SSH

Das SSH-Protokoll (Secure Shell) unterstützt einen verschlüsselten Zugriff auf Dateien, sowie einen sicheren Linux-Shellzugang zum persönlichen Bereich (im AI-Labor das H-Laufwerk), über eine „normale“ Internetverbindung. Beliebte freie Programme, die das SSH-Protokoll verwenden, sind: filezilla (http://filezilla.de) oder WinSCP (http://winscp.net) für Filetransfer und putty (http://www.putty.org) für einen Shell-Zugang.

Auf dieser Seite stehen die Zugangsinformationen, Fingerprints (zur Identifizierung des Servers) für den Zugriff auf den persönlichen Bereich, sowie eine kurze Beschreibung zum Nutzen eines SSH-Schlüsselpaares und eine Anleitung zur Erzeugung eines SSH - Schlüsselpaares mit Putty unter Windows.

Zugangsinformationen:

Server: `ssh.informatik.haw-hamburg.de`
Port: 22
Übertragungsprotokoll: SFTP
User: <HAW-Account>
Passwort: <HAW-Account>

Fingerprints

Der Server authentifiziert sich durch die Präsentation eines öffentlichen Schlüssels. Bei der ersten Kontaktaufnahme mit der Maschine wird der Anwender üblicherweise gebeten, diesen Schlüssel anhand eines Fingerprints zu identifizieren. Unten sind die Fingerprints für diese Maschine angegeben:

MD5 Fingerprints

RSA (4096 Bit)	94:8d:d4:9b:cf:b1:12:5b:6a:b8:17:d5:86:e7:44:7f
ED-25519 (256 Bit)	1a:5d:b7:77:a5:2a:b9:d9:e8:c7:ca:cc:a0:32:e9:e9

SHA256 Fingerprints

RSA (4096 Bit)	7DpHXck6pNVM1q97e8y979jiS4koXO2U0eKnSWAlzO0
ED-25519 (256 Bit)	GLke1NfyrnDrUxypKpyROyGQEUZD3SLiWkumdzZRFzI

SFTP

Um Dateien sicher zu Übertragen empfiehlt sich das SFTP Protokoll, das auf SSH aufsetzt. Die Zugangsinformationen sind die gleichen wie für SSH, nur dass der Dienst über die Maschine

`sftp.informatik.haw-hamburg.de` geleistet wird. Initiales Verzeichnis auf dem Server ist der persönliche Bereich.

SSH - Schlüsselpaar

Oft ist es mühsam immer wieder sein Passwort eingeben zu müssen. Abhilfe schafft hier die Nutzung eines SSH-Schlüsselpaares, bestehend aus einem öffentlichen und einem privaten Schlüssel. Dieses Schlüsselpaar sollte mit einem Passwort geschützt werden, für den Fall, dass ungewollt ein Dritter an diesen Schlüssel kommt. Der öffentliche Schlüssel muss auf dem jeweiligen SSH-Server hinterlegt sein. Der private Schlüssel kann dann in einen Agenten geladen werden, und schon kann man sich ohne Passwort (jedoch mit einem Passwort geschützten Schlüsselpaar) auf dem SSH-Server anmelden.

Für den Zugang zum persönlichen Bereich an der HAW haben wir eine Anleitung zur Erzeugung eines SSH - Schlüsselpaares mit Putty unter Windows geschrieben.