BLOGS

IBM

# SSL Concept and Implementation in Datapower
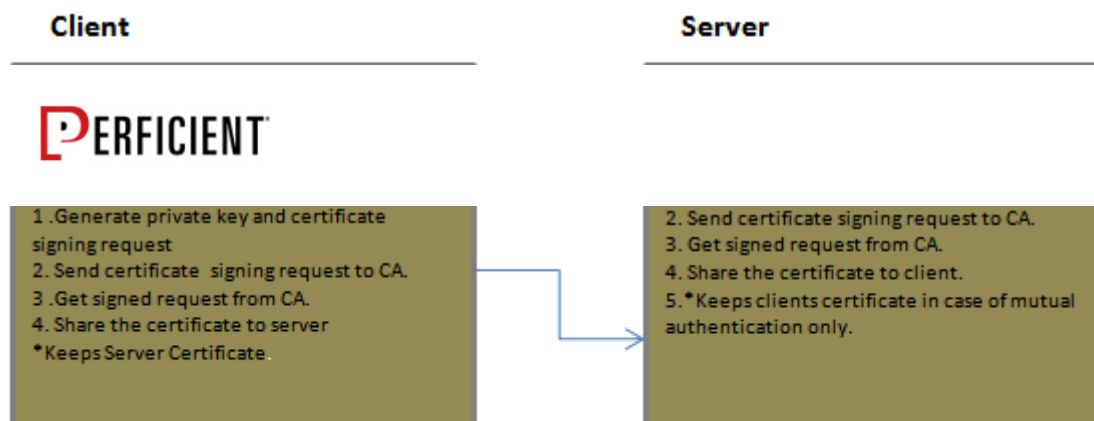
by Santosh Pericharla on September 25th, 2013 | 2 minute read
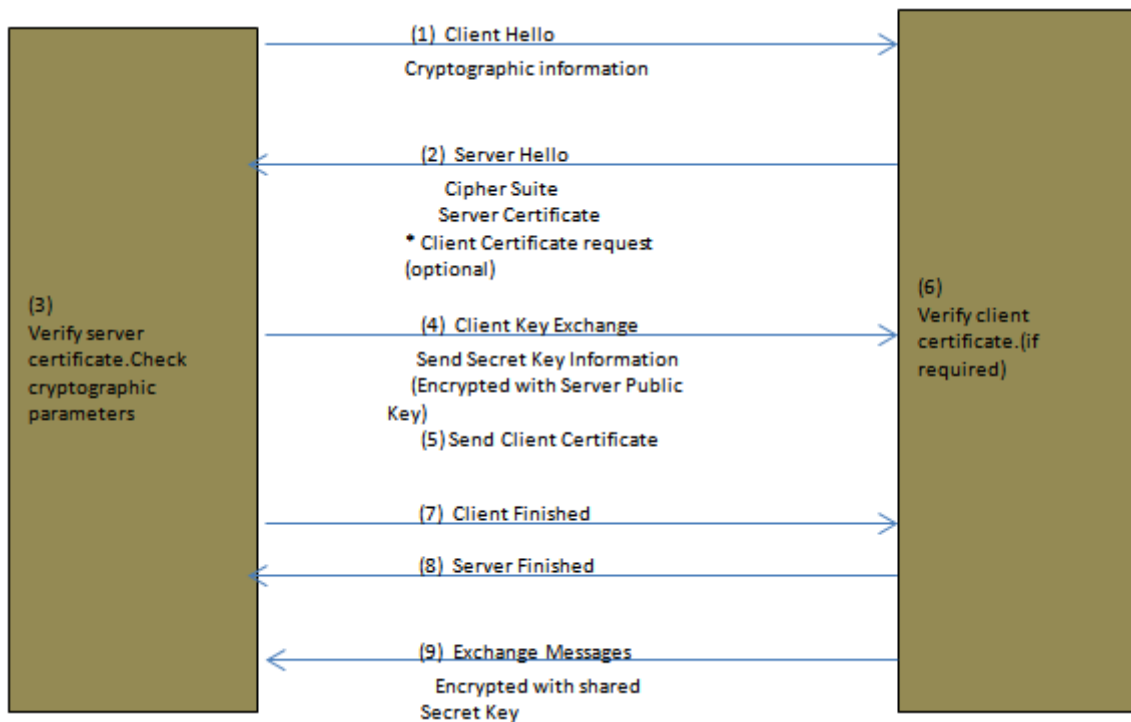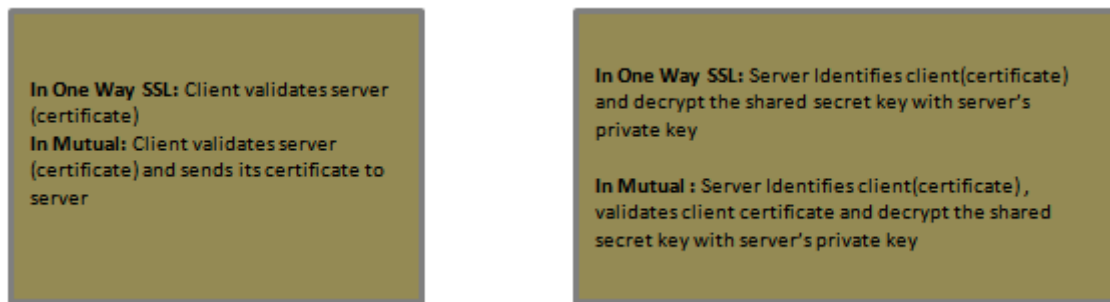
in⁴   f¹   [Twitter]   [Email]   [More]

SSL(Secure Socket Layer) is used for security over network. This blog explores implementation of SSL in Datapower along with basic concepts

**SSL Concept:**

**Key Pair Generation:**



| Client | Server |
|---|---|
| PERFICIENT | |
| 1.Generate private key and certificate signing request<br>2. Send certificate signing request to CA.<br>3.Get signed request from CA.<br>4. Share the certificate to server<br>*Keeps Server Certificate. | 2. Send certificate signing request to CA.<br>3. Get signed request from CA.<br>4. Share the certificate to client.<br>5.*Keeps clients certificate in case of mutual authentication only. |

**In One Way SSL:** Client validates server (certificate)
**In Mutual:** Client validates server (certificate) and sends its certificate to server

**In One Way SSL:** Server Identifies client(certificate) and decrypt the shared secret key with server's private key

**In Mutual :** Server Identifies client(certificate), validates client certificate and decrypt the shared secret key with server's private key

(1) Client Hello
Cryptographic information

(2) Server Hello
Cipher Suite
Server Certificate
* Client Certificate request
(optional)

(3)
Verify server certificate.Check cryptographic parameters

(4) Client Key Exchange
Send Secret Key Information
(Encrypted with Server Public Key)
(5) Send Client Certificate

(6)
Verify client certificate.(if required)

(7) Client Finished

(8) Server Finished
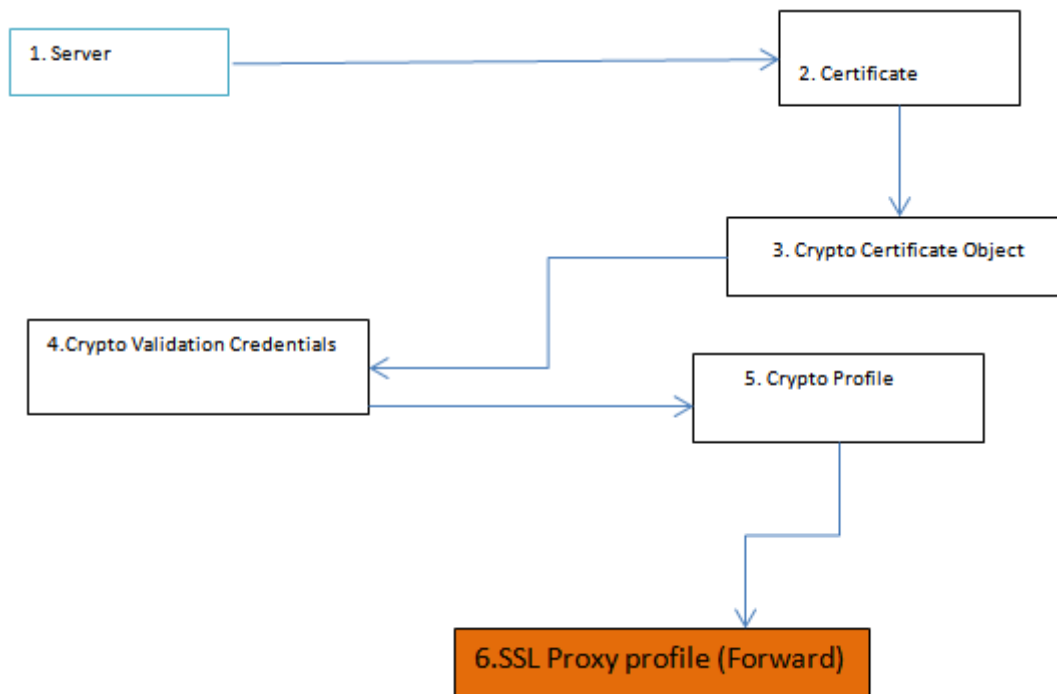
(9) Exchange Messages
Encrypted with shared Secret Key

**PERFICIENT**

**When Data power Acts as a client:**
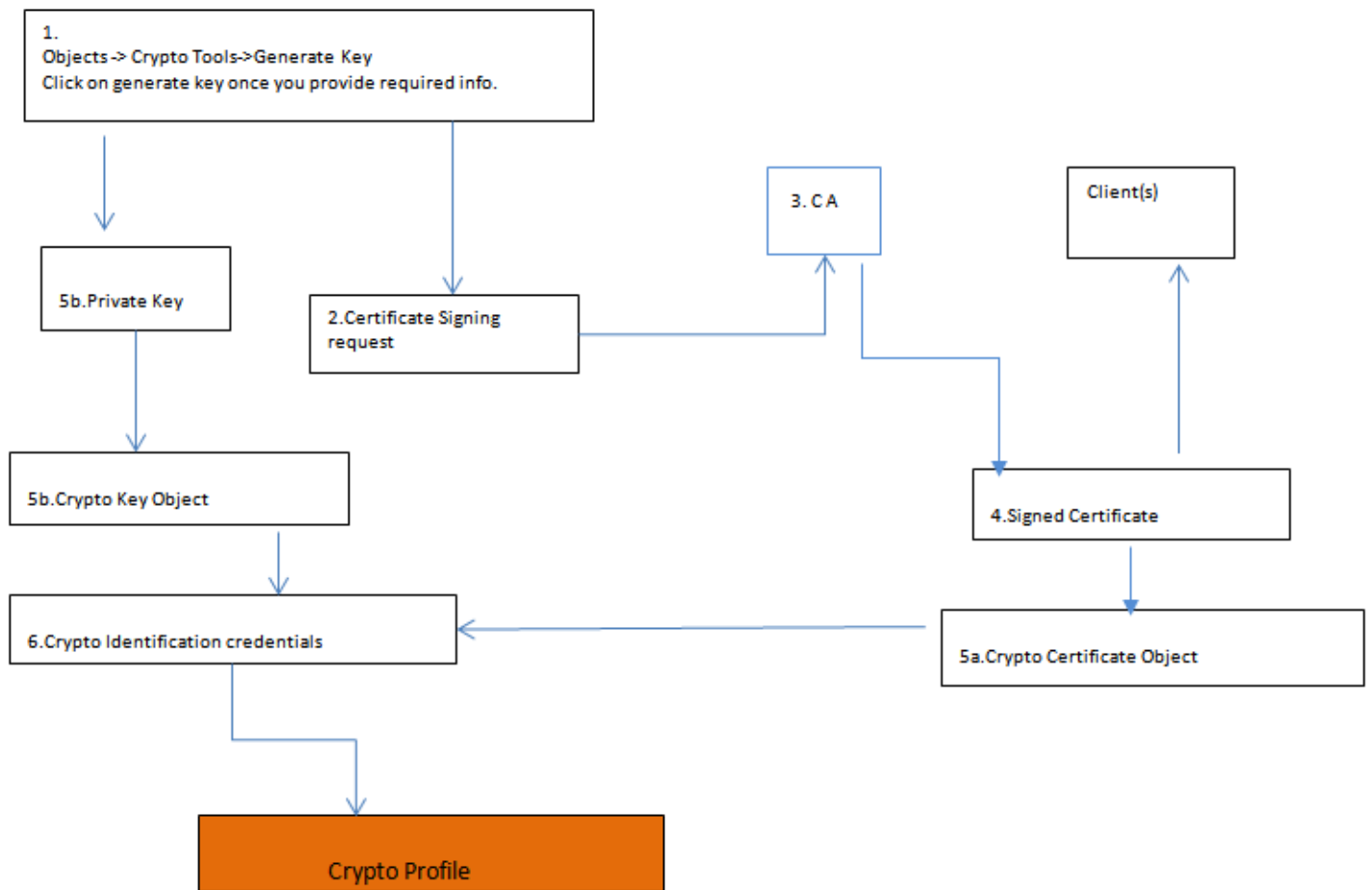
- Upload certificate shared by server in cert/pubcert directory of Datapower File Management.
- Create SSL proxy profile as shown below.This can be either referred in proxy settings or set dynamically using routing-ssl-profile variable

- Server to which Datapower acts as client will share its certificate to Datapower(Client).

- Using certificate shared, a crypto certificate object is created.

- Crypto Validation credentials created using crypto certificate object will be included in crypto profile.

- Crypto profile created will be used in Datapower as SSL proxy profile.

**When DataPower Acts as Server**

```
┌─────────────────────────────────────┐
│ 1.                                   │
│ Objects -> Crypto Tools->Generate Key│
│ Click on generate key once you       │
│ provide required info.               │
└─────────────────────────────────────┘
```

1. Objects -> Crypto Tools->Generate Key. Click on generate key once you provide required info.

3. C A

Client(s)

5b.Private Key

2.Certificate Signing request

5b.Crypto Key Object

4.Signed Certificate

6.Crypto Identification credentials

5a.Crypto Certificate Object

Crypto Profile

- Just like Crypto Validation credentials is created when datapower acts as client, Crypto identification credentials is created with combination of crypto key object and crypto certificate object.

PERFICIENT

used in request flow(When Datapower acts as  SSL server to front end systems).

# Subscribe to the IBM Weekly Digest

Email Address

**\***

**Go**

**PERFICIENT**

**Related Posts:**

**API Connect: Map Gateway cluster to**

Leave a Reply

Enter your comment here...

← PREVIOUS POST

NEXT POST →

**Subscribe to the IBM Weekly Digest:**

Your email address

Go

Perficient IBM Blog

Trends, best practices, and technical perspectives from IBM experts and thought leaders. Gain valuable insights to enable digital transformation through analytics, cloud, commerce, digital experience, and middleware solutions.

Recent Posts

- IBM Bluemix Ranked As Leading PaaS Platform
- Video: Optimizing Financial Analysis with IBM WebSphere Portal
- Everything IBM Customers Need to Know about PVU
- Getting Started with IBM Script Portlet
- Get Ready for Fall with Hybrid Cloud

Categories

- Cloud



- Digital Experience
- Systems and Middleware

Contributors



Albert Qian

Narendra Singh



Praveen Muthusamy



Heather Bowman



Stephanie Banks



David Reiber





Milan Das



Glenn Kline

Chuck Misuraca

View More Less

## Follow Us

## Archives

Archives  Select Month ▼

# CONTACT US

*Indicates a required field.*

## 1 (855) 411-PRFT

You will receive emails from Perficient about upcoming events and guides. We will never give your contact information to a third party.

First Name *

Last Name *

Work Email *

PERFICIENT

Company *

How can we help your business? *

Privacy Policy

Share This Page

**PERFICIENT**