SSL securing Oracle DB - Goodbye passwords

Harris Baskaran - hpb@google.com

How I stopped worrying and started loving database security

Only 4.2 % data was encrypted

1.4 Billion records

59% identity data

Up 86% since 2015

Source: gemalto 2016 security breaches report

Scary Database Security questions

- Who has access to your database?
- How many people have access to an account's password?
- How often do you rotate your passwords? Do you only rotate because you are under SOX?
- Does your audit trail actually show who can login to your database or is it filled with shared account names?
- If someone intercepts my TNS session can they see my data?

About me

- Engineer for life!
- Security buff
- Been with Google for 3 years

- https://www.linkedin.com/in/harrisbaskaran
- http://dontbouncethatdb.blogspot.com/
- hpb@google.com
- @harry2040

Requirements first!

If you give the command **"SECURE THE BUILDING"**, here is what the different services would do:

The **NAVY** would turn out the lights and lock the doors.

The **ARMY** would surround the building with defensive fortifications, tanks and concertina wire.

The **MARINE CORPS** would assault the building, using overlapping fields of fire from all appropriate points on the perimeter.

The **AIR FORCE** would take out a three-year lease with an option to buy the building.

Our Requirements for Databases

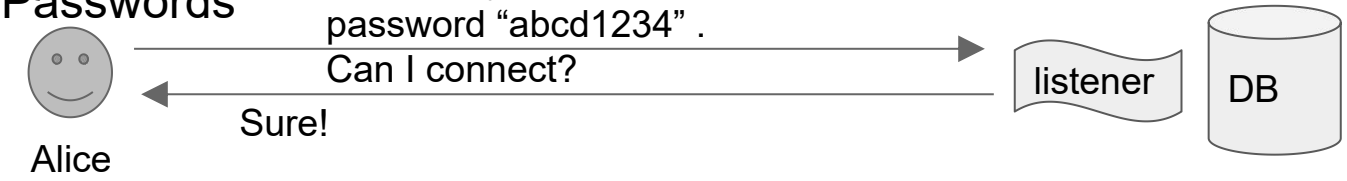
1. Improve Authentication to something stronger than password, preferably two factor authentication.
2. Authorization should be tightly controlled, changes should be reviewed.
3. Encryption of all data in transit.
4. Reduce operational overhead of managing passwords

Session overview

- Problem space
- What is SSL/TLS?
- Killing 3 birds with one stone.
  - Authentication
  - Authorization
  - Encryption
- 2 Factor authentication for Oracle
- How can I make this work for my organization?

Section 1: Problem Space

Challenges with Passwords




```
20:00:13.843648 IP (tos 0x0, ttl 64, id 10152, offset 0, flags [DF], proto TCP (6), length 1253)
    myclient.mycompany.com.32922 > myserver.mycompany.com.6021: Flags [P.], cksum 0x6ac6 (incorrect -> 0xd63a), seq 2995239108:2995240321, ack
1675012994, win 245, length 1213
        0x0000:  4500 04e5 27a8 4000 4006 a87c 6460 de2d  E...'.@.@..|d`.-
        0x0010:  ac19 7747 809a 1785 b287 b8c4 63d6 ab82  ..wG........c...
        0x0020:  5018 00f5 6ac6 0000 04bd 0000 0600 0000  P...j...........
        0x0030:  0000 0373 03fe ffff ffff ffff ff1b 0000  ...s............
        0x0040:  0001 0100 00fe ffff ffff ffff ff13 0000  ................
        0x0050:  0000 0000 00fe ffff ffff ffff fffe ffff  ................
        0x0060:  ffff ffff ff09 6a61 6d65 7362 6f6e 6424  ......jamesbond$
        0x0070:  0000 000c 4155 5448 5f53 4553 534b 4559  ....AUTH_SESSKEY
        0x0080:  2001 0000 6035 3745 3245 3634 4134 4133  ....`57E2E64A4A3
        0x0090:  3342 4543 3636 4641 4644 4233 3332 4137  3BEC66FAFDB332A7
        0x00a0:  4231 4434 3634 3035 3146 3032 3131 4639  B1D464051F0211F9
        0x00b0:  4142 4544 3144 4338 3342 4638 3443 3339  ABED1DC83BF84C39
        0x00c0:  4637 4239 3432 3341 4238 4545 4242 3633  F7B9423AB8EEBB63
        0x00d0:  3433 3533 4634 3541 4535 3646 3836 4531  4353F45AE56F86E1
        0x00e0:  3634 4342 3301 0000 0027 0000 000d 4155  64CB3....'....AU
        0x00f0:  5448 5f50 4153 5357 4f52 44c0 0000 0040  TH_PASSWORD....@
        0x0100:  3134 3839 3839 3234 3834 3639 3039 3443  1489892484690 94C
        0x0110:  4235 4239 4635 3935 4635 4331 4542 3944  B5B9F595F5C1EB9D
        0x0120:  4637 4332 3332 4232 4538 3536 3631 4444  F7C232B2E85661DD
        0x0130:  3538 4642 3033 4439 3137 4542 4430 3735  58FB03D917EBD075
        0x0140:  0000 0000 1800 0000 0841 5554 485f 5254  .........AUTH_RT
        0x0150:  5412 0000 0006 3132 3038 3336 0000 0000  T.....120836....
        0x0160:  2700 0000 0d41 5554 485f 434c 4e54 5f4d  '....AUTH_CLNT_M
        0x0170:  454d 0c00 0000 0434 3039 3600 0000 0027  EM.....4096....'
        0x0180:  0000 000d 4155 5448 5f54 4552 4d49 4e41  ....AUTH_TERMINA
        0x0190:  4c12 0000 0006 7074 732f 3137 0000 0000  L.....pts/17....
        0x01a0:  2d00 0000 0f41 5554 485f 5052 4f47 5241  -....AUTH_PROGRA
        0x01b0:  4d5f 4e4d 8a00 0000 2e73 716c 706c 7573  M_NM.....sqlplus
```

Problems with passwords

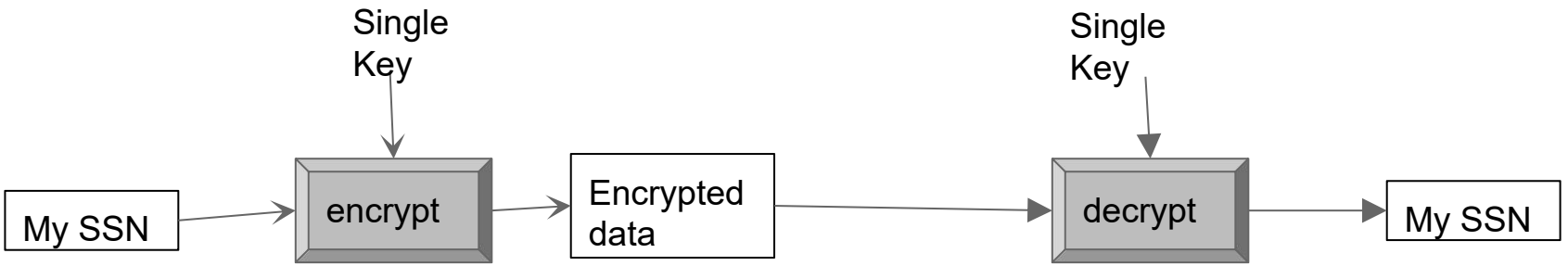
- Unless you have all 12c clients and all 12c database password are still stored in not so strong hashes
- 11g - SHA1, 12c - SHA256+PBKDF2, APEX - MD5
- Remember CVE-2012-3137?
- ALLOWED_LOGON_VERSION
- When is the last time you rotated your password.
- How many people know an account’s password?

No Encryption? What is the hacker seeing?

```
tcpdump: listening on em1, link-type EN10MB (Ethernet), capture size 65535 bytes
20:08:25.256350 IP (tos 0x0, ttl 64, id 13580, offset 0, flags [DF], proto TCP (6), length 338)
    myclient.mycompany.com.33036 > myserver.mycompany.com.1521: Flags [P.], cksum 0x6733 (incorrect -> 0xd733), seq 4044042160:4044042458, ack 2893510618, win
502, length 298
        0x0000:  4500 0152 350c 4000 4006 9eab 6460 de2d  E..R5.@.@...d`.-
        0x0010:  ac19 7747 810c 1785 f10b 2fb0 ac77 77da  ..wG....../..ww.
        0x0020:  5018 01f6 6733 0000 012a 0000 0600 0000  P...g3...*......
        0x0030:  0000 1169 17fe ffff ffff ffff ff01 0000  ...i............
        0x0040:  0000 0000 0003 0000 0003 5e18 6180 0000  ..........^.a...
        0x0050:  0000 0000 feff ffff ffff ffff 6f00 0000  ............o...
        0x0060:  feff ffff ffff ffff 0d00 0000 feff ffff  ................
        0x0070:  ffff ffff feff ffff ffff ffff 0000 0000  ................
        0x0080:  0100 0000 0000 0000 0000 0000 0000 0000  ................
        0x0090:  0000 0000 0000 0000 0000 0000 feff ffff  ................
        0x00a0:  ffff ffff 0000 0000 0000 0000 feff ffff  ................
        0x00b0:  ffff ffff feff ffff ffff ffff feff ffff  ................
        0x00c0:  ffff ffff 0000 0000 0000 0000 feff ffff  ................
        0x00d0:  ffff ffff feff ffff ffff ffff 0000 0000  ................
        0x00e0:  0000 0000 0000 0000 0000 0000 0000 0000  ................
        0x00f0:  0000 0000 0000 0000 2573 656c 6563 7420  ........%select.
        0x0100:  6372 6564 6974 5f63 6172 6420 6672 6f6d  credit_card.from
        0x0110:  2062 616e 6b2e 6163 636f 756e 7473 0100  .bank.accounts..
        0x0120:  0000 0000 0000 0000 0000 0000 0000 0000  ................
        0x0130:  0000 0000 0000 0000 0000 0100 0000 0000  ................
        0x0140:  0000 0080 0000 0000 0000 0000 0000 0000  ................
        0x0150:  0000                                     ..
20:08:25.294811 IP (tos 0x0, ttl 64, id 13581, offset 0, flags [DF], proto TCP (6), length 40)
```

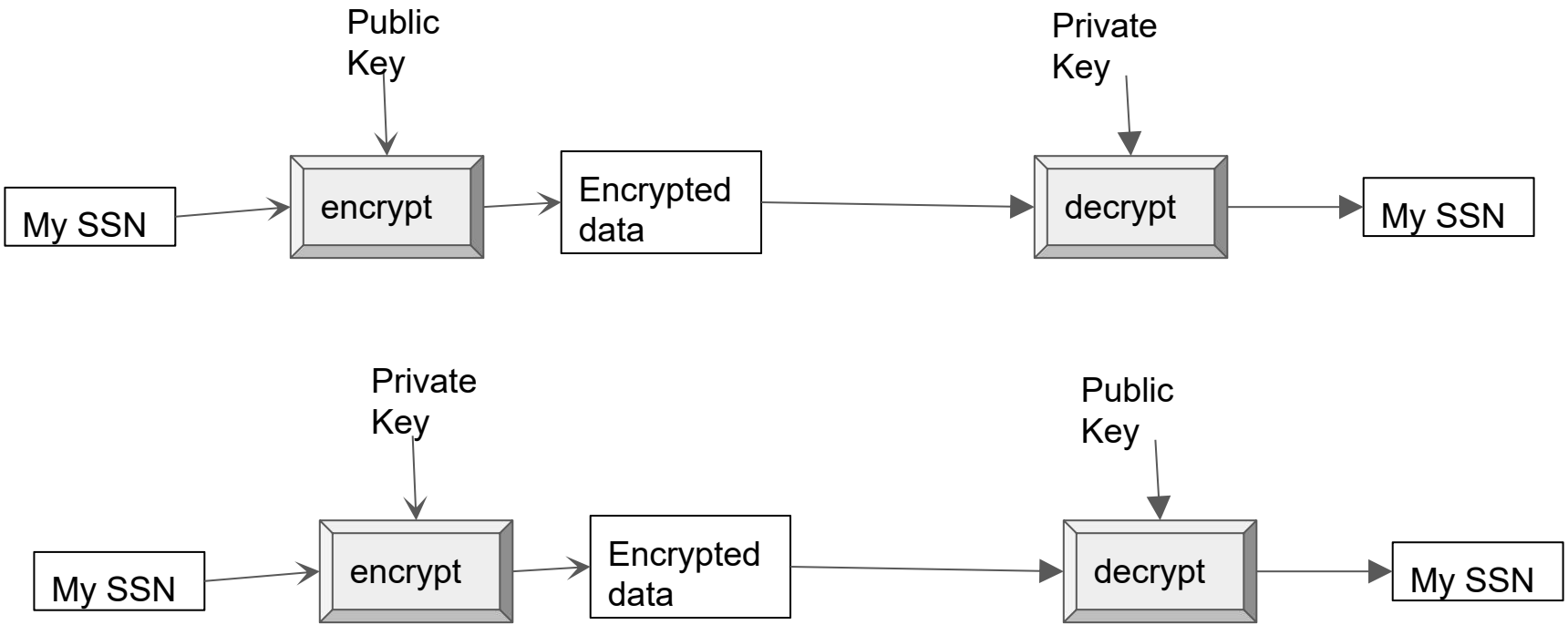
Section 2: SSL and TLS; back to basics

Back to Basics: Symmetric Key Encryption

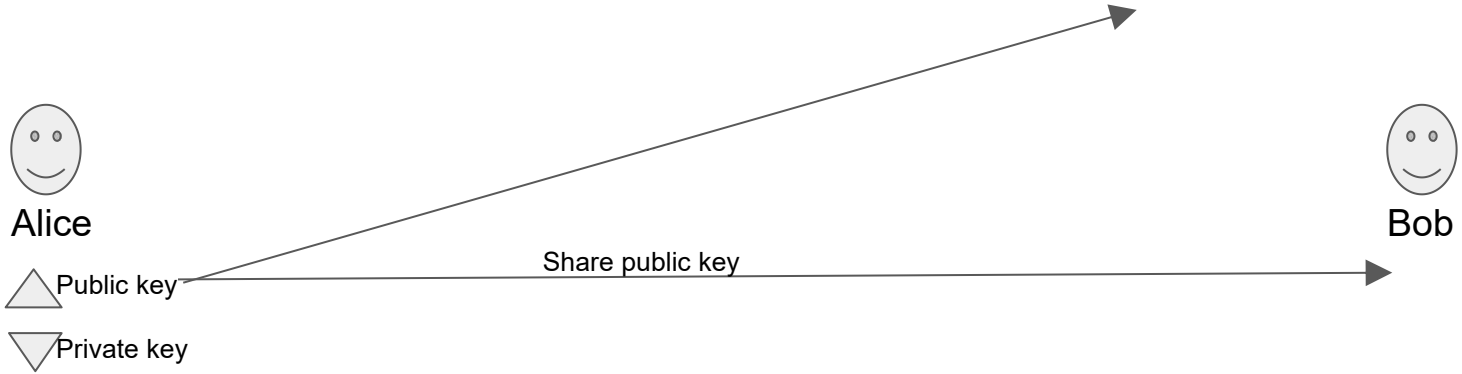


Key Pair - Asymmetric Encryption

A key pair is private key and public key setup.



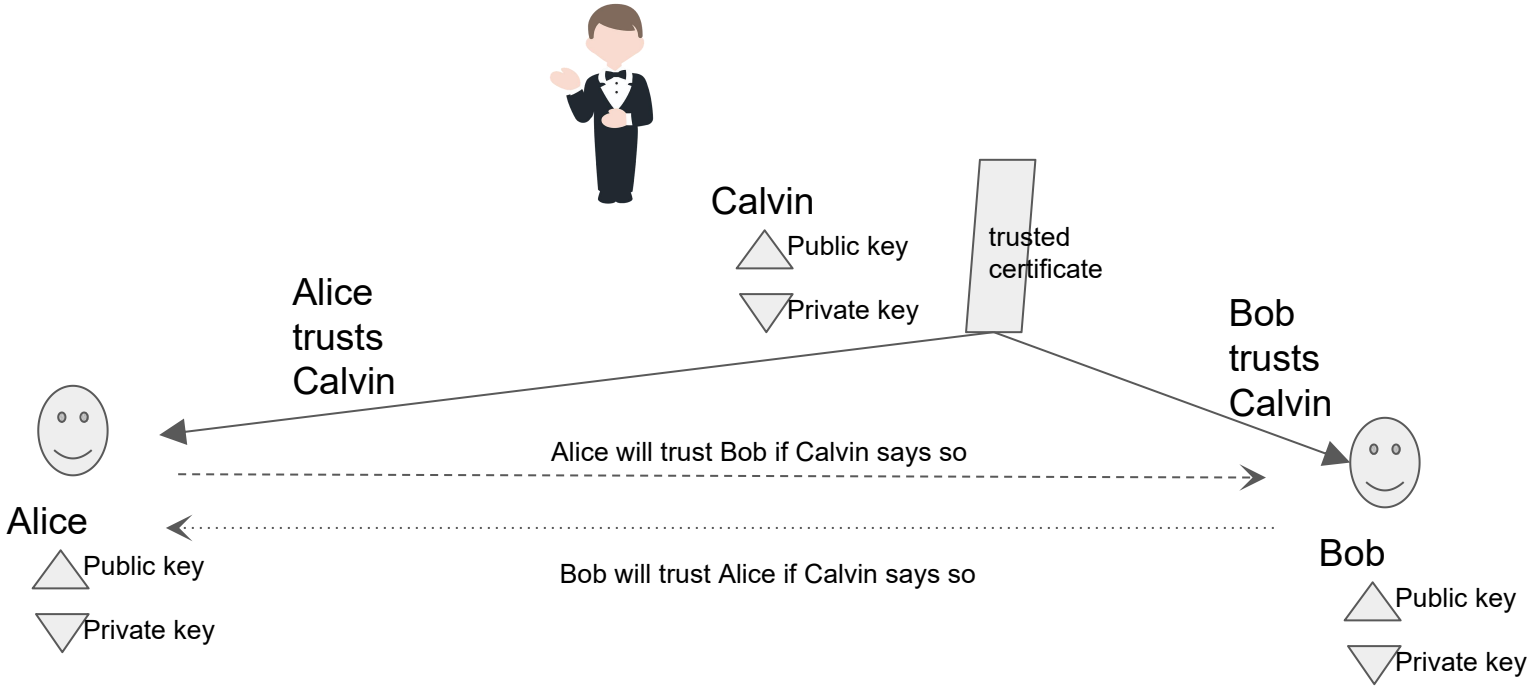
Handshake with just keys?



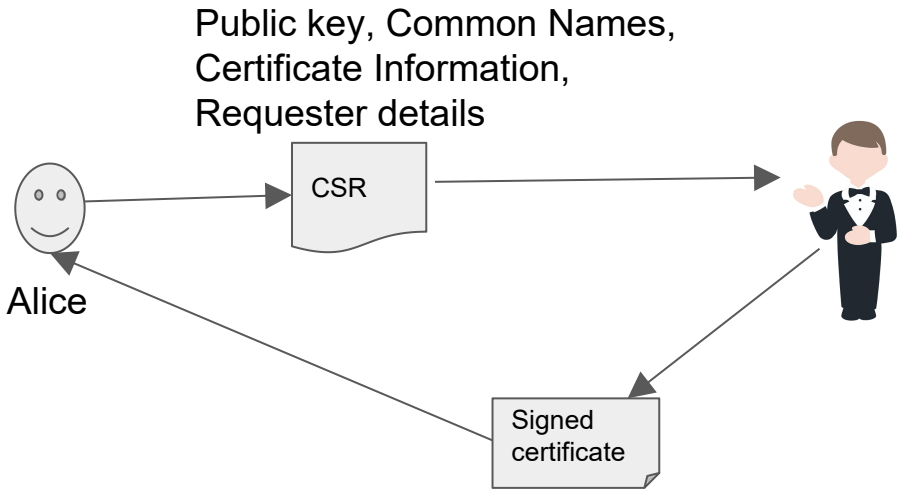
1. Alice encrypts using private key
2. Bob who has a copy of Alice's public key can decrypt.
3. But so can anyone with Alice's public key.

1. Bob encrypts using Alice's public key
2. Only Alice can decrypt as private key resides with Alice
3. But how can Alice trust the message is coming from Bob? Anyone with Alice's public key can send the message

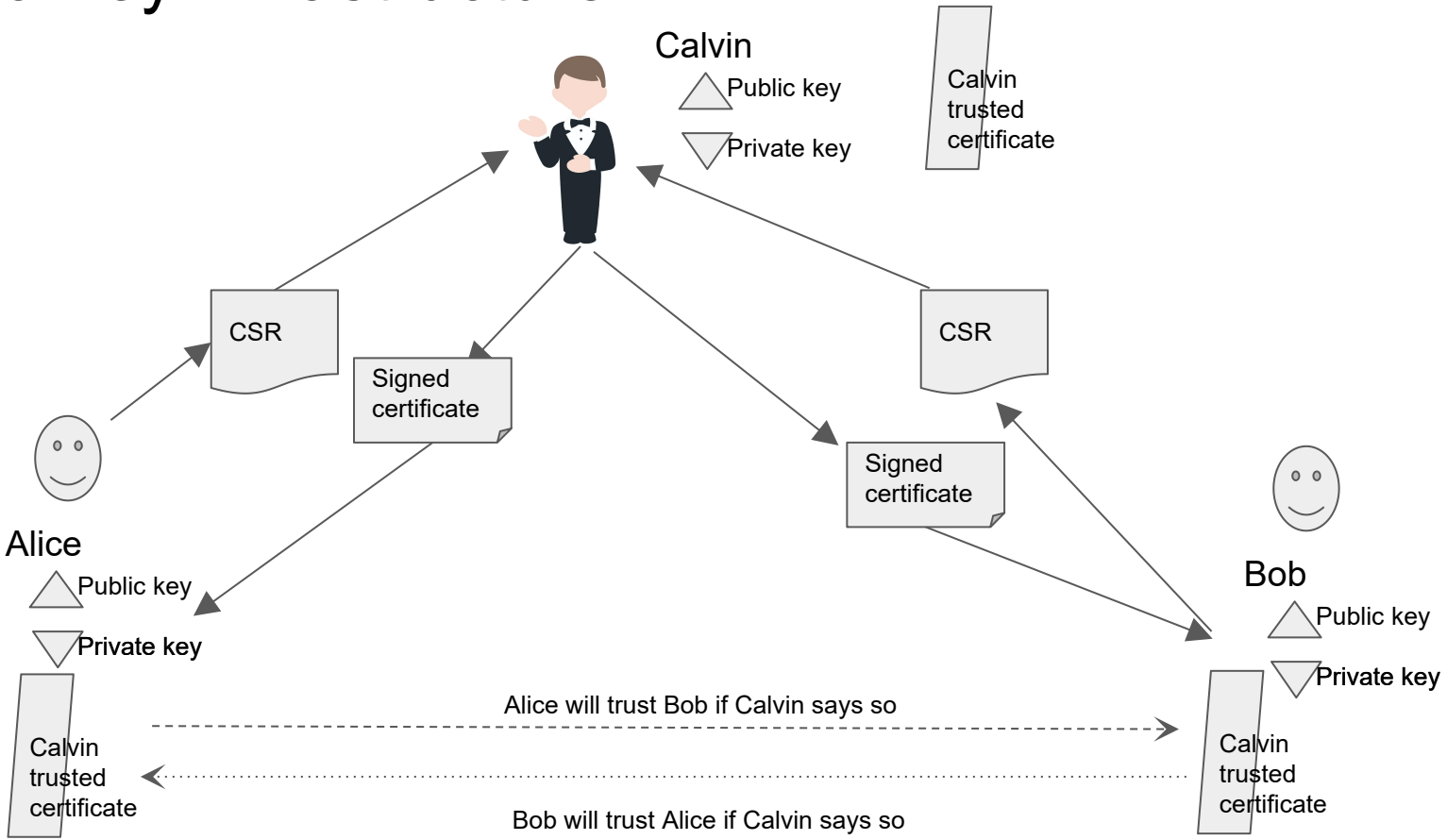
Certificate Authority



CSR - Certificate Signing Request



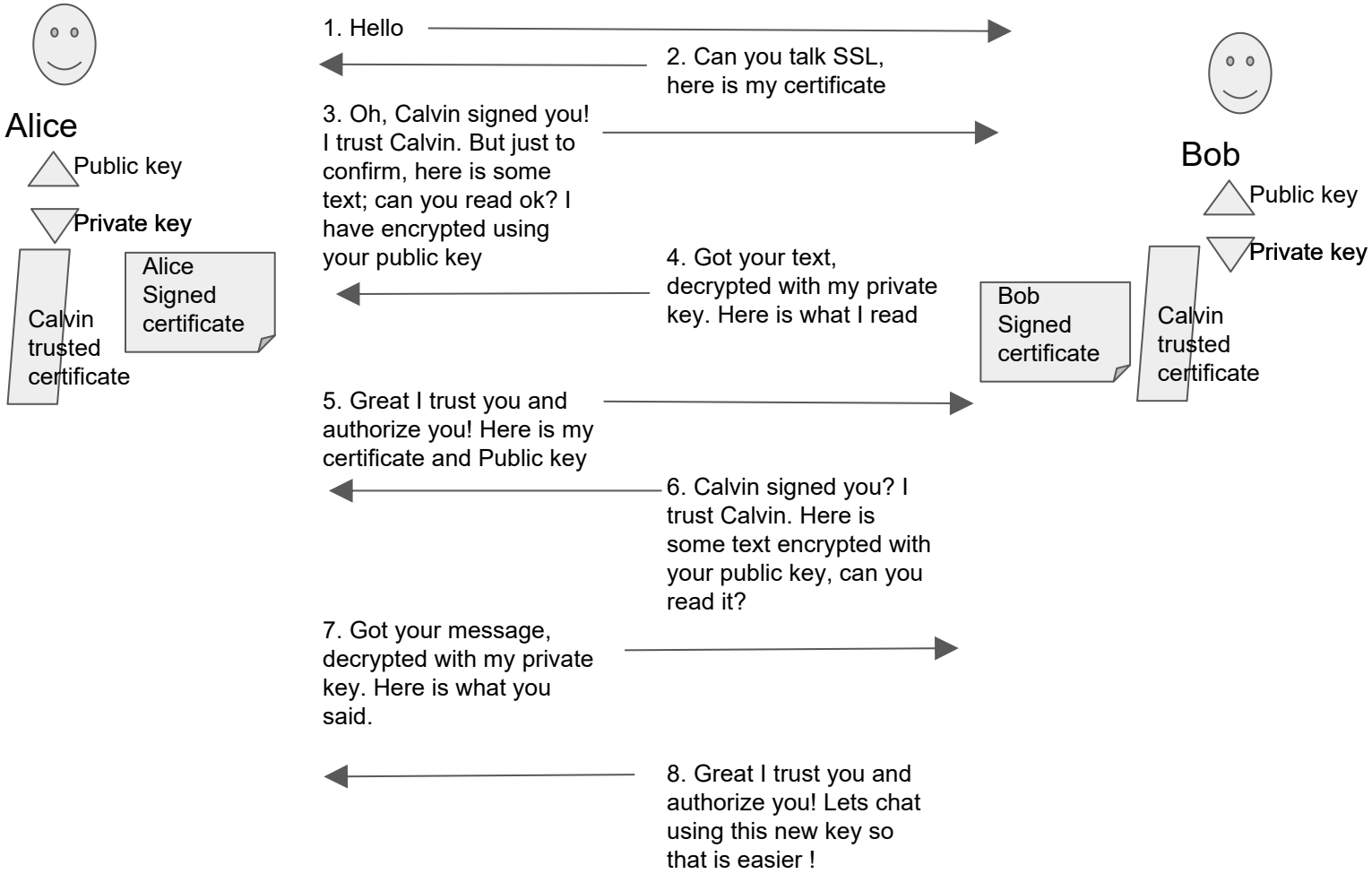
Public Key Infrastructure



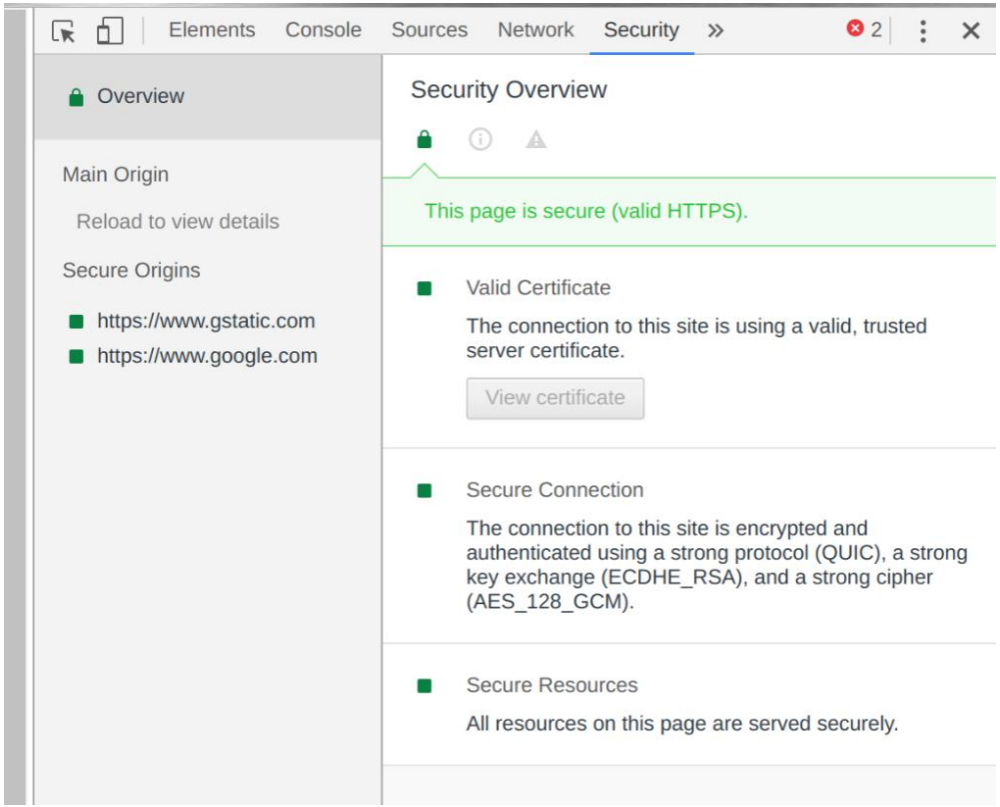
x509

The structure of an X.509 v3 digital certificate is as follows:

- Certificate
  - Version Number
  - Serial Number
  - Signature Algorithm ID
  - Issuer Name
  - Validity period
    - **Not Before**
    - **Not After**
  - **Subject name- CN, DN**


Alice
Public key
Private key
Calvin trusted certificate
Alice Signed certificate
1. Hello
2. Can you talk SSL, here is my certificate
3. Oh, Calvin signed you! I trust Calvin. But just to confirm, here is some text; can you read ok? I have encrypted using your public key
4. Got your text, decrypted with my private key. Here is what I read
5. Great I trust you and authorize you! Here is my certificate and Public key
6. Calvin signed you? I trust Calvin. Here is some text encrypted with your public key, can you read it?
7. Got your message, decrypted with my private key. Here is what you said.
8. Great I trust you and authorize you! Lets chat using this new key so that is easier !
Bob
Public key
Private key
Bob Signed certificate
Calvin trusted certificate

Same thing in browsers ?



SSL / TLS and its versions

SSL 1.0 - DO NOT USE !!!

SSL 2.0 - DO NOT USE !!!

SSL 3.0 - DO NOT USE !!!

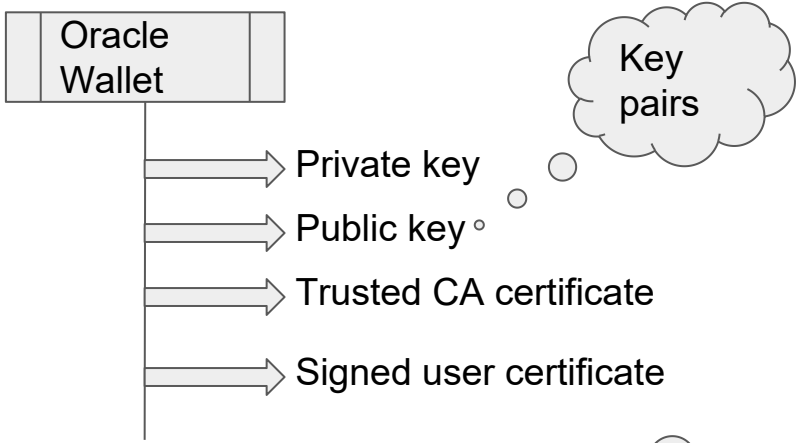
TLS 1.0 - DO NOT USE !!!

TLS 1.1 - Oracle 11g - SSL_RSA_WITH_AES_256_CBC_SHA, get out of here soon!

TLS 1.2 - Oracle 12c only - SSL_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384, SSL_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

TLS 1.3 - Release April 2017

Oracle world



Key pairs

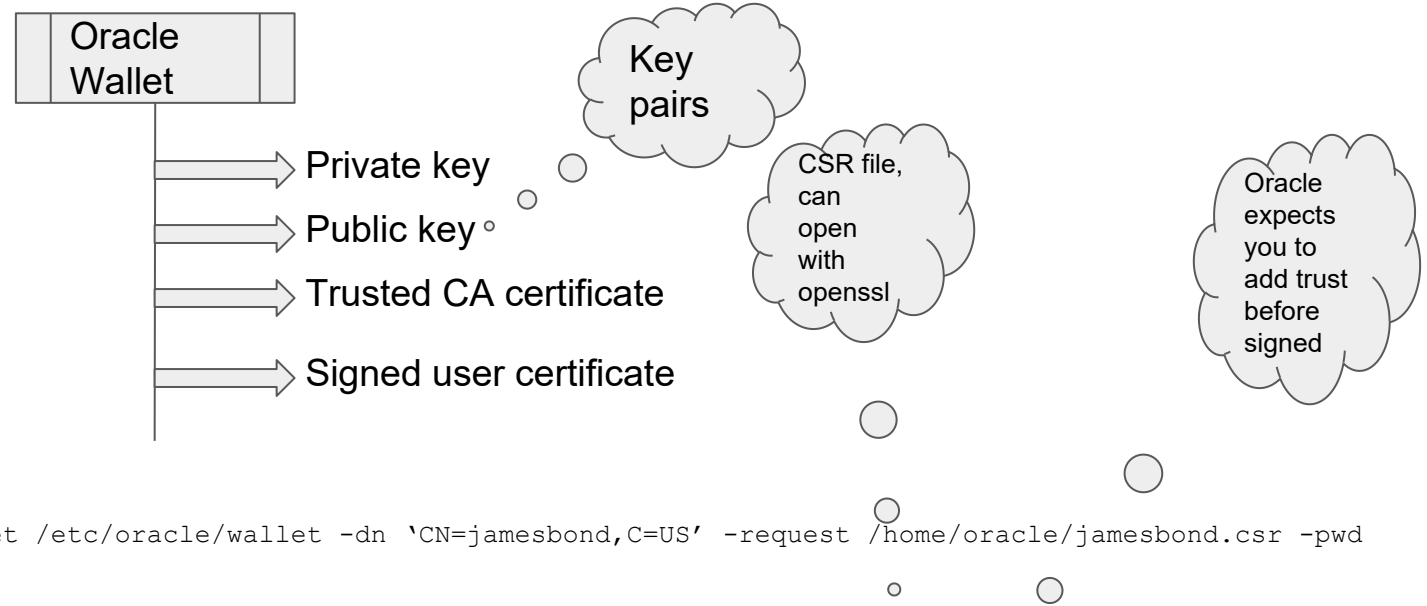
Password max length 10 chars, use a random generator. Keep password in memory and destroy to avoid mods later

Bigger the keysize, better security

```
orapki wallet create -wallet /etc/oracle/wallet -pwd strongPass -auto_login
```

```
orapki wallet add -wallet /etc/oracle/wallet -dn 'CN=jamesbond,C=US' -keysize 2048 -pwd strongPass
```

Oracle world

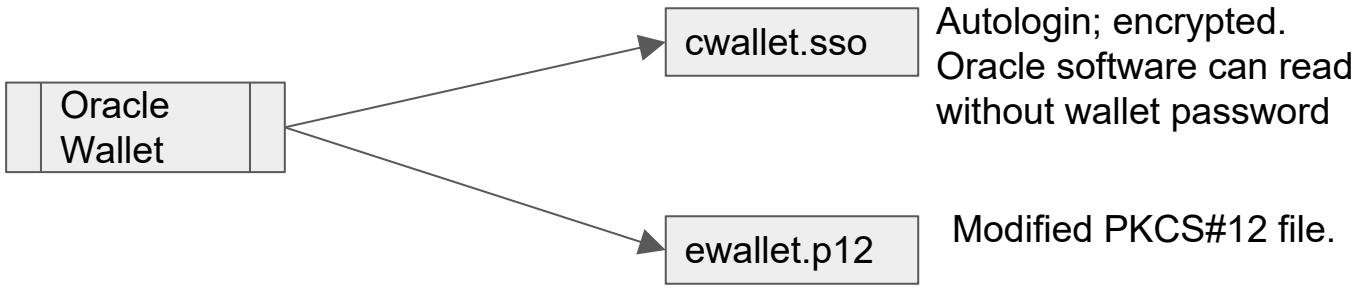



```
orapki wallet export -wallet /etc/oracle/wallet -dn 'CN=jamesbond,C=US' -request /home/oracle/jamesbond.csr -pwd
strongPass
```

```
orapki wallet add -wallet /etc/oracle/wallet -trusted_cert -cert /etc/oracle/myinternalCA.crt -pwd strongPass
```

```
orapki wallet add -wallet /etc/oracle/wallet -user_cert -cert /home/oracle/jamesbond.crt -pwd strongPass
```

Wallet files



Section 3: Solving Authentication, Authorization and Encryption

Multiple Cert types

Internal CA
ca.mycompany.com

CN=mydb.mycompany.com
CSR

Host
/DB

host_cert trusted cert

Signed cert - host leaf

user_cert trusted cert

host_cert type

CSR
CN=myuser

user_cert trusted cert

Signed cert - user leaf

host_cert trusted cert

User

user_cert type

Certificates

User

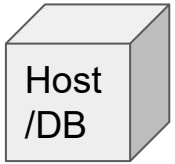
user_cert root

Signed cert - user

```
'CN=jamesbond,OU=user_cert,O=MyCompany,L=New York,ST=NY,C=US';"
```

host_cert root

- x509 cert
- cert type user_cert
- valid 24 hours
- issued to CN = LDAP username



host_cert root

Signed cert - host

```
'CN=mydb.mycompany.com,OU=host_cert,O=MyCompany,L=New York,ST=NY,C=US';"
```

user_cert root

- x509 cert
- cert type host_cert
- valid 90 days
- issued to CN = servername

Changes inside Database

```
CREATE USER JAMESBOND IDENTIFIED EXTERNALLY AS
'CN=jamesbond,OU=user_cert,O=MyCompany,L=New
York,ST=NY,C=US';


GRANT CONNECT, CREATE TABLE to JAMESBOND;
GRANT UNLIMITED TABLESPACE to JAMESBOND;
```

Oracle net changes on server

```
SQLNET.AUTHENTICATION_SERVICES=(TCPS, BEQ)
SSL_CLIENT_AUTHENTICATION=TRUE
SSL_VERSION=1.2
WALLET_LOCATION = (SOURCE=
                     (METHOD = FILE)
                       (METHOD_DATA =
                         (DIRECTORY=/etc/oracle/wallet)
                       )
                   )
SSL_CIPHER_SUITES = (SSL_RSA_WITH_AES_256_CBC_SHA)
```

```
SID_LIST_LISTENER_1521 =
  (SID_LIST =
    (SID_DESC =
      (GLOBAL_DBNAME = MYORADB)
      (ORACLE_HOME = /u1/app/oracle/product/11.2.0.4.0/db)
      (SID_NAME = MYORADB)
    )
  )
```

```
LISTENER_1521 =
  (DESCRIPTION =
     (ADDRESS = (PROTOCOL = IPC)(KEY = REGLSNR_1521))
     (ADDRESS = (PROTOCOL = TCPS)(HOST =
mydbservermycompany.com)(PORT=1521))
  )
```

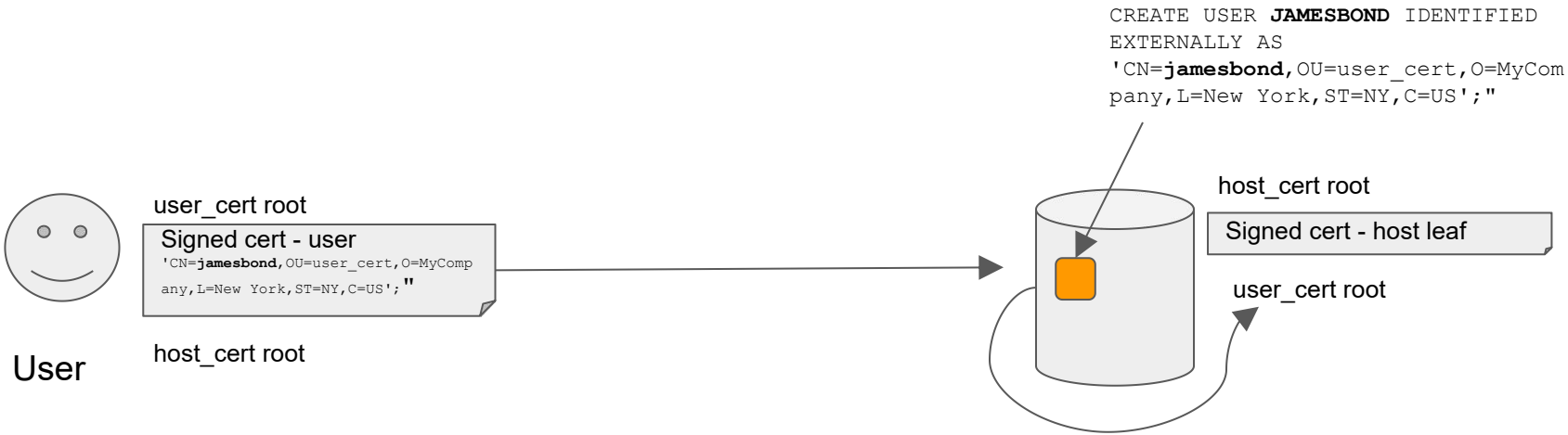
```
ADR_BASE_LISTENER_1521 = /u1/app/oracle
SECURE_REGISTER_LISTENER_1521 = (IPC)
SSL_CLIENT_AUTHENTICATION=FALSE
SSL_VERSION=1.2
WALLET_LOCATION = (SOURCE=
                     (METHOD = FILE)
                       (METHOD_DATA =
                         (DIRECTORY=/etc/oracle/wallet)
                       )
                   )
```

User TNS changes

```
### MYDB ###
MYDB =
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCPS)(HOST = mydb.mycompany.com)(PORT = 1521))
      (CONNECT_DATA =
        (SERVER = DEDICATED)
        (SERVICE_NAME = MYDB)
      )
     (SECURITY=(SSL_SERVER_CERT_DN="CN=mydb.mycompany.com,OU=host_cert,O=MyCompany,L=NewYork,ST=NY,C=US")))
```

```
WALLET_LOCATION = (SOURCE=
         (METHOD = FILE)
                     (METHOD_DATA =
                       (DIRECTORY=/home/jamesbond/wallet)
                     )
                  )
SSL_VERSION=1.2
SQLNET.AUTHENTICATION_SERVICES=(TCPS)
SSL_SERVER_DN_MATCH=TRUE
NAMES.DIRECTORY_PATH=(TNSNAMES,EZCONNECT)
SQLNET.AUTHENTICATION_REQUIRED=TRUE
```

DB server validating correct user

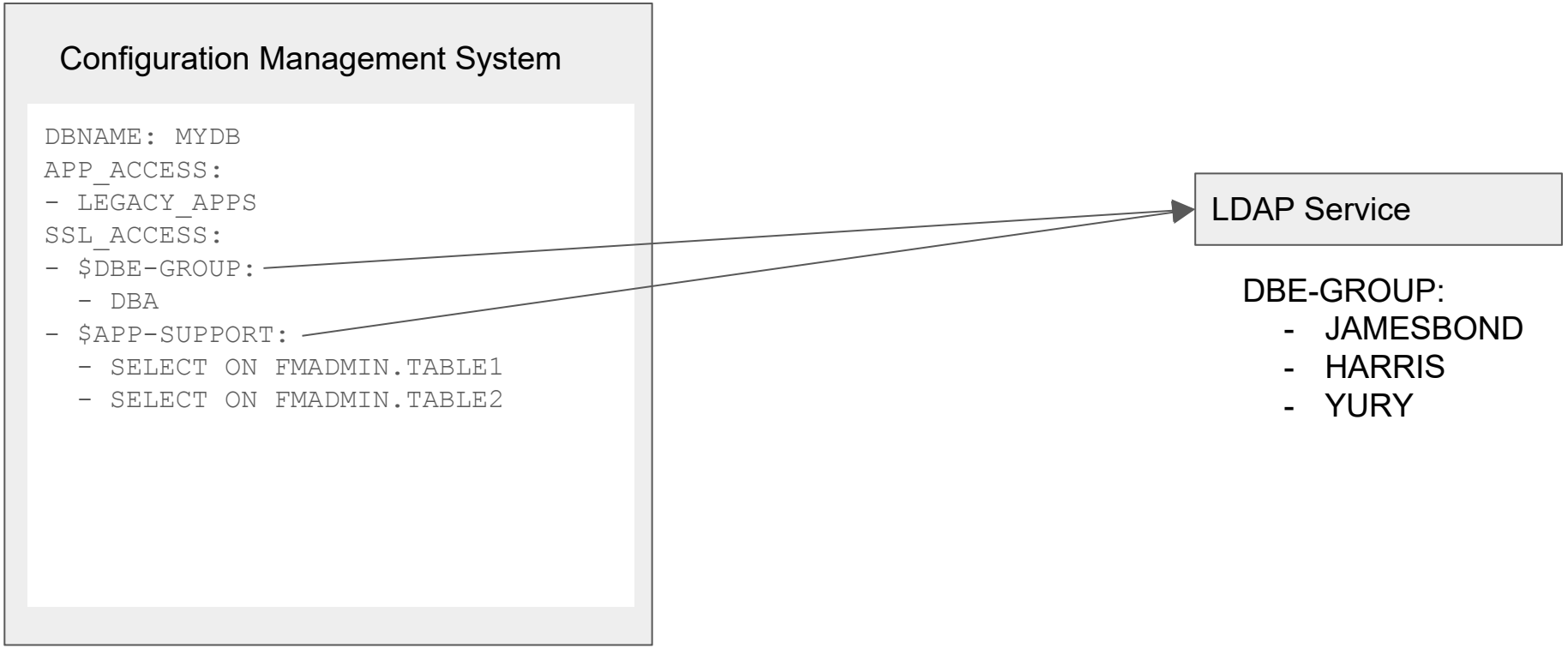


User validating connection to right server

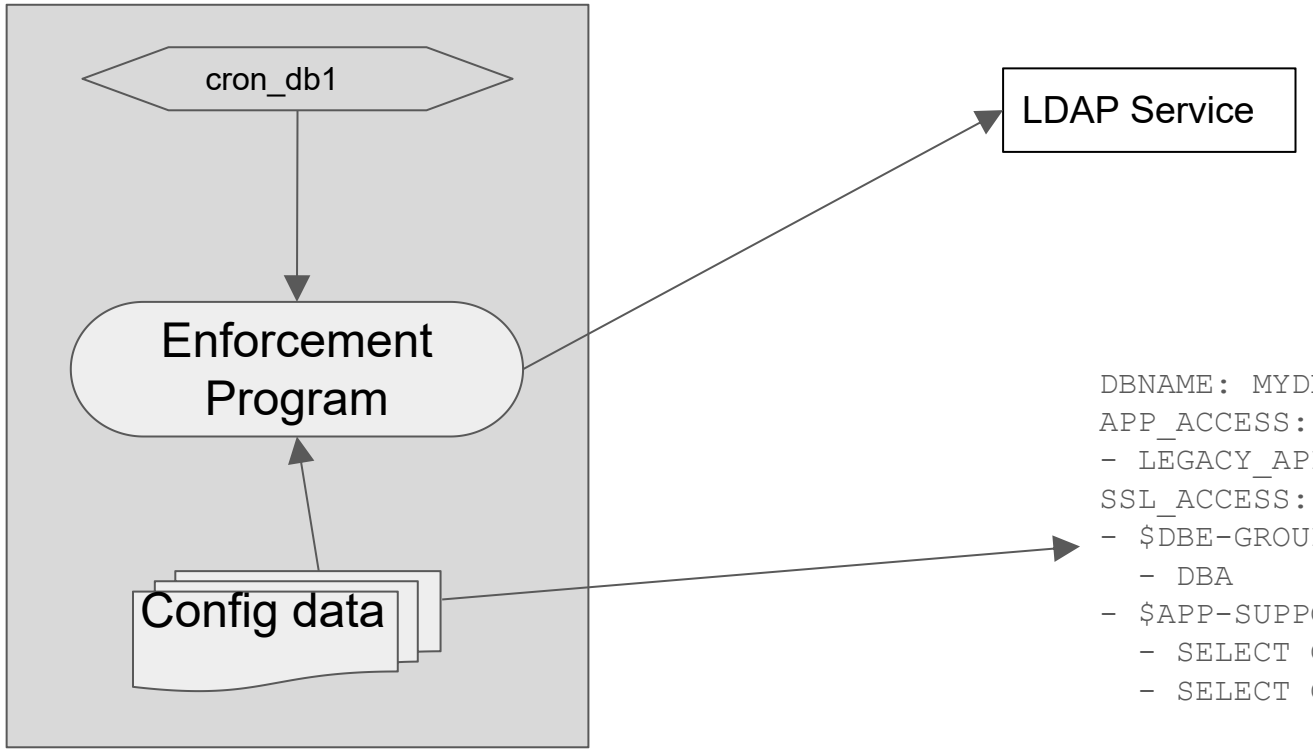
Authorization

Configuration Management System

```
DBNAME: MYDB
APP_ACCESS:
- LEGACY_APPS
SSL_ACCESS:
- $DBE-GROUP:
  - DBA
- $APP-SUPPORT:
  - SELECT ON FMADMIN.TABLE1
  - SELECT ON FMADMIN.TABLE2
```



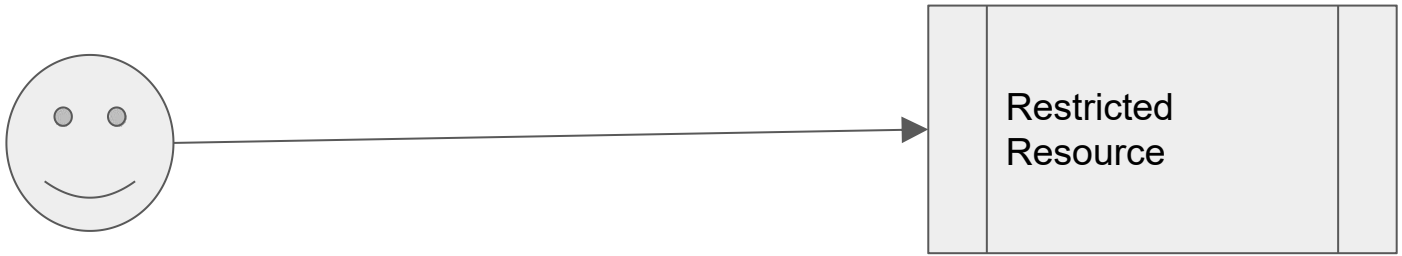
Enforcement program




```
DBNAME: MYDB
APP_ACCESS:
- LEGACY_APPS
SSL_ACCESS:
- $DBE-GROUP:
  - DBA
- $APP-SUPPORT:
  - SELECT ON FMADMIN.TABLE1
  - SELECT ON FMADMIN.TABLE2
```

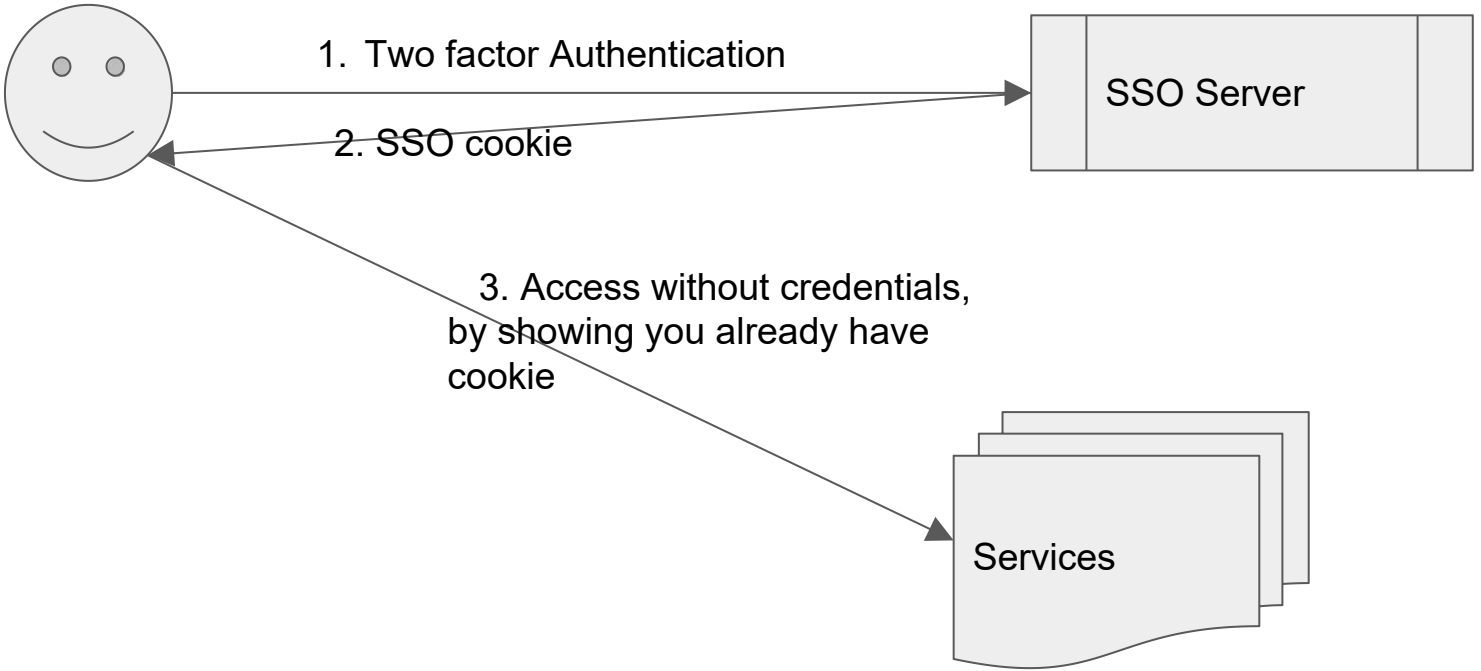
Section 4: 2 Factor Authentication to an Oracle DB

Two factor Authentication



1. Something you know (e.g password)
+
2. Something you have. (e.g. Token)

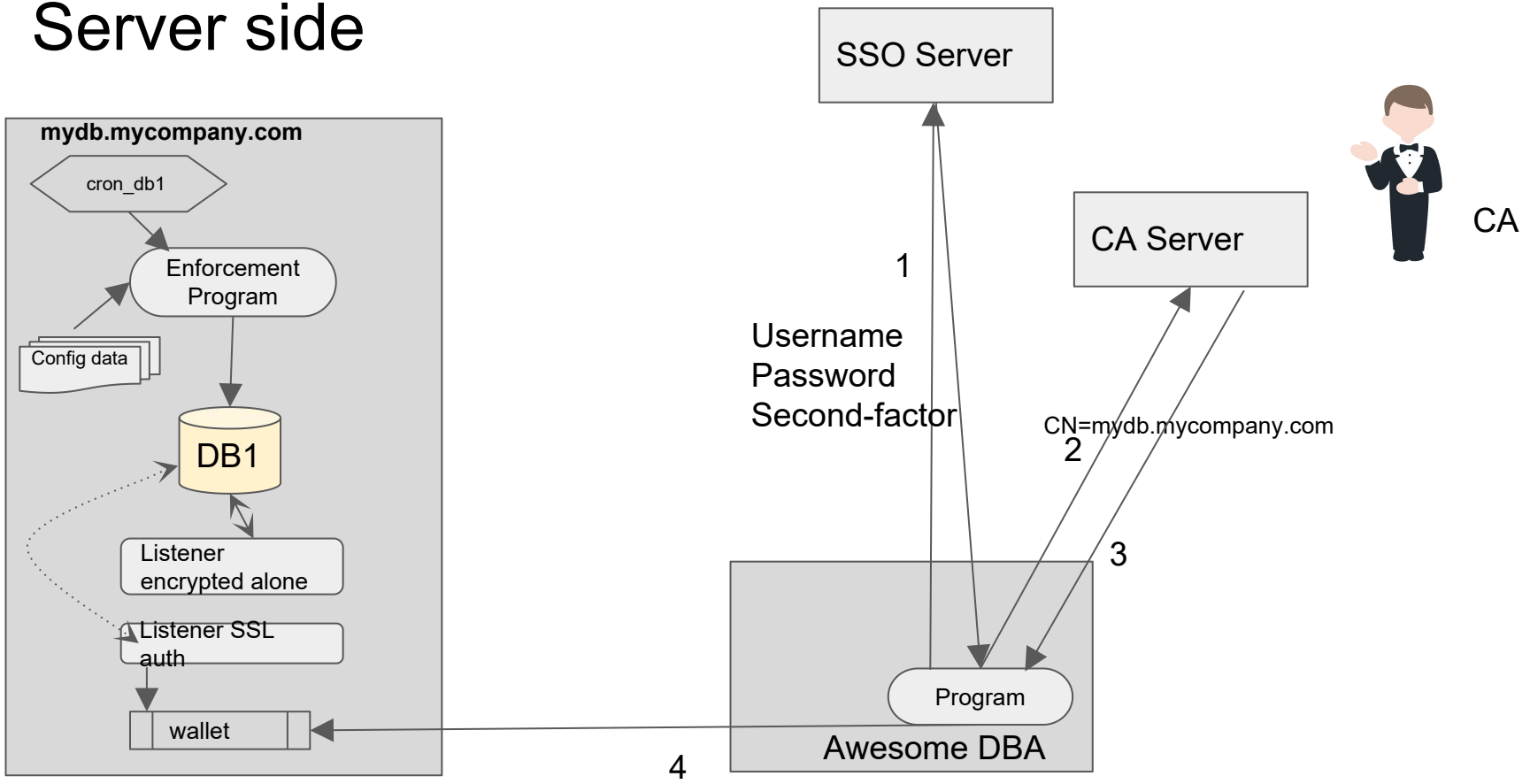
Single Sign On(SSO)



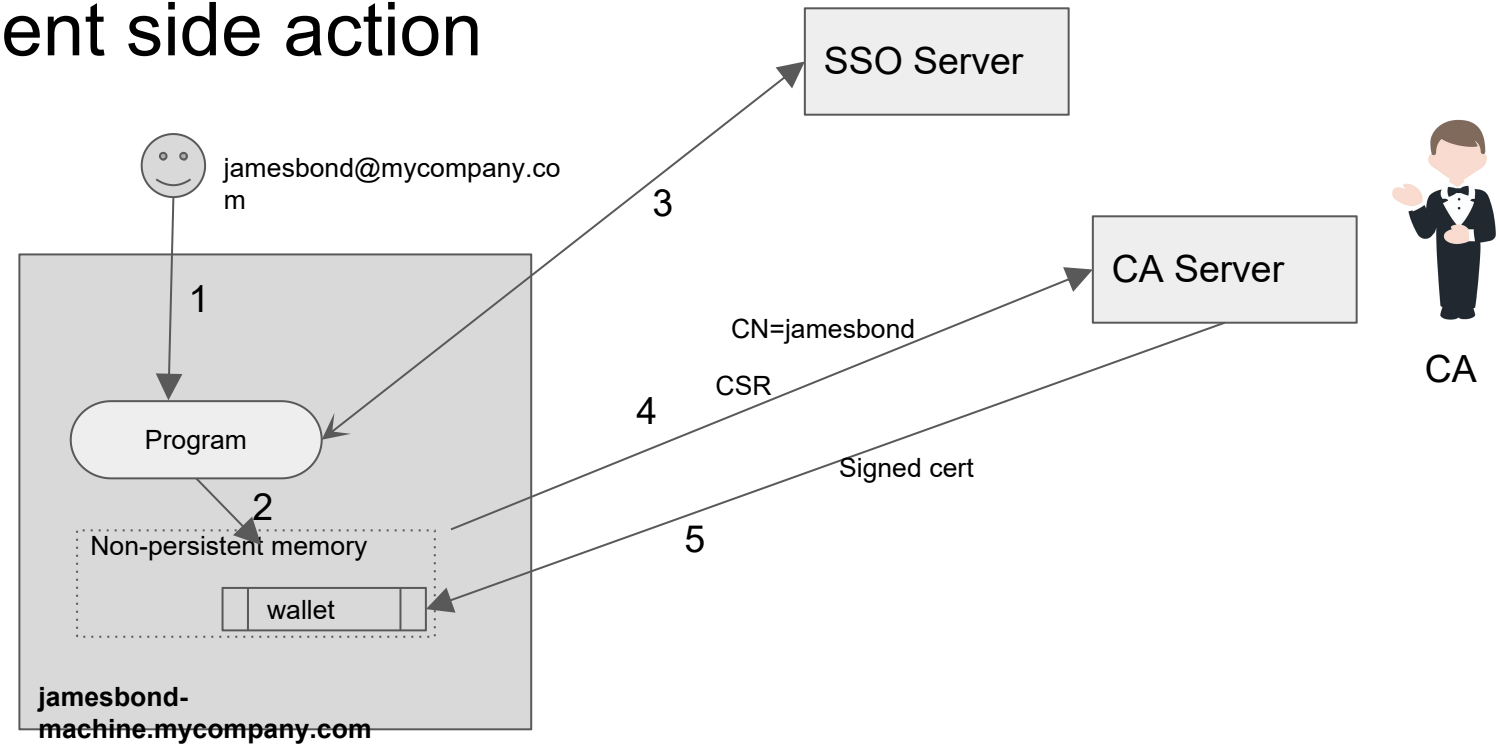
Credential Exchange

Getting one format of credential in exchange for another format.

Server side


SSO Server
CA Server
CA
mydb.mycompany.com
cron_db1
Enforcement Program
Config data
DB1
Listener encrypted alone
Listener SSL auth
wallet
1
Username
Password
Second-factor
CN=mydb.mycompany.com
2
3
4
Program
Awesome DBA

Client side action



Authentication !

```
jamesbond@jamesbond-machine.mycompany.com:~$ sqlplus /@MYDB
SQL*Plus: Release 12.1.0.2.0 Production on Sat Dec 3 19:24:30 2016
Copyright (c) 1982, 2014, Oracle.  All rights reserved.
Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.4.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options

SQL> select SYS_CONTEXT('USERENV','NETWORK_PROTOCOL') from dual;
SYS_CONTEXT('USERENV','NETWORK_PROTOCOL')
--------------------------------------------------------------------------------
tcps

SQL> select SYS_CONTEXT('USERENV','AUTHENTICATED_IDENTITY') from dual;

SYS_CONTEXT('USERENV','AUTHENTICATED_IDENTITY')
--------------------------------------------------------------------------------
CN=jamesbond,OU=user_cert,O=MyCompany,L=New York,ST=NY,C=US
```

Works with SQL Developer, JDBC, Cx_Oracle and other tools as well!

Connect through Proxy

```
ALTER USER JAMESBOND GRANT CONNECT THROUGH APP_USER;


jamesbond@jamesbond-machine.mycompany.com:~$ sqlplus [APP_USER]/@MYDB

SQL*Plus: Release 12.1.0.2.0 Production on Wed Mar 29 19:56:30 2017

Copyright (c) 1982, 2014, Oracle.  All rights reserved.

Last Successful login time: Thu Dec 22 2016 17:29:30 -07:00

Connected to:
Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production
With the Partitioning, OLAP, Advanced Analytics and Real Application Testing options

SQL> show user
USER is "APP_USER"
SQL>
```

Audit!

```
Jamesbond        JAMESBOND                jamesbond-machine.mycompany.com
        pts/17   03-DEC-16        100 LOGON
Authenticated by: NETWORK SERVICE;EXTERNAL NAME:
cn=jamesbond,ou=user_cert,o=MyCompany,l=New York,st=NY,c=US; Client address:
(ADDRESS=(PROTOCOL=tcps)(HOST=120.96.32.45)(PORT=38849))
   7736986          1           1          0 CREATE SESSION 03-DEC-16
07.24.30.779454 PM -08:00 0 31649            0000000000000000
        2689181429
```

Encryption !

```
root@jamesbond-machine:~# tcpdump -vvXS port 39038
tcpdump: listening on em1, link-type EN10MB (Ethernet), capture size 65535 bytes
19:39:52.961489 IP (tos 0x0, ttl 64, id 46626, offset 0, flags [DF], proto TCP (6), length 402)
    jamesbond-machine.mycompany.com.39038 > mydb.mycompany.com.6028: Flags [P.], cksum 0x6773 (incorrect -> 0x0056), seq
2930769214:2930769576, ack 1917441886, win 747, length 362
        0x0000:  4500 0192 b622 4000 4006 1d55 6460 de2d  E....."@.@..Ud`.-
        0x0010:  ac19 7747 987e 178c aeaf fd3e 7249 d75e  ..wG.~.....>rI.^
        0x0020:  5018 02eb 6773 0000 1703 0100 20c2 41fe  P...gs........A.
        0x0030:  001f acf9 c859 7c10 a630 ace3 28cc 62cd  .....Y|..0..(.b.
        0x0040:  513d bcf9 2968 e0fc 2d1d 167e 2617 0301  Q=..)h..-..~&...
        0x0050:  0140 795f 093e b274 519c 2504 63bb 96d0  .@y_.>.tQ.%.c...
        0x0060:  ab77 0b12 0a39 ba39 3beb 7718 4abb ccbf  .w...9.9;.w.J...
        0x0070:  a50f bad3 9e98 312a 4ed3 d0de 8ad5 4552  ......1*N.....ER
        0x0080:  56dc d5dd 6082 5598 6222 6cce 3fe7 d1a9  V...`.U.b"l.?...
        0x0090:  54ba 9bcb 31cb 2b93 c683 6e69 cc08 63e5  T...1.+...ni..c.
        0x00a0:  a28d b992 7f81 e039 33aa 3d0c be98 46f7  .......93.=...F.
        0x00b0:  d7d0 6df9 b916 a741 ec38 88d7 690f 3275  ..m....A.8..i.2u
        0x00c0:  2f7c 87d5 ca5a 5573 f92b 94d9 9f92 0812  /|...ZUs.+......
        0x00d0:  c180 5c66 3746 2769 39c2 ac58 700d 0bc2  ..\f7F'i9..Xp...
        0x00e0:  d66d 1a5d 2d5c a808 e686 33bd 55aa 08d6  .m.]-\....3.U...
        0x00f0:  47dc 81b4 430f 7471 dbc0 c99e 6338 9d76  G...C.tq....c8.v
        0x0100:  4364 e029 fc16 bde9 0995 c6c8 50cc cd77  Cd.).........P..w
        0x0110:  37f2 0484 78cb 2e7a cfbb 3abb 5e6e 771f  7...x..z..:.^nw.
        0x0120:  ad6f faca 7314 6bb3 e237 5a2e 34cf 87f4  .o..s.k..7Z.4...
        0x0130:  ddf2 ae51 90ab b3b5 ea6c a1ea 9529 7df4  ...Q.....l...)}.
        0x0140:  42f0 2342 bd40 1a69 256e adf2 19b4 7658  B.#B.@.i%n....vX
        0x0150:  febc f9c6 93f0 efe0 07ba 9178 9768 5d8b  ...........x.h].
        0x0160:  6b40 80e0 25a6 76f7 5faa d92b b04a 4a47  k@..%.v._..+.JJG
        0x0170:  a5ea 2d97 c61a c5be 9651 4896 66e0 c118  ..-......QH.f...
        0x0180:  b6ac 6c38 54cb 15c5 f452 1cd9 c2e4 efce  ..l8T....R......
        0x0190:  72cc                                     r.
19:39:52.998398 IP (tos 0x60, ttl 59, id 34983, offset 0, flags [DF], proto TCP (6), length 40)
```

Authorization !

SOX report

1. Every user has changed his credentials every 24 hours
2. Server has changed its credentials every 90 days.
3. Who has access? Check my configuration system.

```
DBNAME: MYDB
APP_ACCESS:
- LEGACY_APP
SSL_ACCESS:
- $DBE-GROUP:
  - DBA
- $APP-SUPPORT:
  - SELECT ON FMADMIN.TABLE1
  - SELECT ON FMADMIN.TABLE2
```

What have we achieved so far!

1. Improve **Authentication** to something stronger than password, preferably two factor authentication.
2. **Authorization** should be tightly controlled, changes should be reviewed.
3. **Encryption** of all data in transit.
4. **Reduce operational overhead** of managing ~~passwords~~
5. **Better auditing**

Monitoring and Operational procedures

1. Monitor certificate expiry.
2. Have procedures for trust certificate(root) rotation.
3. Consider multiple roots.
4. Watch audit trail for patterns like users connecting using SSL for unknown servers.
5. Mine the CA logs for evidence for SOX

Scenario 1 - Employee leaves organization

Before: Rotate the passwords for every account employee had access to.

1. Cannot get SSO cookie, hence cannot get certificate, hence cannot login to DB
2. Once employee has been removed from LDAP, configurations automatically remove him.
3. Programs, locks the account on DB

Scenario 2 - Employee joins organization

Before: Manually create user in every DB he needs access to. Clone privileges. OR Share passwords.

1. Once employee comes on board, configurations automatically include the new employee.
2. Programs, creates the user on the DB with privileges already defined.
3. New employee gets a certificate, can log in to database.

Section 5: Making this work for your organization

How can I implement this for my organization?

1. Internal CA
    a. Most org already have them
    b. If not, build one using OpenSSL
    c. Or, use an open source project like EJBCA [has LDAP connectors]

2. SSO Infrastructure
    a. Talk to your security team.
    b. Trust chain is important, User credential + two factor -> SSO -> x509 cert -> DB auth. Document the risks.

How can I implement this for my organization?

3. Configuration Management
    a. Use the code repository, where all your company code resides. Internal Git
    b. Keep it simple, YAML, JSON works best. Do not complicate if by putting in a database.
    c. Ensure NO ONE can modify the configs between git and the servers.
4. Make your tools cross platform
    a. Highly recommend Golang - build for Linux, Mac , Windows
    b. Starts small, Iterate !

How can I implement this for my organization?

5. Get to Oracle 12c
    a. Oracle 12c has stronger crypto
    b. If you can’t ; still use this!

Wrapping up!

NAME SPARE4

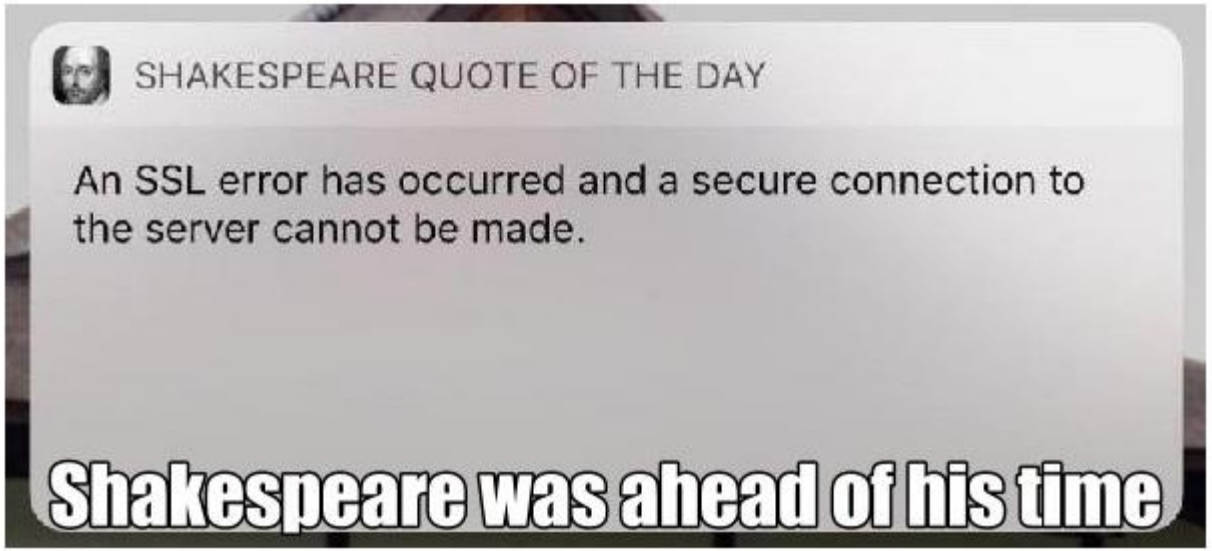
HARRIS

APP_USER
S:B11AD869750777FFBBF41F8A77057EA9880B76E86DF2184D3F8AC8B3F610;H:EC6155DD922E37557AB390D43A840B5A;T:

64A6E1867TA207207909B8FC7460F4C48A3B1172B181D4AA966E484AE5DFC0CDA4319B3YB07A512ECFC3BC20C972CB33BB98
E4FD6F719C191ACB60965210C3D5E54D1C2FD072A8618FC5973E3EF388

Stop worrying, start loving database security!

Thank you!


SHAKESPEARE QUOTE OF THE DAY
An SSL error has occurred and a secure connection to the server cannot be made.
Shakespeare was ahead of his time