Software

ssh Secure Shell

Secure Shell oder SSH bezeichnet ein kryptographisches Netzwerkprotokoll für den sicheren Betrieb von Netzwerkdiensten über ungesicherte Netzwerke.[1] Häufig wird es verwendet, um lokal eine entfernte Kommandozeile verfügbar zu machen, d. h., auf einer lokalen Konsole werden die Ausgaben der entfernten Konsole ausgegeben, und die lokalen Tastatureingaben werden an den entfernten Rechner gesendet. Genutzt werden kann dies z. B. zur Fernwartung eines in einem entfernten Rechenzentrum stehenden Servers. Die neuere Protokoll-Version SSH-2 bietet weitere Funktionen wie Datenübertragung per SFTP.

Dabei dient SSH als Ersatz für andere, unsichere Methoden wie Telnet. Bei diesen werden alle Informationen, auch sensible wie etwa Passwörter, im Klartext übertragen. Dies macht sie anfällig für Man-in-the-Middle-Angriffe sowie einen Vertraulichkeitsverlust durch Packet Analyzer, die die Datenpakete mitschneiden.[2] Die Verschlüsselungstechnik, die durch SSH genutzt wird, hat deshalb den Zweck, die Vertraulichkeit, Integrität und Authentizität von Daten, die über ein unsicheres Netzwerk (wie z. B. das Internet) gesendet werden, sicherzustellen.

SSH verwendet die Client–Server-Architektur. Eine SSH-Client-Anwendung verbindet sich also mit einem SSH-Server. Die Protokollspezifikation wird in zwei Versionen unterschieden, bezeichnet als SSH-1 und SSH-2. SSH war zuerst für unixoide Betriebssysteme verfügbar, später auch für Microsoft Windows.

Die IANA hat dem Protokoll den TCP-Port 22, UDP-Port 22 und SCTP-Port 22 zugeordnet.

FTPS

- FTPS https://en.wikipedia.org/wiki/FTPS

FTPS (also known as FTP-SSL and FTP Secure) is an extension to the commonly used File Transfer Protocol (FTP) that adds support for the Transport Layer Security (TLS) and, formerly, the Secure Sockets Layer (SSL, which is now prohibited by RFC7568) cryptographic protocols.

FTPS should not be confused with the SSH File Transfer Protocol (SFTP), a secure file transfer subsystem for the Secure Shell (SSH) protocol with which it is not compatible. It is also different from FTP over SSH, which is the practice of tunneling FTP through an SSH connection.

Authentifizierung Terminal ja, phpStorm nein

- Lösung https://duckduckgo.com/?q=userauth_pubkey%3A+signature+algorithm+ssh-rsa+not+in+PubkeyAcceptedAlgorithms&t=canonical&ia=web