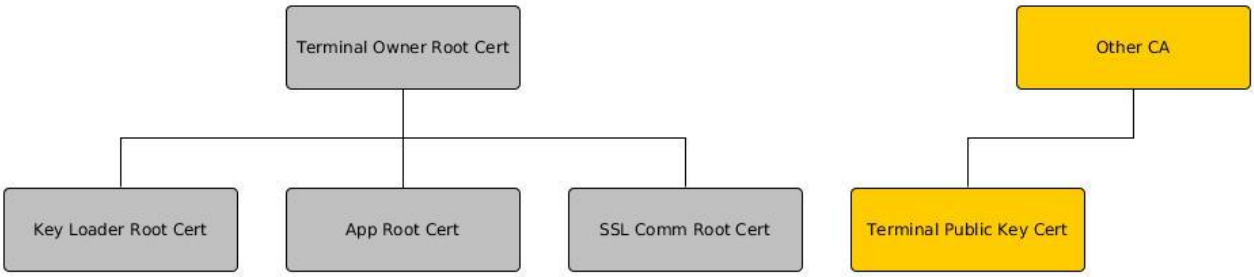
1 Certificate Type

There are 5 types of certificate stored in the terminal's safe module:



They are Terminal Owner Root Cert, Application Root Cert, SSL Communication Root Cert, Key Loader Root Cert and Terminal Public key Cert:

- Terminal Owner Root Cert: The owner of the terminal injects this certificate to the terminal. All other root certificates in the terminal should be signed by this certificate. The new terminal owner root cert should also be signed by the old one. So no one can inject any new terminal root cert, app root cert or SSL comm cert with out the permission of the terminal owner.
- Application Root Cert: It is signed by Terminal Owner Root Cert. It's the root certificate of the applications. All the APKs should be signed by this certificate or its sub-certificate. The user mode terminal will check the signature of the APKs, but the engineering terminal won't.
- SSL Comm Root Cert: It is signed by Terminal Owner Root Cert. It's the certificates stored in the hardware trust store of terminal. When terminal processes HSM based SSL connection, this certificate is used for authenticate the SSL server.
- Terminal Public Key Cert: It's the certificate of the public key of the terminal itself. It's often issued by other CA. Usually it's used for business server to authenticate or identify terminal.
- Key Loader Root Cert: It is signed by Terminal Owner Root Cert. Usually it's the root certificate of the key loader. It's used for terminal to authenticate Key Loader.

We use key usage field to identify these certificates. The "Is Critical" flag and 9 bits of the key usage should be: (empty is No or 0)

KeyUsage	Terminal Owner Root Cert	Key Loader Root Cert	App Root Cert	SSL Comm Root Cert
Is Critical	Yes	Yes	Yes	
Digital Signature			1	1
Non Repudiation		1		1
Key Encipherment	1			1
Data Encipherment				
Key Agreement				

Certificate Sign	1	1	1	
CRL Sign	1			
Encipher Only				
Decipher Only				

Note: The CA flag of App Root Cert should NOT be set, or it should be set as true. If the CA flag is set as false, this App Root Cert will not replace the default wizarpos App Root Cert, it will work as extension App Root Cert.

2 Certificate Injection

2.1 Permission of the Safe Module

The application must declare the permission of the safe module in manifest file, if it wants to inject certificate in the safe module.

The initial root certificate can be injected by factory before the terminal is deployed. The updating of the certificate must follow these rules.

2.2 Certificate Updating Rules

a) All the Key Loader Root Cert, App Root Cert, SSL Comm Root Cert and Key Loader Root Cert must be signed by Terminal Owner Root Cert. It will replace the certificate with same alias.

b) If a new certificate will update the old Terminal Owner Root Cert, it should be signed by the old certificate.

c) The KeyUsage field of the certificate must follow the rules in section 1.

3 Terminal Initialization

The terminal can be initialized before it is deployed from factory. The owner of the terminal needs to submit these:

- The CSR (certificate signature request) of the Terminal Owner Root Cert. So the manufacturer will signed this CSR and inject the certificate to the terminal.
- The other root certificates which are signed by the Terminal Owner Root Cert, especially App Root Cert and Key Loader Cert. So the manufacturer will inject these root certificates to terminal at the same time.