# SSI Prensipleri

Bu temel SSI ilkeleri, herhangi bir dijital kimlik ekosistemi tarafından kullanılmak üzere tasarlanmıştır. Herhangi bir kuruluş, bütünlüğünü bozmamak koşuluyla, bu ilkeleri kendi dijital kimlik ekosistem yönetişim çerçevesine dahil edebilir. SSI prensipleri, yalnızca ilgili bir yargı alanında geçerli olan resmi yasa ve yönetmeliklerle sınırlandırılmalıdır.

### 1. Gösterilim

Bir SSI ekosistemi, varlıkların (insan, tüzel kişilik, doğal varlık, fiziksel veya dijital nesne) herhangi bir sayıda dijital kimlik ile temsil edilebilmeleri için yöntemler sağlamalıdır.

### 2. Birlikte çalışabilirlik

Bir SSI ekosistemi, bir varlığın dijital kimlik verilerinin, kamuya açık ve telifsiz standartlar kullanılarak temsil edilmesine, değiş tokuş edilmesine, güvenlik altına alınmasına, korunmasına ve doğrulanmasına olanak sağlamalıdır.

### 3. Merkeziyetsizlik

Bir SSI ekosistemi, bir varlığın dijital kimlik verilerinin oluşturulması, denetimi ve doğrulanması için merkezi bir sisteme bağımlı olmamalıdır.

### 4. Denetim ve Temsilci

Bir SSI ekosistemi, kimlikleriyle ilgili olarak doğal, insani veya yasal haklara sahip tüzel kişilere ("Kimlik Hakkı Sahipleri"), dijital kimlik verilerinin kullanımını kontrol etme ve isterlerse bu kontrolü, kendi görevlendirdikleri ve/veya seçtikleri (bireyler, kuruluşlar, cihazlar ve yazılımlar gibi) ajans ve vasilere devrederek uygulama yetkisi vermelidir.

### 5. Katılım

Bir SSI ekosistemi, bir kimlik hakları sahibinin katılımını gerektirmemelidir.

### 6. Eşitlik ve Kapsayıcılık

Bir SSI ekosistemi, yönetişimi kapsamında, kimlik hakkı sahiplerini dışlayamaz veya bunlara karşı ayrımcılık yapamaz

### 7. Kullanılabilirlik, Erişilebilirlik ve Tutarlılık

Bir SSI ekosistemi, Agent ve diğer SSI bileşenlerinin, kimlik hakkı sahiplerince kullanılabilirliğini ve erişilebilirliğini, kullanım tutarlılığı da sağlayacak şekilde maksimize etmelidir.

### 8. Taşınabilirlik

Bir SSI ekosistemi, kimlik hakkı sahiplerinin dijital kimlik verilerinin bir kopyasını seçtikleri aracılara veya sistemlere taşıma veya aktarmasına kısıt getirmemelidir.

### 9. Güvenlik

Bir SSI ekosistemi, kimlik hakkı sahiplerine, dijital kimlik verilerini depolarken ve transfer ederken güvenliğini sağlama, kendi tanımlayıcılarını ve şifreleme anahtarlarını kontrol etme ve tüm etkileşimler için uçtan uca şifreleme kullanma yetkisi vermelidir.

### 10. Doğrulanabilirlik ve Otantiklik

Bir SSI ekosistemi, kimlik hakkı sahiplerine, dijital kimlik verilerinin gerçekliğinin doğrulanabilir kanıtını sunmaları için yetki vermelidir.

### 11. Mahremiyet ve Minimum İfşa

Bir SSI ekosistemi, kimlik hakkı sahiplerine, dijital kimlik verilerinin mahremiyetini koruma ve herhangi bir belirli etkileşim için gereken en az miktarda dijital kimlik verisi paylaşma yetkisi vermelidir.

### 12. Şeffaflık

Bir SSI ekosistemi, kimlik hakkı sahiplerinin ve diğer tüm paydaşların, etmenler ve diğer SSI ekosistem bileşenlerinin faaliyetleri ile ilgili teşvikleri, kuralları, politikaları ve algoritmaları anlamaları için gerekli bilgilere kolayca erişmelerine ve bunları doğrulayabilmelerine olanak sağlamalıdır.

*Bu belge, Sovrin Vakfı tarafından bu İlkelerin bir koruyucusu olarak bir araya getirilen küresel SSI topluluğu üyeleri tarafından geliştirilmiştir.*

Bu doküman, Sovrin Foundation tarafından sürdürülmektedir ve Sovrin Utility Governance Framework ve Sovrin Ecosystem Governance Framework içinde bulunması Sovrin Board of Trustees onayı ile gerçekleşmektedir.

Sizi, yorum ve önerilerinizle bu dokümanın herkesin erişimine açık olan yaşayan sürümüne katkı yapmaya davet ediyoruz.

Eğer SSI Prensipleri'nin sürmekte olan geliştirme çalışmasına katılmak istiyorsanız, lütfen Sovrin Governance Framework Working Group Toplantı Sayfasını ziyaret ediniz.



---

SSI Prensiplerini uygulayan ve destekleyenler: