2.1 DISTRIBUTION OF PUBLIC KEYS

KEY MANAGEMENT

There are actually two distinct aspects to the use of public-key cryptography:

● The distribution of public keys

● The use of public-key encryption to distribute secret keys

Methods

- Public announcement
- Publicly available directory
- Public-key authority
- Public-key certificates

(a) Public Announcement of Public Keys

In public-key encryption the public key is public. Thus, if there is some broadly accepted public-key algorithm, such as RSA, any participant can send his or her public key to any other participant or broadcast the key to the community at large as shown in Figure.

Figure. Uncontrolled Public-Key Distribution

Disadvantage:

Anyone can forge such a public announcement. That is, some user could pretend to be user A and send a public key to another participant or broadcast such a public key.

(b) Publicly Available Directory

A greater degree of security can be achieved by maintaining a publicly available dynamic directory of public keys. Maintenance and distribution of the public directory would have to be the responsibility of some trusted entity or organization as shown in Figure.

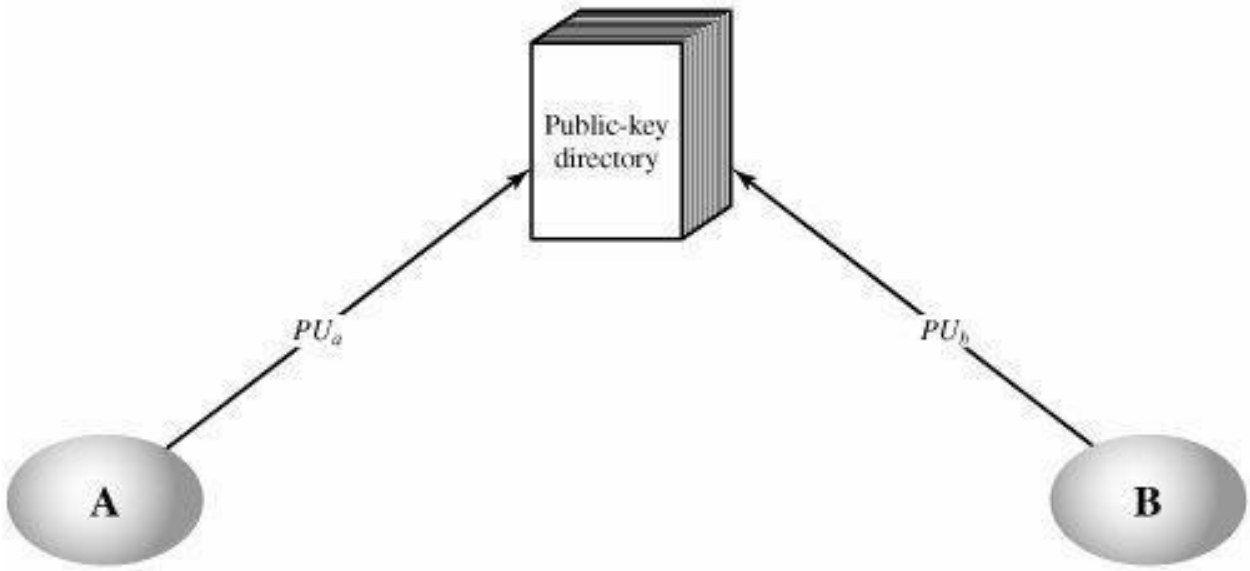
Such a scheme would include the following elements:

1. The authority maintains a directory with a (name, public key} entry for each participant.

2. Each participant registers a public key with the directory authority. Registration would have to be in person or by some form of secure authenticated communication.

3. A participant may replace the existing key with a new one at any time, due to either the key has been used for a large amount of data, or the corresponding private key has been compromised in some way.

4. Participants could also access the directory electronically. For this purpose, secure, authenticated communication from the authority to the participant is mandatory



Limitations:

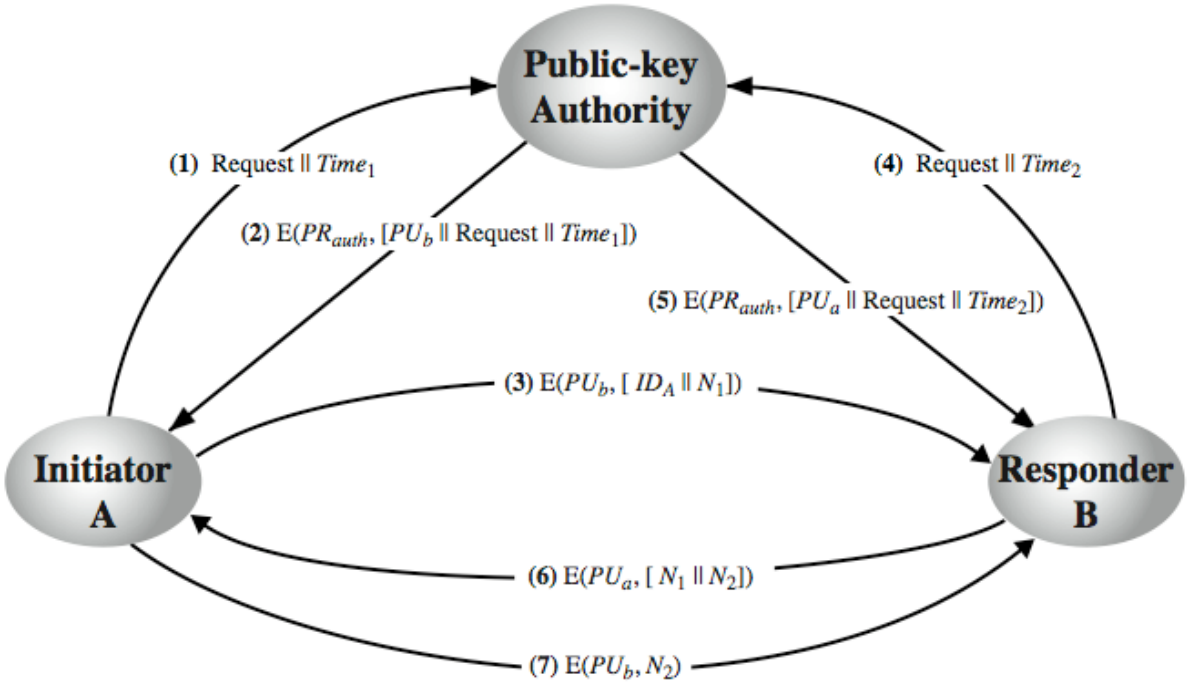
- An Adversary may impersonate by stealing the private key of public key directory and falsely send the public key details.

- An attacker may attack the records stored in the directory.

c) Public-Key Authority

Stronger security for public-key distribution can be achieved by providing tighter control over the distribution of public keys from the directory. A typical scenario is illustrated in Figure.

As before, the scenario assumes that a central authority maintains a dynamic directory of public keys of all participants. In addition, each participant reliably knows a public key for the authority, with only the authority knowing the corresponding private key. The following steps occur:



Disadvantages:

• Bottle neck at the authority

(d) Public-Key Certificates

- The public-key authority could be somewhat of a bottleneck in the system, for a user must appeal to the authority for a public key for every other user that it wishes to contact. As before, the directory of names and public keys maintained by the authority is vulnerable to tampering.

- An alternative approach is to use certificates that can be used by participants to exchange keys without contacting a public-key authority.
- A certificate consists of a public key plus an identifier of the key owner, with the whole block signed by a trusted third party.
- A user can present his or her public key to the authority in a secure manner, and obtain a certificate. The user can then publish the certificate. Anyone needed this user's public key can obtain the certificate and verify that it is valid by way of the attached trusted signature

1. Any participant can read a certificate to determine the name and public key of the certificate ‘s owner.
2. Any participant can verify that the certificate originated from the certificate authority and is not counterfeit.
3. Only the certificate authority can create and update certificates.
4. These requirements are satisfied by the original proposal in. Denning added the following additional requirement:
5. Any participant can verify the currency of the certificate