

19 JANUARI 2024

SOSIALISASI RENEWAL CERTIFICATE SSL DAN HSM

BI-FAST OPS TEAM

Daftar Isi

- 01 *Certificate* Peserta BI-FAST
- 02 Tata Cara Perpanjangan *Soft Token*
- 03 Contoh surat
- 04 Topologi Koneksi Antar Sistem BI-FAST
- 05 Prosedur Teknis dan Alur Pelaksanaan
- 06 Timeline Persiapan & Pelaksanaan
- 07 Peserta *Renewal Certificate* BI-FAST
- 08 Pembahasan Juknis

01 Certificate SSL dan HSM Peserta BI-FAST

- Berdasarkan PADG BI-FAST No. 17 Tahun 2023, masing-masing Peserta **memiliki kewajiban untuk menjamin BI-FAST Connector berfungsi dengan baik**, salah satunya adalah dengan melakukan perpanjangan masa aktif *certificate*.
- Masa aktif *certificate* SSL dan HSM adalah **paling lama 2 (dua) tahun sejak tanggal efektif**. Mengingat proses instalasi BI-FAST sudah dimulai sejak Triwulan-III 2021, maka perlu dilakukan perpanjangan *certificate* SSL dan HSM baik di sisi Penyelenggara maupun Peserta.



Certificate SSL dan HSM Peserta BI-FAST

1. Masa aktif *certificate* SSL dan HSM adalah paling lama 2 (dua) tahun sejak tanggal efektif
2. Mengingat proses instalasi BI-FAST sudah dimulai sejak Triwulan-III 2021, maka masa berlaku *certificate* tersebut saat ini menjelang periode *expired*
3. Maka dari itu, **perlu dilakukan perpanjangan *certificate* SSL dan HSM baik di sisi Penyelenggara, maupun Peserta**

Ketentuan PADG Ekstern BI-FAST (No.17 Tahun 2023)



Pasal 18, huruf l

“Menjamin infrastruktur utama dan infrastruktur cadangan berfungsi dengan baik untuk melakukan berbagai aktivitas BI-FAST sepanjang jam operasional BI-FAST;”



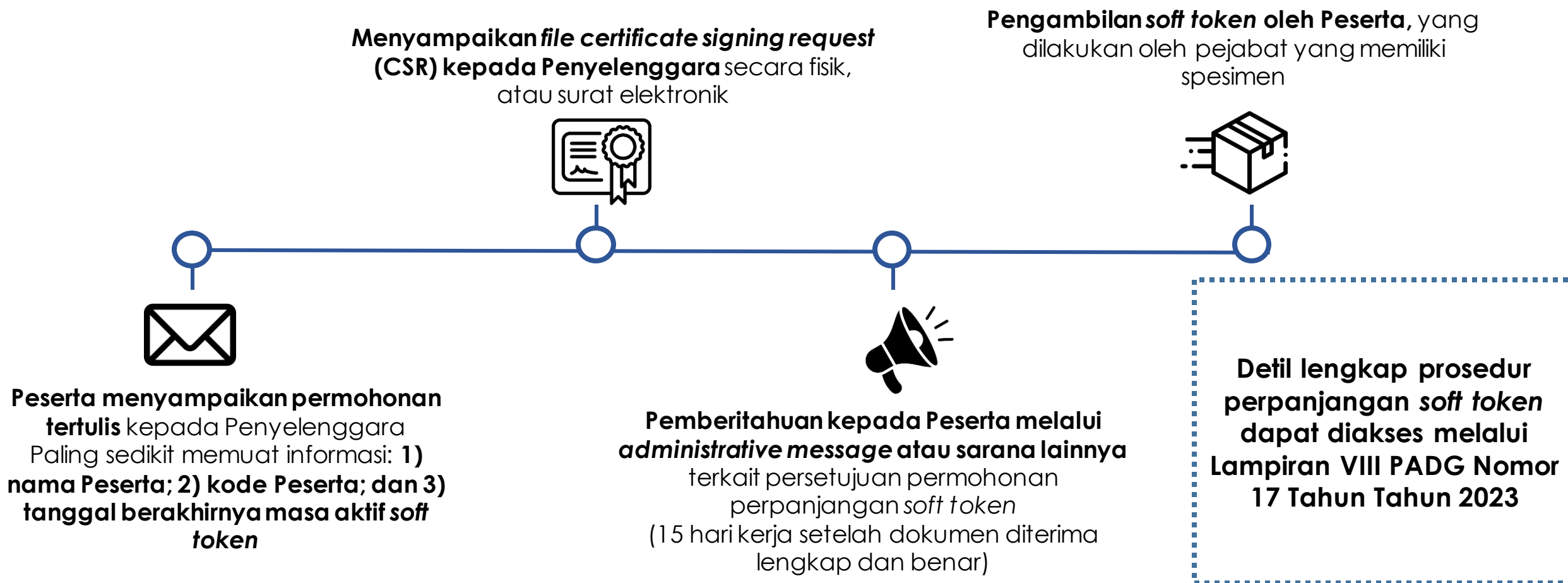
Pasal 25, huruf i

“Melakukan perpanjangan masa aktif *soft token** sesuai dengan waktu yang telah ditetapkan oleh Penyelenggara”

**soft token = certificate*

02 Tata Cara Perpanjangan Masa Aktif Soft Token

Tata cara perpanjangan masa aktif *soft token* mengacu pada Lampiran VIII PADG No. 17 Tahun 2023 dengan alur sebagai berikut:



03 Contoh surat permohonan perpanjangan certificate

Surat Permohonan Perpanjangan Masa Aktif Soft Token BI-FAST

No.

Kepada Yth.
Bank Indonesia
Departemen Penyelenggaraan Sistem Pembayaran
Divisi Operasional Sistem Pembayaran Ritel (OSPR)
Gedung D Lantai 3
Jalan M.H. Thamrin No. 2
JAKARTA 10350

Perihal : **Permohonan Perpanjangan Masa Aktif Soft Token BI-FAST**

Dalam rangka pelaksanaan kegiatan operasional BI-FAST, dengan ini kami mengajukan permohonan dengan data sebagai berikut:

1. Nama Peserta : ____
2. Kode Peserta : ____
3. Permohonan : Perpanjangan certificate HSM (BANK_REALM) BI-FAST yang masa aktifnya akan habis tanggal

Terlampir kami sampaikan file Certificate Signing Request (CSR) terkait dengan permohonan tersebut.

Demikian permohonan kami.

[Kota], [Tanggal, bulan, dan tahun]
[Nama badan hukum]

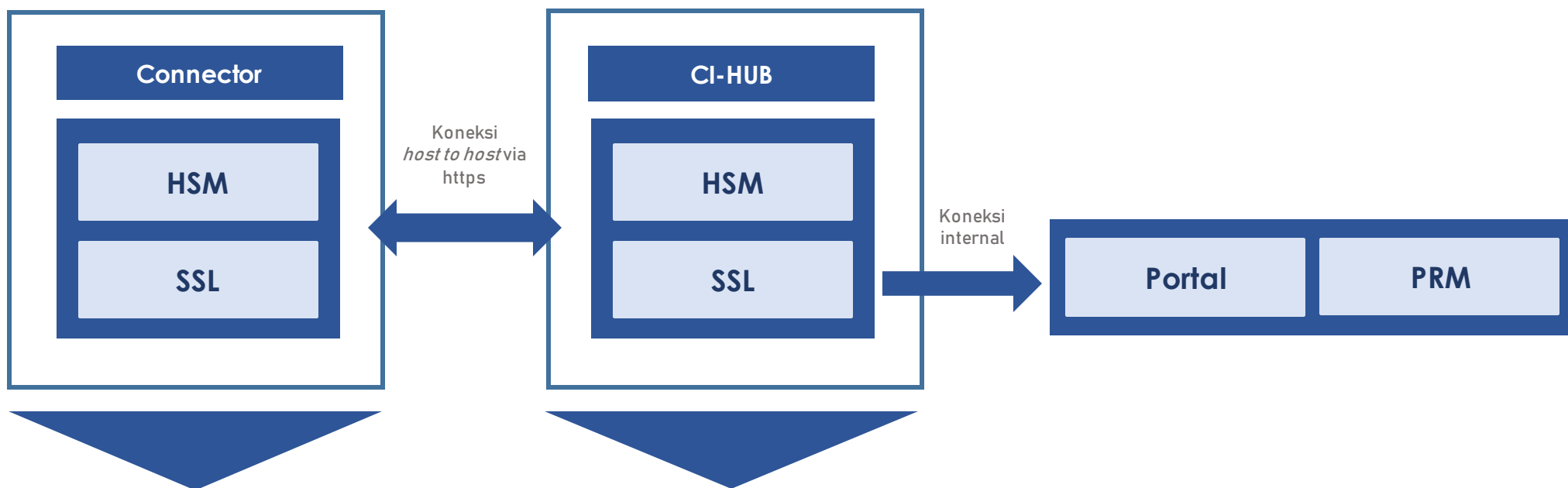
[Tanda tangan dan stempel badan hukum]

[Nama Pimpinan/Pejabat yang berwenang]
Jabatan


04 Topologi Koneksi Antar Sistem BI-FAST

Dalam rangka meningkatkan aspek *security* sistem BI-FAST, telah diterapkan pengamanan berlapis yang meliputi aspek i). jaringan dan ii). protokol koneksi.

Protokol koneksi sistem BI-FAST menggunakan HSM untuk proses *message signing* dan *verifying*, dimana Connector peserta harus menyimpan *public key* dari *certificate* Bank Indonesia, begitu juga sebaliknya CI-HUB Bank Indonesia harus menyimpan *public key* dari *certificate* Peserta.



CERTIFICATE PESERTA	EXPIRED
Bank HSM	Maret 2024 (beberapa peserta) 
Bank SSL	Februari 2024 (beberapa peserta) 

CERTIFICATE BI	EXPIRED
HUB HSM	September 2025
HUB SSL	Februari 2023 (kecuali bank-bank yang sudah uplift) 

05 Prosedur Teknis

Renewal HUB SSL

Pembaharuan *certificate* HUB SSL di sisi Bank Indonesia berdampak ke seluruh peserta BI-FAST

CI-HUB	CONNECTOR
1. Penyesuaian HUB SSL ID peserta pada Config Builder sesuai dengan peserta yang terlibat	1. Replace HUB SSL ID dengan <i>certificate</i> SSL baru pada Platform Manager 2. <i>Restart</i> ICE-XS Eksternal

Renewal BANK SSL

Pembaharuan *certificate* BANK SSL di sisi Bank Peserta akan mengubah konfigurasi di sisi Bank Indonesia

CONNECTOR	CI-HUB
1. <i>Create</i> CSR Bank SSL baru di sisi Connector 2. Kirim CSR tersebut ke Bank Indonesia untuk proses <i>signing</i> 3. Bank Indonesia akan mengirimkan SSL <i>certificate</i> yang sudah di <i>sign</i> ke bank peserta 4. <i>Replace</i> eksisting Bank SSL ID dengan <i>certificate</i> SSL terbaru pada Platform Manager 5. <i>Restart</i> ICE-XS Eksternal	1. <i>Replace</i> Bank SSL ID dengan <i>certificate</i> BANK SSL terbaru pada Platform Manager CI-HUB 2. <i>Restart</i> ICE-XS Eksternal

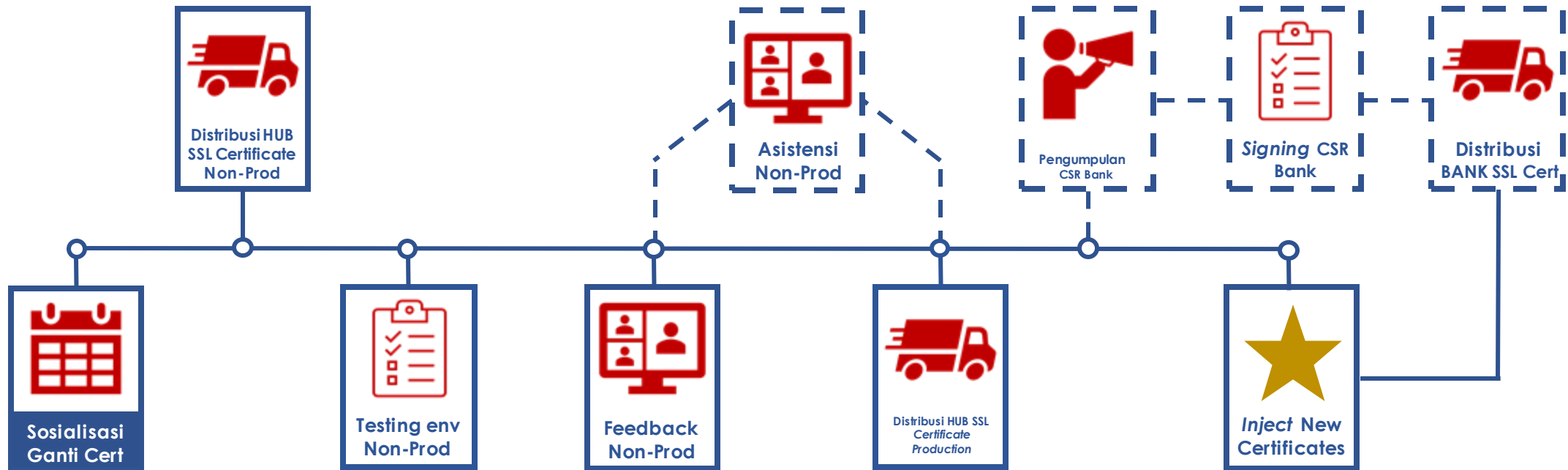
05 Prosedur Teknis

Renewal Bank HSM/Bank Realm

Pembaharuan *certificate* Bank Realm di sisi Bank Peserta akan mengubah konfigurasi di sisi Bank Indonesia

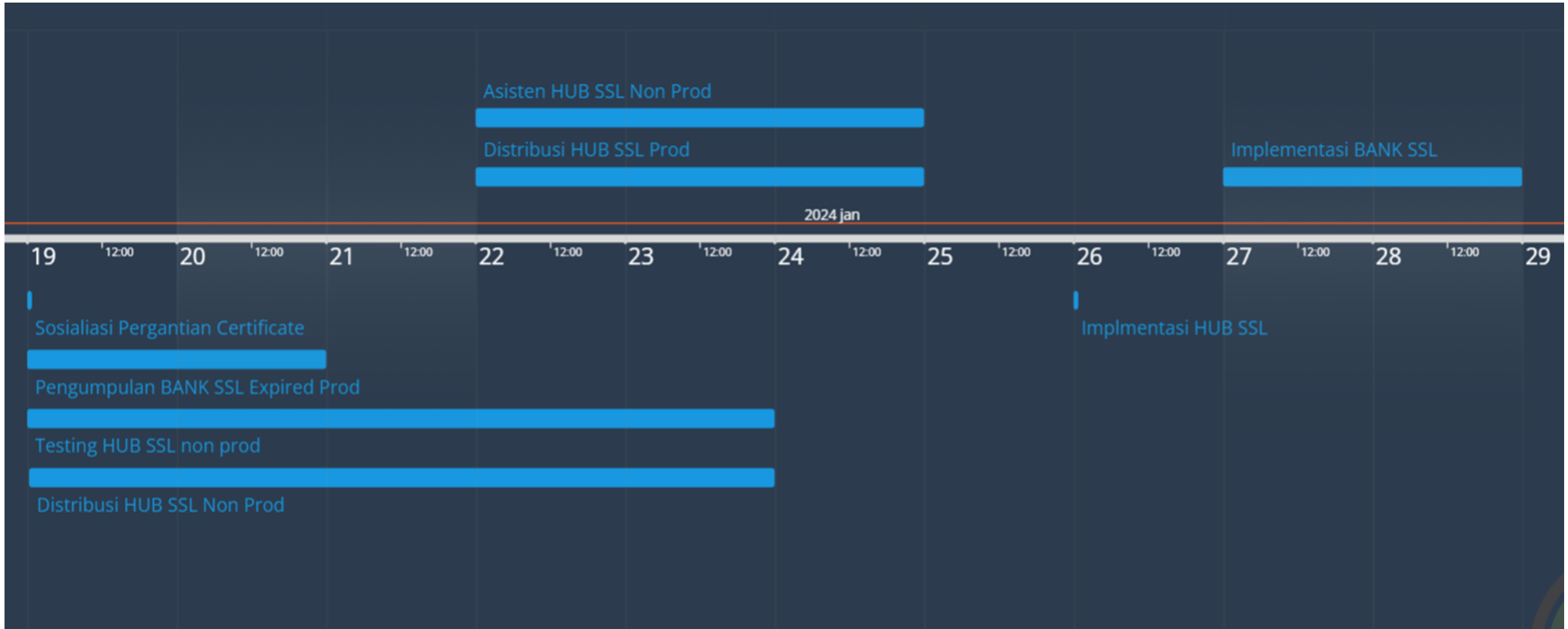
CONNECTOR	CI-HUB
<ol style="list-style-type: none">1. <i>Create</i> CSR Bank Realm baru di sisi Connector2. Kirim <i>certificate</i> tersebut ke Bank Indonesia untuk proses signing3. Bank Indonesia akan mengirimkan <i>certificate</i> yang sudah di sign ke bank peserta4. <i>Replace</i> eksisting Bank Realm dengan <i>certificate</i> Bank Realm terbaru pada Platform Manager5. <i>Restart</i> ICE-XS Eksternal	<ol style="list-style-type: none">1. <i>Replace</i> Bank Realm ID dengan <i>certificate</i> BANK Realm terbaru pada Platform Manager CI-HUB2. <i>Restart</i> ICE-XS Eksternal

05 Alur Pelaksanaan Pergantian Certificate



06 *Timeline* Persiapan & Pelaksanaan

Renewal Certificate HSM & SSL 2024



07 Peserta Renewal Certificate BI-FAST

PESERTA TERLIBAT

BATCH 1 – BANK SSL & BANK HSM (26 Januari 2024)

1. PT. BANK JABAR BANTEN SYARIAH
2. PT. BANK BUMI ARTA
3. PT. BANK ARTHA GRAHA INTERNASIONAL, TBK
4. PT. BANK DKI UNIT USAHA SYARIAH
5. PT. BANK ARTOS INDONESIA (Bank Jago)
6. PT. BANK DKI

BATCH 1 – BANK SSL ONLY (26 Januari 2024)

1. CITIBANK, NA
2. PT. BANK MANDIRI (PERSERO) TBK
3. PT. BANK CENTRAL ASIA Tbk.
4. HSBC Indonesia
5. PT. BANK NEGARA INDONESIA (PERSERO)
6. PT. BANK RAKYAT INDONESIA (PERSERO)
7. PT. BANK CIMB NIAGA TBK
8. PT Bank Syariah Indonesia
9. PT. BANK DANAMON INDONESIA UNIT USAHA SYARIAH
10. PT. BANK DANAMON INDONESIA Tbk.
11. PT. BANK PERMATA,TBK
12. PT. BANK BCA SYARIAH
13. PT. BANK PERMATA,TBK UNIT USAHA SYARIAH
14. PT. BANK MEGA Tbk.
15. PT. BANK SINARMAS
16. PT. BANK CIMB NIAGA TBK - UNIT USAHA SYARIAH
17. PT. BANK DBS INDONESIA
18. PT. BANK UOB INDONESIA
19. PT. BANK OCBC NISP, Tbk.
20. PT. BANK WOORI SAUDARA INDONESIA 1906,TBK
21. PT. BANK MULTI ARTHA SENTOSA
22. PT. KEB HANA INDONESIA
23. PT. BANK MASPION
24. KUSTODIAN CENTRAL EFEK INDONESIA
25. PT. PAN INDONESIA BANK (PANIN)

BATCH 2 – BANK SSL & BANK HSM (22 Maret 2024)

1. PT. BANK PEMBANGUNAN DAERAH RIAU KEPRI
2. PT. BANK RAKYAT INDONESIA AGRONIAGA, TBK (RAYA)
3. PT. BANK MAYAPADA INTERNASIONAL, TBK
4. BANK NANO SYARIAH

BATCH 2 – BANK SSL ONLY (22 Maret 2024)

1. PT. BANK NATIONALNOBU
2. PT. BANK PEMBANGUNAN DAERAH BALI
3. PT. BANK SAHABAT SAMPOERNA
4. PT. BANK PEMBANGUNAN DAERAH JAWA TIMUR
5. PT. BANK GANESHA
6. PT. BANK PEMBANGUNAN DAERAH JAWA BARAT BANTEN
7. PT. BANK MANDIRI TASPEN
8. PT. BANK INA PERDANA, TBK
9. PT. BANK JAWA TIMUR UUS SYARIAH
10. PT BANK PEMBANGUNAN DAERAH JAWA TENGAH UNIT USAHA SYARIAH
11. ALLO BANK
12. PT. BANK PEMBANGUNAN DAERAH PAPUA
13. PT. BANK TABUNGAN NEGARA (PERSERO) UNIT USAHA SYARIAH
14. PT. BANK TABUNGAN NEGARA (PERSERO)
15. PT. BANK MESTIKA DHARMA
16. PT. BANK PEMBANGUNAN DAERAH JAWA TENGAH

07 Peserta Renewal Sertifikat BI-FAST

PESERTA TERLIBAT

BATCH 3 – BANK SSL & BANK HSM (21 JUNI 2024)

1. PT. BANK NEO COMMERCE
2. PT. BPD KALIMANTAN SELATAN UUS
3. PT. BANK MUAMALAT INDONESIA, TBK
4. PT. BANK JASA JAKARTA
5. PT. BPD KALIMANTAN SELATAN
6. PT BANK CAPITAL INDONESIA
7. PT. BANK JAGO UUS, TBK
8. PT. BANK BTPN TBK
9. PT. BANK CTBC INDONESIA
10. PT. BANK MAYORA
11. PT. BANK MAYBANK INDONESIA, TBK UUS
12. PT. BANK MAYBANK INDONESIA, TBK
13. PT. BANK ICBC INDONESIA
14. BANK INDONESIA
15. STANDARD CHARTERED BANK
16. PT. BPD YOGYAKARTA UUS
17. PT. BPD SUMSEL DAN BABEL UUS
18. PT BANK NAGARI UUS
19. PT. BPD KALIMANTAN BARAT UUS
20. PT. BPD YOGYAKARTA
21. PT BANK NAGARI
22. PT. BPD KALIMANTAN BARAT
23. PT. BANK MNC INTERNASIONAL, TBK
24. PT. BPD SUMSEL DAN BABEL
25. BANK INDEX SELINDO

BATCH 4 – BANK SSL & BANK HSM (13 SEPTEMBER 2024)

1. BPD KALTIM DAN KALTARA UUS
2. BPD SULUT GORONTALO
3. BPD SULAWESI TENGGARA
4. BPD NUSA TENGGARAT BARAT UUS
5. BPD KALIMANTAN TIMUR DAN KALIMANTAN UTARA
6. BPD BENGKULU
7. BANK QNB INDONESIA
8. BANK SULSELBAR UUS
9. BANK SULSELBAR
10. BPD JAMBI UUS
11. BPD JAMBI
12. BANK CHINA CONSTRUCTION BANK INDONESIA
13. BANK ALADIN SYARIAH
14. MUFG BANK
15. BANK OF AMERICA NA
16. PT. BANK OCBC NISP TBK UNIT USAHA SYARIAH
17. BPD MALUKU DAN MALUKU UTARA
18. BANK BTPN SYARIAH
19. BANK RESONA PERDANIA
20. BANK ACEH UUS
21. BANK VICTORIA INTERNATIONAL
22. BPD SUMUT UUS
23. BPD SUMUT
24. BPD KALIMANTAN TENGAH (KALTENG)
25. BPD BANTEN
26. BANK IBK INDONESIA
27. BANK MEGA SYARIAH
28. BANK OF CHINA

08 Pembahasan Juknis

BANK SSL

1.1 Generate Keystore and Truststore Connector

1.1.1 Generate Keypair Connector

1. In primary MCAS server create a directory call "SSL_CERT" in "/opt/aci/UPF"

```
cd /opt/aci/UPF/  
  
mkdir SSL_CERT  
  
cd SSL_CERT  
  
[bifast@DEVFASTCOUPF02 UPF]$ cd /opt/aci/UPF  
[bifast@DEVFASTCOUPF02 UPF]$ pwd  
/opt/aci/UPF  
[bifast@DEVFASTCOUPF02 UPF]$ mkdir SSL_CERT  
[bifast@DEVFASTCOUPF02 UPF]$ cd SSL_CERT
```

2. Run below command to create keypair and JKS file. Edit the command accordingly (dname info, bankcode, CN hostname, dns hostname, O, and OU)

```
keytool -genkeypair -alias SSL_BankBICCode -keyalg RSA  
-keysize 2048 -sigalg SHA256withRSA -keystore  
SSL_BankBICCode_MonthYear_keystore.jks -storepass  
bifast123 -validity 1825 -dname "CN=host name(server  
name),O=Bank Indonesia,OU=DPSI,C=ID,L=Jakarta" -ext  
SAN=dns:(icexs server name),dns:(icexs server name)
```

Example:

```
keytool -genkeypair -alias SSL_DEUTIDJA -keyalg RSA -  
keysize 2048 -sigalg SHA256withRSA -keystore  
SSL_DEUTIDJA_Mar2024_keystore.jks -storepass bifast123  
-validity 1825 -dname  
"CN=devfastcoupf01.xnet.bi.go.id,O=Bank  
Indonesia,OU=DPSI,C=ID,L=Jakarta" -ext  
SAN=dns:devfastcoupf01.xnet.bi.go.id,dns:devfastcoupf0  
2.xnet.bi.go.id
```

