PrivyLink TrustField Platform SDK[*]

The Ready Cryptographic Solution for Applications

May 2003

In today's Information Technology environment, individuals and companies alike find a need to safeguard their valuable data or files. There are always security risks and exposures, especially when the Internet is prevalently used. Files transmitted over such public network are vulnerable to interception, electronic vandalism, theft and alteration. This document is targeted at System Integrators (SI) or Software Developers who recognized that by introducing cryptographic functionality into their applications, they are addressing this concern of their users and customers.

For those environments where cryptographic functionality needs to be integrated with existing back-end operations or applications, PrivyLink TrustField Platform SDK is available.

Intended Audience

Application developers who wish to build strong information systems with cryptographic functionality.

Purpose

PrivyLink TrustField Platform SDK is a suite of sophisticated and easy-to-use **A**pplication **P**rogramming **I**nterface (API) for software developer to build cryptographic functionality on other applications. The self-contained and standalone API provides a warm environment for software developer to seamlessly integrate cryptographic feature(s) to the target applications.

In deployment, PrivyLink TrustField Platform SDK suite provides a generic interface to use PKI and crypto functions and objects, as well as providing a generic and simple interface to perform crypto operations on file/message. This allows cryptographic feature(s) to be integrated into any

[*] The information contained in this document represents the current view of PrivyLink International Ltd, and is correct as of the date of publication. This document is for information purposes only. PrivyLink International Ltd makes no warranties, express or implied, in this document. Information in this document is subject to change without notice, and does not represent a commitment on the part of PrivyLink International Ltd. PrivyLink International Ltd cannot guarantee the accuracy of any information presented after the dat e of publication.

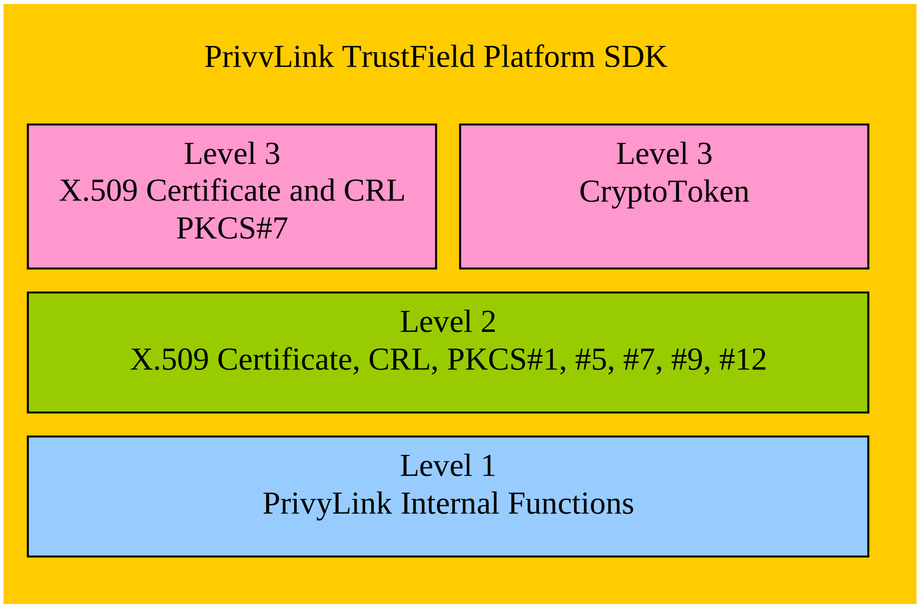
systems requiring the most demanding secured file application. The TrustField Platform SDK conforms to the widely used ITU-T X.509, PKCS #7 and PKCS #12 standards.

Scope

This document covers the following main aspects:

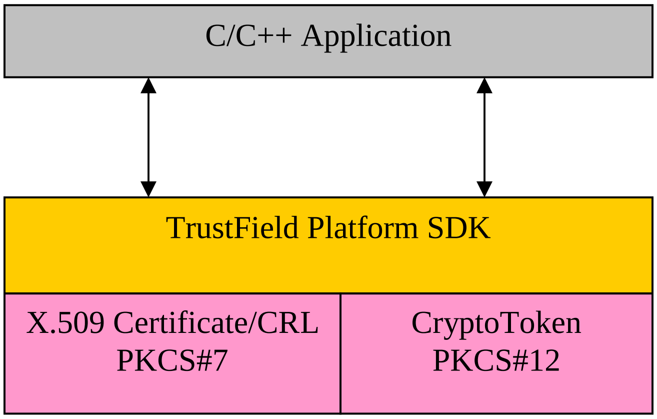
1. High Level description of the TrustField Platform SDK
2. Software Architecture of TrustField Platform SDK
3. X.509 Certificate/CRL Library
4. PKCS #7 Document Library
5. TrustField CryptoToken Library
6. Overview of TrustField Crypto Library
7. Deployment Scenario
8. Benefits
9. Conclusion

TrustField Platform SDK


PrivvLink TrustField Platform SDK
Level 3
X.509 Certificate and CRL
PKCS#7
Level 3
CryptoToken
Level 2
X.509 Certificate, CRL, PKCS#1, #5, #7, #9, #12
Level 1
PrivyLink Internal Functions

PrivyLink TrustField Platform SDK is organized in different levels. There are a total of 3 levels, starting with level 1 the lowest. The higher level API builds on top of the lower level API. Level 1 is PrivyLink internal functionality, which is not exposed. Level 2 and 3 APIs are exposed for public usage. It is recommended to use Level 3 as it is a high level API containing quick and easy to use functionality. Level 3 also uses the PrivyLink TrustField Platform SDK CryptoToken object to perform cryptographic functions. If there is feature not found in Level 3, developers can always use the rich and complicated API found in Level 2 for their work.

Software Architecture



Using the libraries inside PrivyLink TrustField Platform SDK, software developer can develop an application including cryptographic functionality and capability to their existing applications. In order to minimize the development effort to software developer, the TrustField Platform SDK provides both static and Dynamic Link Library.

TrustField Platform API

X.509 Certificate/CRL Library

This library provides the necessary APIs for X.509 certificate and CRL management. It has certificate/CRL file import/export function, retrieval of certificate/CRL details and creation of certificate/CRL.

```
string filename = “.\\privylink.cer”;

try {
      X509Certificate certificate(filename);

      cout<<certificate.getVersion()<<endl;

} catch(TFPException& ex) {
      cout<<ex.what()<<endl;

}
```

PKCS #7 Document Library

This library provides APIs for handling of SignedData, EnvelopedData and SignedAndEnvelopedData file specified in PKCS #7. Each type has a class that has methods particular to the type.

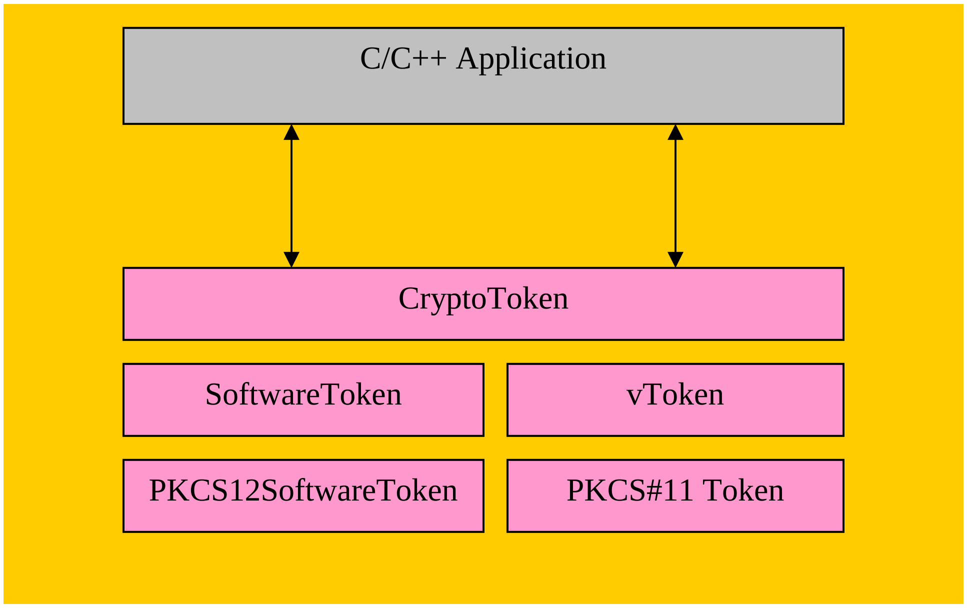
```
string filename = “.\\document.p7”;

try {
      SignedAndEnvelopedData sed(filename);

      int numberOfRecipient =
            sed.getNumberOfRecipient();

      X501Name* name = NULL;

      for(int i=0; i<numberOfRecipient; i++) {
            name = sed.getRecipientIssuerName(i);
            name.print();
      }

} catch(TFPException& ex) {
      cout<<ex.what()<<endl;

}
```

TrustField CryptoToken Library

This library handles all cryptographic related functions in the concept of a token. The entry class this library provides is SoftwareToken. It consists of DES, 3DES, RSA, MD5, and SHA-1 cryptographic algorithms. This class which is under the CryptoToken architecture can be used with the TrustField X.509 Certificate/CRL and PKCS#7 document handling API.

```
try {
      SoftwareToken token;

      token.generateSymmetricKey()

      token.symmetricEncryptInit();

      ByteArray* ciphertext =
            token.symmetricEncryptUpdate(plaintext);

      ciphertext.printHex();

} catch(TFPCryptoException& ex) {
      cout<<ex.what()<<endl;

}
```

Overview of PrivyLink Crypto Library



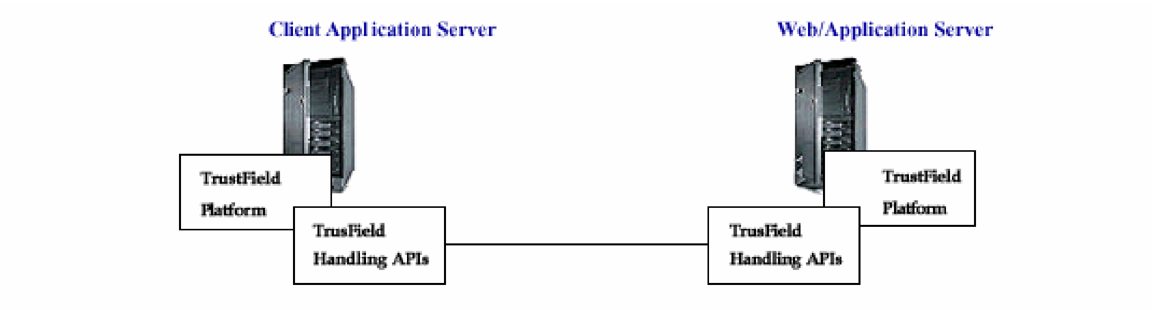
For greater flexibility, the TrustField Crypto Library is accessible by PrivyLink CryptoToken interface. The CryptoToken architecture allows the use of 3rd party cryptographic token that has a PKCS#11 interface.

The SoftwareToken contains cryptographic algorithm like DES, 3DES, RSA, MD5 and SHA-1. The PKCS12SoftwareToken leverage on the SoftwareToken with PKCS#12 feature. It contains import/export, password authentication, and manipulation of PKCS#12 PFX structure.

The vToken is an interface to PKCS#11 type token. It has been tested with Aladdin, and Rainbow USB token.

Deployment Scenario

The below diagram depict a scenario which highlights the deployment of PrivyLink TrustField Platform SDK.



Step 1: The Application running in the Client Application Server will invoke the relevant Handling API to format the files according to PKCS #7 and also to encrypt the files.

Step 2: The encrypted files are transferred to the destination server.

Step 3: The received encrypted files are verified and then decrypted by the corresponding Handling API located at the destination server.

Benefits

Convenience

The Handling APIs are self-contained and standalone; hence the cryptographic functionality can be deployed in the shortest time possible.

Standard Compliance

Our TrustField Platform SDK uses NIST FIPS certified crypto algorithm, namely, 1024-bit RSA and 192-bit 3DES-CBC digital envelope to encrypt any specified file and transfer it to the destination server over a TCP/IP channel.

PrivyLink TrustField Platform SDK has been successfully tested against X.509 digital certificates issued by multiple CA, such as VeriSign, NetTrust, ID.Safe, HKPO (Hong Kong), HiTrust (Taiwan) and DigiCert (Malaysia).

Flexibility

PrivyLink TrustField Platform SDK is designed to allow the incorporation of new cryptographic algorithms or the change of cryptographic key length to counter new vulnerabilities discovered.

Operating Environment

A C++ version of PrivyLink TrustField Platform SDK is currently supported on Windows 9x/NT/2000/XP operating systems.

Conclusion

In conclusion, the securing of critical data and file is of utmost importance to e-businesses today, and a solution that is timely, robust, reliable and secure will certainly enable an enterprise to shift into a higher gear, and realized their e-operation objectives within the shortest timeframe. PrivyLink TrustField Platform SDK can play a vital part by addressing the security needs of application developers who wanted cryptographic functionality for their applications, which in turn offers a strong and steadfast protection to their users and customers who want to safeguard their critical data and files.

About PrivyLink

Founded in 1997, PrivyLink is a response to strong industrial demands for high assurance delivery channel for electronic transactions, especially in the government and financial sectors. PrivyLink offers a comprehensive suite of software and hardware solutions to address end-to-end e-Security of today and tomorrow's businesses in the e-Commerce, e-Business, and e-Marketplace arenas.