

Public key infrastructure – PKI

- ▶ How do we know a key belongs to Bob?
- ▶ One solution: PKI
 - ▶ Trust certification/root authority (VeriSign, etc.)
 - ▶ Everyone must know the public key of root authority
 - ▶ Check your browser, you can find many
 - ▶ Root authority can sign certificates
 - ▶ Certificates identify others, including other authorities

DocuSign is a SaaS product that businesses use to send electronic signatures
<https://en.wikipedia.org/wiki/DocuSign>