

vTrack

Description of Certificate Policy

Version 1.0

TietoEnator^{TE}

Building the Information Society

Table of Contents

1	Introduction	3
2	Concept/theory	4
3	If You Were a Bank... ..	5
4	Recommendation	6

1 Introduction

This whitepaper describes a simple solution for having secure data exchange among a group of well-known identities over the Internet. The purpose of the document is to suggest a simple and effective certificate policy between the authorities.

The solution is based on secure communication via the HTTPS protocol becoming a de-facto data exchange standard between Fishery Control Authorities in the North Atlantic.

2 Concept/theory

It is important to distinguish between how certificates are...



Certificates are **constructed** as a private and a public key. The certificate owner uses the private key to encrypt outgoing data. The data can only be decrypted and read using the public key.

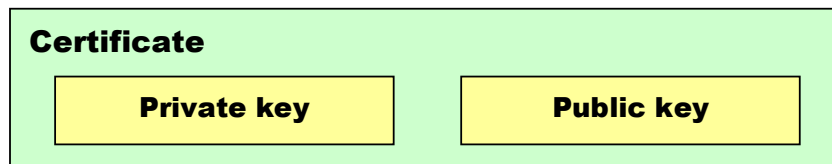


Figure 1: A certificate and its contents.

All certificates are **generated** using license-free mathematical algorithms. There are several ways to have a certificate generated:

1. Use a free-of-charge web site like <http://www.cacert.org>.
2. Use open-source software like <http://www.openssl.org>.
3. Pay a certificate authority (CA) like <http://www.verisign.com>.

All the above produce the same thing; a unique certificate containing a private and a public key - a fact often not mentioned by the established certificate authorities...

The final step is getting the certificates **verified** by whomever you want to exchange data. Here you can choose to use a central verification authority called a certificate authority or CA. This solution is typically used for securing web sites.

Alternatively you may choose to handle the verification manually by exchanging public keys with your data exchange partners.

These two solutions are described in the following two chapters.

3 If You Were a Bank...

You would need your web site to be secure. You would normally contact a CA, since a CA can add identity verification to your certificate (also called cross signing). The CA verification is trusted by all commercial browsers and ensures you that customers are really doing business with their bank and not a fake server.

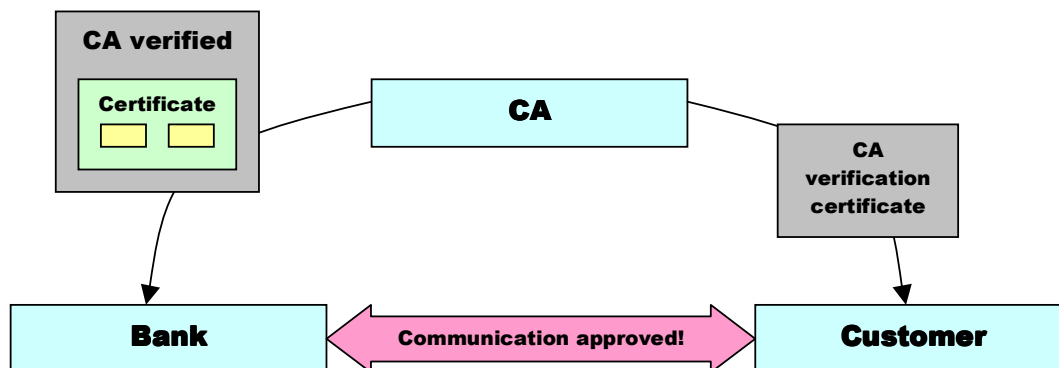


Figure 2: A typical setup of a public-accessed web server.

This setup works well for web servers accessed by standard browsers. The customers can access the web server and the browser will automatically verify the bank's certificate. However, the solution has drawbacks:

1. The CA is well paid. A site license can easily cost \$1.000 per year.
2. The certificate has limited life span. It must be renewed every 2 years.
3. Both ends must accept the CA verification certificate.
4. The solution may provide false security if not understood completely.

4 Recommendation

For a closed group of data exchange partners like the Fishery Control Authorities these drawbacks are critical. The solution is both expensive, complicated and time consuming. Our recommendation is described in the following diagram:

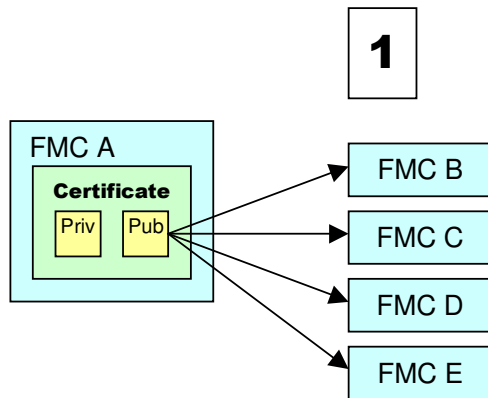


Figure 3.1: FMC A generates a certificate and distributes the public key.

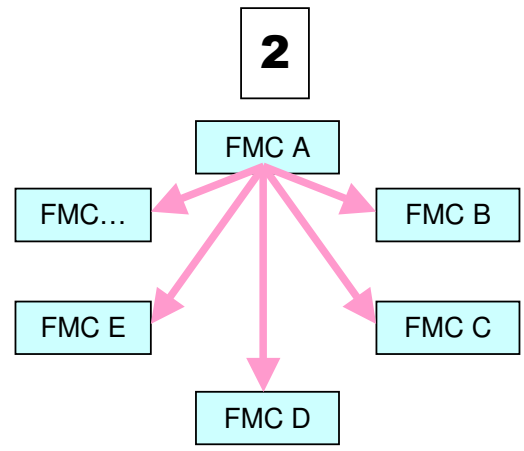


Figure 3.2: With public key installed, FMC A can now send data.

As the diagram illustrates, each FMC generates or buys a certificate and distributes its public key to all relevant data recipients. The data recipient must install the public key on their side in order to read the incoming data.

For maximum security, the public key should be distributed on a closed network (by ordinary mail or similar). This will prevent eavesdropping, since the data is only readable using the public key.

To conclude, the benefits are:

1. Certificates may be self-generated free-of-charge.
2. The certificates may have a longer life span reducing maintenance.
3. The communication is secured by public keys (easy concept).
4. The solution is easy to understand, maintain, and use.