Entrust Technologies White Paper

The Concept of Trust in Network Security

Author: Ian Curry
Date: December 1995
Version: 1.1

1. Introduction

Every security system depends on trust, in one form or another, among users of the system. In general, different forms of trust exist to address different types of problems and mitigate risk in certain conditions. Which form of trust to apply in a given circumstance is generally dictated by corporate policy.

In a network security solution such as Entrust, there are two important forms of trust that customers should understand: third-party trust and direct (personal) trust. The purpose of this paper is to introduce these concepts and provide additional information so that customers understand which form of trust should be applied in a given situation.

To fully explain third-party and direct trust, the paper also introduces the following concepts: Certification Authorities, Certification Authority domains, certificates, and cross-certification.

This paper assumes the reader has a basic understanding of public-key cryptography.

2. Third-Party Trust

Third-party trust refers to a situation in which two individuals implicitly trust each other even though they have not previously established a personal relationship. In this situation, two individuals implicitly trust each other because they each share a relationship with a common third party, and that third party vouches for the trustworthiness of the two people.

Third-party trust is a fundamental requirement for any large-scale implementation of a network security product based on public-key cryptography. Public-key cryptography requires access to users' public keys. In a large-scale network, however, it is impractical and unrealistic to expect each user to have previously established relationships with all other users. In addition, because users' public keys must be widely available, the association between a public key and a person must be guaranteed by a trusted third party to prevent masquerading. In effect, users implicitly trust any public key certified by the third-party because their organization owns and operates the third-party certification agent in a secure manner.

In Entrust, the third-party certification agent is referred to as a "Certification Authority" (CA).
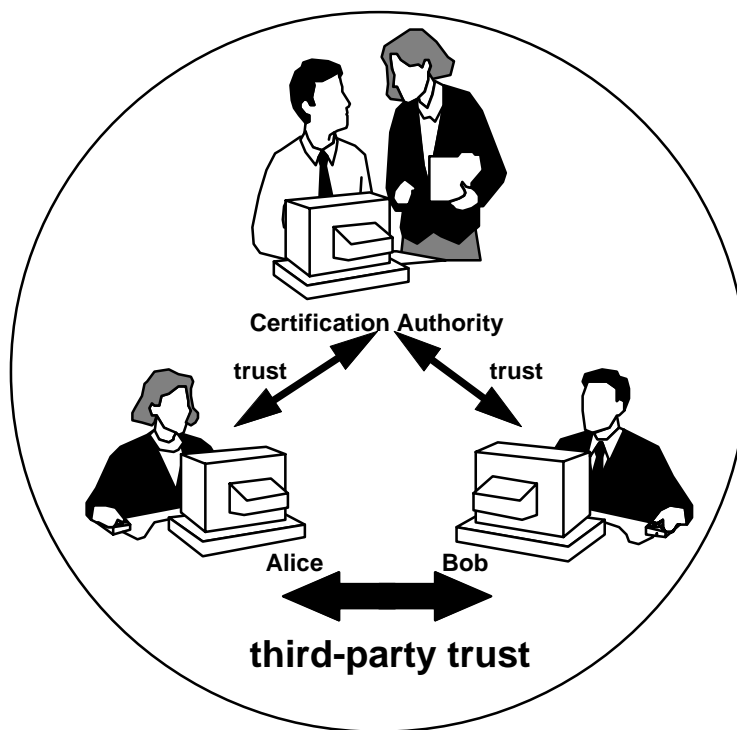
Figure 1. Third-Party Trust through a Certification Authority

2.1   Certification Authority

A Certification Authority (CA) is a trusted entity whose central responsibility is certifying the authenticity of users. In essence, the function of a CA is analogous to that of the passport issuing office in the Government. A passport is a citizen's secure document, issued by an appropriate authority, certifying that the citizen is who he claims to be (a "paper identity"). Any other country trusting the authority of that country's Government passport office will trust the citizen's passport -- a good example of third-party trust.

Similar to a passport, a network user's "electronic identity," issued to him by a CA, is that user's proof that he is trusted by the CA; therefore, through third-party trust, anyone trusting the CA should also trust the user.

Both a passport issuing office and a Certification Authority are combinations of policies and physical elements. In the case of the passport office, there is a set of policies determined by the Government dictating which people are deemed to be citizens and the process to obtain a passport. Similarly, a CA can be thought of as the group of people in an organization who determine network security policies and decide which people in the organization can be issued electronic identities on the network.

From a physical perspective, a passport office can be looked upon as the creator of secure, authorized paper documents. The passport office has special equipment to securely bind together information on a citizen (name, picture, date of birth, …) in such a way that it is extremely difficult to alter the passport without detection. Consequently, someone examining a passport is assured that the passport has integrity.

While the passport office has physical equipment to create secure paper documents, a CA has a computing platform and electronic cryptographic keys that are used to create and verify secure electronic identities for network users. Specifically, the CA creates electronic "certificates," the authenticity and integrity of which is guaranteed through a digital signature created by the CA's signing private key. Users verify the CA's signature on certificates by using the CA's verification public key.

The passport office must protect physical access to its passport generation equipment to guarantee the authenticity of passports; similarly, access to the CA's signing private key must be carefully protected and granted only to highly trusted individuals within the CA domain.

Before proceeding to a discussion of certificates, there is one additional network security trust concept that benefits from the passport office analogy. The concept is that of a "CA domain." The term CA domain refers to the population of users for which the CA has the authority to issue certificates. This is analogous to a passport office because one country does not have the right to issue passports for citizens of another country. The domain of a passport office is restricted solely to citizens of its own country.

2.2 Certificates

A network user's certificate is the electronic equivalent of his passport. As such, a certificate contains secure information that can be used to verify the identity of the owner. For instance, a certificate contains the owner's name. One critical piece of information contained in a user's certificate is his public key. The public key in a certificate is used either to encrypt data for the certificate owner or to verify the owner's digital signature.

With respect to trust, there are two central issues relating to certificates. The first issue relates to how the information in a certificate is secured. How can anyone trust that the name and public key in a certificate actually belong to the certificate's owner? Indeed, without that level of trust, public-key cryptography completely breaks down because no one is assured that he is encrypting data for the correct person or verifying a digital signature that can be associated with a specific individual.

To establish trust in the binding between a user's public key and other information (e.g., name) in a certificate, the CA digitally signs the certificate information using its signing private key. The CA's digital signature provides three important elements of security and trust to the certificate. First, by definition, a valid digital signature on a certificate is a guarantee of the certificate's integrity. Second, since the CA is the only entity with access to its signing private key, anyone verifying the CA's signature on the certificate is guaranteed that only that CA could have created the signature. Third, since only the CA has access to its signing private key, the CA cannot deny signing the certificate (a concept often referred to as non-repudiation).

Given that a certificate is secured by a CA's digital signature, the second issue relating to trusting a certificate concerns whether or not the issuing CA is itself trustworthy. If we relate this scenario to the passport analogy, the correct interpretation would be a measure of an individual's trust in the issuer of a passport. For instance, if a citizen entering country A presents an apparently valid passport issued by the passport office of country B, the customs officer must evaluate whether or not country B's passport office is trustworthy. To make this decision, the customs officer of country A would likely refer to a current list of trusted countries, as determined by a higher level policy group within the border control agency.

The analogy of trusted countries in the context of network security is referred to as "cross-certified CA domains."

2.3   Cross-certification

Cross-certification is a process in which two CAs securely exchange keying information so that each can effectively certify the trustworthiness of the other's keys. Essentially, cross-certification is simply an extended form of third-party trust in which network users in one CA domain implicitly trust users in all other CA domains which are cross-certified with their own CA.

From a technical perspective, cross-certification involves the creation of cross-certificates between two CAs. When CA *X* and CA *Y* cross-certify, CA *X* actually creates and digitally signs a certificate containing the public key of CA *Y* (and vice versa). Consequently, users in either CA domain are assured that each CA trusts the other; therefore, users in one CA domain can trust users in the other domain through extended third-party trust.

There is a great deal more to cross-certification than the technical details involved in securely exchanging keying information (which are non-trivial in themselves). Since cross-certification extends third-party trust, it is important for each CA domain to be completely comfortable

with the other's security policies. Referring back to the passport analogy, it would be highly unlikely for one country to claim trust in another country's passports without first examining the policies used to create and distribute passports to citizens of that country. For example, prior to establishing trust, each country would likely want to understand, in detail, the process by which the other country verifies the identity of an alleged citizen before issuing a passport.

Similar issues apply when cross-certifying CA domains. For example, prior to cross-certifying, both CA domains would likely want to understand the other's security policies, including information on which people have access to high-level security functions with the domain. It is also likely that legal agreements would be signed by representatives of both CA domains. These agreements would state the required security policies in both domains and provide signed assurance that these policies would be executed.
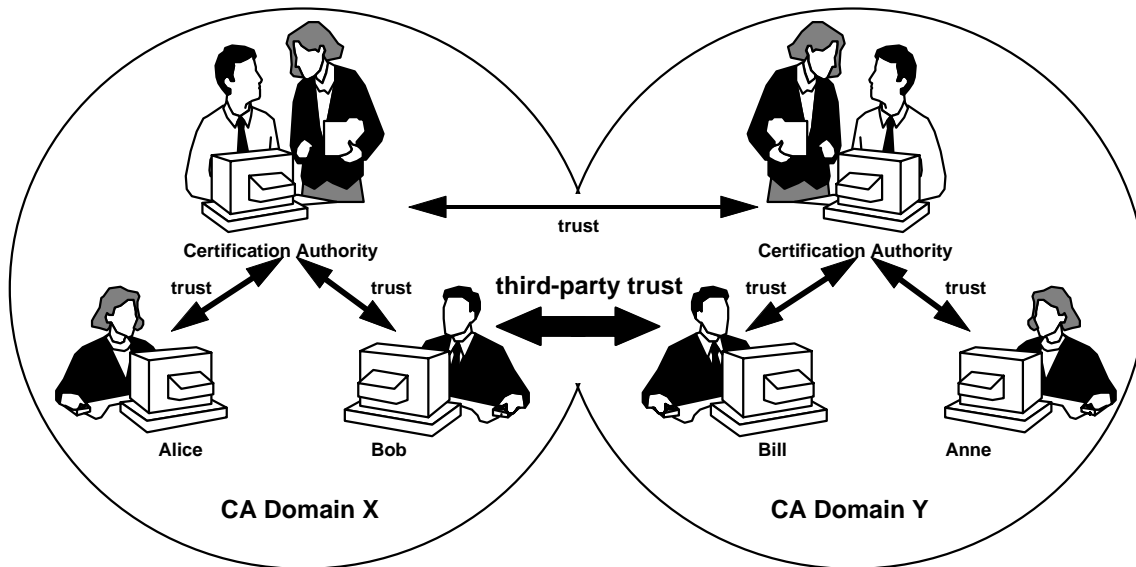

Figure 2. Extended Third-Party Trust through Cross-Certification

3. Direct Trust

Direct trust refers to a situation in which two individuals have established a trusting relationship between themselves. Whereas third-party trust allows individuals to implicitly trust each other without a personal relationship, direct trust is predicated on the existence of a personal relationship prior to exchanging secure information.

In network security, direct trust is required when individuals from separate CA domains (not cross-certified) exchange keying information to secure their communications. Because the respective CA's of these

users have not established a trust relationship (through cross-certification), the users must trust each other on a personal basis. Without personal trust in this scenario, exchanging keying information is of no value because the keying information itself should not be trusted. When direct trust is applied to secure communications, it is solely the responsibility of each of the parties to ensure that they are comfortable with their level of personal trust in the other party.
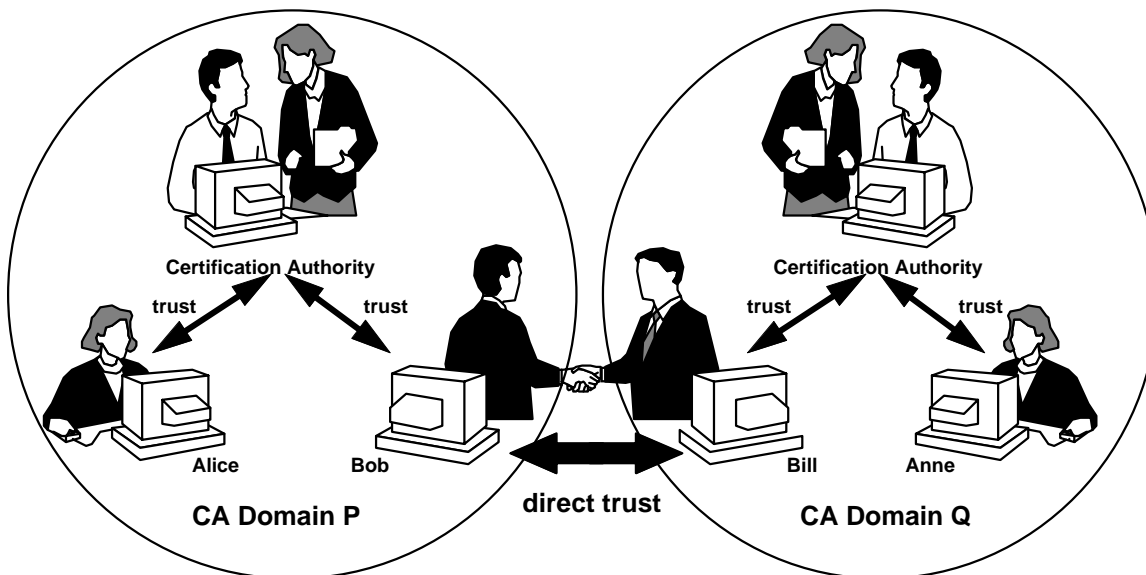

Figure 3. Direct Trust between Individuals

When direct trust is present, key exchanges among individuals with personal relationships provide a powerful mechanism to ensure secure communications. Users of Entrust in one CA domain can perform direct trust key exchanges with users in other Entrust CA domains through the use of *Address Book Services* provided in Entrust/Client.