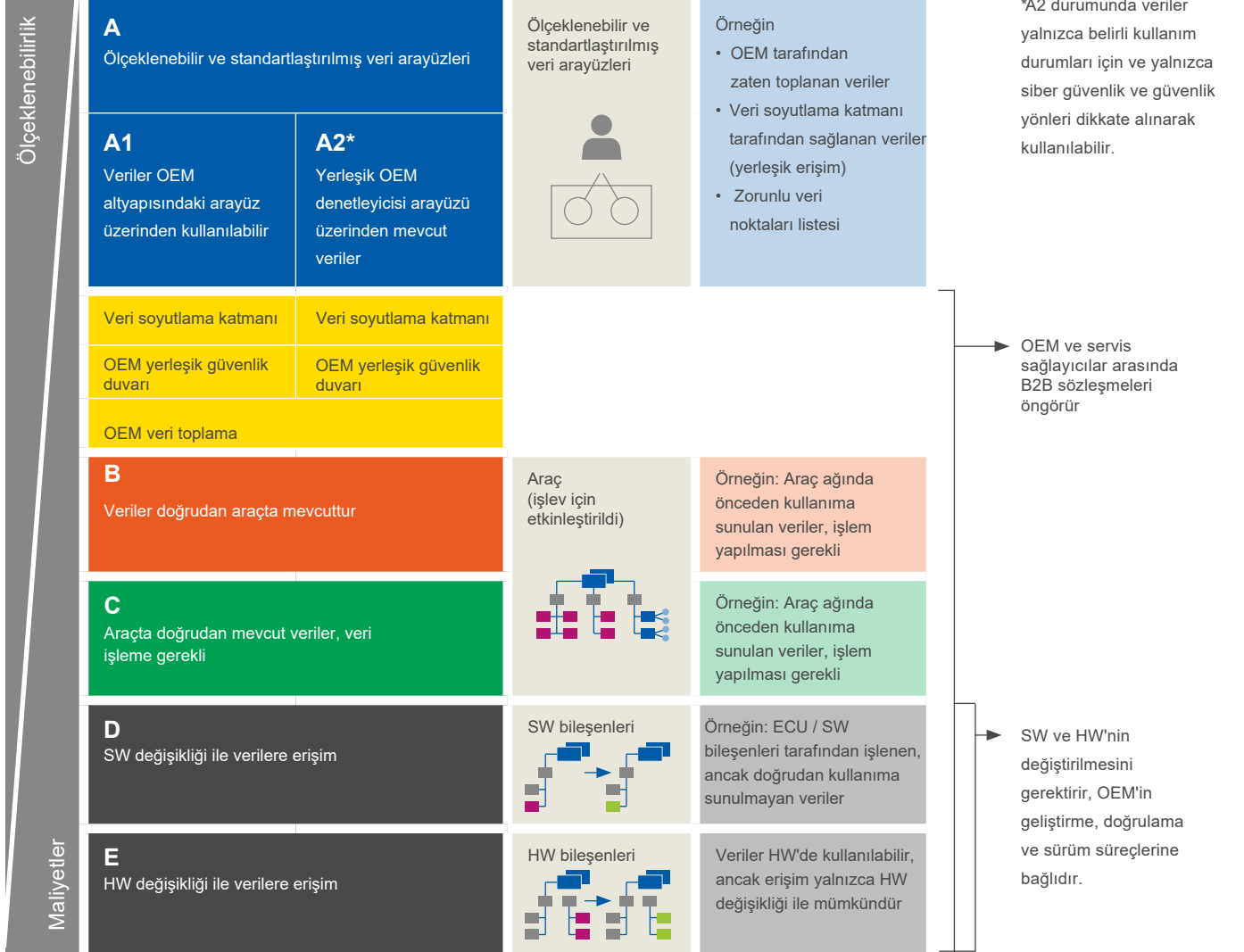
Araçtaki veri mimarisi, kamuya açık bilgilerin erişilebilir olduğu bir internet ile karşılaştırılabilir bir genel (A) ve özel (B–E) alan ile örneğin güvenlik önlemleriyle korunan bir intranet arasında açıkça ayırım yapar.

Alan A, ölçeklenebilir ve standartlaştırılmış arabirimler aracılığıyla kimliği doğrulanmış üçüncü taraflara sunulan veriler içindir. A'daki veri kümesi sürekli olarak genişletilir.

Burada, OEM arka ucunda (A1) bulunan bir ExVe arabirimi ile yalnızca belirli kullanım durumları için veri sağlayabilen yerleşik arabirim (A2) arasında ayırım yapıyoruz.

Siber güvenlik gereksinimleri, verilerin ne ölçüde ve hangi amaçla kullanılabileceğini belirler. Yerleşik erişimin daha büyük riskleri nedeniyle, mevcut verilerin potansiyel kapsamı A2 ile A1'den daha küçük olacaktır.

Araçta çeşitli veri mimarileri



B ve C Durumlarının Detaylandırılması: (B) Doğrudan yerleşik bir kaynak olarak kullanılabilen ve A Seviyesine yükseltilebilen veriler kullanıma sunulur. (C) Bu veriler, ek verilerin kullanılabilmesi için önceden işlenebilir. Ancak bu ek kaynaklar gerektirir.

B ve C'ye atanabilen ve A'da kullanıma sunulması gereken veriler, OEM ile üçüncü taraf arasında ek bir B2B sözleşmesi gerektirir, yani bu yalnızca OEM'in onayı ile veya yasal bir temel temelinde mümkündür. Bu tür bir anlaşmaya ve teknik olanaklarına dayanarak, OEM üçüncü tarafa arayüz üzerinden araçtan ek veriler sağlayacaktır (Servis talebi B) veya yerleşik ön işleme tabi tutacaktır (Servis Talebi C). Üçüncü taraf, bu tür bir ön işleme ilişkin spesifikasyonu gereksinimler veya sahte kod biçiminde sağlamalıdır ve OEM entegrasyonu gerçekleştirir. Belirtimi zamanında ve işleme frekans tabanlı veri ekonomisi, veri noktası (sayı) uygun arayüz genişliği ve gecikme gibi bir olay düşünmek gerekir.

D ve E Durumlarının Detaylandırılması: Henüz erişilemeyen veriler de vardır (D ve E). D durumunda, veri toplama yalnızca yazılım bileşenlerinde yapılan bir değişiklikle mümkündür. Örneğin, bir ECU tarafından bir tarih hesaplandı ancak henüz iletilmedi. E durumunda, toplama yalnızca donanım bileşenlerinde yapılan bir değişiklikle mümkündür, örneğin ECU teknik olarak soyutlama katmanına bağlı değilse veya sensörler takılı değilse.

Bu nedenle, D ve E'ye atanabilecek kullanım durumları, OEM ile üçüncü taraf arasında ek bir B2B sözleşmesi gerektirir, yani yalnızca OEM'in onayı ile veya yasal bir temel temelinde mümkündür.

Verilerin toplanması mimariye ne kadar derine inerse, uygulama o kadar karmaşıktır (maliyet ve zaman).

Araç sistemleri için yazılım geliştirme ve veri sağlama yazılımı, gereksinim özellikleri, üreticiye özgü standartlar ve tasarım yönergeleri, endüstri çapında güvenlik ve işlevsel güvenlik yönergeleri ve düzenleyici çerçeve koşulları gibi açık yönergelere tabidir. Ayrıca, kaynak gereksinimleri (örneğin, RAM ve CPU'lar) ayrı ayrı karşılaştırılır.

Araç üreticisinin kendisi tarafından tanımlanan ve kullanılan doğrulama ve onay süreçlerine uyulmalıdır. Çünkü örneğin güvenlik ve güvenlik gereklilikleri ancak tüm sistem göz önünde bulundurularak yönetilebilir (bkz. Özellikle varyant çeşitliliği, test uygulaması ve güvenli koruma süreçleri).

Bu nedenle, bu süreçlerden ayrılan yazılımların geliştirilmesi ve entegrasyonu mümkün değildir.

Araç üreticisi her zaman entegrasyon, işlevsel güvenlik ve güvenliğin yanı sıra yapılandırma ve kaynak yönetiminden sorumludur. Bugün olduğu gibi, üçüncü taraf yazılımların olası entegrasyonu ancak kaynak kodun açıklanmasının ek öncülüyle mümkündür.

Tüm veriler üçüncü şahıslara verilmeden önce soyutlanır. Bu soyutlamanın amacı, tamamen teknik araç sinyallerini kullanılabilir hale getirmek ve bunları üretici ve araç üretiminden mümkün olduğunca tutarlı bir şekilde tanımlamaktır (örn. araç sinyal özellikleri, VSS). Sağlanan verilere erişim her zaman bu soyutlama katmanının üzerinde gerçekleşir. Soyutlama derecesi, E / E mimarisinin oluşumuna bağlı olarak değişebilir. Güvenli veri sağlama konusundaki mevcut yüksek entegrasyon çabası, sanallaştırma ve yazılım geliştirme teknolojilerinin kullanımıyla gelecekteki E/ E mimarisi nesillerinde azaltılabilir.

ADAXO konsepti, muhtemelen araçtaki HW veya SW değişikliklerinin yardımıyla yeni içeriğin temsil edilmesini de sağlar. ADAXO konsepti, araçta uygulanan fonksiyonel güvenlik gereksinimlerini destekler (örneğin, araç fonksiyonlarının ISIL uygunluğu).

Arayüz üzerinden erişilebilen araç verilerine salt okuma erişiminin aksine (yani aracın kendisini etkilemeden), işlevler kullanıldığında araç sistemlerinin bütünlüğü ve operasyonel güvenlik açısından ek riskler söz konusudur.

Uzaktan tanılama (veya yerleşik API'ler aracılığıyla yazma erişimi) için araç üreticisi, özellikle riskli işlemleri ve işletim durumlarını engellemek için tanıyla ilgili tüm verileri ve işlevleri bir soyutlama katmanı aracılığıyla kullanıma sunar. Buradaki geçerli ilke, yetkili üçüncü tarafların bu tür uzaktan tanılama hizmetlerine ve yerleşik API'lere, ilgili üreticinin yetkili bayileri, atölyeleri ve servis sağlayıcıları ile aynı ölçüde ve kararlaştırılan amaç doğrultusunda erişim sağlamasıdır.

Not: Uzaktan tanılama kullanım durumunun ayrıntılı akışı Ek V.2'de bulunabilir.

Araç, örneğin yuvarlanmaya veya pencereye hapsolmuş kişilere karşı yazma erişimi için yeterince emniyete alınmalıdır. Bu güvenli durum, araçta HMI (araç kilitlenmemişse) veya bir uygulama aracılığıyla (araç kilitliyse) sorumlu bir kişi tarafından onaylanmalıdır. İlgili mevzuat önerilir.

III.7.1. Yerleşik yazılımın kurulumu ve yürütülmesi

Yeni mimariler ortaya çıktıkça, örneğin bilginin ön işleminin gelecekte üçüncü şahıslar tarafından da mümkün olacağı ölçüde donanım soyutlamasını sağlayacak hipervizör teknolojileri kullanıma sunulacaktır.

Yerleşik kaynakların kullanımı, araç sistemlerinin bütünlüğü ve operasyonel güvenlik için ek riskler barındırmaktadır. Olası seçenekler veya gelişmeler dikkate alındığında, tüm şirketler her zaman tüm yol kullanıcılarının ve onarım sürecine katılanların güvenliğine öncelik vermektedir.

Araç üreticisinin kendisi tarafından tanımlanan ve kullanılan doğrulama ve onay süreçlerine uyulmalıdır. Çünkü örneğin güvenlik ve güvenlik gereklilikleri ancak tüm sistem göz önünde bulundurularak yönetilebilir (bkz. Özellikle varyant çeşitliliği, test uygulaması ve güvenli koruma süreçleri).

Araç sistemleri için yazılım geliştirme ve veri sağlama yazılımı, gereksinim özellikleri, üreticiye özgü standartlar ve tasarım yönergeleri, endüstri çapında güvenlik ve işlevsel güvenlik yönergeleri ve düzenleyici çerçeve koşulları gibi açık yönergelere tabidir. Ayrıca, kaynak gereksinimleri (örneğin, RAM ve CPU'lar) ayrı ayrı kararlaştırılır.

Bu nedenle, bu süreçlerden ayrılan yazılımların geliştirilmesi ve entegrasyonu mümkün değildir.

Araç üreticisi her zaman entegrasyon, işlevsel güvenlik ve güvenliğin yanı sıra yapılandırma ve kaynak yönetiminden sorumludur. Bugün mevcut haliyle, üçüncü taraf yazılımların olası entegrasyonu, yalnızca kaynak kodun açıklanmasının ek öncülüyle mümkündür.

Bununla birlikte, temel olarak, yalnızca aracı sertifikalandırmaktan sorumlu olan şirket yazılımı onaylayabilir ve araç kaynaklarını yönetebilir. Bu, araca üçüncü taraflardan yazılım yükleyse, yasal gerekliliklere (örneğin, siber güvenlik konusunda UNECE R155), sertifikasyon hususlarına ve yazılım güncelleme yönetim sistemlerine (UNECE R156) ilişkin gerekliliklere uygun olarak yapılmalıdır.

Bu amaçla, araçlara üçüncü taraf yazılımların yüklenmesi için güvenli bir temel sağlamak üzere derneklerle iş birliği içinde kılavuzlar hazırlanmalıdır. Bölüm IV.2'de açıklanan yapılandırılmış forum bunun için bir temel oluşturabilir.

III.HMI (insan-makine arayüzü) üzerinden sürücü ile etkileşim

HMI'ye erişirken aşağıdaki koşullara uyulmalıdır:

- yasal kurallar, NHTSA'dakilere benzer sürücü oyalama kuralları, etik / ahlaki kurallar;
- Tip boyutları, düzen, sürücü merkezliliği, animasyonlar gibi HMI tasarım yönergeleri;
- mimari, kaynaklar ve güvenlik kuralları.

Kullanılan teknolojilere (OEM'e özgü çözüm veya öngörülen mod) bağlı olarak, bu yönetim rolü araç üreticisi veya platformdan sorumlu tarafça üstlenilir (örneğin, CarPlay için Apple). Teknolojiler ayrıca işlevsellik, ölçeklenebilirlik ve uygulama için gereken zaman ve maliyetler bakımından farklılık gösterir.

İşlevsel güvenlik nedeniyle, bazı ekranlar / sinyaller hemen veya hiç takip etmeyebilir (sürüş sırasında video akışı gibi).

Değerlendirme kriterleri:

- OEM için Ölçeklenebilirlik: OEM'in üçüncü taraf çözümlerini test etme ve onaylama çabası yönetilebilir olmalıdır.
- Üçüncü taraf için ölçeklenebilirlik: Her OEM veya çözüm için gereken minimum uyarlamalar evrensel olarak kullanılabilir.
- Üçüncü taraf gereksinimlerinin yerine getirilmesi: işlevsel gereksinimler, örn. bakım uygulamaları, müşteri ile etkileşim.
- Kısa vadeli başarılabilirlik: Teknoloji zaten piyasada mevcut veya kısa vadede tanıtılabilir.

Teknolojilerin Değerlendirilmesi

	Öngörülen mod	Bildirimler	Ana ünitesinde yerel uygulama (OEM app store)
Tanım	Tüm araçlarda öngörülen modun kullanılabilirliği / cross OEM	Üçüncü taraflar için Bağılı Sürücü mesajlaşma servisinin açılması	Android uygulamalarının üçüncü taraf gelişimi, OEM app store'a dahil edilmesi
İşlevsellik	İzin verilen şablonlara dayalı özel uygulamalar	Mesaj içeriği (metin) ve gönderen (gezilebilir adres ve telefon numarası) içeren bilgilendirme bildirimleri	Özel uygulamalar (Android uygulaması)
Teknoloji Tedarikçileri ve Yönetişim	Apple/Google	OEM	OEM
Markalar arası ekosistem / üçüncü taraf perspektifinden ölçeklenebilirlik	+++	++	+
OEM Bağlamında Çaba ve Ölçeklenebilirlik	+++	++	---
Üçüncü taraf gereksinimlerinin yerine getirilmesi	0	+	+++
Kısa vadeli başarılabirlik	++	++	---
Potential for improvement	İzin verilen işlevlerin genişletilmesi	CarData API'sine entegrasyon, muhtemelen dönüş kanalı	

1. Öngörülen modlar

- OEM ve üçüncü taraf için iyi ölçeklenebilirlik sunun. Öngörülen mod durumunda, üçüncü tarafın yalnızca bir kez geliştirmesi gerekir; OEM uyarlamaları gerekli değildir. Test / yeterlilik, OEM'lerin aksine, bunun temel bir iş olduğu platform sağlayıcısının (ör. Google veya Apple) sorumluluğundadır.
- son müşteri etkileşimi için kullanılabilir, ancak kapsamlı iş durumları için kullanılamaz (örn. uzaktan tanılama)
- hemen kullanılabilir.
- şu anda mevcut olan mesajlaşma, bilgi-eğlence ve navigasyon alanlarının ötesine genişletilmelidir, yani üçüncü tarafların işlevsel gereksinimleri henüz karşılanmamıştır. Örneğin, Apple / Google'a öngörülen modların işlevselliğini genişletme konusunda ortak yaklaşım. Piyasada öngörülen modların kullanımı hızla artmaktadır (özellikle ABD'de), bu nedenle mevcut alan adlarının sayısının genişletileceği varsayılabilir.

2. Mesaj merkezleri

- OEM ve üçüncü taraf için iyi ölçeklenebilirlik sunun.
- son müşteri etkileşimi için kısıtlamalarla kullanılabilir: sınırlı etkin içeriğe sahip kısa mesaj (örn. coğrafi konum, telefon numarası), confirmasyon için teklif dönüş kanalı veya benzeri.
- hemen kullanılabilir.
- bu nedenle, çok çeşitli kullanım durumlarıyla ilgili olarak üçüncü tarafların işlevsel gereksinimlerini karşılar, ancak etkileşim olanakları açısından sınırlıdır.
- standart formatlar geliştirilmelidir.

3. OEM yerel uygulamalar (OEM uygulama mağazası)

- OEM'ler ve üçüncü taraflar aracılığıyla çok sınırlı ölçeklenebilirlik sunun.
- kapsamlı son müşteri etkileşimi sunun.
- kısmen mevcuttur.
- böylece üçüncü tarafların işlevlerini tam olarak karşılar.

Değerlendirilen kriterlere dayanarak, OEM tarafında bir teklif ve teknoloji 1 ve 2'nin üçüncü taraflarca kullanılması önerilir (bkz. şekil "Teknoloji değerlendirme"). Ayrıca, üçüncü taraf teklifleri bu şekilde tanımlanabilir olmalıdır.

Şu anda, Çözüm 3, kapsamlı geliştirme, doğrulama ve onay süreçleri (uygulama ve OEM başına) gerektirdiği ve bu nedenle ölçeklendirilmediği için kriterleri yerine getirmemektedir.

Hmı'ye üçüncü taraf erişimini sağlayan çeşitli teknolojiler bugün zaten mevcuttur. Bununla birlikte, yalnızca ikisi OEM'ler ve üçüncü taraflar tarafından ölçeklenebilir şekilde kullanılabilir. Bunlar, Bölüm III.7.1'de açıklandığı gibi yerleşik ve yerleşik API'lerle birleştirilebilir.

III.8. Yerleşik tanılama (OBD) arabirimi üzerinden erişim

OBD arabirimi üzerinden üreticinin atölyelerinde bulunan tüm veriler ve işlevler, üçüncü taraf sağlayıcılara ayrımcılık yapılmaksızın da kullanılabilir hale getirilir. Erişim detayları AB Tip Onay Yönetmeliği 2018/858, Ek X, No. 2.9'da belirtilmiştir. Araç üreticileri, UNECE Yönetmeliği R155 ve R156'nın (Siber Güvenlik) uygulanmasının bir parçası olarak sertifika teşhisinin uygulanması gibi önlemler almışlarsa, bunlar, ilgili sertifikaların doğrulanması / alınması koşuluyla, ayırım gözetilmeksizin bağımsız piyasa katılımcılarına da sunulacaktır.

Onarım ve hata teşhisi için OBD erişimi korunur. OBD arayüzü, yeni gereksinimlere uygun olarak ve en son teknolojiye göre değiştirilmiştir. Veriler Bölüm III.7'de açıklandığı şekilde kullanıma sunulmuştur.

IV Otomotiv sektörü için bütüncül bir kavramdan ilerici eylem önerisi

ADAXO konsepti, araç verilerine daha güvenli, daha rekabetçi ve yeniliği teşvik edecek şekilde erişim sağlar.

Eyleme ilişkin amaç ve öneriler bu sonuç bölümünde özetlenmiştir.

IV.1. Tesisler ve birincil hedefler

Adaxo'nun iki temel amacı şudur:

- **"Müşterilere araç ve mobilite verilerini kullanarak kendileri ve toplum için katma değer yaratma yetkisi veriyoruz."**
Kişisel araç kullanıcısı ve hareketlilik verileriyle ilgili karar doğrudan müşterilere (yetkili taraflara) aittir. Kişisel hareketliliklerini ve hareketliliklerini herkes için daha güvenli, daha sürdürülebilir ve daha rahat hale getirmek için verilerinin paylaşılmasından elde edilen katma değer nereden oluşturulacağına tek başlarına karar verirler. VDA üyesi şirketler konseptlerini müşterilere odaklayarak verilerinden katma değer üretmelerini sağladı.
Eylem önerileri, diğer piyasa katılımcılarıyla adil işbirliği içinde gerekli koşulları oluşturmayı amaçlamaktadır.
- **"Yenilikleri ve geleceğe yönelik iş modellerini teşvik etmek için Avrupa veri stratejisinin aldığı yönü destekliyoruz."**
Araç ve mobilite verileri, Avrupa'yı gelecek için rekabetçi kılacak yenilikleri ve iş modellerini geliştirmek için önemli bir kaldıraçtır. Bunlar, örneğin, çok çeşitli ve aynı zamanda açıkça sektörler arası veri kaynaklarının birleştirilmesinden kaynaklanan yeni girişim iş modelleri olabilir. Bununla birlikte, örneğin bağımsız bakım ve onarım sektöründe yerleşik iş modelleri bile, veri kullanımı yoluyla katma değerlerini ve hizmetlerini geliştirebilir.

Bütün bunlar, Avrupa ekonomik bölgesini küresel olarak daha rekabetçi ve dirençli hale getirmeye katkıda bulunuyor. VDA üyesi şirketler, veri ekonomisine Avrupa'nın gelecekteki uygulanabilirliğine de katkıda bulunma yükümlülüğü olarak görüyorlar. Avrupa veri stratejisinde formüle edilen Avrupa değerleri ve ilkeleri, bu konuda nasıl gideceğimizin temelidir.

Aşağıdaki koşullar yerine getirilmelidir:

- **Önce güvenlik**

Bir araba akıllı telefon değildir. Araç verilerine erişim ancak aracın ve yolcularının güvenliğinden ödün verilmeyen bir dikkatle gerçekleştirilebilir. Hiçbir yenilik ve hiçbir iş modeli, araç kullanıcılarının tehlikeye atılmasını veya kişisel verilerinin uygunsuz kullanımını haklı çıkarmaz. Siber güvenlikle ilgili geçerli tüm düzenlemelere mutlak uyum, veri koruma ve yazılım güncelleme yönetimi, bu güvenlik düzeyini sağlamak için bir çerçevedir.

- **Dürüstlük**

VDA üyesi şirketler, verilerden elde edilen katma değer ancak ilgili herkes için çalışan iş modelleri temelinde oluşturulabileceği konusunda hemfikirdir. Ortak hedeflere ancak tüm piyasa katılımcılarının veri paylaşması durumunda ulaşılabilir.

IV.2. Otomotiv endüstrisinde bir veri ekonomisinin uygulanmasına yönelik eylem önerisi

Ortak ADAXO konsepti ile VDA üyesi şirketler, Avrupa Birliği'nin hedeflerini ve dolayısıyla Avrupa'nın veri ekonomisini güçlendirmeye yönelik AB veri stratejisinin hedeflerini ve aynı zamanda dijital tek bir pazar yaratmanın tanımlanmış hedefini açıkça desteklemektedir. Bunun için gerekli teknik çerçeve ve uygulamalar - bkz.

Bölüm III - FRAND koşullarına ve genişletilmiş araç konseptine uyumu sağlarken, veri arayan üçüncü taraflar için veri kullanımını ve veri alışverişini daha da teşvik etmeyi mümkün kılar. Ayrıca, araçların sistemsel bütünlüğü ve buna bağlı olarak tüm yol kullanıcılarının yakın güvenliği, temel güvenlik hususlarına uygun olarak sağlanabilir (dahil. siber güvenlik) ve böylece Vizyon Zero yönünde ilgili bir katkı sağlar.

Bu nedenle temel unsurlar, piyasa katılımcılarının yeni yeniliklere ve iş modellerine sürekli katılımının yanı sıra Avrupa Birliği içinde çalışılması gereken uyumlu bir yaklaşımı da içermektedir. Bunun ışığında, yatay düzenlemelerle tutarlı bir uyum sağlanmasını öneriyoruz (dahil. Veri Yasası ve Veri Yönetimi Yasası).

Bu nedenle Alman otomotiv endüstrisi aşağıdaki eylemleri önermektedir:

(1) Veri egemenliği: Müşterinin veri egemenliğini korurken ve genişletilmiş araç konsepti temelinde ve FRAND koşulları altında siber güvenliği sağlarken verilere erişim her zaman sağlanır.

⁸ <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN>

⁹ <https://op.europa.eu/en/publication-detail/-/publication/d7ee4b58-4bc5-11ea-8aa5-01aa75ed71a1>

(2) Yetkilendirme yönetimi: Verilerin kullanımına ilişkin karar alma yetkisi nihai olarak müşteriye aittir. Müşteri için OEM'de yetkilendirme yönetiminin şeffaf ve merkezi yönetimi de bunu siber güvenlik ve OEM'in müşteri güvenliği konusundaki üst düzey sorumluluğu bağlamında gerçekleştirmektedir.

(3) Üçüncü taraf iş modellerinin korunması: Üçüncü tarafların verilerinin veya kullanım durumlarının ticari takibinin engellenmesi hem teknik hem de sözleşmeyle sağlanır. Buna göre, üçüncü taraflar için genişletilmiş araç arayüzünün kullanımı- bireysel servis sağlayıcılar, araçlar anlamında pazar yerleri- kullanım durumlarının izlenmesinin engellenebilmesini sağlar. Belirli yasal, sözleşmeye dayalı ve / veya güvenlik nedenlerinin yanı sıra veri aktarımı ve yetkilendirme yönetiminin optimizasyonu için özel bir kapsamda izleme gereklidir.

(4) Mevcut verilerle ilgili şeffaflık: Tek bir OEM'in mevcut verileriyle ilgili şeffaflık, OEM başına görüntülenebilir bir veri kataloğu aracılığıyla sağlanmalıdır. Katalog, genişletilmiş araç konsepti veya buna karşılık gelen bir web arayüzü aracılığıyla elektronik formatta sunulur. Teknik açıklamalar ve yeni araç nesilleri nedeniyle bu kataloğa art arda daha fazla veri eklenebilir. Bireysel B2B sözleşmeleri temelinde A Kategorisine ek veri eklemek de mümkündür.

(5) Tekdüze çerçeve: Veri kullanıcıları tarafında daha fazla şeffaflık ve anlayış yaratmak amacıyla araç verilerinin tanımlanması için tekdüze bir çerçevenin geliştirilmesi. Buna göre, meta veri tanımı anlamında ortak bir terminoloji, sadece OEM'lerden daha fazlası ile birlikte geliştirilmelidir.

(6) Katma değerli hizmetler için veri kümesi: Üreticiler arası katma değerli hizmetler için temel, başlangıç ve üreticiler arası veri kümesinin geliştirilmesi konusunda fikir birliği vardır. Amaç, zaman içinde gelişecek ve adapte olacak statik olmayan bir veri kümesidir.

(7) Yaklaşım: Kapsayıcı bir veri kümesinin öncülüğü ve dolayısıyla aynı şeyin temel, sürekli olarak daha da geliştirilmesi, temel bir kullanım durumu ve dolayısıyla katma değere dayalı bir mantıktır. Bu kullanım durumu yapılandırılmış bir forum aracılığıyla oluşturulacaktır. Burada, OEM'in verilerini ve veri sağlayıcılarını kullanmak isteyen üçüncü tarafların, ilgili kullanım durumlarının türetilmesinde somut veri gereksinimlerini göz önünde bulundurması ve önceliklendirmesi ve son olarak bunları genel ekonomik uygulanabilirlik öncülü altında değerlendirmesi esastır. Ayrıca, mevcut veri tabanının yeni araç nesilleri nedeniyle temelde ve sürekli genişleyeceği ve gelişmeye devam edeceği temel bir hipotez olarak vurgulanmalıdır.

Yapılandırılmış forum, ilgili veri kullanıcılarının ve bireysel OEM'lerin katılımı ile yürütülmelidir. Ayrıca, forumun temel tarafsızlığının korunması için AB Komisyonu'nun, örneğin organizatör ve moderatör olarak öncü bir rol oynaması çağrısında bulunuyor.

Alman otomotiv endüstrisi, ADAXO konseptinin Avrupa veri stratejisinin uygulanmasına alt düzeyde katkı sağlayacağına inanıyor. Uygulanmasını aktif olarak teşvik edeceğiz ve ilgili tüm tarafları şekillendirmeye yardımcı olmaya çağıracağız.

¹⁰ See Section III.7

V Ekler

V.1. AB Komisyonu çalışması: TRL çözüm önlemleri ve ilk değerlendirme

Avrupa Komisyonu tarafından yaptırılan çalışma, işleyen bir veri piyasasının kurulması için gerekli olduğu sonucuna varılan aşağıdaki eylem önerilerini içermektedir.

1. Veri ve fonksiyon kataloğunun kullanılabilirliği

Araç verilerine dayalı bağımsız, üçüncü taraf hizmetlerin etkin bir şekilde geliştirilmesi için üreticiler arasında verilerin kullanılabilirliğine ilişkin şeffaflık özellikle gereklidir.

2. Veri ve fonksiyonların standardizasyonu

Hizmetler için veri ve fonksiyonların standardizasyonu (okuma / yazma), tamamen teknik araç sinyallerini daha verimli bir şekilde kullanılabilir hale getirmeyi ve bunları üreticiden ve araç üretiminden mümkün olduğunca bağımsız olarak tanımlamayı amaçlamaktadır (örneğin, araç sinyal spesifikasyonu, VSS).

3. Minimum işlevler ve minimum veri kümeleri

Üreticiler arasında veri ve işlevlerin bulunması, özellikle araç verilerine dayalı bağımsız, üçüncü taraf hizmetlerin geliştirilmesi için gereklidir. Bu, arz ve talep temelinde büyümeye devam eden bir ekosistem oluşturmak amacıyla üçüncü taraf çok markalı hizmetlerin ilk etkinleştirilmesini mümkün kılmalıdır.

4. B2B sözleşmeleri için standart sözleşme şartları

Antitröst yasası uyarınca izin verilirse, verilere dayalı bağımsız, üçüncü taraf hizmetlerin etkin bir şekilde geliştirilmesi için tek tip sözleşme bileşenleri özellikle memnuniyetle karşılanacaktır.

5. Veri / işlev erişimi için maksimum ücretler

Maksimum fiyat talep etmek, yeni iş modellerinin sağlanmasını güvence altına alabilir. Bununla birlikte, bu talebin veri teklifi üzerinde de engelleyici bir etkisi olabilir.

6. Kaynak sağlayıcı tarafından uygunsuz iş zekasının önlenmesi

Veri erişim analizinin önlenmesine yönelik talep, geliştirilmekte olan yeni iş modellerinin üçüncü şahıslar tarafından korunmasına hizmet eder.

Araca doğrudan erişim durumunda OEM'den servis sağlayıcıya düzenlenmiş bir sorumluluk devri sağlanması gerektiğinden, OEM arka ucuna (araç sistemlerini etkilemeden) okunan veri erişimi ile OEM arka ucu üzerinden araca uzaktan tanımlama desteği (RDS) arasında ayırım yapmak gerekir.

7. Şifrelenmemiş OBD erişimini koruma

OBD arabirimi üzerinden üreticinin atölyelerinde bulunan tüm veriler ve işlevler, üçüncü taraf sağlayıcılara ayrımcılık yapılmaksızın da kullanılabilir hale getirilir. Erişim detayları AB Tip Onay Yönetmeliği 2018/858, Ek X, No. 2.9'da belirtilmiştir.

8. Paketlenmiş hizmetler olmadan OEM bağlantı sözleşmesi

Araç tarafından veri iletimi, OEM tarafından sunulan bir hizmetle birleştirilir ve bu nedenle üçüncü taraflar için veri iletimi de öyledir. Temel bir bağlantı, üçüncü tarafların son müşterilere eşit düzeyde hizmet sunmasını mümkün kılmalıdır.

9. OEM'ler için maksimum yanıt süreleri

Veriler ve işlevler tüm piyasa katılımcıları (OEM'ler ve üçüncü taraflar) için aynı kalitede (gecikme süresi ve tetikleyici) mevcut olmalıdır. Yeni veri ve işlevler sağlama süreci, müşterilerin dijital son ürünleri ve bunlara dayalı hizmetleri kullanırken alışkın oldukları pazara özgü yanıt süreleri için çaba göstermelidir.

10. Adil, makul ve ayrımcı olmayan (FRAND) ilkelere dayalı olarak uzaktan erişilebilen veri ve işlevlere erişim

Arka uçta saklanan araç verilerine salt okunur erişimin aksine (yani aracın kendisini etkilemeden), araca ve verilerine yazma (veya okuma-yazma) bağlantısı olduğunda araç sistemlerinin bütünlüğü ve operasyonel güvenlikleri açısından ek riskler söz konusudur ve kaynaklar - yani uzaktan tanılama ve bakım işlevleri. Yetkili üçüncü şahıslar tarafından erişim için geçerli ilke, bu tür uzaktan tanılama hizmetlerine ve işlevlerine aynı anda ve ilgili üreticinin yetkili bayileri, atölyeleri ve servis sağlayıcılarıyla aynı ölçüde erişilebilirlerdir.

11. FRAND ilkelerine uyumu izlemek için Komisyona raporlama bilgileri

Bu konudaki raporlar üreticiler, servis sağlayıcılar veya tarafsız sunucular tarafından AB Komisyonu'na sunulacaktır.

12. Görevlerin ayrılması

Erişim onaylayıcısı ve veri sahibi tek bir rolde birleştirilmez. Veri sahibi değil müşteri verilere erişimi onaylar. Burada, OEM arka ucuna (araç sistemlerini etkilemeden) okunan veri erişimi ile OEM arka ucu üzerinden araca uzaktan tanılama desteği (RDS) arasında ayırım yapmak gerekir. Süreç, OEM, telematik müşteri (OEM'in telematik kapsamı için sözleşme ortağı) ve servis sağlayıcılar arasında ayırım yapmalıdır.

13. Yerleşik uygulama platformu

Araçtaki veri, fonksiyon ve kaynakların yanı sıra teknik koşullar çerçevesinde müşteriye arayüzlere erişim sağlar. Bunun için araçta ilave arayüzler sağlanmalıdır. Bu, güvenlik ve araç onayı ile ilgili seviyelere kadar erişimin sağlandığı anlamına gelir.

Araç sistemleri için yazılım geliştirme ve veri sağlama yazılımı, gereksinim özellikleri, üreticiye özgü standartlar ve tasarım yönergeleri, endüstri çapında güvenlik ve işlevsel güvenlik yönergeleri ve düzenleyici çerçeve koşulları gibi açık yönergelere tabidir. Araç üreticisi her zaman entegrasyon, işlevsel güvenlik ve güvenliğin yanı sıra yapılandırma ve kaynak yönetiminden sorumludur. Bu nedenle OEM, her zaman veri toplama ve veri kullanımının yankı içermediğinden emin olmalıdır. Bu sadece şu yollarla mümkündür;

Veri toplama ve fonksiyonların kontrollü kullanımı. Bu amaçla araç üreticisi ile kontrollü kullanım alanları tanımlanmalıdır.

14. ExVe için özel onay yönetimi ve kimlik doğrulama prosedürleri

Veri toplama ve kullanma temeli, müşterinin belirli bir amaç için açık rızasıdır. Kimlik doğrulaması ile ilgili olarak, OEM arka ucuna (araç sistemlerini etkilemeden) okunan veri erişimi ile OEM arka ucu üzerinden araca uzaktan tanılama desteği (RDS) arasında ayırım yapmak gerekir, çünkü OEM'den servis sağlayıcıya düzenlenmiş bir sorumluluk devri sağlanmalıdır.

V.2. Uzaktan tanılama işlemlerinin detaylandırılması

Uzaktan tanılama (RD) – Müşteri yolculuğu

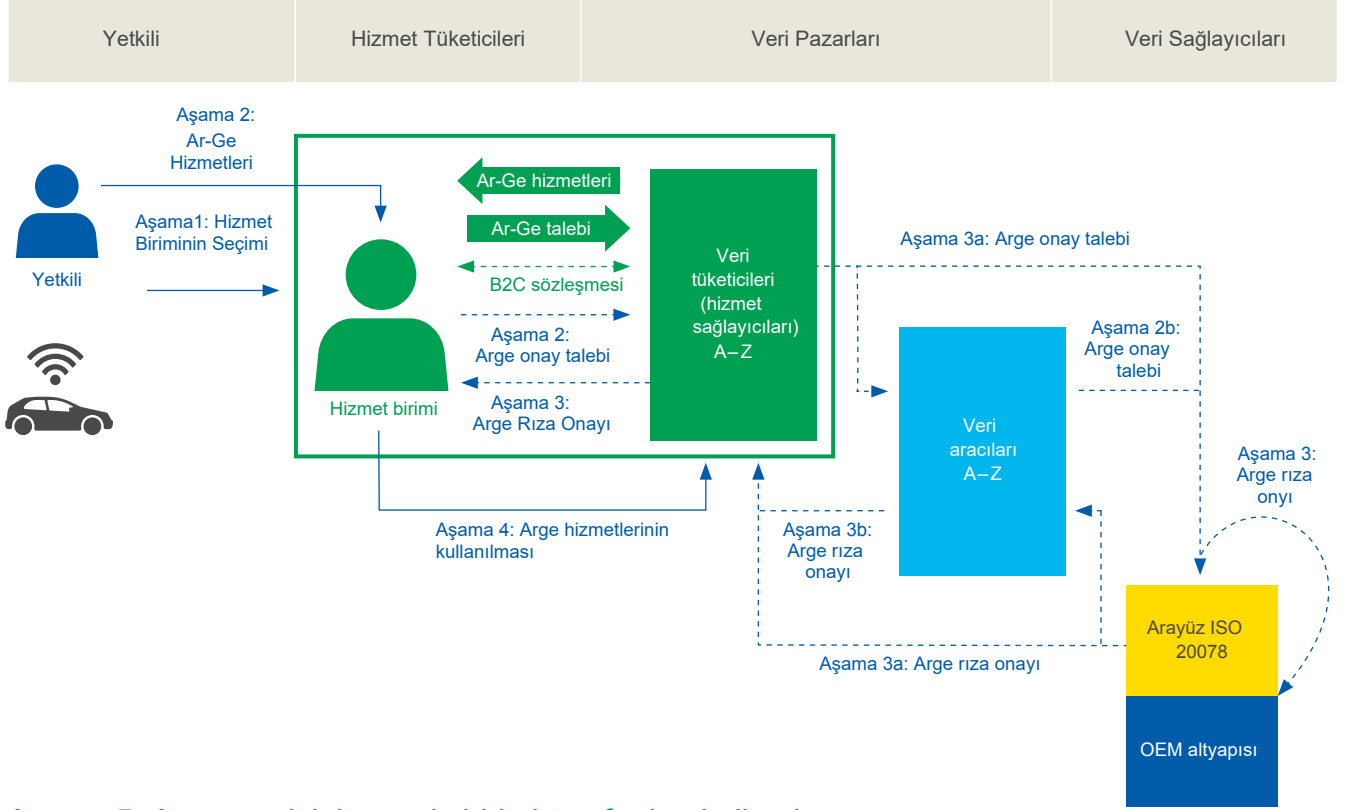
Etkinlik Aşamaları:	Aşama 1***: Arge servis Yetkilendiricisinin seçimi	Aşama 2: Arge servis Yetkilendiricisinin siparişi	Aşama 3: Onay Yetkilendiricisi	Aşama 4: Servis birimi tarafından RD servisinin kullanımı
Eylem:	Yetkili bir servis biriminin Arge servisini seçer * Arge servis sağlayıcısı aracılığıyla**	Yetkili servis birimini* Arge servis sağlayıcısı aracılığıyla Arge gerçekleştirmek üzere görevlendirir**	Yetkilendirici, Arge servis sağlayıcısına ** (aracı) aracılığıyla çift yönlü veri talep etme izni verir OEM (okuma ve yazma)	Servis birimi* Arge servis sağlayıcısı tarafından sağlanan Arge servisini kullanır**
Temas noktası:		<ul style="list-style-type: none"> * Arge servis sağlayıcı web arayüzü * (Aracı web arayüzü) 	<ul style="list-style-type: none"> * Arge servis sağlayıcı web arayüzü * (Aracı web arayüzü) • OAuth üzerinden OEM web arayüzü 	<ul style="list-style-type: none"> • Arge servis sağlayıcı web arayüzü
Aktör:	<ul style="list-style-type: none"> • Yetkilendiren 	<ul style="list-style-type: none"> • Yetkili • Servis ünitesi • Arge servis sağlayıcı (komisyon aracı) 	<ul style="list-style-type: none"> • * Yetkilendirici • * * * * Arge servis sağlayıcı (komisyonlar arası arabuluculuk) • • OEM 	<ul style="list-style-type: none"> • Servis ünitesi • Arge servis sağlayıcı (komisyon aracı) • OEM
Çevre:		<ul style="list-style-type: none"> • Arge servis sağlayıcı arayüzüne erişim 	<ul style="list-style-type: none"> • OEM arayüzüne erişim 	<ul style="list-style-type: none"> • * * * * Arge servis sağlayıcı arayüzüne erişim • * Araca erişim
Tanım:	<ul style="list-style-type: none"> • Yetkili, görevlendirilen servis biriminin * bir Arge servis sağlayıcısının Arge servisini tüketebileceğine karar verir** • Yetkili, servis birimini * Arge servis sağlayıcısının Arge sunucusu üzerinden Arge'nin uygunluğu ile görevlendirir ** ve onay sürecini tetikler 	<ul style="list-style-type: none"> • * Yetkili, servis biriminin * Arge servis sağlayıcısı aracılığıyla bir tanılama oturumu gerçekleştirdiğini bildirir** 	<ul style="list-style-type: none"> • * Yetkili, Arge servis sağlayıcısının ** servis birimi için Arge servisini ** sağlayabileceğini kabul eder (aracı aracılığıyla) 	<ul style="list-style-type: none"> • * Yetkilendirici, Arge servisini servis birimi aracılığıyla kullanır * Arge servis sağlayıcısı aracılığıyla**

* İş yapan bireysel hizmet birimi = hizmet tüketicisi.

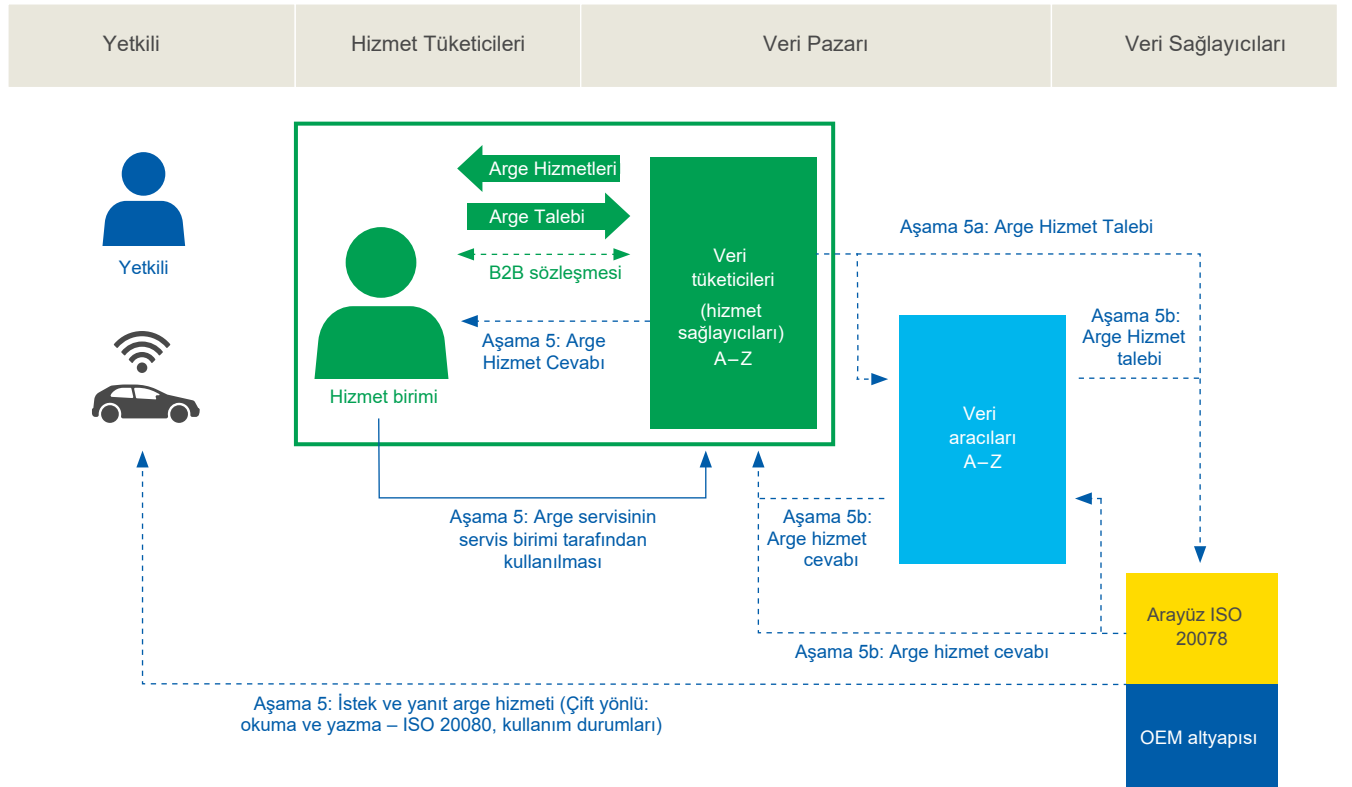
** Uzaktan tanılama servis sağlayıcısı = veri tüketicisi.

*** Varsayım: Yetkilendirici OEM'e zaten kayıtlı ve araç bir kullanıcı hesabına bağlı.

Uzaktan tanı onayı süreci (Aşama 1 – 4)



Aşama 5: Arge servisinin servis birimi tarafından kullanılması



V.3. Glossary

Abbreviation	Meaning
ADAXO	Automotive Data Access – Extended & Open
API	Application Programming Interface
ASIL	Automotive Safety Integrity Level
B2B	Business to Business
B2C	Business to Customer
B2G	Business to Government
CPU	Central Processing Unit
CSMS	Cybersecurity Management System
DA	Data Act
DGA	Data Governance Act
DMA	Digital Markets Act
DSA	Digital Services Act
GDPR	General Data Protection Regulation
ECU	Electronic Control Unit
ExVe	Extended Vehicle
FRAND	Fair, Reasonable and Non-Discriminatory
HMI	Human Machine Interface
HW	Hardware
NHTSA	National Highway Traffic Safety Administration
OBD	On-board Diagnostic
OEM	Original Equipment Manufacturer
RAM	Random-Access Memory

Abbreviation	Meaning
RDS	Remote Diagnostic Support
ROA	Remote Online Access
SUMS	Software Update Management System
SW	Software
TRL	The TRL group of companies based in Crowthorne House, UK, is part of the Transport Research Foundation (TRF).
UNECE	United Nations Economic Commissions for Europe
V2V	Vehicle-to-Vehicle Communication
VO	Regulation
VSS	Vehicle Signal Specification

Contact Persons

Dr. Joachim Damasky
Managing Director
joachim.damasky@vda.de

Matthias Krähling
Head of Department Automotive Technologies and Ecosystems
matthias.kraehling@vda.de

Dr. Joachim Göthel
Senior Consultant
joachim.goethel@vda.de

Angela Pasch
Senior Consultant
angela.pasch@vda.de

Publisher German Association of the Automotive Industry
Behrenstraße 35, 10117 Berlin
www.vda.de/en

Copyright German Association of the Automotive Industry
Reprinting and all other forms of duplication are only
permitted with indication of the source.

Version Version 1.0, December 2021