Much of what happens on-line, particularly e-commerce, depends on establishing a web of trust relationships among the parties.

**Question:** Why should $A$ trust $B$ with whom he’s never previously dealt?

**Possible Answer:** $A$ might rely on a known third party to “vouch for” $B$.

The Chamber of Commerce, Better Business Bureau, credit reporting agencies, friends all function in part as certification authorities for some commercial transactions.
Need for Trust

With a public key infrastructure (PKI), if A knows B’s public key, then A can:

- send a message securely to B;
- be assured that a message from B really originated with B.

But, how does A know that the public key B presents is really B’s public key and not someone else’s?

The most common circumstance in which trust is needed in a distributed on-line context is reliably binding a public key to an identity.
A *certificate* is the electronic equivalent of a “letter of introduction.”

A certificate is constructed with digital signatures and hash functions.

A public key and a user’s identity are bound together within a *certificate*, signed by a *certification authority*, vouching for the accuracy of the binding.
Suppose X is the president of a company; Y is her subordinate. Each have an RSA public key pair.

1. Y securely passes message \{Y, K_Y\} to X.
2. X produces a cryptographic hash of the message, i.e., \(h(\{Y, K_Y\})\).
3. X produces \(\{Y, K_Y, \{h(\{Y, K_Y\})\}_K^{-1}\}\).

This last then becomes Y’s certificate, signed by X.
Suppose \( Y \) presents to \( Z \) the certificate:

\[
\{ Y, K_Y, \{ h(\{ Y, K_Y \}) \}\}_{K_X^{-1}}
\]

*What does \( Z \) do with this? What does \( Z \) learn?*

- The message certifies the binding of \( Y \) and \( K_Y \).
- \( X \) is the certifying authority.
- Data items \( Y \) and \( K_Y \) were not altered or corrupted.

This scheme assumes that \( Z \) has a trustworthy public key for \( X \), to verify \( X \)'s signature.
Certificates are needed to establish a web of trust in a distributed environment.

A trusted individual can “vouch for” another party by certifying the binding of identity to public key.

A third party can check the validity of the binding.

**Next lecture:** Certificates II