PuTTYgen

ทฤษฎีที่เกี่ยวข้อง

• Asymmetric Cryptography (Private/Public Key)



• SSH Authentication



Client Provides User's Identity to the Server

Private key

1. เปิดโปรแกรม PuTTYGen

puttygen.exe

2. สร้างรหัสแบบ EdDSA algorithm

PuTTY Key Generator		? ×
File Key Conversions Help		
Key No key.		
Actions Generate a public/private key pair Load an existing private key file Save the generated key	Save public key	2 Generate Load Save private key
Parameters Type of key to generate: ORSA ODSA OECDSA Curve to use for generating this key:	1	○ SSH-1 (RSA) Ed25519 (255 bits) ~

💕 PuTTY Key Generator			? ×		
File Key Conversions Help					
Key Please generate some randomness by mov	ing the mouse over the	blank area.			
	Move M	ouse			
Actions					
Generate a public/private key pair			Generate		
Load an existing private key file			Load		
Save the generated key		Save public key	Save private key		
Parameters					
Type of key to generate:	ECDSA	EdDSA	O SSH-1 (RSA)		
Curve to use for generating this key:		E	Ed25519 (255 bits) ~		

PuTTY Key Generat	or			?	\times
File Key Conversions	Help				
Key					
Public key for pasting i	nto OpenSSH authorized	l_keys file:			
ssh-ed25519 AAAAC3 20250622	NzaC1IZDI1NTE5AAAAI	IJB+r8X0mmaOy	9eG3i5Ubv5lq724Xjw/37vzł	Pc5AGXzN eddsa-key-	^
					\sim
Key fingerprint:	ssh-ed25519 255 SHA256:EDxBvyhYTsVRKgjgudTizBXK9RyG5hqFK8zD7PogAZ8				
Key comment:	eddsa-key-20250622				
Key passphrase:					
Confirm passphrase:					
Actions					
Generate a public/priv	ate key pair			Generate	
Load an existing privat	e key file			Load	
Save the generated ke	эy	[Save public key	3 Save private key	
Parameters					
Type of key to generate RSA	te: ODSA	OECDSA	EdDSA	◯ SSH-1 (RSA)	
Curve to use for genera	ating this key:		E	d25519 (255 bits)	\sim





• ขั้นตอนที่ 4 ไม่ใส่ Passphrase (รหัสผ่านสำหรับใช้งาน Private Key)

```
Using username "somchai"
Authenticating with public key "eddsa-key-20240626"
```

• ในกรณีที่ใส่ Passphrase เมื่อ login

```
Using username "somchai"
Authenticating with public key "eddsa-key-20240626"
Passphrase for key "eddsa-key-20240626": [hidden]
```

Public Key

1. บันทึก public key เพื่อใช้กับ OpenSSH บนเซิร์ฟเวอร์

New text file > somchai.pub > Paste "ssh-ed25519 AAAAC3 ..."

😴 PuTTY Key Generato	r				? ×
File Key Conversions	Help				
Key					
Public key for pasting in	to OpenSSH authorized	_keys file:			
ssh-ed25519 AAAAC3N	vzaC1IZDI1NTE5AAAAI	JB+r8X0mmaOy	9eG3i5Ubv5lq724Xjw/37v	/zPc5AGXzN eddsa-key-	^
20230022		Co	DV.		
		00	РУ		~
Key fingerprint	ssh-ed25519 255 SHA25	6:EDxBvvhYTsV	/RKajaudTizBXK9RvG5h	aFK8zD7PogAZ8	
Keymigerprint					
Key comment.	eddsa-key-20250622				
Key passphrase:					
Confirm passphrase:					
Actions					
Generate a public/priva	te key pair			Genera	te
Load an existing private	key file			Load	
Save the generated key	/		Save public key	Save privat	e key
Parameters					
Type of key to generate RSA	e: ODSA	OECDSA	EdDSA	⊖SSH-1 (F	RSA)
Curve to use for genera	ting this key:			Ed25519 (255 bits)	\sim

- 2. สร้างไฟล์ authorized_keys เพื่อเก็บ public key บนเซิร์ฟเวอร์
 - login เข้าเซิร์ฟเวอร์ด้วย username/password
 - สร้างไดเรกทอรี (dot นำหน้า)

mkdir .ssh

สร้างไฟล์

nano .ssh/authorized_keys

- วาง public key จากไฟล์ somchai.pub
- บันทึกไฟล์
- 3. หากต้องการเพิ่ม public key ของคนอื่น ให้เพิ่มต่อในบรรทัดถัดไป