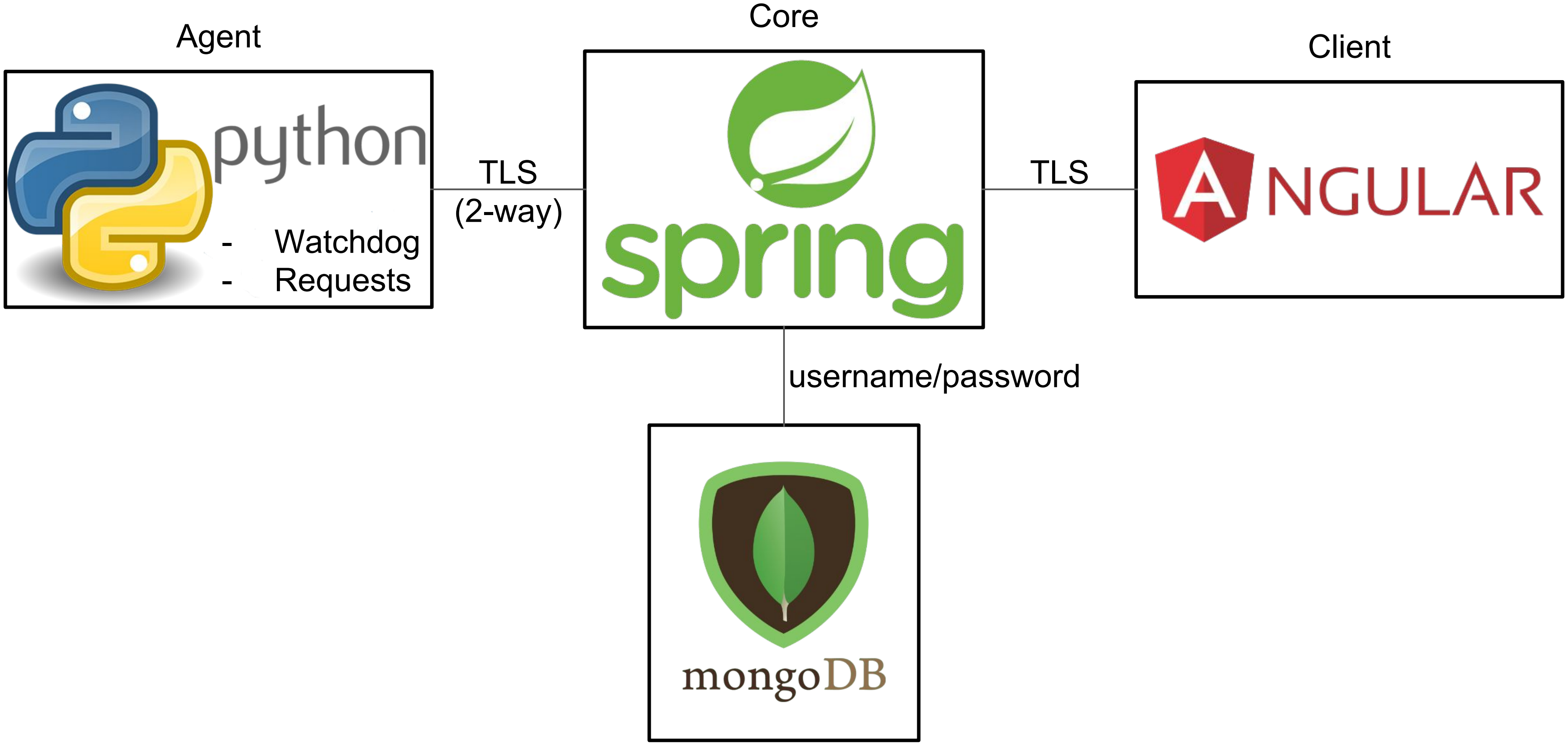
SIEM monitor by code10

Helena Zečević, SW-6/2014
Luka Maletin, SW-7/2014
Aleksandar Nikolić, SW-25/2014

Agenda

1. Technology stack
2. Client demo
3. Agent config
4. TLS config

1. Technology Stack



2. Client demo...

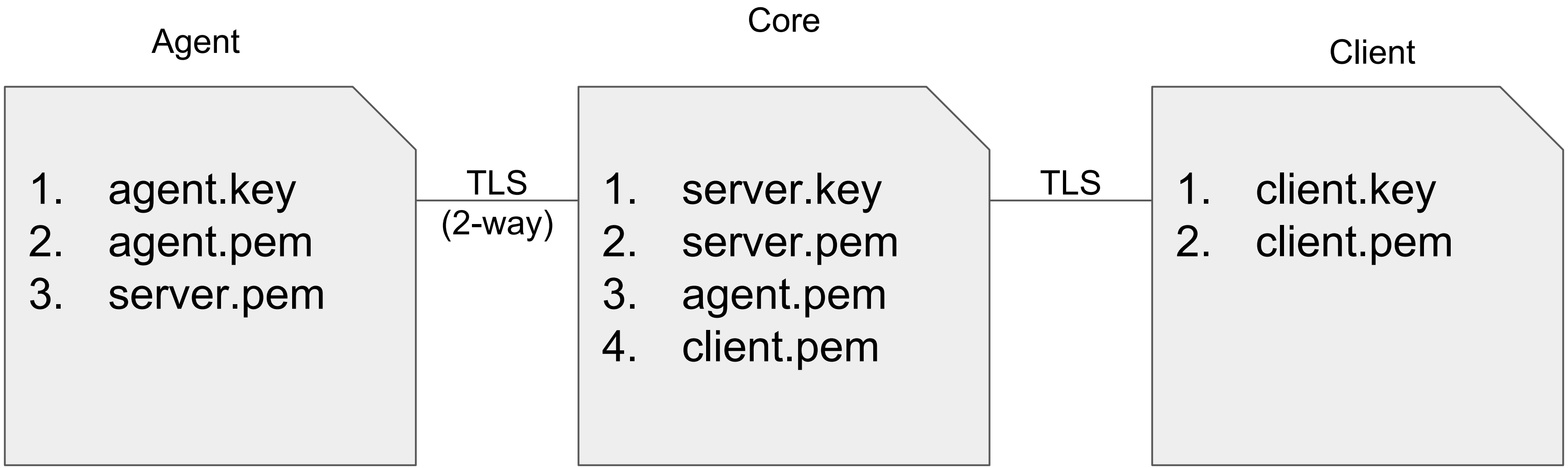
3. Agent config (YAML)

```yaml
api-url: https://localhost:8080/api/logs

read-os-logs: True
os-logs-regex: .*
os-logs-interval: 0

logs:
- path: C:\Workspace\BSEP\siem-monitor\Agent\test1.log
  regex: .*
  interval: 0 # Real time
- path: C:\Workspace\BSEP\siem-monitor\Agent\test2.log
  regex: .*
  interval: 5 # Polling interval in seconds
- ...
```

4.1 TLS config - PKI



Agent

1. agent.key
2. agent.pem
3. server.pem

TLS
(2-way)

Core

1. server.key
2. server.pem
3. agent.pem
4. client.pem

TLS

Client

1. client.key
2. client.pem

4.2 TLS config - Spring Boot

```yaml
ssl:
  key-store: classpath:serverKeyStore.p12
  key-store-password: ${CODE10_SIEM_CERT_SERVER_KEY_PASS}
  key-password: ${CODE10_SIEM_CERT_SERVER_KEY_PASS}
  trust-store: classpath:serverTrustStore.p12
  trust-store-password: ${CODE10_SIEM_CERT_SERVER_KEY_PASS}
  client-auth: want # Not supported in Angular so we can't use 'need'
  trust-store-type: PKCS12
  key-store-type: PKCS12
  protocol: TLSv1.2
compression:
  enabled: false # CRIME attack prevention
```

4.3 TLS config - OpenSSL

# 1. Generate server (CA) key and certificate.

```
openssl genrsa -out server.key 2048

openssl req -x509 -new -key server.key -out server.pem -sha256 -days 3650
-passout env:CODE10_SIEM_CERT_SERVER_KEY_PASS -subj
"/C=RS/ST=./L=Novi Sad/O=code10ftn/OU=SIEM/CN=localhost"
```

4.3 TLS config - OpenSSL

```
# 2. Generate agent key and certificate signed by our CA.

openssl genrsa -out agent.key 2048

openssl req -new -key agent.key -out agent.csr -sha256 -days 1095 -passout
env:CODE10_SIEM_CERT_CLIENT_KEY_PASS -subj "/C=RS/ST=./L=Novi
Sad/O=code10ftn/OU=SIEM/CN=Agent"

openssl x509 -req -in agent.csr -CA server.pem -CAkey server.key
-CAcreateserial -out agent.pem
```

4.3 TLS config - OpenSSL

# 3. Generate client key and certificate signed by our CA.

```
openssl genrsa -out client.key 2048
```

```
openssl req -new -key client.key -out client.csr -sha256 -days 1095 -passout env:CODE10_SIEM_CERT_CLIENT_KEY_PASS -subj "/C=RS/ST=./L=Novi Sad/O=code10ftn/OU=SIEM/CN=Client"
```

```
openssl x509 -req -in client.csr -CA server.pem -CAkey server.key -CAserial server.srl -out client.pem
```

4.3 TLS config - OpenSSL

# 4. Export server's key and certificate to a keystore.

```
openssl pkcs12 -export -out serverKeyStore.p12 -inkey server.key -in server.pem
-passout env:CODE10_SIEM_CERT_SERVER_KEY_PASS
```

# 5. Export agent's key and certificate to a keystore.

```
openssl pkcs12 -export -out agentKeyStore.p12 -inkey agent.key -in agent.pem
-passout env:CODE10_SIEM_CERT_CLIENT_KEY_PASS
```

4.3 TLS config - OpenSSL

```
# 6. Export server, agent and client certificates to a truststore (required for mutual authentication).

keytool -import -storetype PKCS12 -noprompt -trustcacerts -alias serverCert -file server.pem -keystore serverTrustStore.p12 -storepass $env:CODE10_SIEM_CERT_SERVER_KEY_PASS

keytool -import -storetype PKCS12 -noprompt -trustcacerts -alias agentCert -file agent.pem -keystore serverTrustStore.p12 -storepass $env:CODE10_SIEM_CERT_SERVER_KEY_PASS

keytool -import -storetype PKCS12 -noprompt -trustcacerts -alias clientCert -file client.pem -keystore serverTrustStore.p12 -storepass $env:CODE10_SIEM_CERT_SERVER_KEY_PASS
```

4.3 TLS config - OpenSSL

```
# 7. Delete unnecessary files.
Remove-Item .\agent.csr
Remove-Item .\agent.key
Remove-Item .\agent.pem
Remove-Item .\client.csr
Remove-Item .\server.key
Remove-Item .\server.srl

# 8. Distribute files.
Move-Item -Path .\serverKeyStore.p12 -Destination ..\SiemCore\src\main\resources
Move-Item -Path .\serverTrustStore.p12 -Destination ..\SiemCore\src\main\resources
Move-Item -Path .\agentKeyStore.p12 -Destination ..\SiemAgent\resource
Move-Item -Path .\server.pem -Destination ..\SiemAgent\resources -Force
Move-Item -Path .\client.key -Destination ..\SiemClient\src\assets\ssl
Move-Item -Path .\client.pem -Destination ..\SiemClient\src\assets\ssl
```

The end.