HTTPS - HyperText Transfer Protocol Secure, je protokol, který umožnuje zabezpečenou komunikaci v počítačévé síti, tak, že ji šifruje. Využíván především pro komunikaci webového prohlížeče s webovým serverem. Zajištuje autorizaci, důvěrnost přenášených dat a jejich integritu. Vyvinut v roce 1994. V dnešní době na většíně webů. Pro použití HTTTPS je potřeba certifikát – nejčastěji SSL/TLS. Při vstupu na web, ketrý běží na HTTP a ne na HTTPS, vyskočí varovné okýnko, upozornujicí na nezabezpečenost webu a případné opuštění ho. Halvními klady HTTPS je důvěrnost dat, jen malý pokels výkonu. A zápory, u straěích PC nemusí jet rychle, je potřeba obnovovat certifkát, složitější konfigurace. HTTPS je vytvořen hlavně pro: Eshopy, komunity, sociální sítě. Pro vytvoření HTTPS webu je potřeba pár věcí. 1. Mít registovanou doménu. 2. Mít zařízený webhosting. 3. Platný certifikáti u společnosti, která reálně ověří zabezpečenost, všechny tyto věci na rok vyjedou cca na 750kc. HTTPS může být napadeno tak jako třeba telefoní hovor, jendoduše tak, že místo aby HTTPS soubor dostal jen server dostane ho 3 strana, když má na to strávný HW a SW. Ale protože jsou data zašifrována tak dostane jen věci, ze kterých nedokáže zjistit co znamenají, ale i tak je to probém. Aby jsme tomu zamezili je potřeba speciální typ boxu, ketrý nelze otevřít veřejným klíčem, ale pouze privátním. Který má pouze server a nikdo jiný. A to tak, že server odešle tento box s veřejným klíčem, ale privátní si ponechá. Do tohoto boxu poté date svá data a přidáte i veřejný klíč a celý box zavře veřejný serverový klíč. Poté co box doputuje k serveru, tak jediný kdo ho může otevřít je právě on se svým privátním klíčem. HTTPS protokol je v dnešní době už tedy nutný a potřebný protokol. Bez něj už by byli asi naše data odcizeny a kdoví co ještě.

HTTPS