Certificate Path Verification in Snorkel

– Legal Status

ODYSSEY
cryptic by intent

ODYSSEY TECHNOLOGIES LTD.

Certificate Path Verification in Snorkel

– Legal Status

Snorkel is usually deployed for web services for public key certificate based security and non-repudiation needs, primarily in the banking and financial segments. In all such services, the service caters to only well-known customers. That is, there is a pre-existing trust relationship between the bank and its customers or a stockbroker and his customers. What is required is a technology that would protect that relationship from masqueraders and other hackers in addition to ensuring provable accountability for all the actions of the customers.

It has been suggested by several PKI experts that where there is a pre-existing trust relationship, a third party CA certifying that relationship is superfluous and will become a drag on the system rather than a facilitator. The draft standard X9.59 of ANSI also recognizes this and recommends a model called account based authentication. This model stipulates that the customers' keys be simply registered with the bank. An agreement between the customer and the bank ensures that the customer will abide by his actions using his private key corresponding to the key registered with the bank. This is the model generally followed by Snorkel where certificates are issued to the customers from Snorkel itself or an enterprise CA within the organization.

As handling public keys in their raw form is inconvenient, and as browsers and other applications are already aware of the X.509 digital certificate format, it is convenient for the public keys to be carried and registered in the form of a certificate. This is what Snorkel does. This also ensures that Snorkel remains compliant with the standards at the same time bringing in an efficient operational model.

The model also satisfies the situations where the bank desires to use digital certificates issued by a third party Certifying Authority. Even though the certificates are taken from another authority, the form of trust and the key usage models remain unmodified. The keys are still generated by the customer, the public key is certified by the CA, and then the customer presents the certificate to the bank along with the proof that he is a customer of the bank. Only after all these steps are carried out, the bank proceeds to use the public key contained in the certificate to verify transactions and accept them (through Snorkel).

Thus, even though the certificate comes from a third party CA, and is part of a certificate chain originating from the Controller of Certifying Authorities (CCA) of the country to make it a 'qualified certificate', the trust is till predominantly between the customer and the bank. The bank obviously would not dream of enrolling a new customer entirely on the basis that he holds a digital certificate from an established CA.

Therefore, when it comes to transactional trust, it is directly established between the bank and the customer and reinforced by the public key of the customer embodied in a certificate.

The legal privilege, of course, comes from the CA who has issued the certificate, and who in turn has been certified by the CCA.

The classical PKI envisaged a world where people would meet on the Internet, establish a relationship purely on the basis of digital certificates they hold and even carry out financial transactions between themselves. But that view has never been implemented in practice and has already been given up as utopian and impossible. In such a model, it would not have been enough to just verify the presented certificate, but also its parental chain up to some root that the relying party can trust.

In the present case, the bank is already aware of the trust path, i.e., that the CA does hold a certificate certified by the CCA is already verified before enrolling the CA. When each certificate is registered into Snorkel, it will be verified with the CA's public key as found in the CA certificate. Once the certificate is registered into the system, all subsequent verifications either at the SSL layer

or during signature verification happen only with the stored, registered certificate and NOT with any certificate the user might send along with the signature. Thus as the certificate is a KNOWN one, there is no need at all to verify the chain up to a trusted certificate for establishing its authenticity.

The only remaining check that may have to be done is to check if the certificate is still valid. That is done by doing a CRL check every time a transaction is undertaken. This may still leave the question of the validity of the CA certificate. There is a lot of legal vagueness around a CA certificate being revoked in India. For instance, these following questions are not really answered by the IT Act or by any subordinate legislation.

- If a CA's certificate is revoked, does it mean that all the certificates issued by that CA have to be revoked?
- If they have to be revoked, who will revoke them? Who will sign the CRL? If they are signed by the CA, then the CRL is signed by an invalid certificate. What are the relying parties expected to do?
- If they don't have to be explicitly revoked, but the relying parties are expected to treat them as revoked by virtue of the CA's certificate being revoked, then the same logic will hold for other signed documents. (The certificate of the customer is a document signed by the CA. If we have to treat it as revoked because the CA's key is revoked, then by the same reasoning, all the documents so far signed by the customer also stand repudiated).
- What happens when a CA's key expires but the customer's certificate signed by the CA is still valid as per the validity time in the certificate? How are the applications expected to do chain validation when one of the links in the chain is no more valid? There is an answer to this in the standards but it is an extremely cumbersome solution.
- Even though cross certifications are not done today, it is there in the PKI standards, and the CCA has been attempting to get the CAs to cross certify among themselves as well as with foreign CAs. If that happens, it will lead to multiple paths leading up to the same trusted root and will make the path verification meaningless.

Directly trusting a customer's certificate and watching for revocation of that certificate provides the same level of trust as any attempted path verification at the relying application level. It also keeps the model simple and manageable. This trust can be augmented by having a separate understanding with the CA that in case of revocation of the CA certificate, the CA will directly inform the bank out of band.

The I.T. Act itself does not impose any specific procedure for relying parties. It simply states that if a signature is created out of a valid digital certificate, then the signature will be recognized.

The method of directly trusting the customer's certificate and out of band methods for ensuring the CA's continued operational status suffice to fulfill the legal requirements.

About Odyssey

Odyssey Technologies Limited is a pioneer in PKI technology in the Asia-Pacific region. The company develops products and solutions for transaction security and is recognized by the Controller of Certifications in India as a technology vendor.

By isolating the security components and business logic, Odyssey stays true to its zero-touch philosophy and ensures deployment of solutions quickly and effectively without the need for integration or changes to the existing code-base. The company proudly supports the security needs of major banks and financial institutions in the Asia-Pacific region and has earned their trust as a reliable vendor.

Odyssey Technologies Limited is based in Chennai, India and is listed in the Bombay Stock Exchange.