Chapter 5

Merging Hierarchical PKIs
During Acquisition Of Companies

5.1 Introduction

Hierarchical PKI model uses the basic tree structure. The Root CA, which is also the root node in the tree, controls and provides information to all the intermediate CAs as well as users below it. Certificate path construction in Hierarchical PKI is simple, since the path is unidirectional. Most of the companies use Hierarchical PKI as their security infrastructure because it is simple and scalable[5][6]. Sometimes, one company may acquire one or more other companies. In this case, it is also required to merge their security infrastructures. This chapter explains an efficient method to merge Hierarchical PKIs during acquisition of companies ¹.

5.1.1 Merger and Acquisition of Companies

Although the terms “merger” and “acquisition” are often used as though they were synonymous, there is a slight difference between these terms. When one company

¹The research paper based on this work is accepted for publication in International Journal of Computers and Applications, Actapress Publishers, Volume 32, No.4, 2010.
Also, this work is selected for invention award by Intellectual Ventures
takes over another and clearly establishes itself as the new owner, the purchase is called an acquisition. The company that acquires is called the “acquiring” company and the one which is acquired is called the “acquired” company. From a legal point of view, the acquired company ceases to exist, the acquiring company (buyer) takes over the complete business and the buyer’s stock continues to be traded.

In a pure sense of the term, a merger happens when two firms, often of about the same size, agree to go forward as a single new company rather than remain separately owned and operated. This kind of action is more precisely referred to as a “merger of equals”. Both companies’ stocks are surrendered and new company stock is issued in its place. For example, both Daimler-Benz and Chrysler ceased to exist when the two firms merged, and a new company, DaimlerChrysler, was created. In practice, however, actual mergers of equals do not happen very often. Usually, one company will buy another and, as part of the deal’s terms, simply allow the acquired firm to proclaim that the action is a merger of equals, even if it’s technically an acquisition.

A purchase deal will also be called a merger when both companies agree that joining together is in the best interest of both of their companies. But when the deal is unfriendly - that is, when the target company does not want to be purchased - it is always regarded as an acquisition.

Whether a purchase is considered a merger or an acquisition, really depends on whether the purchase is friendly or hostile and how it is announced. In other words, the real difference lies in how the purchase is communicated to and received by the target company’s higher authorities, employees and shareholders.

5.1.2 Motives behind Mergers and Acquisitions

Mergers and Acquisitions are mainly carried out to get the benefits. The main benefits of Mergers and Acquisitions are the following:

- **Increased value generation**: Mergers and acquisitions often lead to an in-
creased value generation for the company. It is expected that the shareholder value of a firm after mergers or acquisitions would be greater than the sum of the shareholder values of the parent companies. Mergers and acquisitions generally succeed in generating cost efficiency through the implementation of economies of scale.

- **Tax gains:** Mergers and acquisitions lead to tax gains and can even lead to a revenue enhancement through market share gain. Companies go for Mergers and Acquisitions from the idea that, the joint company will be able to generate more value than the separate firms. When a company buys out another, it expects that the newly generated shareholder value will be higher than the value of the sum of the shares of the two separate companies.

- **Come out of tough times:** Mergers and acquisitions can prove to be really beneficial to the companies when they are weathering through the tough times. If the company which is suffering from various problems in the market and is not able to overcome the difficulties, it can go for an acquisition deal. If a company, which has a strong market presence, buys out the weak firm, then a more competitive and cost efficient company can be generated. Here, the target company benefits as it gets out of the difficult situation and after being acquired by the large firm, the joint company accumulates larger market share. This is because of these benefits that the small and less powerful firms agree to be acquired by the large firms.

- **Gaining Cost Efficiency:** When two companies come together by merger or acquisition, the joint company benefits in terms of cost efficiency. A merger or acquisition is able to create economies of scale which in turn generates cost efficiency. As the two firms form a new and bigger company, the production is done on a much larger scale and when the output production increases, there are strong chances that the cost of production per unit of output gets reduced. An increase in cost efficiency is affected through the procedure of
mergers and acquisitions. This is because mergers and acquisitions lead to economies of scale. This in turn promotes cost efficiency. As the parent firms unite to form a bigger new firm, the scale of operations of the new firm increases. As output production rises, there are chances that the cost per unit of production will come down.

Mergers and Acquisitions are also beneficial:

- When a firm wants to enter a new market
- When a firm wants to introduce new products through research and development
- When a firm wants to achieve administrative benefits
- To increase market share
- To lower the cost of operation and/or production
- To gain higher competitiveness
- For Financial leveraging
- To improve profit

In case a financially strong company acquires a relatively distressed one, the resultant organization can experience a substantial increase in market share. The new firm is usually more cost-efficient and competitive as compared to its financially weak parent organization.

5.1.3 Interoperability between PKIs during merger and acquisition of companies

During merger and acquisition of companies, their corresponding PKIs are also needed to be merged to achieve interoperability. Interoperability between PKIs
is a major issue to be considered when different enterprises involve in business transactions. Their corresponding PKIs need to be merged to facilitate user authentication. There are few solutions available to do this. Two of them are the most popular:

1. Merge PKIs with cross-certification between the Root CAs.

2. construct a new Root CA that is common to all the PKIs to be merged and the Root CAs of the PKIs become the subordinate CAs of the new Root CA after merging.

Both these solutions have drawbacks. The first method involves a lot of cross-certifications. It also increases the certificate path length resulting in increased certificate path verification time. The second method introduces an extra CA, i.e., new Root CA common to all the PKIs due to which the method becomes very costly because maintaining Root CA is a costly affair. It also increases the certificate path length which causes increase in certificate path verification time.

The first method described above, i.e., cross-certification at the root CAs is the most commonly used solution to merge PKIs when two or more companies are involved in the business transactions. As shown Figure 5.1, PKI1 and PKI2 are the participant PKIs for the cross-certification and Figure 5.2 shows the resultant PKI after merging with cross-certification.

![Figure 5.1: PKIs before merging with cross-certification](image-url)
But this solution is suitable when the interoperability between the PKIs is temporary and dynamically changes with the market requirements. In other words, this solution suits merging PKIs for merger of companies. However, sometimes PKIs need to be merged for acquisition of companies also. In both the cases, cross-certification at the root is a common solution.

But, during acquisition of companies, cross-certification at the root is not required because, whenever a company acquires another company, the acquired company becomes a part of the acquiring company. So the Root CA of the company to be acquired is not necessary in the future and can be discarded. Considering this fact, a method to merge Hierarchical PKIs during acquisition of companies is proposed. In the proposed method, there is no cross-certification at the root and the Root CAs of the acquired PKIs are ignored. So certificate verification time reduces significantly as compared to the method suggested in [5] and the employment cost of Root CAs is reduced as compared to the method suggested in [5] and [6]. The merging process is less expensive, easily constructed and flexible. The merged PKI is still a strict hierarchical PKI and thus the certificate path verification is also simple and straightforward. The resultant Hierarchical PKI after merging the PKIs shown in Figure 5.1 is as shown in Figure 5.3.
5.2 Proposed method of Merging PKIs during acquisition of companies

In order to reduce the cost of maintaining Root CAs and to reduce the runtime for certificate path processing, a merging method of CAs without cross-certification is proposed. In this method, the Certificate Policies (CP) of the PKIs are also considered. According to X.509[21], a Certificate Policy (CP) is a named set of rules that indicates the applicability of a certificate to a particular community and/or class of applications with common security requirements[15][78]. In the proposed method, the procedure is to set up a new PKI, but it is expensive to construct new CAs. The aim of merging CAs is smooth migration from existing PKIs. First, the CA which will be the New Root CA ($RCA_{\text{new}}$) after the merger is decided. In the proposed method, Root CA of the acquiring PKI is considered as $RCA_{\text{new}}$. If the certificate policies of all the PKIs to be merged are the same, then, $RCA_{\text{new}}$ announces its public key to entities (excluding Root CAs) of all the acquired PKIs and issues certificates for their First level entities in the hierarchy. First level entities are nothing but the subordinate CAs as well as the end entities that are children of the Root CA in the hierarchy. However, if the certificate
policies of the PKIs to be merged are different, then, $RCA_{new}$ announces its public key to entities (excluding Root CAs) of all the acquired PKIs, certifies the First level entities of those PKIs and then recertification occurs in the acquired PKIs. Figure 5.4 depicts the overall process diagram of the proposed merging process.

Figure 5.4: The overall process diagram of the proposed merging process

5.2.1 The Algorithm

The following fundamental sets are defined:

- **ENT** represents the set of all PKI entities. (For example, End-entities and
CA represents the set of all CAs and the subset of ENT.

It is assumed that a certificate is the tuple \((x, y)\) where \(x \in \text{CA}\), \(y \in \text{ENT}\). In detail, \(x\) is the issuer of certificate and \(y\) is the owner of the certificate.

The following procedures are defined in the proposed algorithm for merging:

- **Get Firstlevel Entities**(*X*): The subordinate CAs and end-entities in the next level of *X* are determined

- **Entities**(*X*): All the entities under *X* are determined

- **Announce Public Key**(*X*1, entities(*X*2)): *X*1 announces its public key to all the entities under *X*2

- **Issue Cert**(*X*1, *X*2): *X*1 issues certificate to *X*2

**Steps**

1. Let \(n\) be the number of participating PKIs during acquisition

2. Let \(RCA_1, RCA_2, \ldots, RCA_n\) be the Root CAs of these PKIs

3. Determine the New Root CA:
   
   \(RCA_{\text{new}} \leftarrow \text{RCA of the acquiring PKI}\)

4. Determine the First level entities of acquired PKIs:
   
   \(\exists_{\text{firstlevel}} \leftarrow \text{null}\)
   
   \(\forall RCA_i, \text{ where } 1 \leq i < n \quad \text{//except the } RCA_{\text{new}}\)
   
   \(\text{Entities}_{\text{firstlevel}} \leftarrow \text{Entities}_{\text{firstlevel}} \cup \text{Get Firstlevel Entities}(RCA_i)\)

5. Announce the public key of \(RCA_{\text{new}}\) for entities of RCAs of the acquired PKIs:
   
   \(\forall RCA_i, \text{ where } 1 \leq i < n \quad \text{//except the } RCA_{\text{new}}\)
   
   \(\text{Announce Public Key}(RCA_{\text{new}}, \text{Entities}(RCA_i))\)
6. \( RCA_\text{new} \) issues certificates to First level entities of the acquired PKIs: \( \forall RCA_i \), where \( 1 \leq i < n \) //except the \( RCA_\text{new} \)

\[ \text{Issue}_\text{Cert}(RCA_\text{new}, \text{Entities}_{\text{firstlevel}}) \]

7. If the certificate policies of the PKIs to be merged are different then Recertification occurs in the acquired PKIs

### 5.3 Experimental Results

A prototype for merging two or more Hierarchical PKIs based on the proposed method, is developed using Java with OpenSSL tool. PKI1, PKI2 and PKI3(Figure 5.5) are given as the inputs for the merging process. It is assumed that the company with PKI2 as its security infrastructure acquires the companies with security infrastructures PKI1 and PKI3. The result is the merging of these PKIs with RCA2 as the new Root CA(\( RCA_\text{new} \)) since PKI2 acquires PKI1 and PKI3. After merging, RCA1 and RCA3 will be ignored as they do not have any role in the future.

The results of merging PKI1, PKI2 and PKI3 with same and different certificate policies is shown in Figure 5.6 and Figure 5.7 respectively. RCA1 and RCA3 are discarded after merging operation, thus reducing the cost of managing Root CAs.

The path verification time using the normal merging method, i.e., merging with
Figure 5.6: Merged PKI with RCA2 as new Root CA ($RCA_{new}$) and same certificate Policies

Figure 5.7: Merged PKI with RCA2 as new Root CA ($RCA_{new}$) and different certificate Policies

cross-certification at the root and the proposed method by considering different depths of Hierarchical PKI trees is same as table 4.1 in chapter 4. Figure 4.5 in chapter 4 is the graphical representation of the certificate path verification time. Since the proposed techniques of merging in this chapter and the previous chapter result in a strict Hierarchical model, the result of path verification time is same. In the mesh model, the runtime requirement for cross-certification is $O(n^2)$, where $n$ is the number of CAs. In the bridge CA model, it is $O(n)$. In the proposed model, there are no cross-certifications. Since there is only one Root CA (i.e.,
$RCA_{new}$) after merging, the employment cost of CAs is reduced. Also, certificate path verification takes less time as compared to the normal method that uses cross-certification.

5.4 Summary

The proposed method of merging Hierarchical PKIs can be used during acquisition of companies. A strict hierarchical model is constructed by performing this merging process. So certification path processing is more efficient and simple since certification path is unidirectional.

In the next chapter, a novel method to compare and assess Certificate Policies during merger and acquisition of companies is explained.