Çok Faktörlü/Parolasız Kullanıcı Doğrulama Sistemi (MFA) ve Tekil Kullanıcı Doğrulama Sistemi (SSO) Teknik Şartnamesi

Genel Şartlar;

1. Teklif edilecek çözüm, 2000 personel, 6000 öğrenci ve 16000 mezun olmak üzere 24000 adet kullanıcı lisansına sahip olacaktır. Alternatif olarak kullanıcı sayısından bağımsız site lisansı da teklif edilecektir.
2. Teklifler 3 yıllık olarak yapılacak ancak ödemeler yıllık olarak 3 vadede ödenecektir.
3. Sistem, **bulut tabanlı veya kurum alt yapısında kurulu** olabilir. Kurum alt yapısı kullanılacaksa sistemin tüm bileşenlerinin kurum altyapısında kurulu bulunması beklenmektedir.
4. Firma tarafından çok faktörlü doğrulama için mobil uygulama sağlanmalıdır. Sağlanacak mobil uygulama, üretilmiş sistemin kendi mobil uygulaması olmalı, üçüncü parti bir mobil uygulama kullanılmamalıdır.
5. PHP, .Net, Java, IBM Websphere ve Google Workspace ürünlerini desteklemelidir.
6. Sabancı Üniversitesi altyapısında SSO kullanan tüm uygulamaların 1 ay içerisinde entegrasyonu sağlandıktan sonra ihale kabulü yapılacaktır.

Sistem kurum altyapısında kurulacaksa;

1. Kurumun sağlayacağı vmware sanallaştırma ortamında çalışabilmelidir.
2. Sistem birden fazla sunucu üzerinde aktif/aktif ya da aktif/pasif çalışmayı desteklemelidir.
3. Sistem, yaygın olarak kullanılan Microsoft Active Directory, LDAP, SAML1, SAML2, CAS protokollerini desteklemelidir. Sistem, kurum tarafından kullanılmakta olan CAS sistemine entegre olacaktır. Önerilen sistem kendi SSO çözümünü sunması durumunda kurumda kullanılan uygulamarda hiçbir değişiklik yapılmadan kendi sistemlerini kullanabileceklerdir.
4. Sistem, kullanıcı bilgilerini doğrulamak için Active Directory, LDAP, MSSQL, PostgreSQL bağlantı desteği sunmalıdır. Birden fazla Active Directory, LDAP, MSSQL, PostgreSQL hesapları veya sunucularıyla sorunsuz şekilde çalışabilmelidir.
5. Sistem, Sms Otp, Mail Otp, Soft Otp, Push Notification, QR Code, Voice Bildirim, Voice Otp, Hardware Token, Pin ve Recovery Code ile kullanıcı doğrulama metotlarını desteklemelidir.
6. Sistemde yönetim paneli üzerinden her bir tanımlı uygulama ve servis için kullanılabilecek MFA faktör tipleri seçilebilmeli veya belirli bir MFA faktör tipi zorunlu tutulabilmelidir.
7. Sistem, OTP kullanımlarında Time Based (TOTP) ya da Counter Based (HOTP) kullanımının seçilebilmesine olanak sağlamalıdır. Üretilen tek kullanımlık şifrelerin uzunluklarının ayarlanabilmesine olanak tanımalıdır.
8. Sistemde yönetim paneli üzerinde grup tanımlaması yapılabilmeli ve lokal kullanıcılar bu gruplara atanabilmelidir.

9. Teklif edilen sistem, birincil parolalara karşı oluşabilecek kaba kuvvet saldırılarını engelleyebilmelidir.
10. Kimlik doğrulama yöntemleri kullanıcı, grup veya uygulama bazlı olarak özelleştirilebilmelidir.
11. Grup ve kullanıcı erişim yetkilendirmeleri AD grupları ile yapılabilmelidir.
12. Yönetim paneline hem LDAP kullanıcıları hem de uygulama lokal admin kullanıcıları ile giriş sağlayabilmelidir. Panele giriş sağlayacak LDAP kullanıcıları için rol ve grup bazlı kısıtlama yapılabilmelidir.
13. Sistem, belirlenecek politikalarla çeşitli senaryo doğrulama alt yapısına sahip olmalıdır. Sistem içerisinde birden fazla politikalarla senaryo oluşturulabilmelidir.
14. Yönetim paneli üzerinden her bir tanımlı uygulama ve servis için farklı bir politika seçilebilmelidir.
15. Sistem, içerisinde yer alan politikalarda uygulanacak politika öğeleri şu şekilde olmalıdır;
    - 15.1.1. Kullanıcı Grupları (İzin verilen ve/veya Engellenen Kullanıcı Grupları Seçilebilmelidir)
    - 15.1.2. Kullanıcılar (İzin verilen ve/veya Engellenen Kullanıcılar Seçilebilmelidir)
    - 15.1.3. Kıtalar (İzin verilen ve/veya Engellenen Kıtalar Seçilebilmelidir)
    - 15.1.4. Ülkeler (İzin verilen ve/veya Engellenen Ülkeler Seçilebilmelidir)
    - 15.1.5. Şehirler (İzin verilen ve/veya Engellenen Şehirler Seçilebilmelidir)
    - 15.1.6. IP Adresleri (İzin verilen ve/veya Engellenen IP Adresleri Seçilebilmelidir)
    - 15.1.7. Zaman (İzin verilen ve/veya Engellenen Zaman Aralıkları Seçilebilmelidir)
    - 15.1.8. Browser (İzin verilen ve/veya Engellenen Browserlar Seçilebilmelidir)
    - 15.1.9. İşletim Sistemi (İzin verilen ve/veya Engellenen İşletim Sistemleri Seçilebilmelidir)
16. Her politikanın politika öğeleri, giriş yöntemi ve kullanıcı doğrulaması yapacağı veri tabanı farklı olarak seçilebilmelidir.
17. Kullanıcı özelinde giriş yöntemi farklı olarak seçilebilmelidir. Kullanıcı özelinde seçilen giriş yöntemleri ve varsayılan giriş yöntemi önceliklendirilebilmelidir. Bu sayede politikada seçilen giriş yöntemlerine baskın gelmeli ve ilgili kullanıcı için politika giriş yöntemlerini geçersiz kılabilmelidir.
18. Politikalar üzerinde de kullanıcı özelinde giriş yöntemi seçilmiş ve önceliklendirilmiş olsa dahi her koşulda politika giriş yöntemlerinin geçerli kılınması sağlanabilmelidir.
19. Sistem, kullanıcıların Mobil Uygulamaya kaydolmalarını (self-enrollment) sağlayacak “Mobil Uygulama Profili” oluşturulabilmesi için bir Web Portala sahip olmalıdır ve kullanıcılar, Web Portala kullanmakta oldukları kurum kullanıcı adı ve parolaları ve telefonlarına sms veya sistemde kayıtlı adreslerine mail olarak gönderilen kod ile giriş yapabilmelidir. Ayrıca bu web portal üzerinden Cep telefonlarını girebilmeli ve değiştirebilmelidir.
20. Teklif edilen sistemde, MFA sistemine kaydolma işlemi e-posta üzerinden kullanıcıya gönderilen QR kod okutularak tetiklenebilmeli ve kullanıcıya mobil uygulamayı indirtecek store linklerini göndermeyi ve yönlendirmeyi desteklemelidir.
21. Sistem, mobil uygulamaya indirilecek tek bir profil ile entegrasyon sağlanan tüm uygulamalara erişimi desteklemelidir. Her uygulama için ayrı profil indirmeye gerek olmamalıdır.

22. Belirlenen gruplara kullanıcılar eklendiğinde belirlenen süre sonra otomatik olarak bu kullanıcılara profiller oluşturulup isteğe bağlı olarak mail ve/veya sms ile kullanıcıya bilgilendirme yapılabilmelidir. Kullanıcı gelen mail üzerinden gerekli işlemleri yaparak mobil uygulamayı kullanmaya başlayabilmelidir.
23. Active Directory üzerinden belirlenen gruplarda yer alan ancak 'Disable' olan kullanıcılar 'Enable' yapıldığında belirlenen süre sonra otomatik olarak bu kullanıcılara profiller oluşturulup mail ve/veya sms ile kullanıcıya bilgilendirme yapılabilmelidir. Kullanıcı gelen mail üzerinden gerekli işlemleri yaparak mobil uygulamayı kullanmaya başlayabilmelidir.
24. Active Directory üzerinden belirlenen gruplarda yer alan kullanıcılar, Active Directory üzerinden 'Disable' yapıldığında belirlenen süre sonra otomatik olarak bu kullanıcıların profilleri sistemden kaldırılmalı ve isteğe bağlı olarak mail ve/veya sms ile kullanıcıya bilgilendirme yapılabilmelidir.
25. Sistem, otomatik olarak oluşturulup mail ya da sms yoluyla iletilen profillerin hangilerinin kullanıcılar tarafından mobil uygulamalarına indirilip indirilmediğini raporlayabilmelidir.
26. Sistem, admin yetkisine sahip kullanıcıların diledikleri zaman kullanıcı profillerini silmelerine olanak sağlamalıdır.
27. Sistem, kullanıcıların profillerini farklı cihazlara yükleyebilmeleri için öncelikle kullanmış oldukları cihazdan kaldırmalarına ardından yeni cihazlarına yükleyebilmelerine izin vermelidir. Ancak kullanmış oldukları cihazdan profillerini silmeden farklı bir cihaza aynı profilin yüklenmesine kesinlikle izin vermemelidir.
28. Sistem üzerinden gönderilen SMS, Mail, Voice Push ve Voice OTP mesajlarının içerikleri düzenlenebilmelidir.
29. Sistem, API desteği sağlamalıdır.
30. Sistem, çalışma esnasında servisleri, web soketle vb. arasındaki haberleşmeyi şifreli (encryption) olarak yapmalıdır.
31. Sistem, SSO uygulamalarında kurumun belirleyeceği sayıda yanlış giriş denemesi sonrasında kullanıcının karşısına Captcha çıkarabilme yeteneğine sahip olmalıdır.
32. Mobil uygulamanın Android ve iOS versiyonları bulunmalı ve ilgili çevrimiçi uygulama pazarlarından indirilebilmelidir.
33. Sistem, çoklu profil desteği sunmalı, her kullanıcının mobil cihazına birden fazla profil eklenebilmelidir.
34. Mobil uygulama, mobil cihazda internet olmadığı durumlarda da OTP üretimi yapabilmelidir.
35. Sistem, kullanıcıya, IT personelinin desteğine ihtiyaç duymadan akıllı telefonuna yüklemiş olduğu bu sisteme ait mobil uygulama üzerinden kendisine ait hesabın kilidini kaldırabilmelidir. Bu işlemlerin mobil uygulama üzerinden yapılıp yapılamayacağı kurum tarafından yönetim arayüzü üzerinden seçilebilmelidir.
36. Sistem içerisinden SIEM ürünlerine syslog olarak log gönderimi sağlanmalıdır.
37. Yönetim arayüzü, kurumun sistem yöneticilerine farklı seviyelerde kullanım hakları ve izinleri sağlayabilmeli ve erişebildikleri fonksiyonlar kurumun önceden belirlemiş olduğu kurallar doğrultusunda olmalıdır.
38. Sistem, yönetim arayüzü üzerinden sistemin servis durumlarının görüntülenebilmesine olanak sağlamalıdır.
39. Sistem, yönetim arayüzü üzerinden RealTime Access Log alınabilmesine olanak sağlamalıdır. Alınan logların XLS/CSV/PDF olarak dışa aktarılmasına olanak sağlamalıdır.

Sistem bulut tabanlı ise;

1. Önerilecek çözüm CAS protokolü ile entegre olmalıdır.
2. Sistem, Sms Otp, Mail Otp, Soft Otp, Push Notification, QR Code, Voice Bildirim, Voice Otp kullanıcı doğrulama metotlarını desteklemelidir.
3. Sistemde kullanıcılar, kullanılabilecek MFA faktör tipleri seçilebilmelidir.
4. Sistem, kullanıcıların profillerini farklı cihazlara yükleyebilmeleri için öncelikle kullanmış oldukları cihazdan kaldırmalarına ardından yeni cihazlarına yükleyebilmelerine izin vermelidir. Ancak kullanmış oldukları cihazdan profillerini silmeden farklı bir cihaza aynı profilin yüklenmesine kesinlikle izin vermemelidir.
5. Sistem üzerinden gönderilen SMS, Mail, Voice Push ve Voice OTP mesajlarının içerikleri düzenlenebilmelidir.
6. Mobil uygulama, mobil cihazda internet olmadığı durumlarda da OTP üretimi yapabilmelidir.
7. Uygulama başına ve genel olarak güvenlik politikaları tanımlanabilmeli ve uygulanabilmelidir.
8. Network bazında kurallar uygulanabilmelidir.
9. Kullanıcı veya grup bazında belirlenen politikalar uygulanabilmelidir.