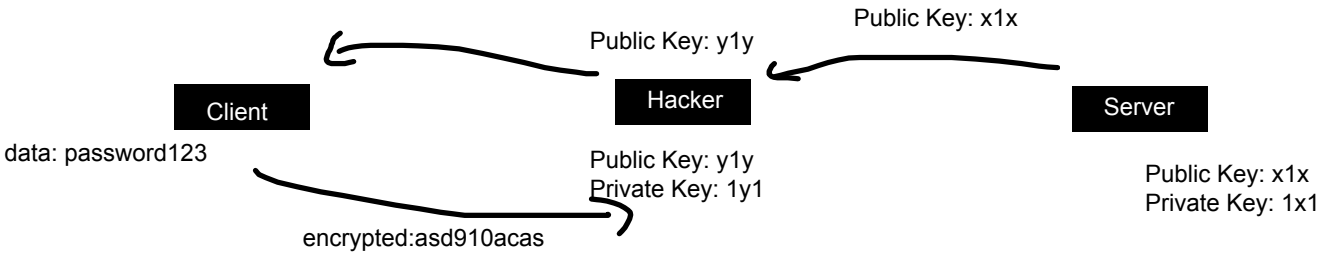
SERTİFİKA OTORİTESİ

Herkese Merhaba bu yazımda sizlere Sertifaka otoritelerini veya herkes tarafından bilenen SSL/TLS nasıl çalıştığını ifade etmeye çalışacağım.ben bu yazımda cümlelerimi Sertifaka otoriteleri olarak kuracağımıda ayrıca bildirmek isterim. ayrıca şunu da beyan etmeyelim ki, bu yazıyı okumadan önce asimetrik ve https handshake yapısıyla ilgili bilgi birikimi olmasında yarar var. Bunlarıda web sitemde bulabilirsiniz.

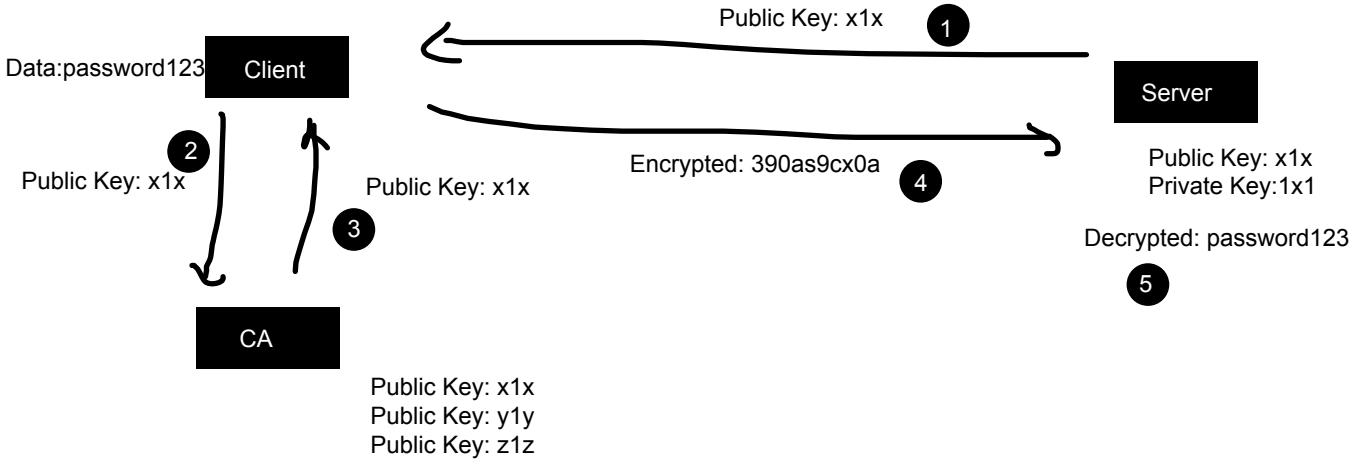
Sertifika Otoriteleri Nedir:

Bir Web sunucusuna güvenli bir şekilde iletişime geçmek istediğimizde, o web sunucusunun herkese açık olarak beyan etmiş olduğu anahtarı üzerinden sunucuya secret key yollama işlemi gerçekleştiririz ve sunucuda kendi gizli anahtarı ile bu açık anahtarı çözümler ve Güvenli bağlantı gerçekleşir. baktığımız zamana pek bir sorun yok gibi gözüksede, ağda bulunan kötü niyetli bir kişi size yapacağı bir MITM atak vektörü ile kendi public key anahtarıyla, sunucunun public key anahtarını değiştirebilir. Bu durumda Sunucuya göndermek istediğiniz gizli veriler aslında saldırgına gidecektir. bu cümlelerime daha vakıf olabilmek açısından aşağıdaki görsele bakabilirsiniz.



işte buradaki sorunlar üzerine Sertifaka Otoriteleri dediğimiz bir topluluk doğdu, bu sertifaka otoriteleri güvenli olan Public key anahtarlarını beyan eden bir topluluk diyebiliriz. cümlemi daha anlaşılır hale getirmem gerekirse, karşıda ki kişinin vermiş olduğu Public keyi eğer bu sertifaka otoriteleri üyelerinden herhangi bir tanesi imzalama görevi görmemişse, bu public key güvenilmez kabul ediliyor. Sertifakaa Otoriteleri çalışma prensibine daha vakıf olabilmek açısından aşağıdaki başlığa bakalım.

Sertifaka Otoriteleri nasıl çalışır:



yukarıdaki görseli maddeler halinde özetlemek daha açıklayıcı olacaktır.

1.Server, kendisinin public key'ini Client'a veriyor.

2.Client, kendisine verilen public key anahtarını Sertifaka Otoritelerine soruyor.

3.Sertifaka Otoriteleri, Public key anahtarının kendisi üyelerinden birisi tarafından imzalandığını ve güvenilir olduğunu client'a bildiriyor

4.Client, Public Key anahtarını kullanarak servera gizli bilgisini yolluyor

5.Server, sahip olduğu Private key anahtarı ile public key anahtarını çözümlüyor.

çok kısa ve öz şekilde Sertifaka Otoriteleri veya SSL/TLS çalışma prensibi bu diyebirim, mülakatlarda çıkabilecek sorulardan birisi olmakla birlikte,bilinmesi gereken konulardan olduğunu söyleme gerekli, ayrıca aşağıda ise sizlere ek bilgi olarak en çok public key anahtarı imzalatılan sertifaka otoriteleri üyelerini verdim.

Sıra	**Sağlayıcı**	**Kullanım**	**Pazar payı**
1	IdenTrust	20.6%	40.0%
2	Comodo	17.9%	34.8%
3	DigiCert	6.3%	12.2%
4	GoDaddy	3.7%	7.2%
5	GlobalSign	1.8%	3.5%

tabi ki de birçoklarımız aklına, bende ilgili domain adresine yönelik sertifaka otoritelerinden, public key imzalatırım." düşüncesi gelecektir fakat sertifaka otoriteleri imzalanan domain adresine karşıdaki kişiyi teyit etme yöntemleri var, yani bu dediğimzde havada kalıyor. o yöntemlerden bahsetmeme gerek yok. şimdilik bu kadar yeter.

e-mail

berathanakcakaya@gmail.com

linkedin

https://www.linkedin.com/in/berathan-akcakaya/