



KeyZula

GÜVENLİK TASARIMI

KeyZula kasanızı nasıl korur?

Mimari, kriptografi, hesap korumaları ve sunucularımızın neyi görebildiğinin sınırları.

SÜRÜM

1.1

TARİH

30 Eylül 2026

YAYIMCI

Netlen İnternet Hizmetleri Ltd. Şti.

İçindekiler

1	Giriş	4
2	Tehdit modeli ve güvenlik hedefleri	4
2.1	Güvenlik hedefleri	4
2.2	Dikkate alınan saldırırganlar	4
2.3	Kapsam dışı	5
3	Kriptografik yapı taşları	5
4	Hesap oluşturma ve giriş	6
4.1	Anahtar türetme	6
4.2	Kayıt	6
4.3	Giriş ve doğrulayıcının saklanması	6
4.4	Oturumlar	6
4.5	İki adımlı doğrulama	7
4.6	Passkey ile giriş	7
4.7	Yeni cihaz uyarıları ve güvenlik e-postaları	7
4.8	İstek sınırları	7
4.9	Ana parola olmadan kilit açma	8
4.10	Ana parola değişikliği ve hesap silme	8
5	Kasa şifrelemesi	8
5.1	Anahtar hiyerarşisi	8
5.2	Kayıtlar	9
5.3	Ek doğrulanmış veri (AAD)	9
5.4	Şifresiz saklanan üst veriler	9
6	Paylaşım ve organizasyonlar	10
6.1	Organizasyonlar ve koleksiyonlar	10
6.2	Üye ekleme ve parmak izi doğrulaması	10
6.3	Yetkiler	10
6.4	Erişimin kaldırılması	11
6.5	Politikalar	11
7	SSO, güvenilir cihazlar ve yönetici kurtarması	11

7.1	Tek oturum açma (SSO)	11
7.2	Ana parolası olmayan hesaplar	11
8	Acil durum erişimi	12
9	Gönder	12
10	Dosya ekleri ve dosyalar	13
11	Servis hesapları ve komut satırı aracı	13
11.1	Servis hesapları	13
11.2	Komut satırı aracı	13
12	Tarayıcı eklentisi	14
13	Mobil uygulamalar	14
14	Web kasası	15
15	Sunucunun görebildikleri ve göremedikleri	15
16	İletim ve altyapı	16
17	Erişim kayıtları ve denetim olayları	17
18	Tasarım tercihleri	17
19	Güvenlik bildirimi	18

1 Giriş

KeyZula; parolalar, passkey'ler, iki adımlı doğrulama (TOTP) kodları, SSH anahtarları, belgeler ve notlar için bireylere ve kurumlara yönelik uçtan uca şifreli bir kasadır. Netlen İnternet Hizmetleri Ltd. Şti. (İstanbul) tarafından geliştirilir ve işletilir. KeyZula; web kasası (app.keyzula.com), tarayıcı eklentileri, iOS/iPadOS ve Android uygulamaları ve komut satırı aracıyla kullanılabilir.

Bu belge KeyZula'nın kasa verilerini nasıl koruduğunu anlatır: anahtarların nasıl türetildiği ve saklandığı, verinin nasıl şifrelenip paylaşıldığı, hesapların ve oturumların nasıl korunduğu, KeyZula sunucusunun neyi görüp neyi göremediği ve bu tercihlerin ardındaki tasarım kararları. Kapakta belirtilen tarihteki uygulamayı yansıtır.

Tüm KeyZula istemcilerinin kullandığı istemci tarafı şifreleme kütüphanesi, Apache 2.0 lisansıyla github.com/KeyZula/keyzula-crypto adresinde açık kaynaktır. Sunucu, web kasası, eklentiler ve uygulamaların kaynak kodu kapalıdır; bu belge bunların güvenlikle ilgili davranışını anlatır.

2 Tehdit modeli ve güvenlik hedefleri

2.1 Güvenlik hedefleri

- **Sunucuya karşı gizlilik.** Kasa içeriği (kayıt adları, kullanıcı adları, parolalar, adresler, notlar, özel alanlar, TOTP gizli anahtarları, passkey'ler, SSH anahtarları, dosya ekleri ve dosya adları) kullanıcının cihazında şifrelenir. Sunucu şifreli veriyi saklar ve eşitler; çözemez.
- **Bütünlük ve bağlam bağlılığı.** Tüm şifreli veriler doğrulanır. Her şifreli değer amacına ve kayıt kimliğine bağlıdır; sunucu şifreli değerleri kayıtlar, alanlar veya dosya ekleri arasında fark edilmeden yer değiştiremez.
- **Sunucu verisiyle çevrimdışı saldırı yapılamaması.** Ana parolayı tahmin etmek dışında bir yol yoktur; Argon2id bu tahminleri bilerek pahalı hâle getirir.
- **Hesap koruması.** Sunucu tarafı doğrulayıcı, istek sınırları, iki adımlı doğrulama ve bildirimlerle parola denemesi ve kimlik bilgisi doldurma saldırılarına karşı koruma.

2.2 Dikkate alınan saldırganlar

- Veritabanının, yedeklerin veya dosya eki deposunun bir kopyasını ele geçiren saldırgan.
- Kötü niyetli veya ele geçirilmiş bir sunucu işletmecisi; değiştirilmiş veri döndürenler dahil (örneğin zayıf KDF parametreleri veya yer değiştirilmiş şifreli değerler).
- İstemci ile sunucu arasındaki ağ saldırganı.
- Yetkilerinin ötesine geçmeye çalışan diğer kullanıcılar; paylaşılan bir organizasyonun üyeleri ve yöneticileri dahil.

2.3 Kapsam dışı

- Kasa açıkken ele geçirilmiş bir kullanıcı cihazı (zararlı yazılım, tuş kaydedici, sayfa içeriğine erişebilen kötü niyetli bir tarayıcı eklentisi).
- Kullanıcının seçtiği zayıf veya başka yerde kullanılmış ana parola.
- Erişilebilirlik: işletmeci hizmeti durdurabilir veya veriyi silebilir; kullanıcılar kasalarını dışa aktarabilir.
- Kötü niyetli istemci kodu. Web kasası her ziyarette KeyZula sunucusundan yüklenir; bu sunucuyu ele geçiren biri değiştirilmiş kod sunabilir. Mağazalardan kurulan uygulamalar ve eklentiler bundan aynı şekilde etkilenmez (bkz. Tasarım tercihleri).

3 Kriptografik yapı taşları

İstemciler libsodium (`libsodium-wrappers-sumo` , WebAssembly) ve `@noble/hashes` kullanır. Tüm rastgele değerler libsodium'un kriptografik rastgele sayı üreticinden gelir.

AMAÇ	ALGORİTMA VE PARAMETRELER
Ana paroladan anahtar türetme	Argon2id (v1.3); varsayılan 3 iterasyon, 64 MiB bellek; hesaba özel 16 baytlık rastgele tuz
Alt anahtar türetme	Ayrı etiketlerle HKDF-SHA256 (örneğin <code>vault/v1/auth-hash</code> , <code>vault/v1/key-encryption-key</code>)
Simetrik şifreleme	XChaCha20-Poly1305 (IETF), 256 bit anahtar, her şifrelemede rastgele 192 bit nonce, bağlama bağlı ek doğrulanmış veri (AAD)
Açık anahtarlı şifreleme	X25519 mühürlü kutular (<code>crypto_box_seal</code>)
Açık anahtar parmak izleri	Etiket, hesap e-postası ve açık anahtar üzerinden BLAKE2b-256; 5 haneli 6 grup olarak gösterilir
Sunucu tarafı doğrulayıcılar	Giriş ve PIN doğrulayıcıları için Argon2id (2 iterasyon, 19 MiB); oturum ve servis belirteçleri için SHA-256

Simetrik şifreli değerler base64url ile `v1.<nonce>.<şifreli metin>` biçiminde saklanır. Sürüm öneki ileride algoritma değişikliğine imkân verir.

4 Hesap oluřturma ve giriř

4.1 Anahtar turetme

Ana parola Unicode NFKC ile normalleřtirilir ve hesabın tuzu ve maliyet parametreleriyle Argon2id'den geirilerek 256 bitlik ana anahtar retilir. Bundan HKDF-SHA256 ile birbirinden baėımsız iki anahtar tretilir:

- **Kimlik doėrulama zeti** (`vault/v1/auth-hash`): parolanın bilindiėini kanıtlamak iin sunucuya gnderilir.
- **Anahtar řifreleme anahtarı (KEK)** (`vault/v1/key-encryption-key`): cihazdan hi ıkmaz; kullanıcı anahtarını zer.

Ana anahtar tretmeden sonra bellekten silinir. İstemciler sunucudan gelen KDF parametrelerine sınır uygular (yalnızca Argon2id; 2–10 iterasyon; 19 MiB – 1 GiB bellek; 16 baytlık tuz). Bylece kt niyetli bir sunucu KDF'yi zayıflatamaz veya istemciyi kilitleyemez. Sunucu da aynı sınırları doėrular.

4.2 Kayıt

Kayıt sırasında istemci cihazda řunları retir:

- KEK ile řifrelenen rastgele 256 bitlik bir **kullanıcı anahtarı** (`protectedUserKey`);
- bir **X25519 anahtar ifti**; gizli anahtar kullanıcı anahtarıyla řifrelenir (`protectedPrivateKey`), aık anahtar řifresiz saklanır.

Sunucu yalnızca KDF parametrelerini, kimlik doėrulama zetini, aık anahtarı ve bu iki řifreli deėeri alır. Kayıttan sonra bir doėrulama e-postası gnderilir.

4.3 Giriř ve doėrulayıcının saklanması

- İstemci nce hesabın KDF parametrelerini ister (n giriř). Kayıtlı olmayan adresler iin sunucu, sunucu sırrından HMAC-SHA256 ile tretilen deterministik parametreler dndrr; bylece n giriř bir adresin kayıtlı olup olmadıėını ele vermez.
- Sunucu kimlik doėrulama zetinin kendisini saklamaz; onun Argon2id ile iřlenmiř hlini saklar (libsodium `crypto_pwhash_str`). Bu nedenle veritabanının bir kopyası giriř yapmak iin kullanılamaz.
- Hesap yoksa sunucu yine de sahte bir doėrulayıcıyla karřılařtırma yapar ve bilinmeyen adres ile yanlıř parola iin aynı hatayı dndrr.
- Bařarılı giriřten sonra istemci kullanıcı anahtarını KEK ile, gizli anahtarı da kullanıcı anahtarıyla zer. zlmř anahtarlar yalnızca bellekte tutulur.

4.4 Oturumlar

- Oturum belirteci 32 rastgele bayttır (`vs_` nekli). Sunucu yalnızca SHA-256 zetini saklar.

- Belirteçler **Authorization: Bearer** başlığıyla gönderilir; kimlik doğrulamada çerez kullanılmaz. Sunucunun istek günlüğü bu başlığı maskeler.
- Oturumların sabit bir ömrü vardır (varsayılan 30 gün). Kullanıcılar oturumlarını (cihaz, IP adresi, son etkinlik) görebilir ve istediğini kapatabilir. Ana parola değiştirildiğinde diğer tüm oturumlar kapatılır.

4.5 İki adımlı doğrulama

- **Doğrulayıcı uygulama (TOTP):** SHA-1, 6 hane, 30 saniyelik periyot, 160 bitlik gizli anahtar; ± 1 zaman adımı kabul edilir; kullanılmış bir zaman adımı (eşzamanlı isteklerde de) tekrar kullanılamaz. Sunucunun kodları doğrulayabilmesi gerektiğinden TOTP gizli anahtarları, sunucu sırrından türetilen bir anahtarla AES-256-GCM kullanılarak şifreli saklanır.
- **Güvenlik anahtarları (WebAuthn):** hesap başına en fazla 20 anahtar; 5 dakika geçerli, tek kullanımlık meydan okumalar.
- **Kurtarma kodu:** 160 bitlik tek bir kod; anahtarlı HMAC-SHA256 olarak saklanır. Kullanıldığında iki adımlı doğrulama kapatılır, olay kaydedilir ve e-posta gönderilir.
- İki adımlı doğrulama ayarlarını açmak veya değiştirmek yeniden kimlik doğrulama gerektirir. 15 dakika içinde 10 hatalı ikinci adım denemesinden sonra yeni denemeler reddedilir.

4.6 Passkey ile giriş

Kullanıcılar KeyZula'ya giriş için passkey ekleyebilir. Kayıt, kullanıcı doğrulamalı ve bulunabilir (discoverable) bir kimlik bilgisi gerektirir. Girişte WebAuthn PRF eklentisi kimlik doğrulayıcıda sabit bir jirdiyle çalıştırılır; PRF çıktısı HKDF ile (`vault/v1/passkey-key`) kullanıcı anahtarını saran bir anahtara dönüştürülür. PRF çıktısı cihazdan çıkmaz; sunucu yalnızca sarılmış kullanıcı anahtarını ve kimlik bilgisinin açık anahtarını saklar. Passkey'in kendisi sahiplik ve kullanıcı doğrulaması gerektirdiğinden passkey ile girişte hesabın iki adımlı doğrulaması ayrıca istenmez; organizasyonun SSO zorunluluğu yine uygulanır.

4.7 Yeni cihaz uyarıları ve güvenlik e-postaları

Her istemci rastgele bir cihaz kimliği tutar; sunucu yalnızca SHA-256 özetini saklar. Daha önce bilinen cihazları olan bir hesaba yeni bir cihazdan giriş yapıldığında (parola, passkey veya SSO ile) kullanıcıya cihaz adı, IP adresi, zaman ve tarayıcı bilgisini içeren bir e-posta gönderilir. Ana parola değişikliği, e-posta adresi değişikliği (eski adrese), iki adımlı doğrulamanın açılması veya kapatılması ve hesap silme için de e-posta gönderilir.

4.8 İstek sınırları

- IP adresi başına genel sınır (dakikada 300 istek) ve kimlik doğrulama uç noktalarında daha sıkı IP sınırları (varsayılan dakikada 10).
- Kaynak IP'den bağımsız olarak hesap başına hatalı ana parola denemesi sınırı (varsayılan 15 dakikada 20).
- Kayıt, e-posta gönderimi, davetler, Gönder erişimi ve servis hesabı kimlik doğrulaması için ayrı sınırlar.

4.9 Ana parola olmadan kilit açma

İstemciler kilitli kasayı PIN, biyometri veya (web kasasında) sayfa yenilemeleri arasında yeniden açabilir. PIN ve yenileme ile kilit açmada kullanıcı anahtarı, yerel bir sır ile rastgele 32 baytlık bir **sunucu payından** HKDF ile türetilen bir anahtarla sarılır (vault/v1/unlock-key). Sunucu payı yalnızca onu oluşturan oturuma verir:

- **PIN:** PIN cihazda Argon2id ile işlenir; sunucu elde edilen doğrulayıcının Argon2id özetini saklar ve 5 hatalı PIN'den sonra payı siler; bundan sonra ana parola gerekir. Bu nedenle yerelde saklanan sarılmış anahtarın çalınmış bir kopyası çevrimdışı kaba kuvvetle açılmaz.
- **Yenileme (web):** pay, ayarlanabilir bir hareketsizlik süresinden sonra (en fazla 12 saat) geçersiz olur ve oturum bitince silinir.
- **Biyometri (mobil):** kullanıcı anahtarı iOS Anahtar Zinciri / Android Keystore destekli güvenli depolamada, kullanıcı doğrulaması zorunlu ve "yalnızca bu cihaz" erişilebilirliğiyle saklanır.

Paylar oturumlarıyla birlikte silinir (çıkış, oturum kapatma, ana parola değişikliği).

4.10 Ana parola değişikliği ve hesap silme

Ana parola değiştirildiğinde yeni bir tuz üretilir ve değişmeyen kullanıcı anahtarı yeni KEK ile yeniden sarılır; kasa kayıtları yeniden şifrelenmez. Hesap silme yeniden kimlik doğrulama gerektirir ve hesabı, oturumlarını, cihazlarını, kimlik bilgilerini ve kişisel kasa verisini siler.

5 Kasa şifrelemesi

5.1 Anahtar hiyerarşisi

ANAHTAR	KORUYAN	ŞİFRELEDİĞİ
Ana anahtar	Ana paroladan türetilir, saklanmaz	— (KEK ve kimlik doğrulama özetinin kaynağı)
Kullanıcı anahtarı	KEK (isteğe bağlı olarak passkey, PIN, cihaz veya kurtarma sarmaları)	Gizli anahtar, kişisel kayıt anahtarları, klasör adları, Gönder anahtarları
X25519 gizli anahtar	Kullanıcı anahtarı	Kullanıcıya mühürlenmiş koleksiyon, acil durum erişimi ve cihaz onayı anahtarlarını açar
Koleksiyon anahtarı	Yetkili her üyenin açık anahtarına mühürlü	Paylaşılan kayıtların anahtarları, koleksiyon adları
Kayıt anahtarı (kayıt başına)	Kullanıcı anahtarı veya koleksiyon anahtarı	Kayıt verisi, dosya eki anahtarları

ANAHTAR	KORUYAN	ŞİFRELEDİĞİ
Dosya eki anahtarı (dosya başına)	Kayıt anahtarı	Dosya içeriği, dosya adı ve türü

5.2 Kayıtlar

Her kaydın kendi rastgele 256 bitlik anahtarı vardır. Kaydın tüm içeriği (tür, ad, kullanıcı adı, parola, adresler, notlar, özel alanlar, favori işareti, TOTP gizli anahtarı, passkey, SSH anahtarı ve parola geçmişi) tek bir şifreli değer olarak saklanır. Bir kayıt kişisel kasa ile bir koleksiyon arasında taşındığında yalnızca kayıt anahtarı yeniden sarılır; içerik yeniden şifrelenmez.

5.3 Ek doğrulanmış veri (AAD)

Her şifreleme bir bağlam dizesini ek doğrulanmış veri olarak bağlar. Farklı bir bağlamla şifre çözme doğrulamadan geçmez; bu, sunucunun şifreli verileri kayıtlar veya alanlar arasında taşımalarını engeller.

DEĞER	AAD
Kullanıcı anahtarı (KEK ile sarılı)	<code>vault/v1/user-key</code>
Gizli anahtar	<code>vault/v1/private-key</code>
Kayıt anahtarı / kayıt verisi	<code>vault/v1/item-key:<id></code> , <code>vault/v1/item:<id></code>
Klasör / koleksiyon adı	<code>vault/v1/folder:<id></code> , <code>vault/v1/collection:<id></code>
Dosya eki anahtarı / üst verisi	<code>vault/v1/attachment-key:<id></code> , <code>vault/v1/attachment-meta:<id></code>
Gönder anahtarı / içeriği	<code>vault/v1/send-key:<id></code> , <code>vault/v1/send:<id></code>
Kullanıcı anahtarının diğer sarmaları	<code>vault/v1/pin-user-key</code> , <code>vault/v1/reload-user-key</code> , <code>vault/v1/passkey-user-key</code> , <code>vault/v1/device-user-key</code>
Doğrulanmış üye anahtarı (sabitleme)	<code>vault/v1/key-pin:<üyelik kimliği></code>

5.4 Şifresiz saklanan üst veriler

Eşitleme için sunucu her kayıta şunları tutar: kimlik, sahip (kullanıcı veya koleksiyon), klasör kimliği, revizyon sayacı, oluşturma, güncelleme ve silme (çöp kutusu) zamanları ve şifreli verinin boyutu. Silinen kayıtlar kullanıcı kalıcı olarak silene kadar çöp kutusunda kalır. Sunucu kayıtların sürüm geçmişini tutmaz; parola geçmişi şifreli kaydın parçasıdır.

6 Paylaşım ve organizasyonlar

6.1 Organizasyonlar ve koleksiyonlar

Organizasyonlar üyeleri departmanlarda toplar ve kayıtları koleksiyonlar üzerinden paylaşır. Her koleksiyonun rastgele bir anahtarı vardır. Erişimi olan her üye için koleksiyon anahtarı o üyenin X25519 açık anahtarına mühürlenerek sunucuda saklanır; üye bunu kendi gizli anahtarıyla açar. Koleksiyon adları koleksiyon anahtarıyla şifrelenir.

Organizasyon adları, departman adları, üye e-posta adresleri, roller ve yetkiler şifresiz saklanır; çünkü sunucu erişim denetimini bunlara göre yapar.

6.2 Üye ekleme ve parmak izi doğrulaması

Üyeler e-postayla davet edilir, doğrulanmış bir e-posta adresiyle daveti kabul eder ve ardından bir sahip veya yönetici tarafından onaylanır. Koleksiyon anahtarlarını yalnızca onaylanmış üyeler alır; yöneticinin istemcisi bunları otomatik olarak mühürlar.

Açık anahtarları sunucu dağıttığından, sunucu ilke olarak bir üye için farklı bir açık anahtar gösterebilir. Bunu fark etmek için onay penceresi üyenin açık anahtar parmak izini gösterir; her üye de kendi parmak izini hesap ayarlarında görebilir. Yöneticiler onaylamadan önce bu ikisini ayrı bir kanaldan karşılaştırır.

Yöneticinin onayladığı anahtar ardından **sabitlenir**: yöneticinin istemcisi bu anahtarı yöneticinin kendi kullanıcı anahtarıyla, üyeliğe bağlı olarak (vault/v1/key-pin:<üyelik kimliği>) şifreler ve sonucu sunucuda saklar; sunucu bir sabitlemeyi fark edilmeden oluşturamaz veya değiştiremez. Bir üyeye koleksiyon anahtarı veya organizasyonun kurtarma anahtarı mühürlenmeden önce yöneticinin istemcisi sunucunun verdiği açık anahtarı sabitlemeyle karşılaştırır. Anahtarlar farklıysa ya da bu yönetici üyeyi doğrulamamışsa hiçbir şey mühürlenmez ve yöneticiye parmak izini (yeniden) karşılaştırması gereken üyeler gösterilir. Her yönetici kendi sabitlemelerini tutar; yöneticinin kendi anahtarı istemcisiince bilindiğinden sabitleme gerektirmez. Hesap açık anahtarları kayıttan sonra değiştirilemez; bu nedenle olağan kullanımda farklı bir anahtar beklenmez.

6.3 Yetkiler

Koleksiyon yetkileri *yönetme*, *düzenleme*, *görüntüleme* ve *görüntüleme*, *parola gizli*'dir. Sahipler ve yöneticiler tüm koleksiyonları yönetebilir. Kimin kayıt okuyabileceğini, oluşturabileceğini, değiştirebileceğini ve silebileceğini sunucu denetler. *Görüntüleme*, *parola gizli* yetkisi bir kullanım denetimidir: üyeler kaydı kullanabilir (örneğin otomatik doldurma), ancak istemciler gizli değerleri göstermez, kopyalamaz ve dışa aktarmaz. Bu üyeler koleksiyon anahtarına sahip olduğundan yetki kriptografik bir sınır değildir; değiştirilmiş bir istemci gizli değerleri gösterebilir. Bu yetkiyle dosya eki indirme istekleri sunucu tarafından reddedilir.

6.4 Erişimin kaldırılması

Bir üye çıkarıldığında veya bir koleksiyona erişimi kaldırıldığında sunucu o üyenin mühürlü koleksiyon anahtarlarını siler. Koleksiyon anahtarları yenilenmez. Bir koleksiyon anahtarının ve şifreli verinin kopyasını saklamış olan çıkarılmış bir üye, çıkarılmadan önce bu anahtarla şifrelenmiş veriyi çözebilir.

6.5 Politikalar

Organizasyonlar üyelerin kasayı dışa aktarmasını kapatabilir. Politikalar istemciler tarafından uygulanır.

7 SSO, güvenilir cihazlar ve yönetici kurtarması

7.1 Tek oturum açma (SSO)

Organizasyonlar bir OpenID Connect kimlik sağlayıcısı bağlayabilir. KeyZula sunucusu yetkilendirme kodu akışını PKCE, state ve nonce ile yürütür; istemci tek kullanımlık bir bileti kendi PKCE doğrulayıcısıyla alır. Kimlik sağlayıcıdan gelen e-posta alan adı, organizasyonun DNS TXT kaydıyla doğruladığı bir alan adıyla eşleşmelidir; doğrulanmamış olarak bildirilen e-posta adresleri reddedilir. Sağlayıcının istemci sırrı, sunucu sırrından türetilen bir anahtarla şifreli saklanır. SAML desteklenmez.

Kullanıcının kimliğini kimlik sağlayıcı doğrular; kasa anahtarları kimlik sağlayıcıya hiç gitmez. Organizasyonlar üyeler için SSO'yu zorunlu kılabilir; sahipler bu zorunluluğun dışındadır.

7.2 Ana parolası olmayan hesaplar

SSO ile katılan kullanıcılar KeyZula'yı ana parola olmadan kullanabilir. Kullanıcı anahtarları ve anahtar çiftleri cihazda üretilir. Kullanıcı anahtarı diğer cihazlarda üç yolla açılır:

- **Güvenilir cihaz.** Rastgele 256 bitlik bir cihaz anahtarı cihazda kalır. Web'de tarayıcı depolamasında, IndexedDB'de tutulan dışa aktarılamayan bir AES-GCM anahtarıyla şifreli saklanır; böylece saklanan değer tek başına anahtarı vermez. Mobilde güvenli depolamada tutulur. Sunucu, bu cihaz anahtarıyla sarılmış kullanıcı anahtarını saklar. Kullanıcılar güvenilir cihazlarını görebilir ve kaldırabilir.
- **Cihaz onayı.** Yeni cihaz geçici bir X25519 anahtar çifti üretir ve açık anahtarını yayımlar. Aynı kullanıcının oturum açmış başka bir cihazı veya bir organizasyon yöneticisi (aşağıya bakın) kullanıcı anahtarını bu anahtara mühürlür. İki taraf da karşılaştırma için bir doğrulama numarası (geçici anahtarın parmak izi) gösterir. İstekler 15 dakika sonra geçersiz olur ve sonuç yalnızca isteği yapan oturuma iletilir.
- **Yönetici kurtarması.** Organizasyonun kendi X25519 anahtar çifti vardır; gizli anahtarı her sahip ve yöneticiye, yalnızca parmak izi doğrulamasında anlatıldığı gibi sabitlenmiş anahtarlara mühürlenir. Üyelerin kullanıcı anahtarları organizasyonun açık anahtarına mühürlenir. Bu nedenle bir yönetici, bir üyenin yeni cihazını onaylayabilir ve bu sırada o üyenin kasa anahtarını çözebilecek duruma gelir.

Yönetici kurtarması kullanıcıya bildirilir ve kullanıcının onayını gerektirir. SSO ile yeni bir hesap oluşturulurken kayıt ekranı organizasyon yöneticilerinin kasayı açabileceğini belirtir ve açık onay ister; sunucu da bu onayı denetler. Mevcut bir hesap bir organizasyonun SSO'su ile giriş yaptığında ve o organizasyon için henüz kurtarma kopyası yoksa, hiçbir şey paylaşılmadan önce aynı bildirim gösterilir: kurtarma kopyası yalnızca kullanıcı kabul ettikten sonra oluşturulup gönderilir ve sunucu onay içermeyen gönderimleri reddeder. Kullanıcı kabul etmezse kopya paylaşılmaz; bu durumda yöneticiler kullanıcının yeni cihazlarını onaylayamaz veya erişimini geri veremez, bildirim de bir sonraki SSO girişinde yeniden gösterilir.

Hassas işlemlerde ana parolası olmayan hesaplar bir anahtar kanıtıyla yeniden doğrulanır: sunucu rastgele bir değeri hesabın açık anahtarına mühürlar ve istemci çözdüğü değlerle yanıt verir (tek kullanımlık, 5 dakika geçerli).

8 Acil durum erişimi

Kullanıcılar güvendikleri kişileri (en fazla 50) acil durum kişisi olarak belirleyebilir. Kişi e-postayla davet edilir, doğrulanmış bir adresle kabul eder ve kasa sahibi tarafından onaylanır. Onay sırasında kasa sahibinin istemcisi, sahibin kullanıcı anahtarını kişinin açık anahtarına mühürlar; onay ekranı ayrı bir kanaldan karşılaştırma için aynı anahtarın parmak izini gösterir ve anahtar yalnızca o anda mühürlenir.

Kişi istediği zaman erişim talep edebilir. Kasa sahibine e-postayla bildirilir; sahip talebi onaylayabilir veya reddedebilir. Sahip bir şey yapmazsa erişim, sahibin seçtiği bekleme süresinden (1, 2, 7, 14 veya 30 gün) sonra açılır; bu süre sunucu tarafından uygulanır. Erişim yalnızca görüntülemadır ve sahibin kişisel kasasındaki kayıtları ve dosya eklerini kapsar; organizasyon koleksiyonlarını kapsamaz. Mühürlü anahtar bir kez teslim edildikten sonra erişimin geri alınması sahibin kullanıcı anahtarını yenilemez.

9 Gönder

Gönder, metin için süreli ve uçtan uca şifreli bir bağlantı oluşturur. İçerik rastgele bir bağlantı anahtarıyla şifrelenir. Bağlantı <https://app.keyzula.com/send/<id>#<anahtar>> biçimindedir; anahtar, tarayıcıların sunucuya göndermediği adres parçasında (#) bulunur. Bağlantı anahtarının sahibin kullanıcı anahtarıyla sarılmış bir kopyası, sahibin bağlantıyı daha sonra yeniden kopyalayabilmesini sağlar.

- Süre: en fazla 31 gün. İsteğe bağlı en fazla görüntüleme sayısı (1–1000), atomik olarak uygulanır.
- İsteğe bağlı parola: istemci, bağlantı anahtarıyla anahtarlanmış bir BLAKE2b doğrulayıcı gönderir; sunucu bunun Argon2id özetini saklar ve hatalı denemeleri sınırlar. Parola sunucuda erişimi denetler; ek bir şifreleme katmanı değildir.
- Kullanılmayan, süresi dolmuş ve var olmayan Gönder bağlantıları aynı yanıtı döndürür.

10 Dosya ekleri ve dosyalar

Her dosya ekinin kendi rastgele anahtarı vardır ve bu anahtar kayıt anahtarıyla sarılır. Dosya adı ve MIME türü şifrelenir. Dosya içerikleri parçalı **KZA1** biçimini kullanır:

```
dosya = "KZA1" || parça_0 || ... || parça_n
parça = nonce (24 bayt) || XChaCha20-Poly1305(düz metin ≤ 1 MiB), 16 baytlık etiket dahil
AAD   = "vault/v1/attachment:<id>" || 0x00 || u32be(sıra) || u8(sonParça)
```

Parça sırasının ve "son parça" işaretinin bağlanması; parçaların yer değiştirmesini, dosyanın kesilmesini ve dosyalar arasında parça karıştırılmasını engeller. Dosyalar yüklenmeden önce şifrelenir ve sunucunun diskinde rastgele kimliklerle saklanır. Sunucu, kota denetimi için yüklenen boyutun bildirilen şifreli boyutla eşleştiğini kontrol eder; şifreli boyut, dolayısıyla dosyanın yaklaşık boyutu sunucu tarafından görülebilir. Varsayılan sınırlar dosya başına 25 MB ve hesap başına 100 MB'tır.

11 Servis hesapları ve komut satırı aracı

11.1 Servis hesapları

Servis hesapları sunuculara, CI işlerine ve otomatik ajanlara seçilen koleksiyonlara salt okunur erişim verir. Erişim belirteci yöneticinin tarayıcısında üretilir ve yalnızca bir kez gösterilir:

- 256 bitlik belirteç sırrı HKDF ile bir **auth anahtarına** ve bir **wrap anahtarına** ayrılır. İstemciler yalnızca auth anahtarını gönderir (`kzsa_auth_...`); sunucu bunun SHA-256 özetini saklar ve ham belirteçleri reddeder.
- Her belirtecın kendi X25519 anahtar çifti vardır. Gizli anahtarı wrap anahtarıyla şifrelenir; koleksiyon anahtarları belirtecın açık anahtarına mühürlenir. Sunucu belirteç sırrını, wrap anahtarını, gizli anahtarı ve koleksiyon anahtarlarını hiçbir zaman görmez.
- Belirteçlere son kullanma tarihi verilebilir ve her biri ayrı ayrı iptal edilebilir; iptal, doğrulayıcıyı, şifreli gizli anahtarı ve mühürlü koleksiyon anahtarlarını siler. Her okuma organizasyonun denetim kaydına yazılır.

11.2 Komut satırı aracı

Komut satırı aracı (`keyzula`) sunucu adresini, e-postayı, oturum belirtecini ve şifreli anahtar materyalini yalnızca kullanıcının okuyabildiği bir yapılandırma dosyasında (izin 0600) saklar. Ana parola ve çözülmüş anahtarlar yalnızca yerel bir ajan sürecinin belleğinde tutulur. Servis belirteçleri bir ortam değişkeninden okunur ve diske yazılmaz.

Yerleşik SSH agent, kasadaki SSH anahtarlarını yalnızca kullanıcının erişebildiği bir soket üzerinden sunar. Gizli anahtarlar bellekte kalır; isteğe bağlı olarak her imza için onay ve hareketsizlikte kilitleme kullanılabilir; ajan protokolü üzerinden anahtar ekleme veya silme istekleri reddedilir.

12 Tarayıcı eklentisi

- **Anahtarların saklanması.** Çözölmüş anahtarlar arka plan hizmet çalışığında ve tarayıcının bellekte tutulan, tarayıcı kapanınca silinen oturum depolamasında bulunur. Eklentinin yerel depolamasında oturum belirteci, şifreli hesap anahtarları, ayarlar ve kasanın şifreli bir kopyası bulunur.
- **Otomatik kilit.** Kullanıcılar belirli bir hareketsizlik süresinden sonra veya işletim sistemi kilitletiğinde kilitlemeyi seçebilir; varsayılan olarak kasa tarayıcı kapanınca kilitletlenir.
- **Otomatik doldurma eşleşmesi.** Varsayılan olarak bir kayıt, aynı kayıt edilebilir alan adındaki (eTLD+1) sayfalarla eşleşir; Public Suffix List özel son ekler dahil kullanılır, yani `a.github.io` ile `b.github.io` eşleşmez. Adres başına kurallarla tam ana makine, önek, tam adres veya "asla" seçilebilir. Kayıtlı tüm adresleri `https` olan kayıtlar düz `http` sayfalarına doldurulmaz.
- **Kullanıcı eylemi gerekir.** Eklenti sayfa yüklenirken hiçbir zaman doldurmaz. Doldurma için açılır pencerede bir tıklama, klavye kısayolu veya satır içi menüde bir tıklama gerekir; satır içi menü kapalı bir shadow DOM içinde çalışır ve yalnızca gerçek kullanıcı olaylarını kabul eder. Her çerçeve doldurmadan önce kendi adresini kayıtlı yeniden karşılaştırır; sayfa kaynağı sayfa mesajlarından değil tarayıcıdan alınır.
- **Gömülü çerçeveler.** Satır içi öneriler ve doldurma yalnızca üst düzey sayfada ve üst düzey sayfayla aynı sitedeki (kayıt edilebilir alan adı) çerçevelerde sunulur; örneğin `www.ornek.com` içindeki bir `login.ornek.com` çerçevesi. Çerçevenin ve sayfanın adresi tarayıcıdan alınır. Farklı bir siteden gömülü çerçevelerde satır içi menü gösterilmez ve doldurma yapılmaz; açılır pencereden böyle bir çerçeveye doldurma istenirse açıklamayla reddedilir.
- **Passkey'ler.** Eklenti passkey sağlayıcısı olarak çalışabilir. Bağlı taraf kimliğini (RP ID) isteği yapan kaynağa göre doğrular (yalnızca HTTPS; RP ID ana makine veya onun üst alan adı olmalı ve genel bir son ek olamaz) ve kendi katmanında gerçek bir tıklama ister. Passkey istekleri yalnızca üst düzey sayfada karşılanır; gömülü çerçevelerde tarayıcının kendi passkey akışı kullanılır.
- **Pano.** Kopyalanan gizli değerler ayarlanabilir bir sürenin (varsayılan 60 saniye) sonunda temizlenir.
- **Passkey ile giriş.** Eklenti, web kasasını adres parçasında (#) geçici bir açık anahtarla açar; web kasası kullanıcı anahtarını (veya PRF çıktısını) bu anahtara mühürler ve yalnızca KeyZula kaynağıyla sınırlı bir kanal üzerinden geri gönderir. İstekler tek kullanımlıktır ve süresi dolar.

13 Mobil uygulamalar

- **Anahtarların saklanması.** Oturum belirteci ve kilit açma verileri, iOS Anahtar Zinciri / Android Keystore destekli güvenli depolamada "cihaz kilidi açıkken, yalnızca bu cihaz" erişilebilirliğiyle saklanır. Biyometrik kilit açma her erişimde kullanıcı doğrulaması ister. Android yedeklemesi kapalıdır.
- **Otomatik kilit.** Uygulama arka planda ayarlanabilir bir süre (varsayılan 5 dakika) kaldıktan sonra kilitletlenir ve uygulama değiştiricide içeriğini gizler.
- **iOS Otomatik Doldurma.** Otomatik Doldurma eklentisi, Anahtar Zinciri'nde kullanıcı varlığı korumasıyla tutulan bir cihaz anahtarına şifrelenmiş bir önbellegi okur; her doldurma Face ID,

Touch ID veya cihaz parolası gerektirir. *Görüntüleme, parola gizli* yetkisindeki kayıtlar önbellege alınmaz.

- **Otomatik doldurma eşleşmesi.** iOS ve Android'de web siteleri, tarayıcı eklentisinde olduğu gibi Public Suffix List'e göre kayıt edilebilir alan adıyla eşleştirilir. Uygulama her kaydın eşleşme anahtarlarını hesaplar (kayıt edilebilir alan adı; ana makine, önek ve tam adres kurallarında ana makine adı, çünkü otomatik doldurma hizmetlerine yalnızca sitenin ana makine adı ulaşır); otomatik doldurma hizmeti de doldurulan site için aynı anahtarları uygulamayla birlikte gelen liste kopyasından türetir. Android'de doldurma isteğinde bildirilen web alan adı yalnızca isteği yapan uygulama, imza sertifikası yayımlanmış tarayıcı listesiyle eşleşen bilinen bir tarayıcıysa kullanılır; diğer uygulamalar paket adlarıyla eşleştirilir.
- **Android Otomatik Doldurma.** Öneriler yalnızca ad ve kullanıcı adını gösterir. Parolalar ve kodlar, her kullanımda doğrulama isteyen bir Keystore anahtarıyla yalnızca biyometrik veya cihaz kimlik bilgisi doğrulamasından sonra çözülür.
- **Pano.** iOS'ta kopyalanan değerler yalnızca yereldir (Evrensel Pano ile paylaşılmaz) ve süresi dolar; Android'de hassas olarak işaretlenir ve süre sonunda temizlenir.

14 Web kasası

- Çözülmüş anahtarlar yalnızca bellekte tutulur ve kasa kilitletiğinde veya çıkış yapıldığında silinir. Tarayıcı depolamasında oturum belirteci, şifreli hesap anahtarları, etkinse yukarıda anlatılan PIN veya yenileme ile sarılmış kullanıcı anahtarı ve güvenilir SSO cihazlarında şifreli cihaz anahtarı bulunur.
- Kasa hareketsizlikten sonra kilitletlenir (varsayılan 15 dakika). Kopyalanan gizli değerler varsayılan olarak 60 saniye sonra panodan temizlenir.
- Web kasası katı bir içerik güvenliği politikasıyla (betikler yalnızca kendi kaynağından; satır içi betik yok; çerçeveye alınamaz) sunulur ve analitik veya reklam betiği içermez. Anahtar türetme bir Web Worker'da çalışır.
- Sızıntı kontrolleri Have I Been Pwned aralık API'sini k-anonimlikle kullanır: parolanın SHA-1 özetinin yalnızca ilk beş karakteri, yanıt dolgusuyla gönderilir. Kontrolleri kullanıcı başlatır.

15 Sunucunun görebildikleri ve göremedikleri

VERİ	SUNUCUNUN ERİŞİMİ
Ana parola, ana anahtar, KEK	Hiç ulaşmaz
Kullanıcı anahtarı, gizli anahtar, koleksiyon anahtarları, kayıt anahtarları	Yalnızca şifreli

VERİ	SUNUCUNUN ERİŞİMİ
Kayıt içeriği: adlar, kullanıcı adları, parolalar, adresler, notlar, alanlar, TOTP gizli anahtarları, passkey'ler, SSH anahtarları, kayıt türü, favoriler	Yalnızca şifreli
Klasör ve koleksiyon adları	Yalnızca şifreli
Dosya eki içerikleri, dosya adları ve türleri	Yalnızca şifreli
Gönder içerikleri ve bağlantı anahtarları	Yalnızca şifreli (bağlantı anahtarı hiç gönderilmez)
Passkey PRF çıktıları, güvenilir cihaz anahtarları, servis belirteci sırları	Hiç ulaşmaz
Yöneticilerin sabitlediği doğrulanmış üye anahtarları	Yalnızca şifreli (yöneticinin kullanıcı anahtarıyla)
Kimlik doğrulama özeti, PIN doğrulayıcısı	Argon2id özeti olarak saklanır
E-posta adresi, ad, hesap ayarları	Görülebilir
Kayıt kimlikleri, sayılar, zamanlar, klasör ataması, şifreli veri boyutları	Görülebilir
Organizasyon ve departman adları, üyeler, roller, yetkiler	Görülebilir
Oturumlar ve cihazlar (cihaz adı, IP adresi, tarayıcı bilgisi), erişim ve denetim olayları	Görülebilir
KeyZula hesabının kendi iki adımlı doğrulaması için TOTP gizli anahtarı	Sunucu anahtarıyla şifreli (kodları doğrulamak için gerekli)
Site simgeleri açıkken web sitesi ana makine adları	Simge isteklerinde görülebilir (aşağıya bakın)

Site simgeleri üçüncü taraf bir simge hizmetinden değil, KeyZula sunucusu tarafından doğrudan web sitesinden alınır. İstemciler simgeleri ana makine adıyla istediğinden sunucu hangi ana makine adlarının istendiğini görebilir; simge uç noktası istekleri günlüğe yazmaz. Simgeler ayarlardan kapatılabilir.

16 İletim ve altyapı

- **Barındırma.** KeyZula'nın sunucuları Türkiye'dedir ve Netlen İnternet Hizmetleri Ltd. Şti. tarafından işletilir.

- **TLS.** Tüm trafik otomatik yönetilen sertifikalarla HTTPS üzerinden taşınır (TLS 1.2 veya üstü; HTTP/3 desteklenir). HTTP Strict Transport Security, alt alan adları dahil bir yıllık süreyle etkindir.
- **Başlıklar.** Web kasası ve API bir içerik güvenliği politikasıyla (`default-src 'self'` , `script-src 'self' 'wasm-unsafe-eval'` , `frame-ancestors 'none'` , `object-src 'none'` , `base-uri 'none'` , `form-action 'self'`) ve kısıtlayıcı bir Permissions-Policy ile sunulur. API taşıyıcı belirteç kullanır ve kimlik bilgili kaynaklar arası isteklere izin vermez.
- **Yalıtım.** Uygulama, veritabanı ve ters vekil sunucu ayrı kapsayıcılarda çalışır; veritabanı ağa açık değildir.
- **Sunucu sırrı.** Tek bir sunucu sırrı, sunucu tarafı işlevlerde kullanılan anahtarların köküdür (TOTP gizli anahtarlarının ve SSO istemci sırlarının şifrelenmesi, imzalı e-posta bağlantıları, bilinmeyen adresler için ön giriş parametreleri). Sunucunun çözemediği kasa verisi için hiçbir zaman kullanılmaz.
- **Yedekler.** Veritabanı her gün yedeklenir. Yedekler hem sunucuda hem sunucu dışındaki kopyalarda 14 gün tutulur ve ardından otomatik olarak silinir. Sunucu dışındaki kopyalar gönderilmeden önce şifrelenir (AES-256, GnuPG); hizmetten silinen dosya ekleri bu kopyalardan da en geç 14 gün içinde çıkarılır. Yedeklerde kasa verisi yalnızca şifreli hâliyle bulunur.
- **İstek güvenliği.** İstek gövdesi boyutları sınırlıdır, NUL karakter içeren istekler reddedilir ve veritabanı hataları istemcilere döndürülmez.

17 Erişim kayıtları ve denetim olayları

KeyZula güvenlik olaylarını (girişler, başarısız girişler, parola ve e-posta değişiklikleri, iki adımlı doğrulama değişiklikleri, passkey değişiklikleri, cihaz güveni ve onayları, organizasyon, üye, koleksiyon ve politika değişiklikleri, servis hesabı etkinliği) ve kayıt erişim olaylarını (görüntüleme, parolanın gösterilmesi, kopyalama, otomatik doldurma, passkey kullanımı, SSH anahtarı kullanımı, dosya eki indirme, komut satırı veya servis hesabıyla okuma) kaydeder.

- İstemciler erişim olaylarını yalnızca kayıt kimliği ve işlem türüyle bildirir; kayıt adı veya içeriği hiçbir zaman gönderilmez. Sunucu IP adresini, istemci türünü ve cihaz adını ekler ve kullanıcının kayda erişimi olduğunu denetler.
- Erişim olayları 365 gün saklanır.
- Kişisel kasadaki kayıtlara ait olayları yalnızca kasanın sahibi görür; organizasyon yöneticileri bunları hiçbir zaman göremez. Paylaşılan kayıtlara ait olayları organizasyonun sahipleri ve yöneticileri görür; diğer üyeler yalnızca kendi olaylarını görür.

18 Tasarım tercihleri

Aşağıdaki ödünleşimler KeyZula'nın tasarımından kaynaklanır; KeyZula'nın nasıl kullanılacağına karar verirken dikkate alınabilmeleri için burada belirtilmiştir.

- **Kapalı kaynak.** Yalnızca şifreleme kütüphanesi açık kaynaktır. Sunucu, web kasası, eklentiler ve uygulamaların kaynak kodu kapalıdır; bu belge bunların davranışını anlatır.
- **Web kodunun teslimi.** Her web uygulamasında olduğu gibi web kasasının kodu her yüklemde sunucudan gelir. Ele geçirilmiş bir sunucu web kullanıcılarına değiştirilmiş kod sunabilir. Uygulama mağazalarından kurulan uygulamalar ve eklentiler kodlarını KeyZula sunucularından yüklemeyiz.
- **Üst veriler.** Yukarıda listelenen üst veriler (hesap bilgileri, kayıt sayıları ve zamanları, organizasyon yapısı, IP adresleri, erişim olayları) sunucu tarafından görülebilir.
- **Erişim kaldırılınca anahtar yenileme.** Bir üyenin çıkarılması, bir servis hesabı belirtecinin iptali veya acil durum erişiminin sonlandırılması sunucudaki anahtar kopyalarını siler, ancak koleksiyon anahtarlarını veya kullanıcı anahtarlarını yenilemez.
- **İstemcide uygulanan denetimler.** *Görüntüleme, parola gizli yetkisi* ve organizasyon politikaları kriptografik olarak değil, KeyZula istemcileri tarafından uygulanır.
- **Parmak izi karşılaştırması.** İstemciler yöneticinin onayladığı anahtarı sabitler ve buna göre davranır; onay sırasında parmak izinin kişiyle gerçekten karşılaştırılıp karşılaştırılmadığı yöneticiye bağlıdır.
- **Yönetici kurtarması.** SSO ve hesap kurtarma kullanan organizasyonlarda yöneticiler, tasarım gereği üyelerin kasa anahtarlarına erişebilir; bu kullanıcılara bildirilir ve kurtarma kopyası yalnızca kullanıcı kabul ettikten sonra paylaşılır.
- **Ana parola.** KeyZula unutulmuş bir ana parolayı sıfırlayamaz. Başka bir kilit açma yöntemi olmayan hesaplar kasalarına erişimi kaybeder.

19 Güvenlik bildirimi

Güvenlik bildirimlerini memnuniyetle karşılıyoruz. Lütfen **info@keyzula.com** adresine konu satırına **"Güvenlik"** yazarak sorunu, nasıl tekrarlanabileceğini ve olası etkisini anlatan bir e-posta gönderin. Ayrıntıları yayımlamadan önce düzeltmemiz için bize makul bir süre tanıyın, testlerinizi kendi hesabınızla sınırlayın ve başka kullanıcıların verilerine erişmeyin, hizmeti aksatmayın veya sosyal mühendisliğe başvurmayın. İletişim bilgileri <https://keyzula.com/.well-known/security.txt> adresinde de yayımlanır.

Açık kaynak kütüphaneye ilgili bildirimler de aynı adrese gönderilebilir; depodaki [SECURITY.md](#) dosyasına bakın.