1 Public Key Infrastructure \textit{PKI}

X.509, Hierarchical Tree Structure

1.1 Certification Authority

![Hierarchical Tree Structure](image)

Figure 1: Hierarchical Tree Structure

User-1 sends $\{V_{k_{\text{user1}}}\}$ Certified by $CA_1$ and $\{V_{KCA1}\}$ Certified by CARoot to user 3.
User 3 checks Certification on $\{V_{KCA1}\}$ certified by CARoot using $\{V_{K\text{CARoot}}\}$
Checks Certification of CA1 on $\{V_{kuser1}\}$ and if OK then accepts $\{V_{Kuser1}\}$

2 PGP-line, P2P style

3 ID-Based Cryptography

$h(Alice) \rightarrow$ ID belongs to a group. User sends their ID to TA, a trusted authority which gives the user back his corresponding secret key. Then a user’s public key is his/her identity.