KeyShield SSO

Václav Šamša
CEO, Inventor
Project leader
TDP Ltd
vsamsa@tdp.cz

TDP

TDP - Novell partner and developer

Since 1988

Prague, Czech Republic

SW & HW development

Data Recovery

Network Administration

TDP Novell partner and developer

www.groupwise.cz

www.cealogs.co.uk

www.tdp.cz/downloads

www.zfcr.com - old but nice

www.securewinbox.com

www.keyshieldsso.com

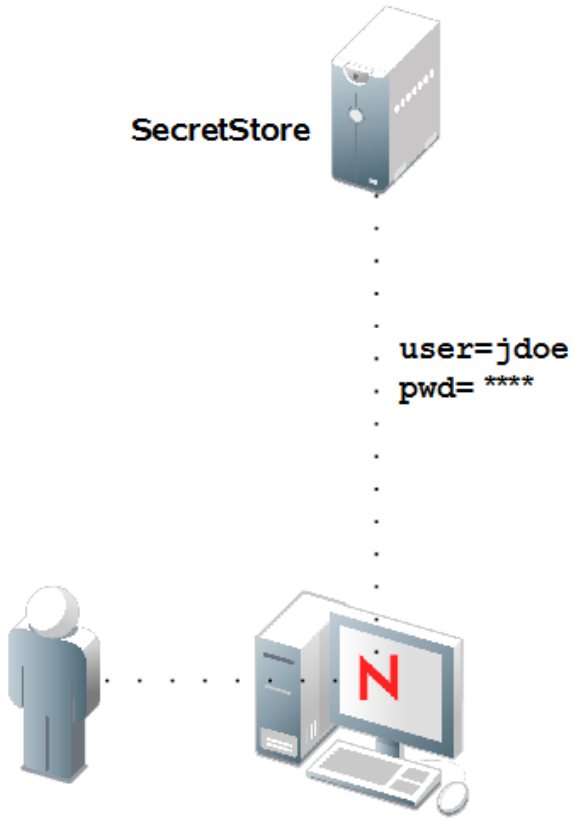
KeyShield SSO

SSO?

TDP

SecureLogin

SecureLogin



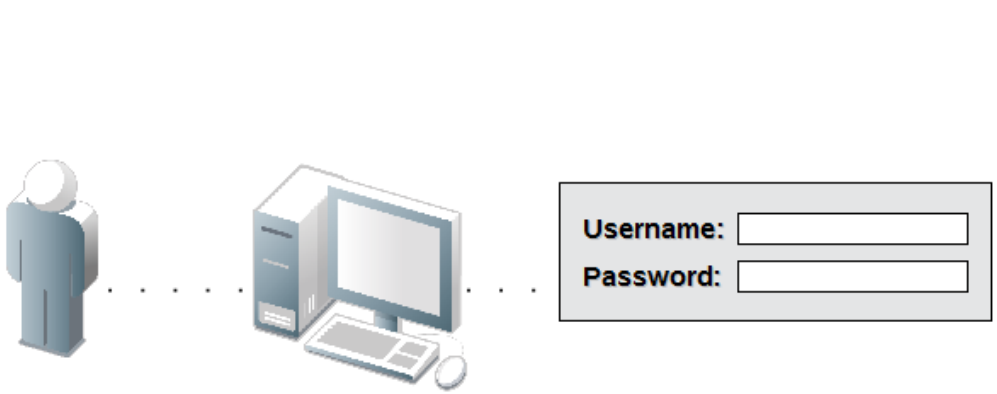
KeyShield SSO

SecureLogin

TDP

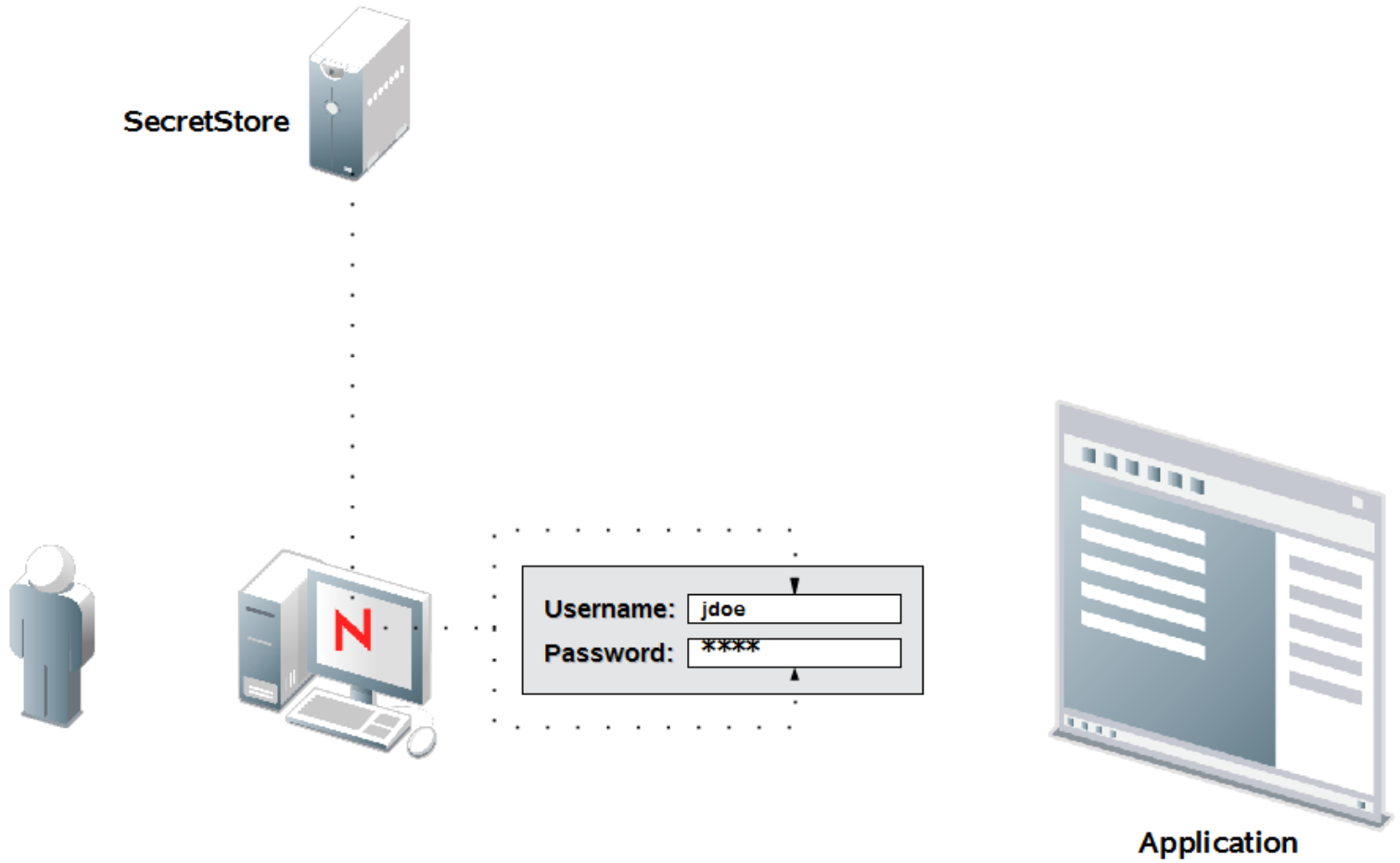
KeyShield SSO

SecureLogin

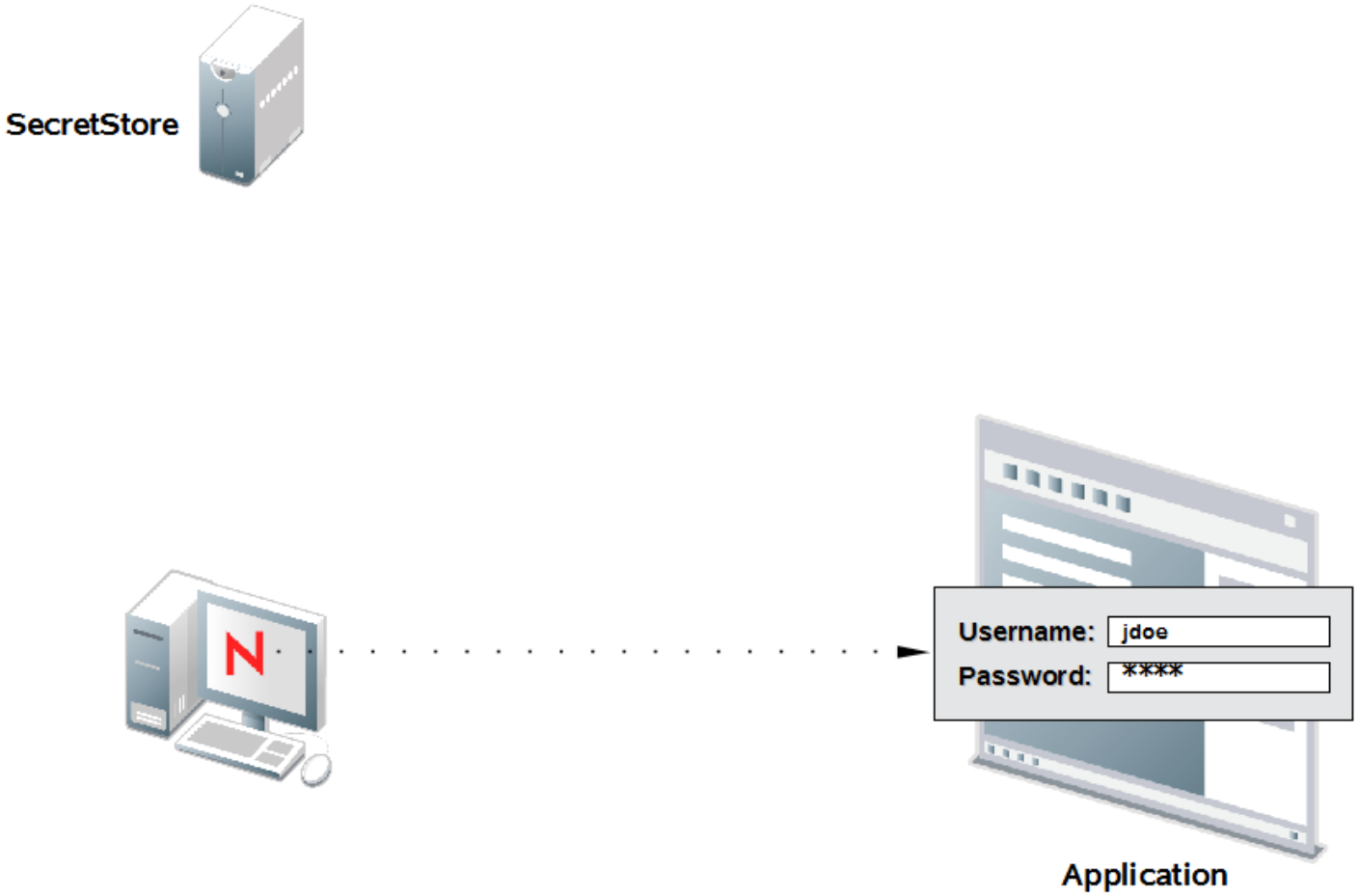


TDP

SecureLogin



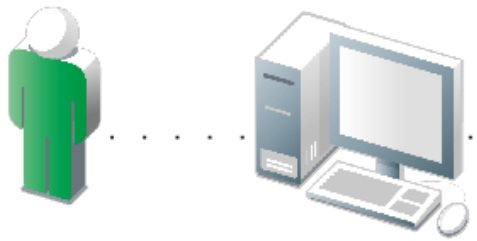
SecureLogin



KeyShield SSO

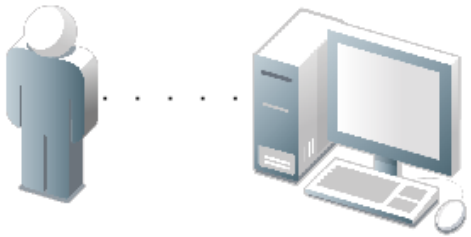
SecureLogin

Successfully logged in!

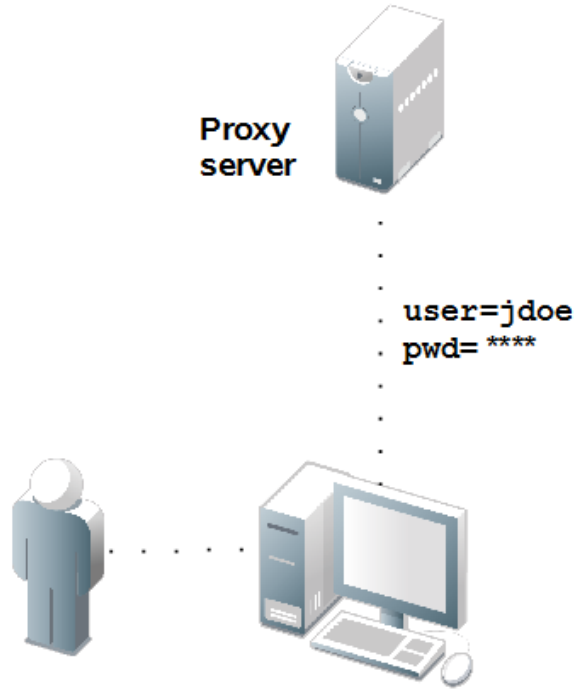


TDP

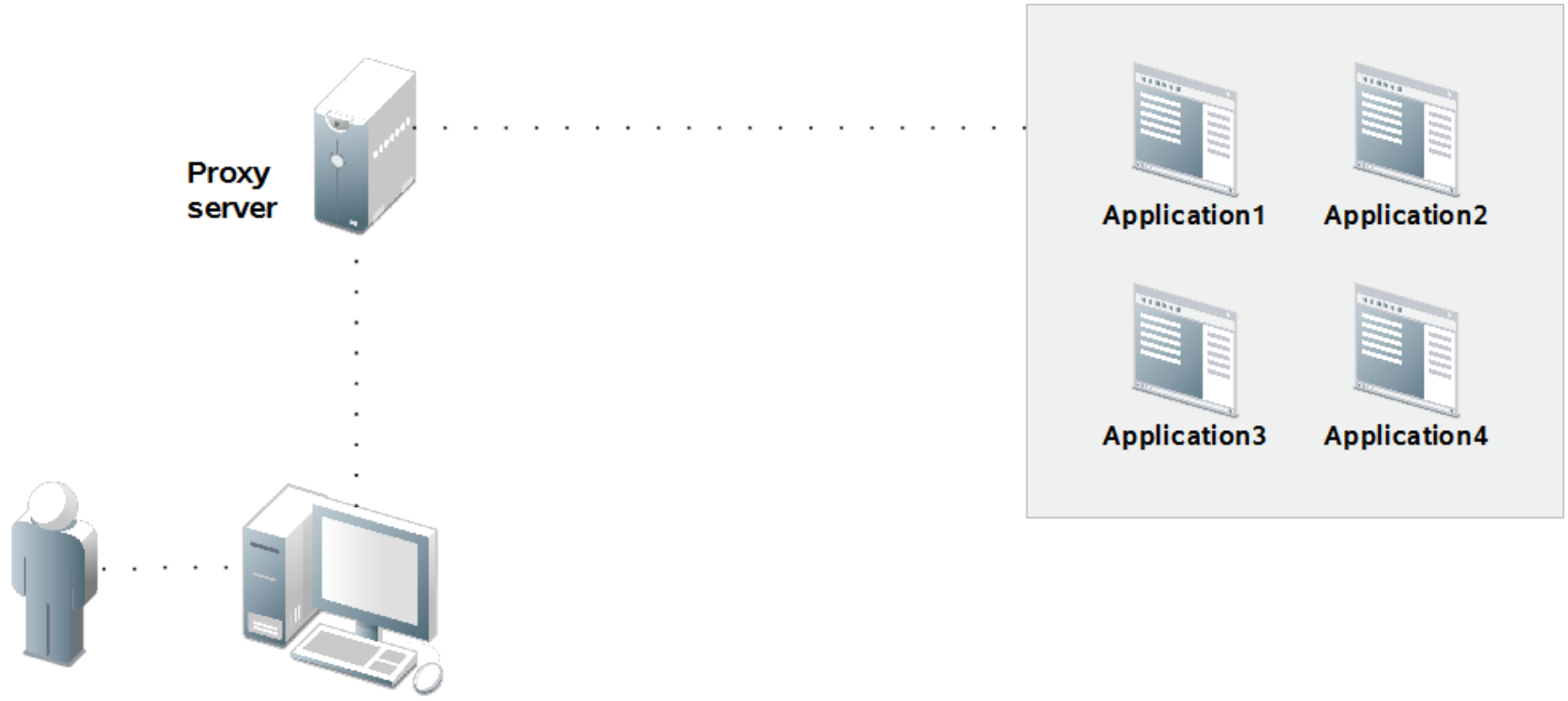
NetIQ Access Manager



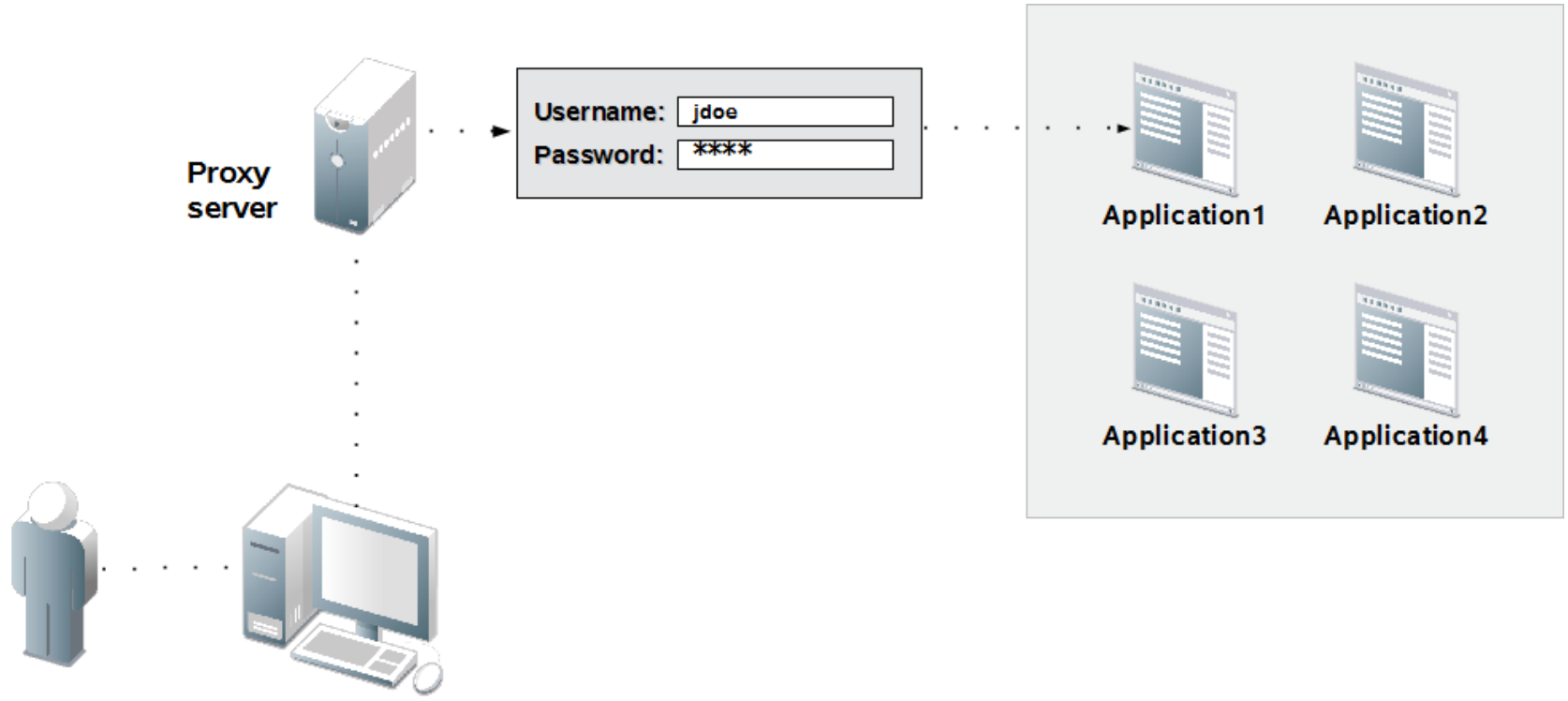
NetIQ Access Manager



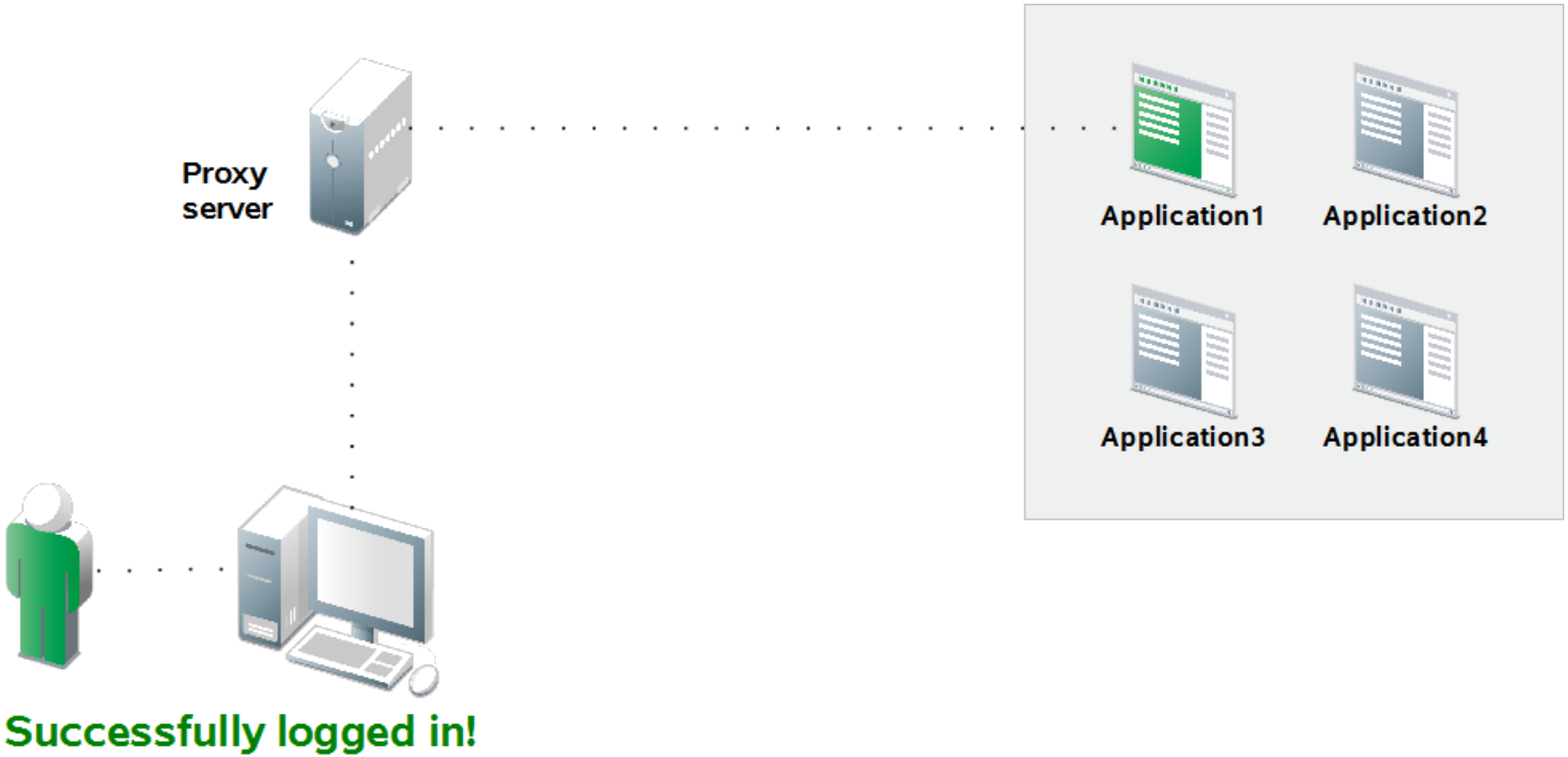
NetIQ Access Manager



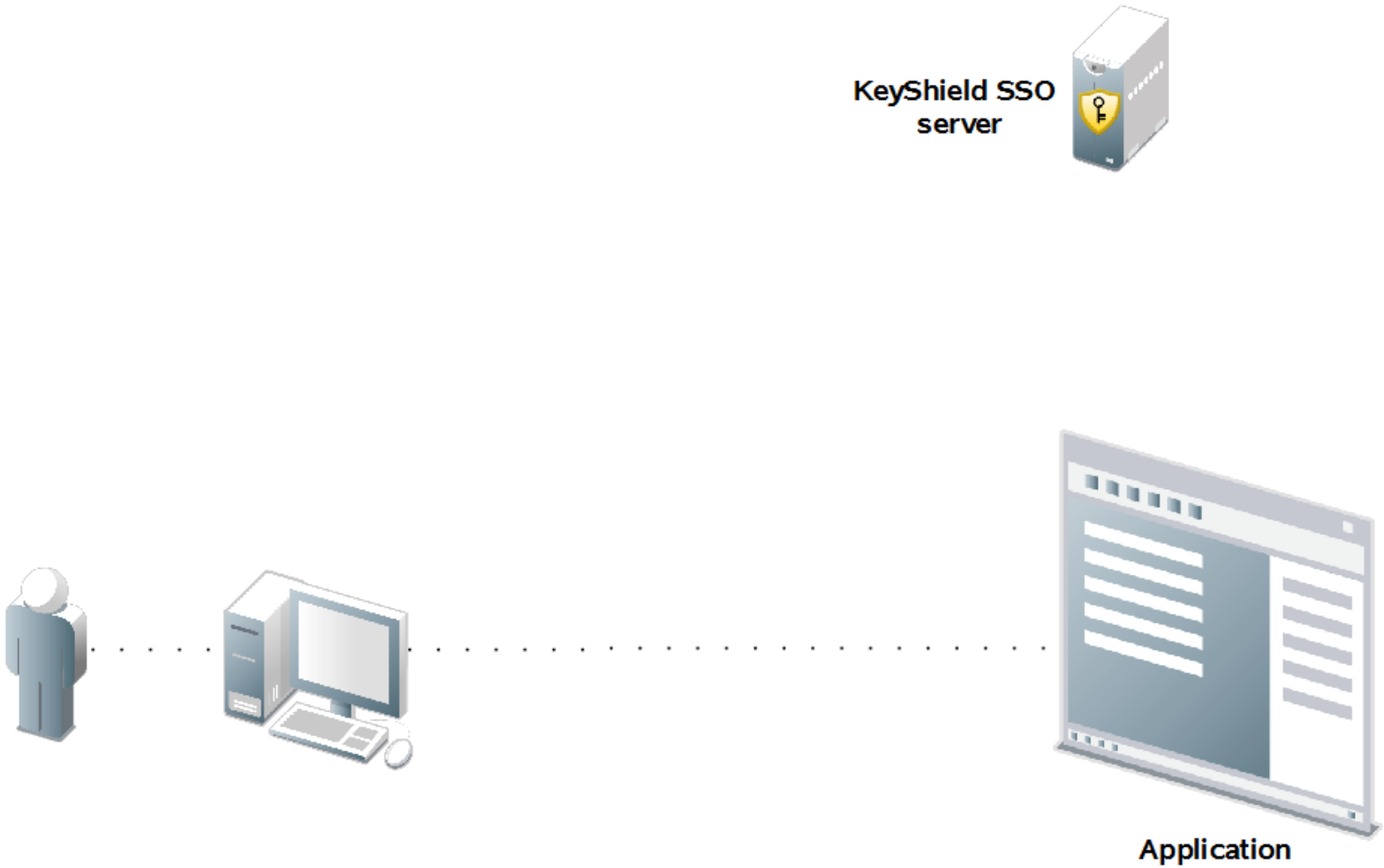
NetIQ Access Manager



NetIQ Access Manager

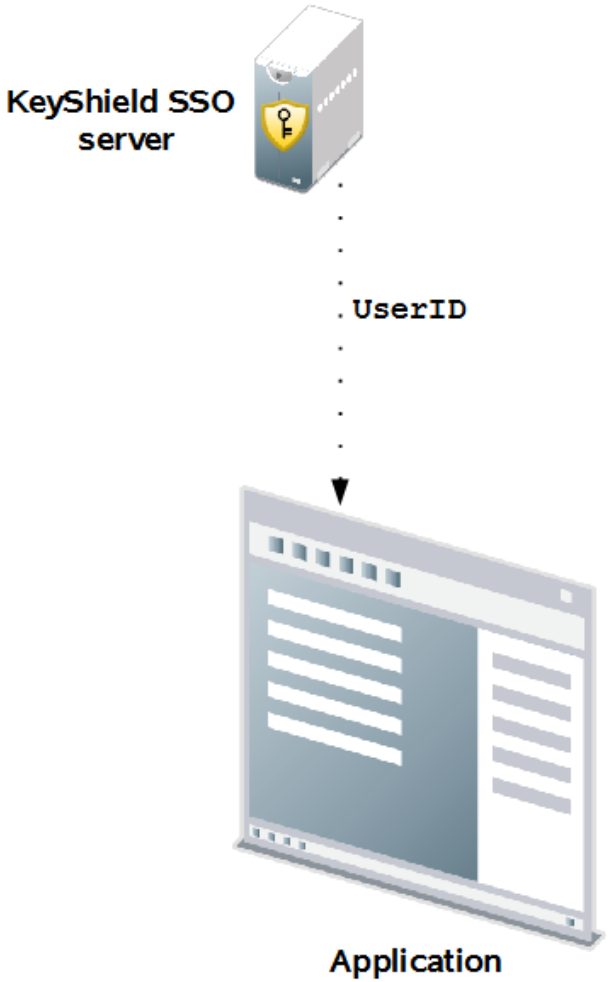


KeyShield SSO



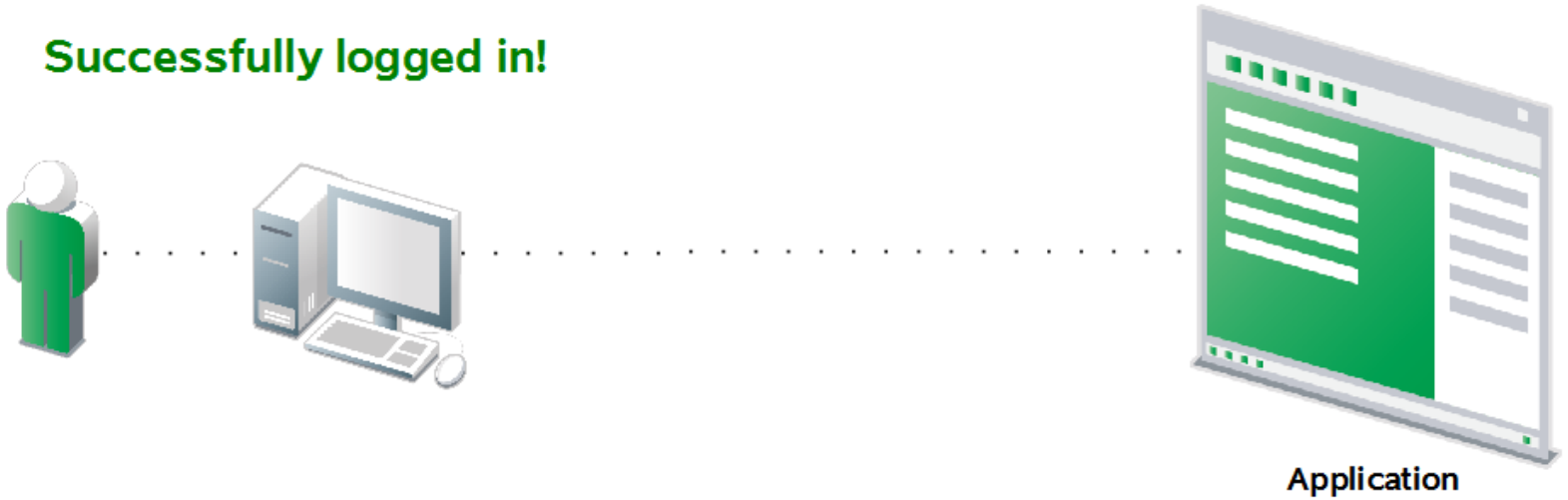
KeyShield SSO

KeyShield SSO



KeyShield SSO

Successfully logged in!

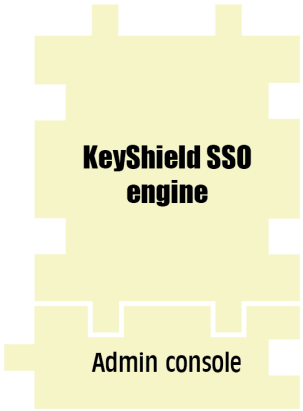


KeyShield SSO

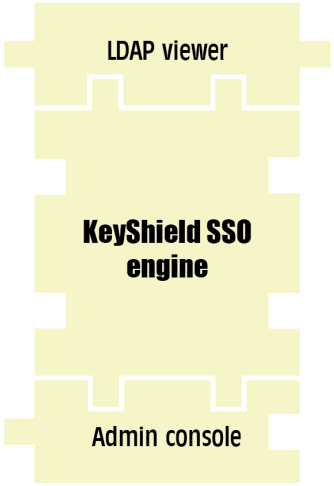
DEMO

Optimized Java Engine

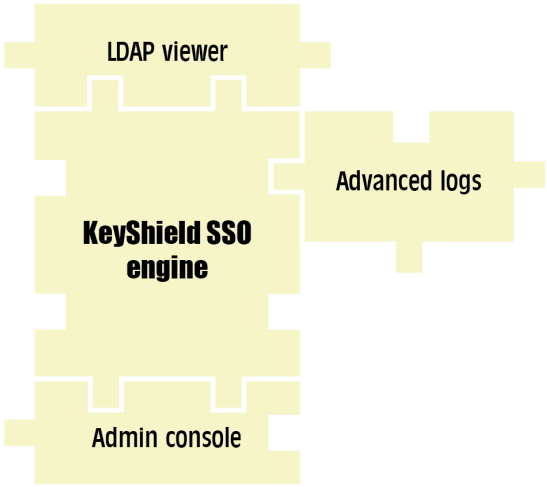
Comfort and useful Admin Console



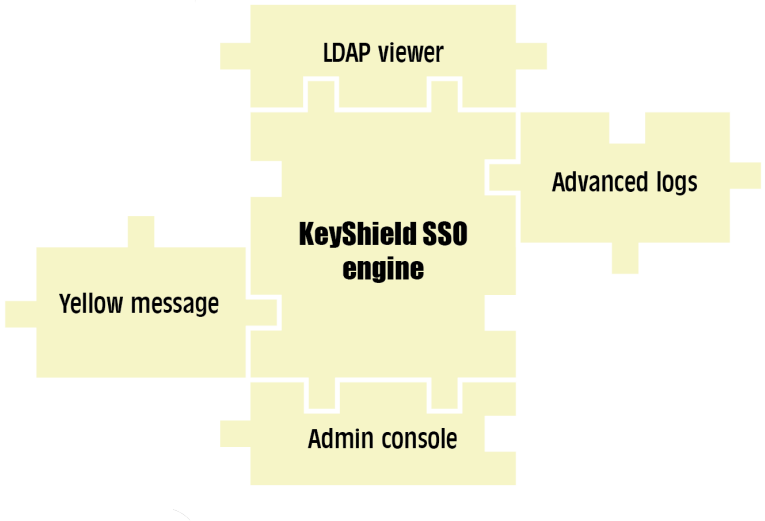
LDAP browser for easy troubleshooting



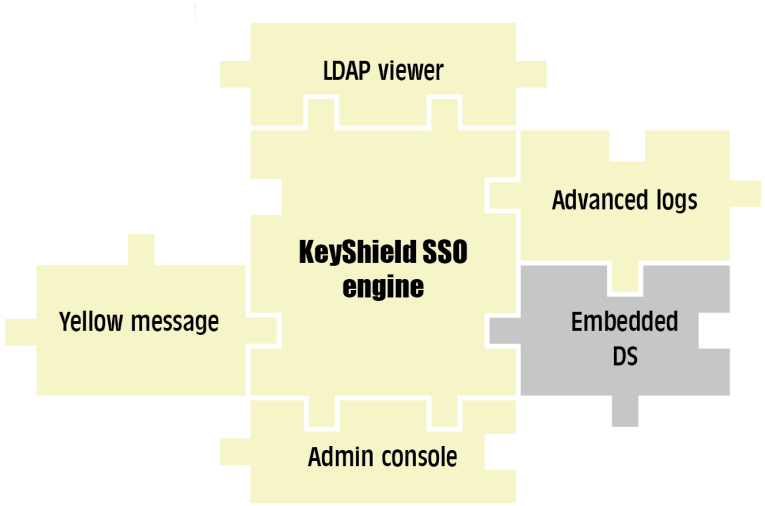
Log debug level setup and online view



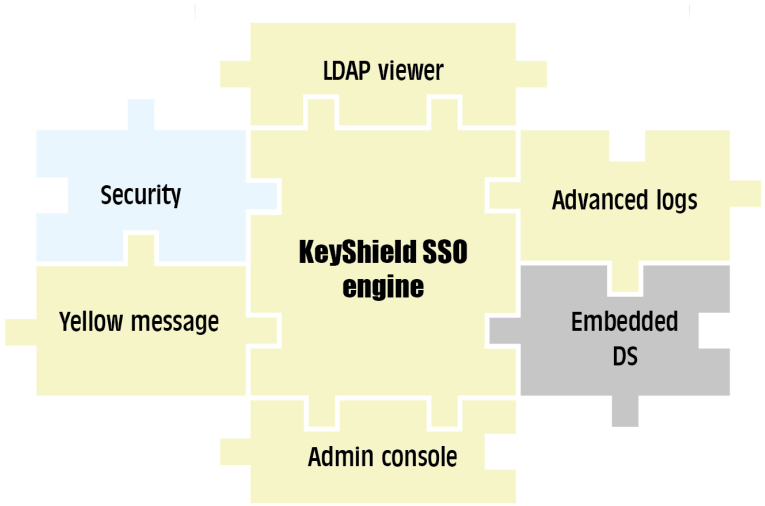
Yellow message –> all client platforms



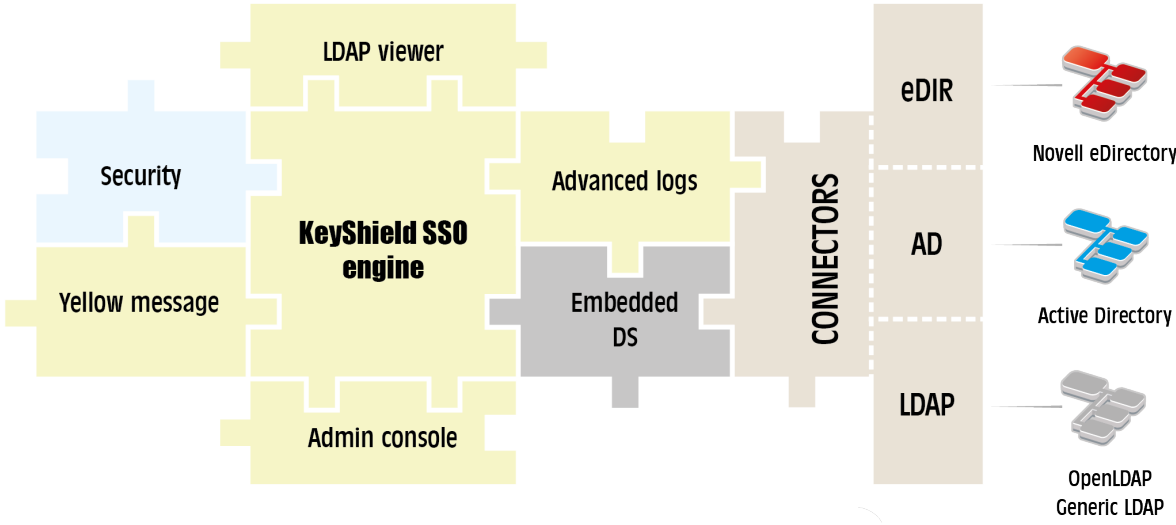
Embedded Apache DS



SSL, AppKey, Win client installation

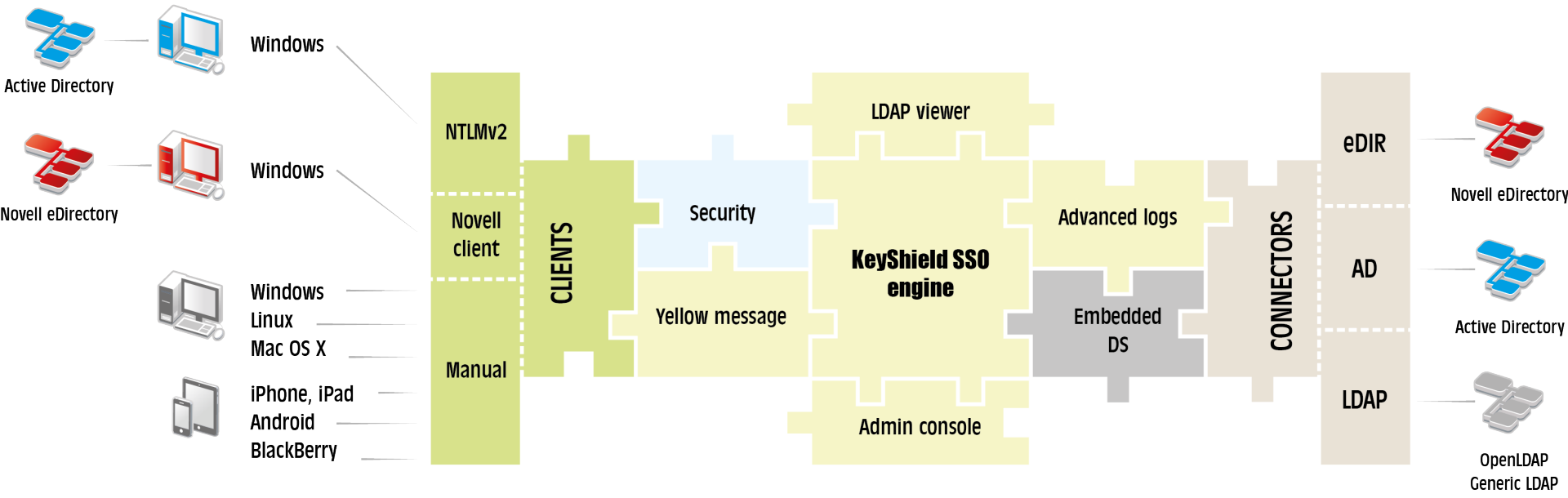


As many as you need – eDIR, AD, LDAP



KeyShield SSO

Win, Mac, Linux, iOS, Android, BB



TDP

KeyShield SSO

Novell
eDirectory

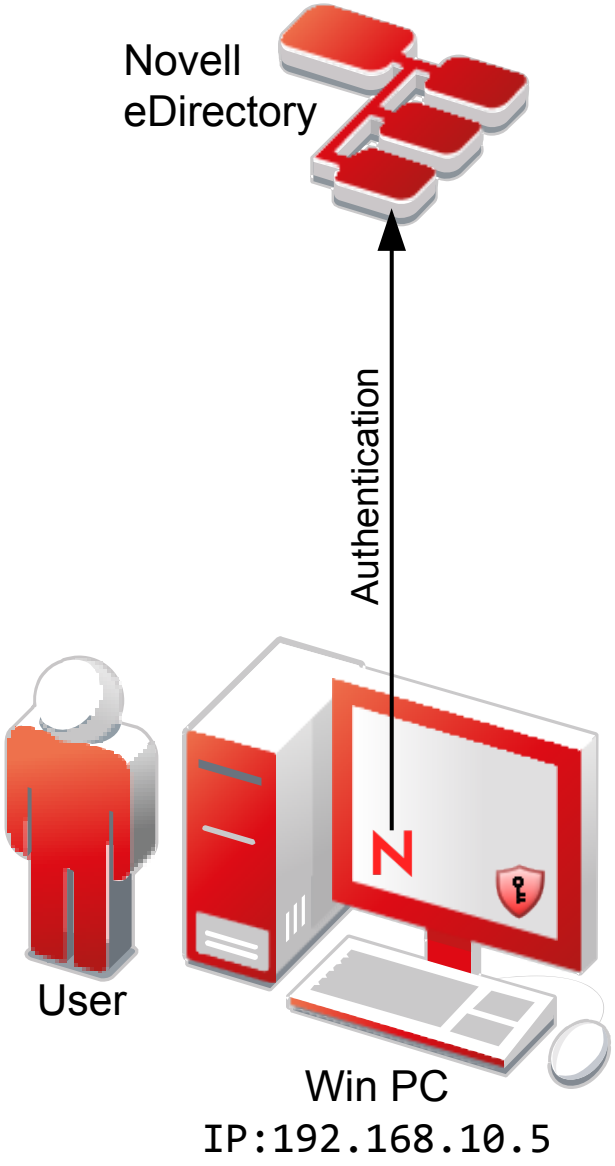
KeyShield SSO
server

User

Win PC
IP:192.168.10.5

TDP

KeyShield SSO



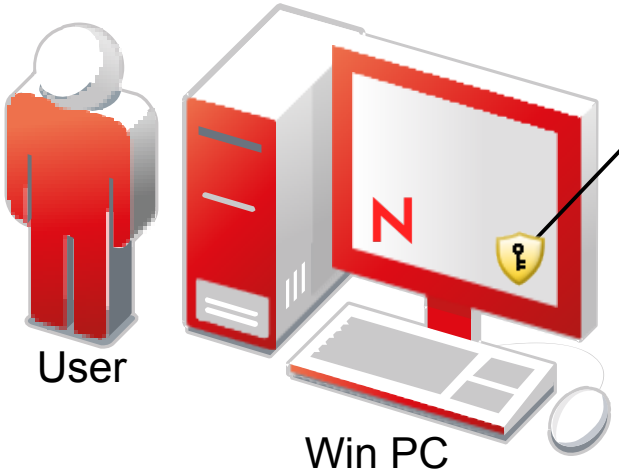
KeyShield SSO
server

TDP

KeyShield SSO

FDN = cn=msmith,o=org; IP Address:192.168.10.5

```
FDN = cn=msmith,o=org
IP:192.168.10.5
```



TDP

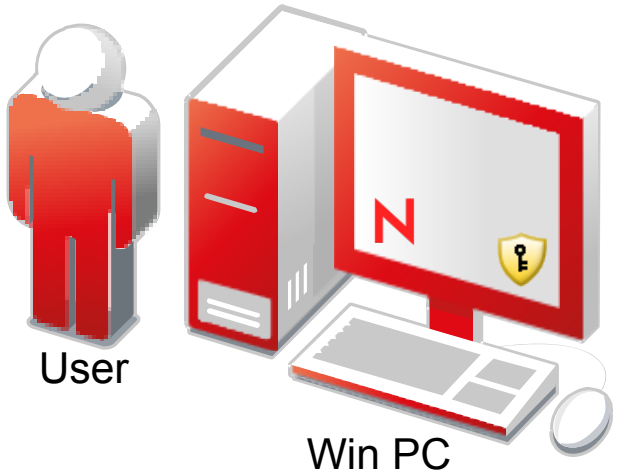
KeyShield SSO

Novell
eDirectory

Writing token to cn=msmith,o=org

KeyShield SSO
server

```
FDN = cn=msmith,o=org
IP:192.168.10.5

Writing token to
cn=msmith,o=org
```

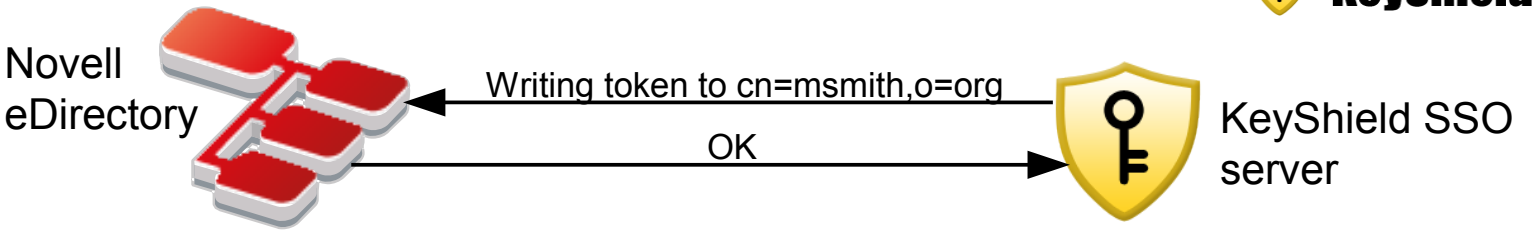


User

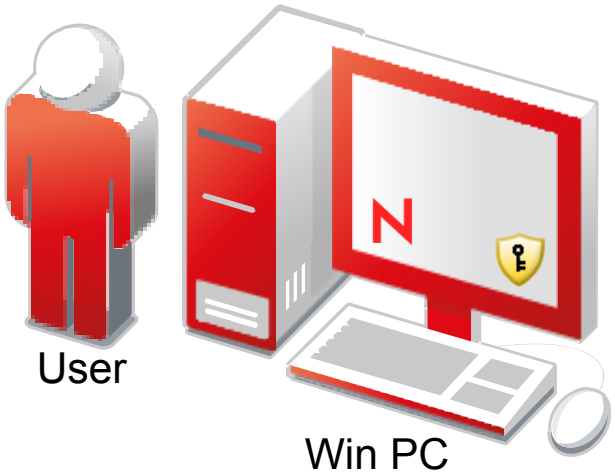
Win PC
IP:192.168.10.5

TDP

KeyShield SSO




```
FDN = cn=msmith,o=org
IP:192.168.10.5

Writing token to
cn=msmith,o=org
Token was written
```

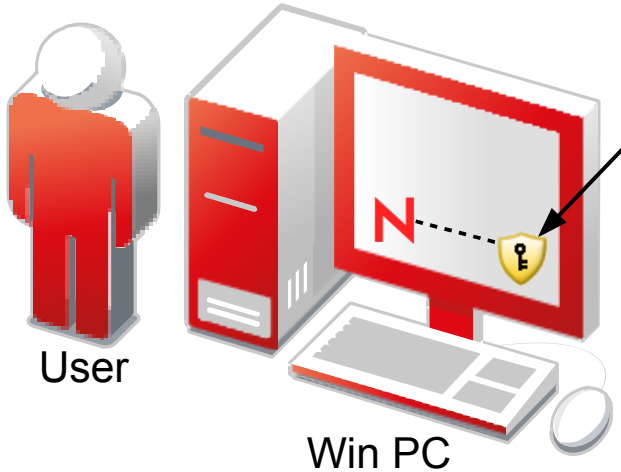


TDP

KeyShield SSO

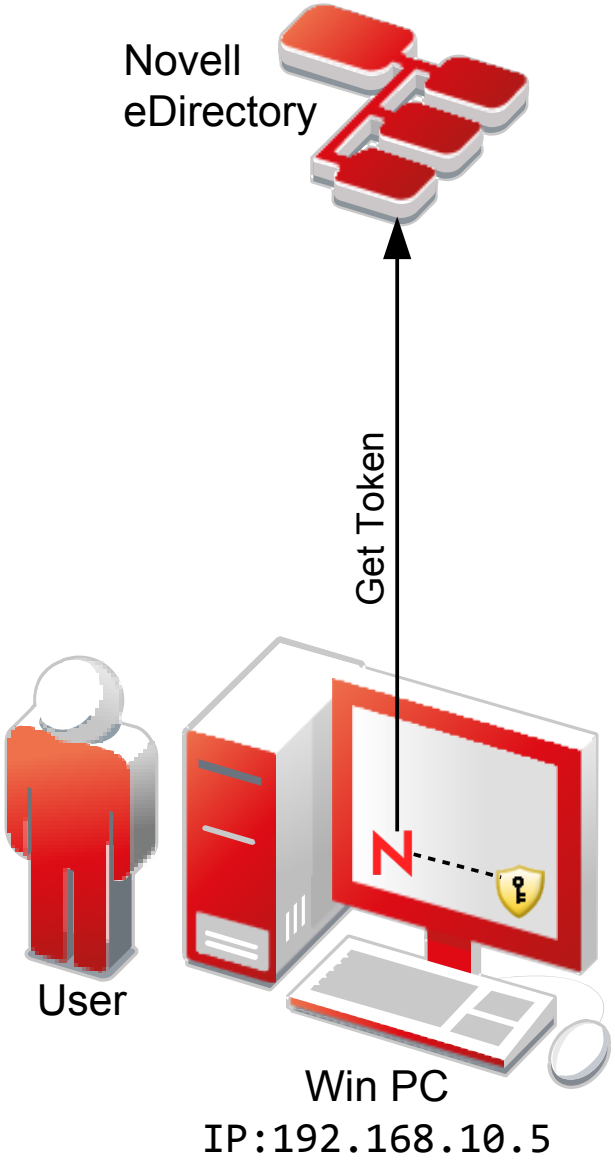
Token ID + Challenge

```
FDN = cn=msmith,o=org
IP:192.168.10.5

Writing token to
cn=msmith,o=org
Token was written

Send Token ID and
Challenge
```



TDP

KeyShield SSO

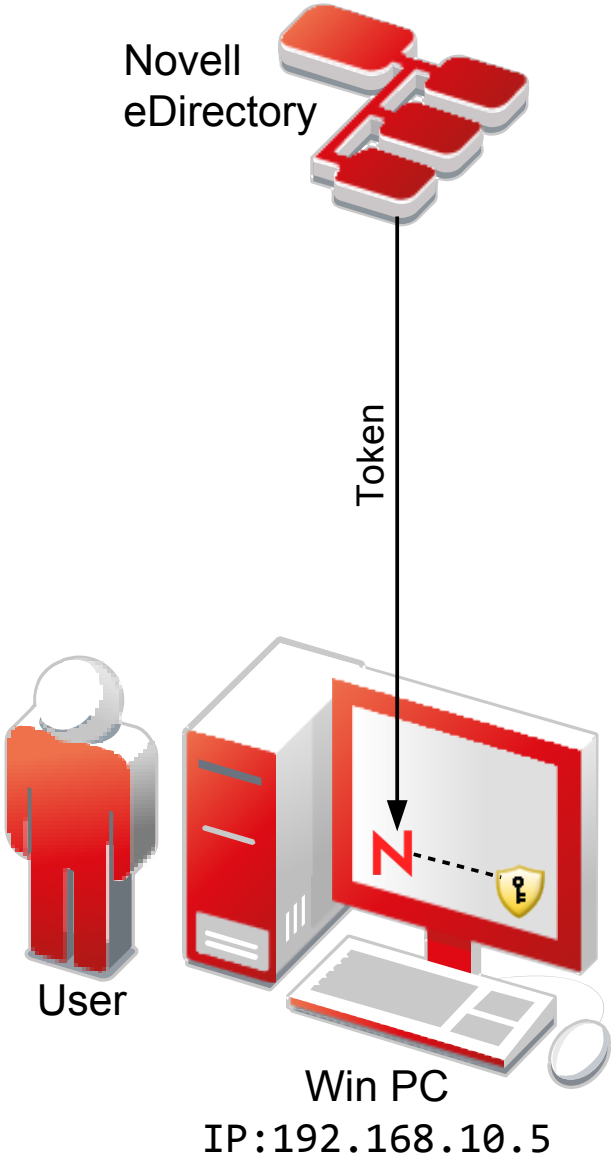


KeyShield SSO server

```
FDN = cn=msmith,o=org
IP:192.168.10.5

Writing token to
cn=msmith,o=org
Token was written

Send Token ID and
Challenge
```

TDP

KeyShield SSO



KeyShield SSO server

```
FDN = cn=msmith,o=org
IP:192.168.10.5

Writing token to
cn=msmith,o=org
Token was written

Send Token ID and
Challenge
```

TDP

KeyShield SSO

Novell
eDirectory

KeyShield SSO
server

Generated response

```
FDN = cn=msmith,o=org
IP:192.168.10.5

Writing token to
cn=msmith,o=org
Token was written

Send Token ID and
Challenge
```

User

Win PC
IP:192.168.10.5

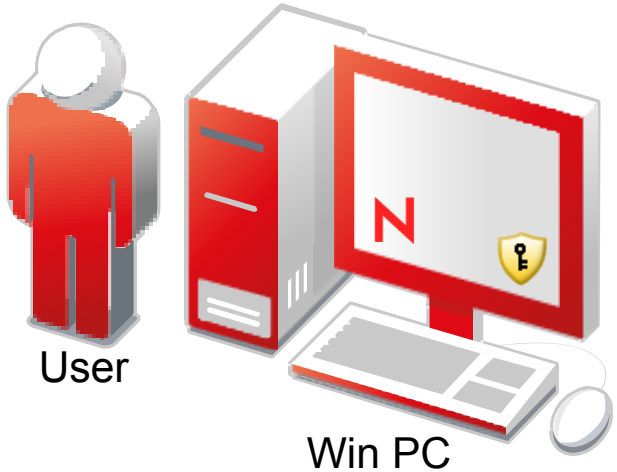
TDP

KeyShield SSO

Novell
eDirectory

KeyShield SSO
server

```
FDN = cn=msmith,o=org
IP:192.168.10.5

Writing token to
cn=msmith,o=org
Token was written

Send Token ID and
Challenge

Response Validity Check
```



User

Win PC
IP:192.168.10.5

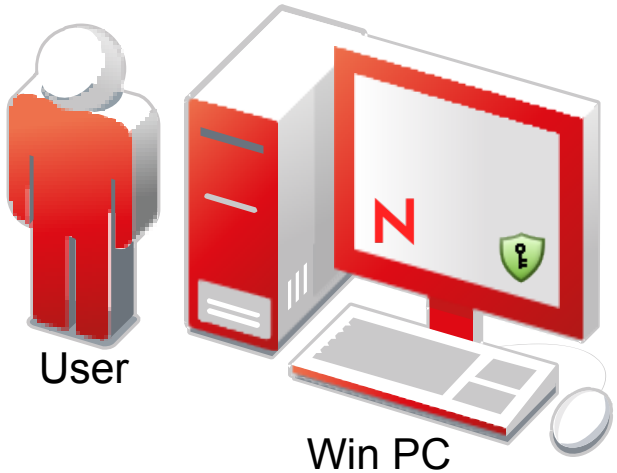
TDP

KeyShield SSO

Novell
eDirectory

KeyShield SSO
server

```
FDN = cn=msmith,o=org
IP:192.168.10.5

Writing token to
cn=msmith,o=org
Token was written

Send Token ID and
Challenge

Response Validity Check

OK
```



User

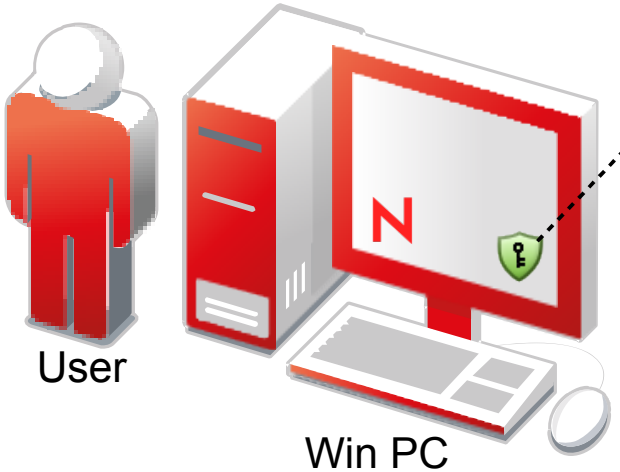
Win PC
IP:192.168.10.5

TDP

KeyShield SSO

KeyShield SSO server

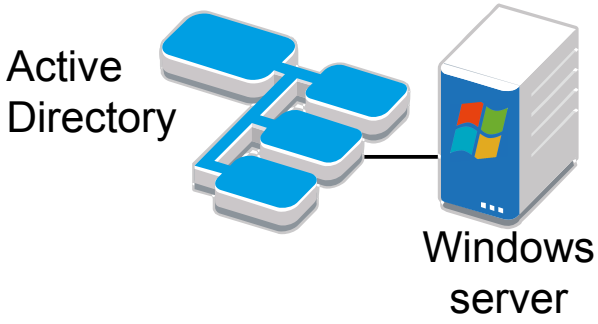
KeyShield SSO keep alive (2–4 min by default)



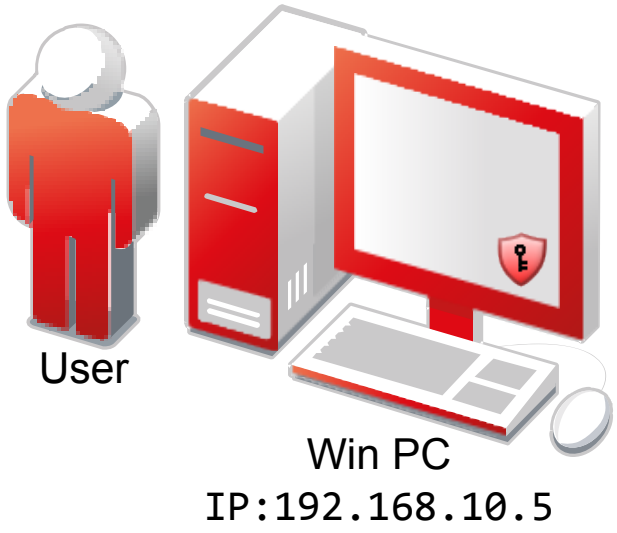

```
FDN = cn=msmith,o=org
IP:192.168.10.5

Writing token to
cn=msmith,o=org
Token was written

Send Token ID and
Challenge

Response Validity Check

OK
Keep
[IP: 192.168.10.5 is
cn=msmith,o=org]
```

TDP

KeyShield SSO

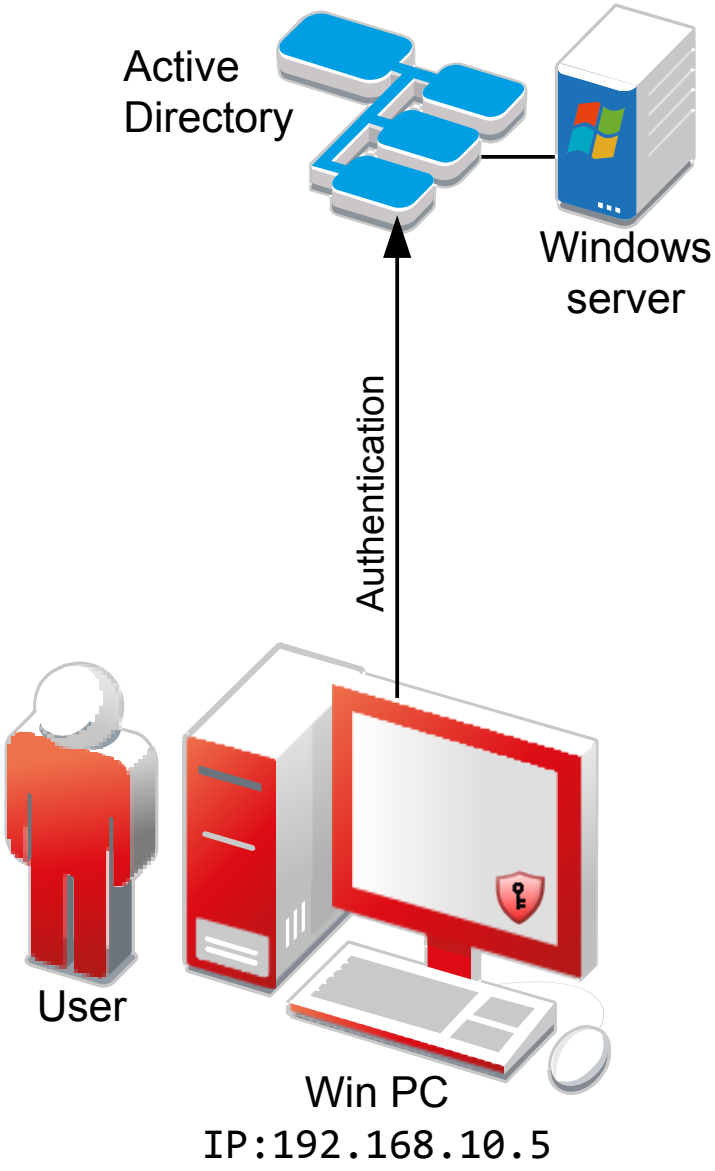


KeyShield SSO
server



TDP

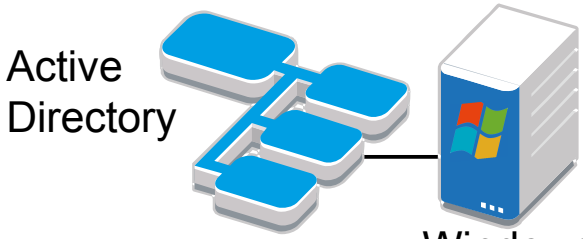
KeyShield SSO



KeyShield SSO
server

TDP

KeyShield SSO

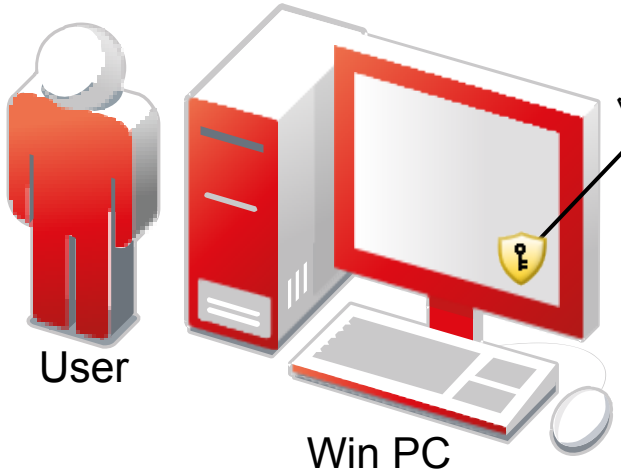


Windows
server

KeyShield SSO
server

AUTH (NTLMv2 Type 1 Negotiate) ; IP:192.168.10.5

```
AUTH NTLMv2 T1 Negotiate
IP:192.168.10.5
```

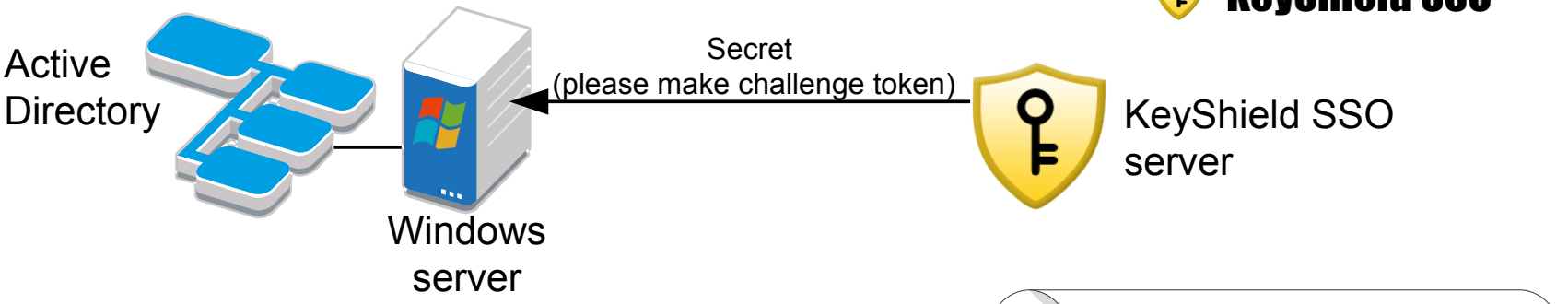


User

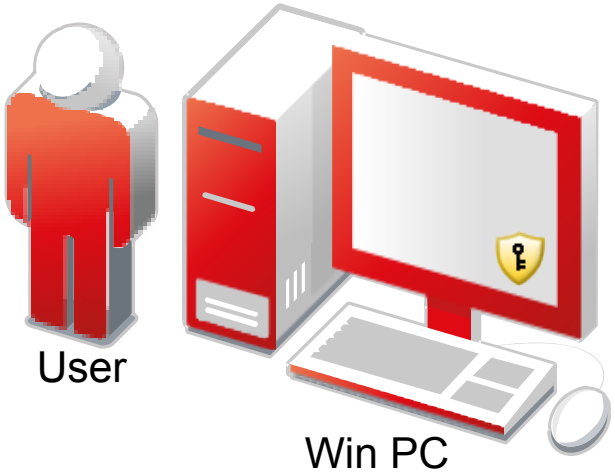
Win PC
IP:192.168.10.5

TDP

KeyShield SSO

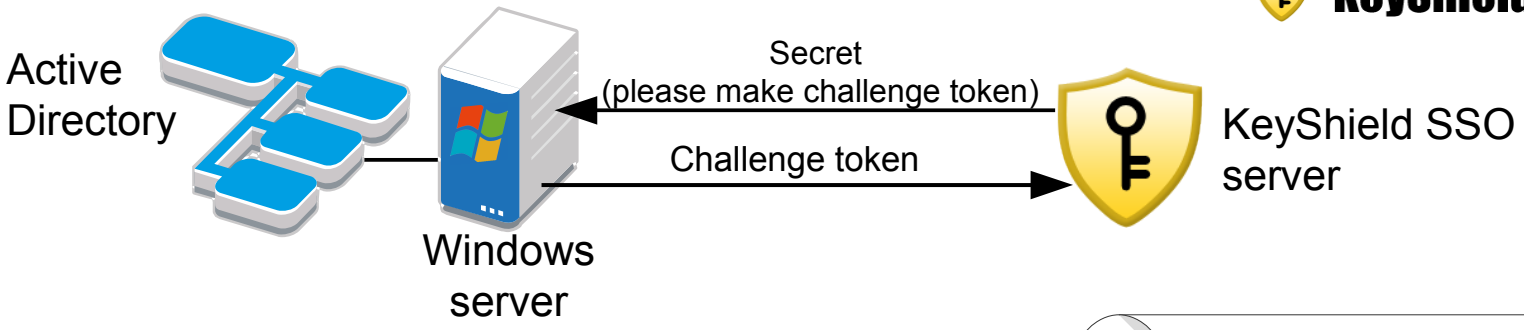


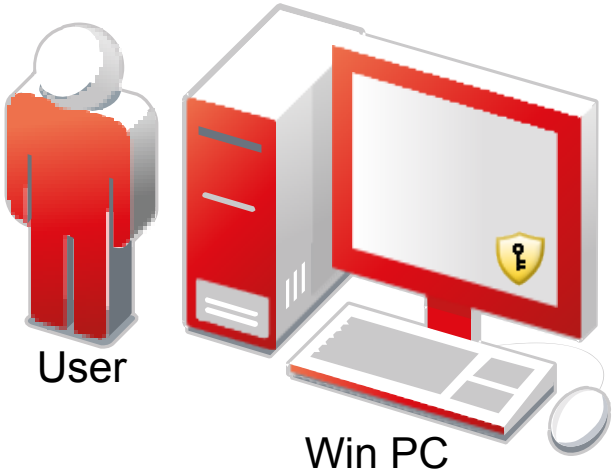

```
AUTH NTLMv2 T1 Negotiate
IP:192.168.10.5

Secret (Token request)
```



TDP

KeyShield SSO

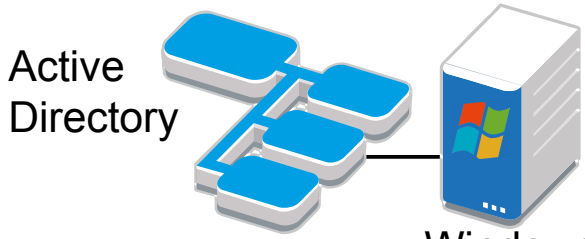





```
AUTH NTLMv2 T1 Negotiate
IP:192.168.10.5

Secret (Token request)
Token
```

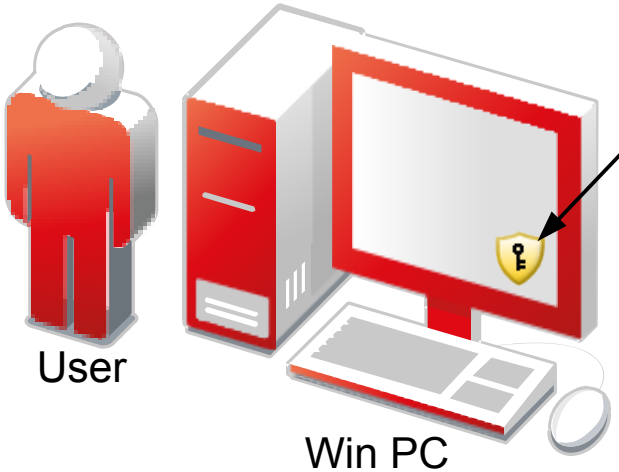
TDP

KeyShield SSO



KeyShield SSO
server

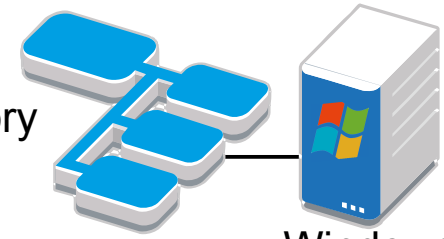
TOKEN (NTLMv2 Type2 Challenge)




```
AUTH NTLMv2 T1 Negotiate
IP:192.168.10.5

Secret (Token request)
Token

Sending Challenge
```

TDP

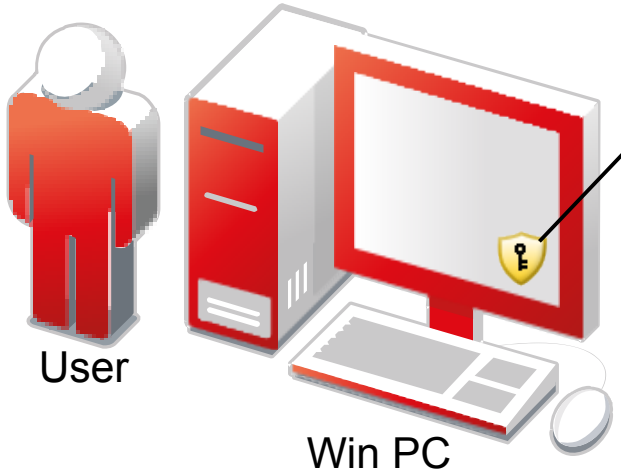
KeyShield SSO



Windows
server

KeyShield SSO
server

RESP (NTLMv2 Type 3 Response)



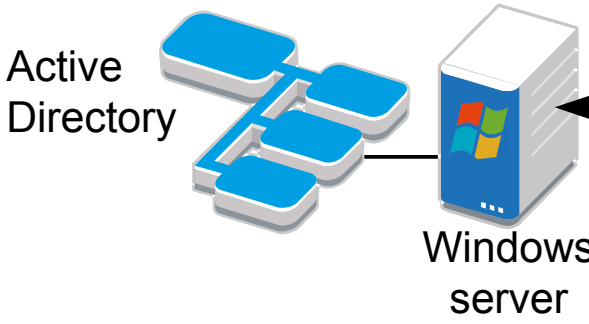
User

Win PC
IP:192.168.10.5

```
AUTH NTLMv2 T1 Negotiate
IP:192.168.10.5

Secret (Token request)
Token

Sending Challenge
```

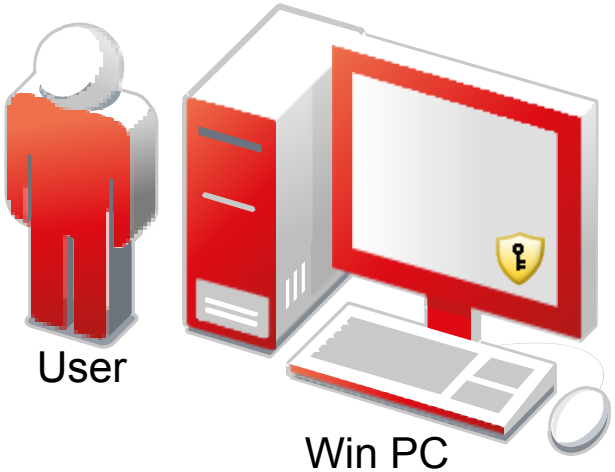
TDP

KeyShield SSO



Response

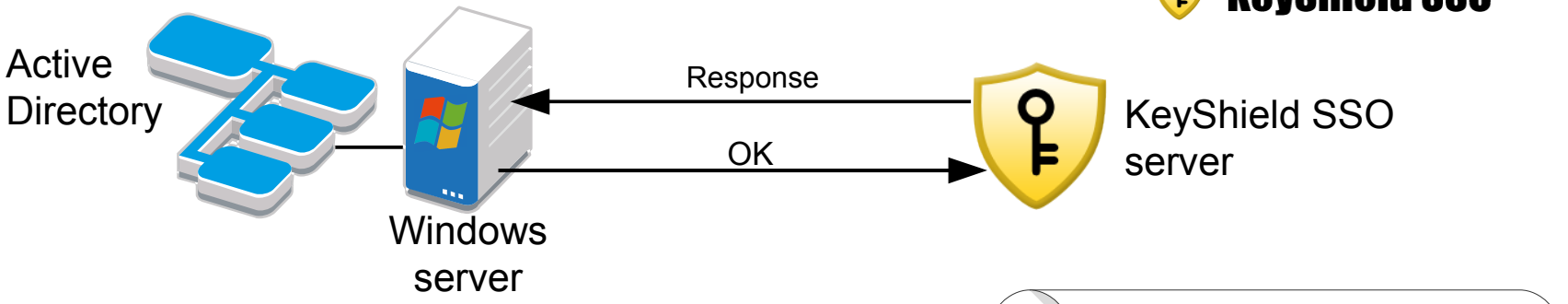
KeyShield SSO
server

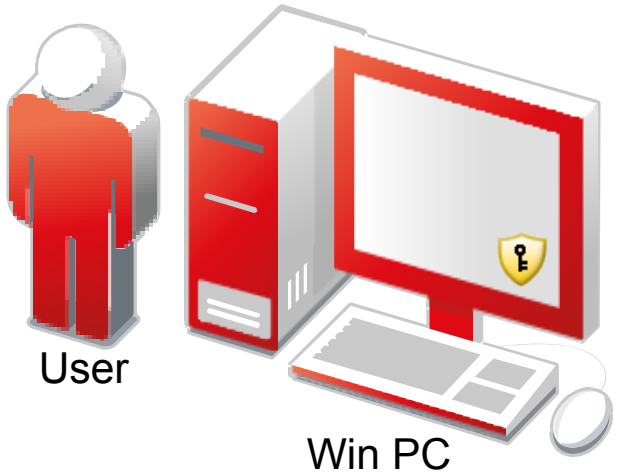



```
AUTH NTLMv2 T1 Negotiate
IP:192.168.10.5

Secret (Token request)
Token

Sending Challenge

Response validity check
```

TDP

KeyShield SSO

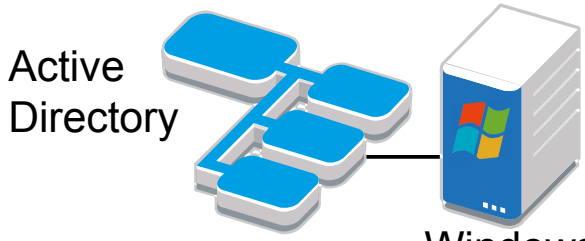





```
AUTH NTLMv2 T1 Negotiate
IP:192.168.10.5

Secret (Token request)
Token

Sending Challenge

Response validity check
Response OK
```

TDP

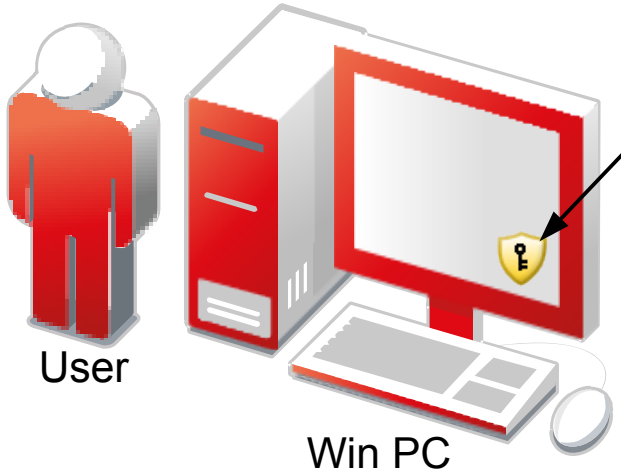
KeyShield SSO



KeyShield SSO
server

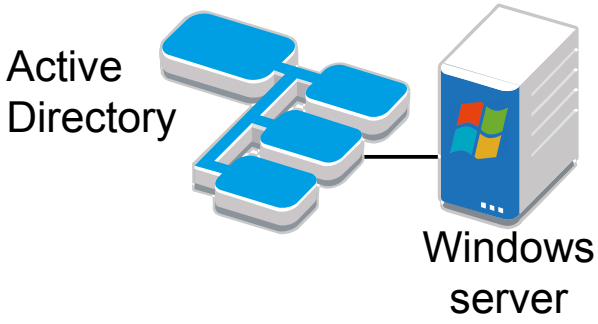
Login successful

```
AUTH NTLMv2 T1 Negotiate
IP:192.168.10.5

Secret (Token request)
Token

Sending Challenge

Response validity check
Response OK

Login successful
```

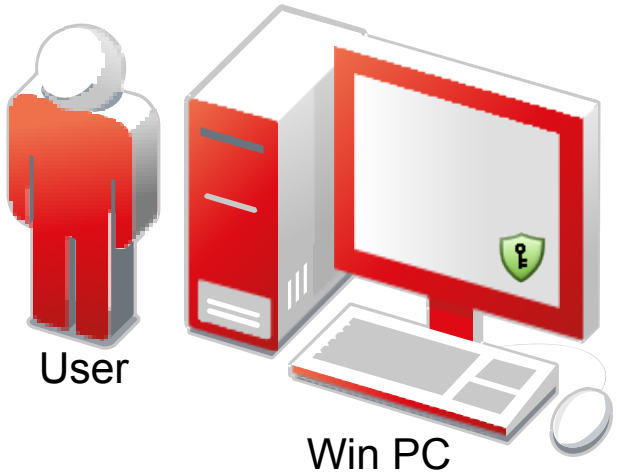


TDP

KeyShield SSO



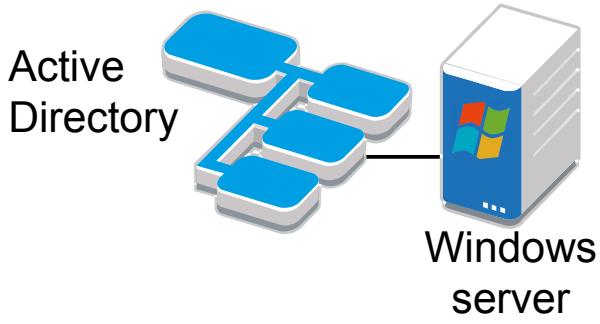
KeyShield SSO
server




```
AUTH NTLMv2 T1 Negotiate
IP:192.168.10.5

Secret (Token request)
Token

Sending Challenge

Response validity check
Response OK

Login successful

Keep
[IP: 192.168.10.5 is
domain://TDP\msmith]
```

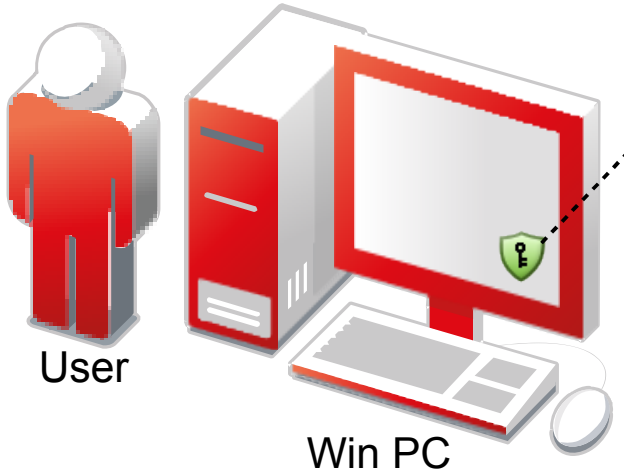
TDP

KeyShield SSO



KeyShield SSO
server

KeyShield SSO keep alive (2–4 min by default)

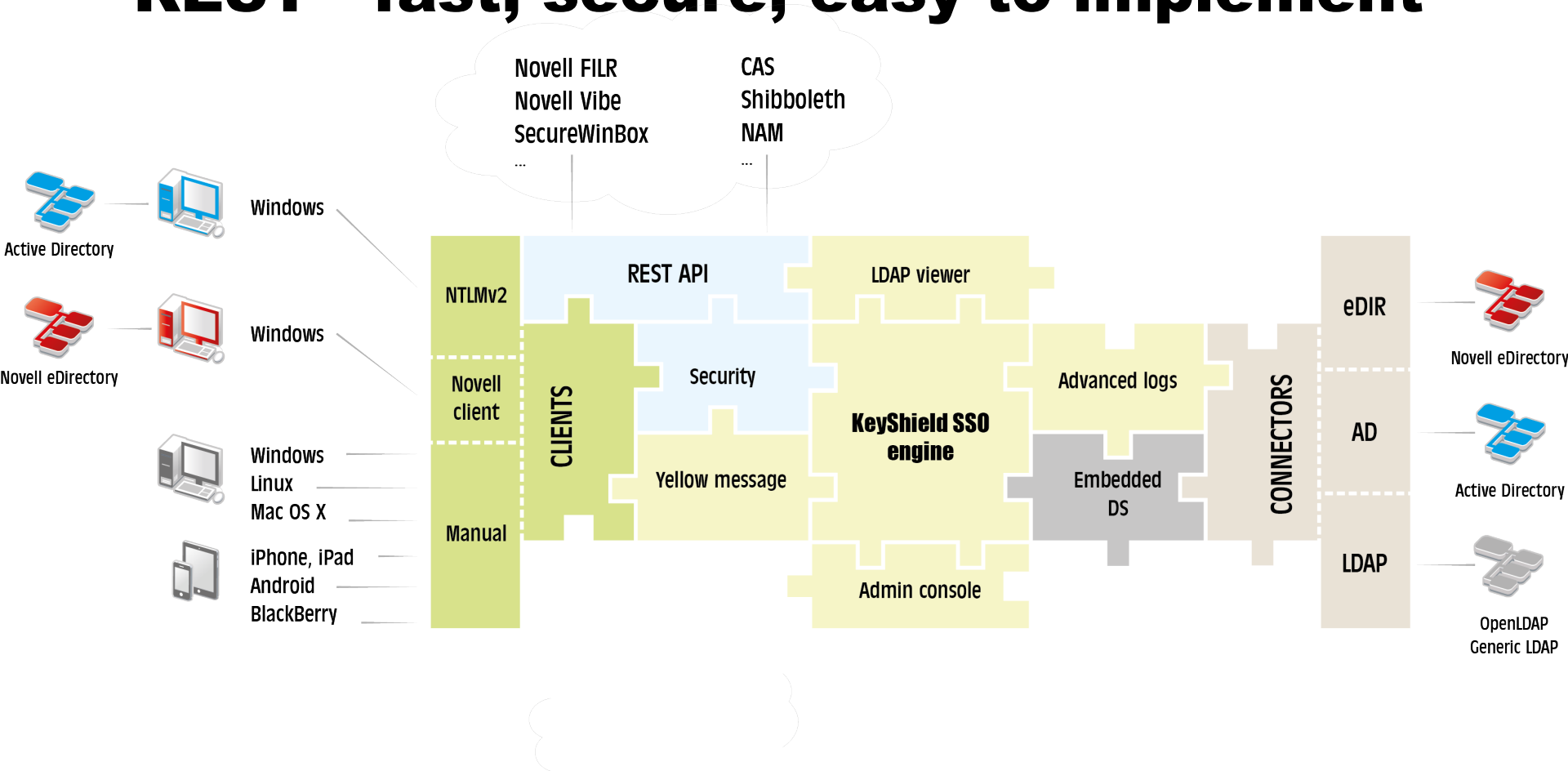



```
AUTH NTLMv2 T1 Negotiate
IP:192.168.10.5

Secret (Token request)
Token

Sending Challenge

Response validity check
Response OK

Login successful

Keep
[IP: 192.168.10.5 is
domain://TDP\msmith]
```

TDP

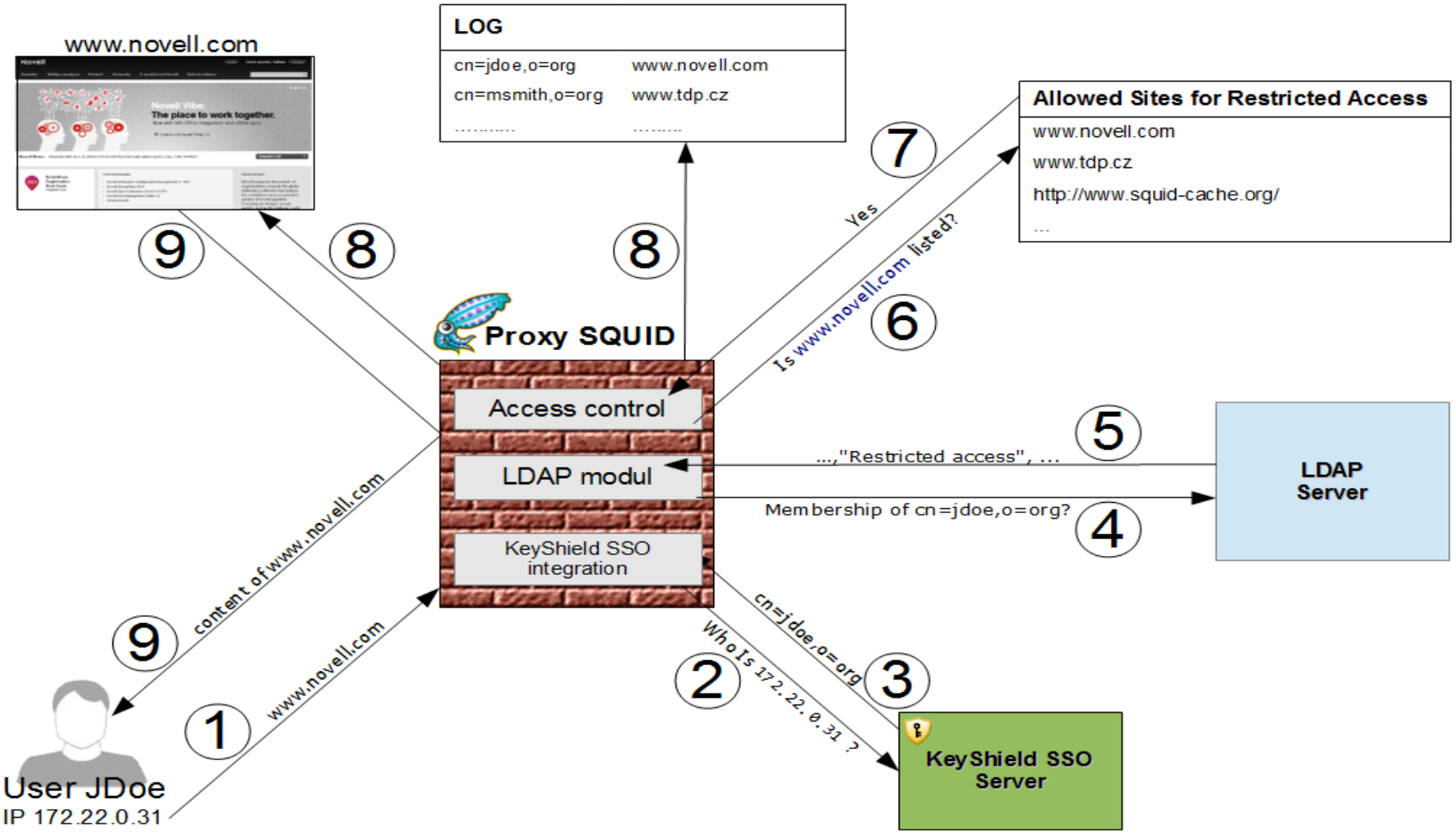
KeyShield SSO

REST - fast, secure, easy to implement

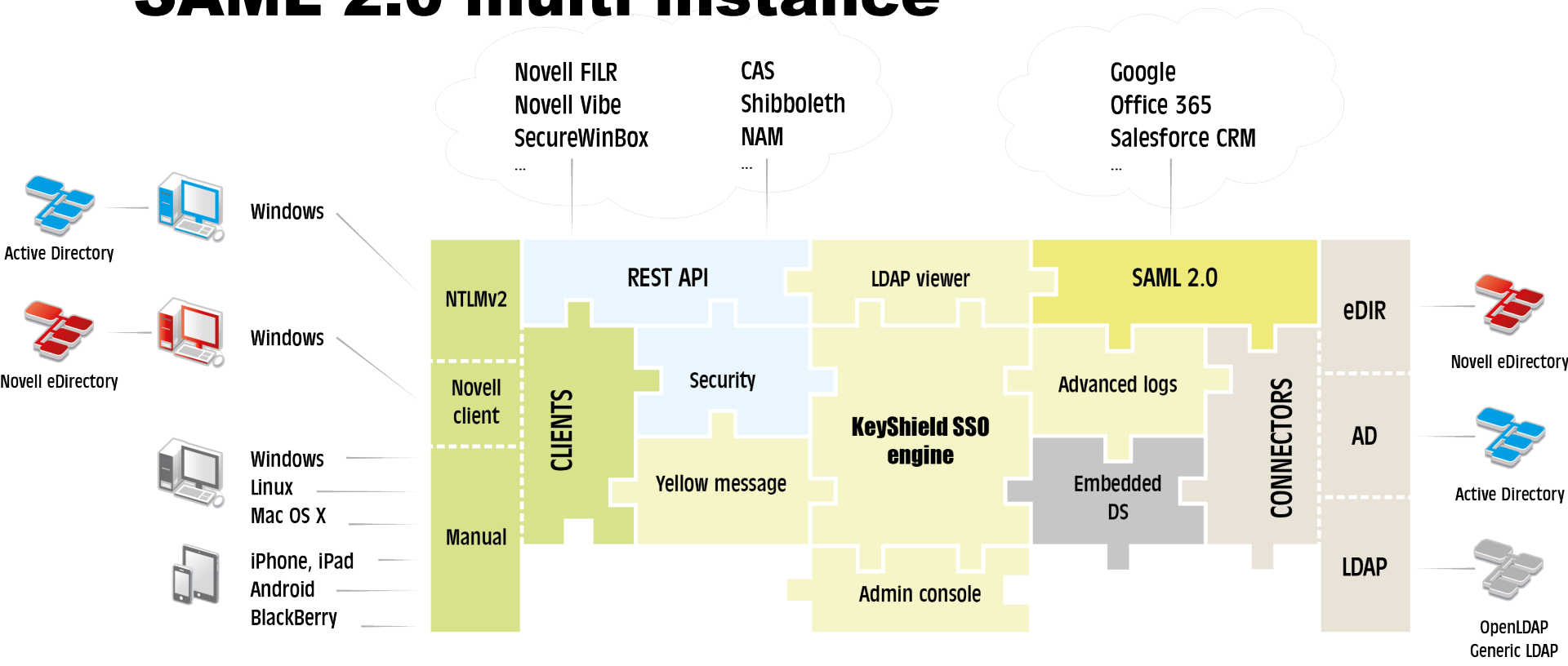


TDP

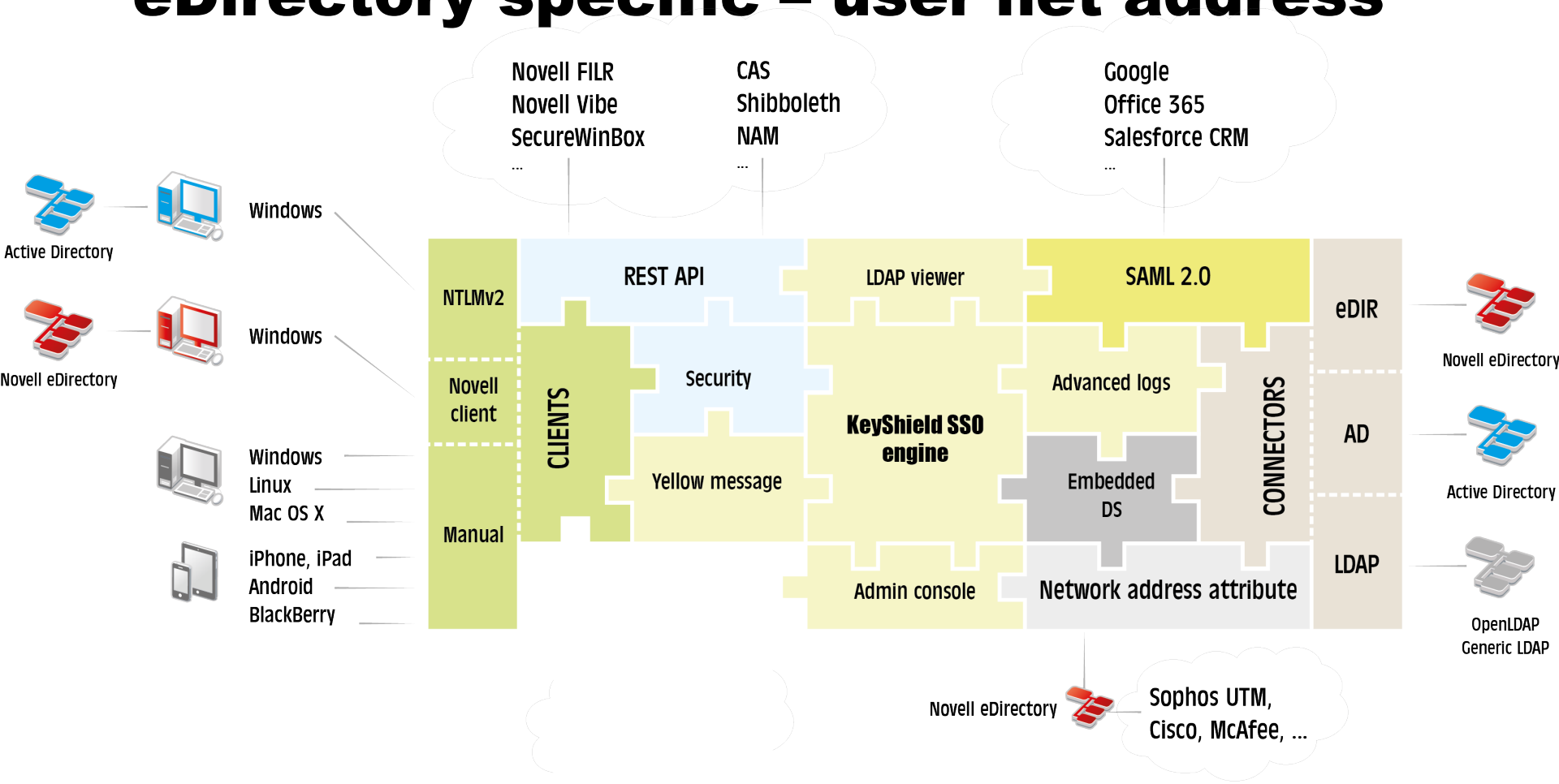
KeyShield SSO – SQUID



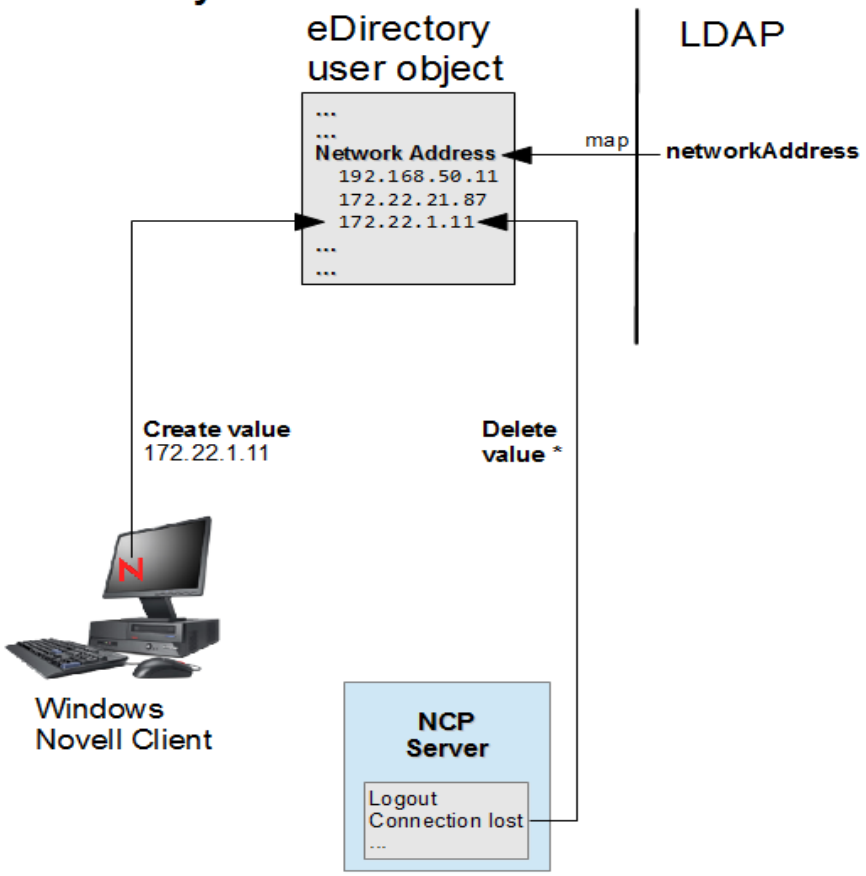
SAML 2.0 multi instance



eDirectory specific – user net address

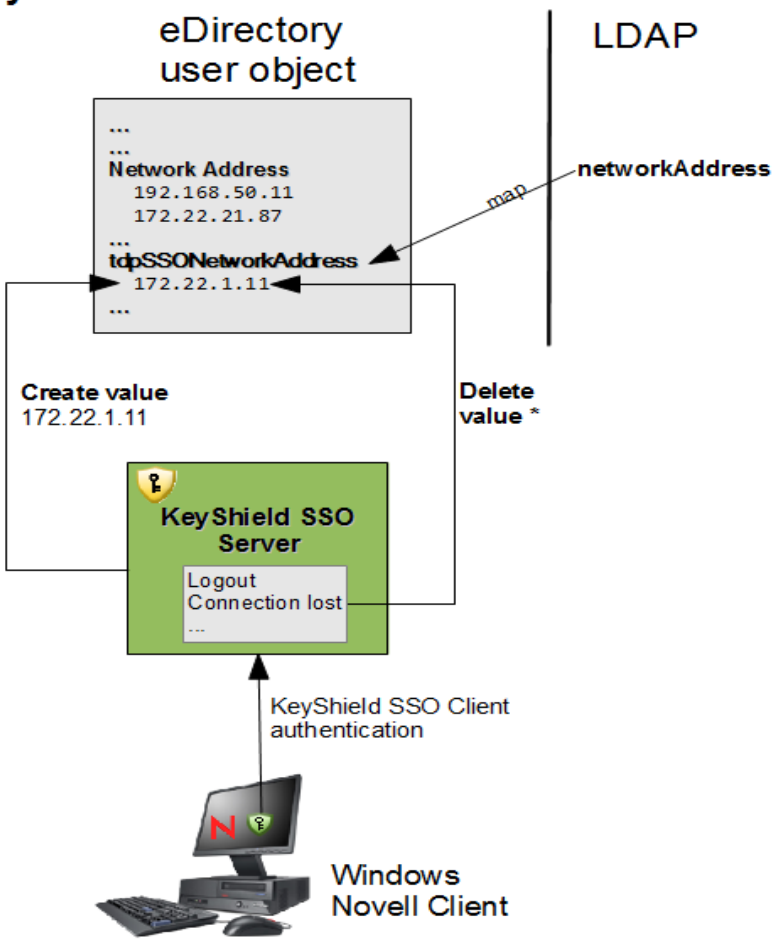


eDirectory standard



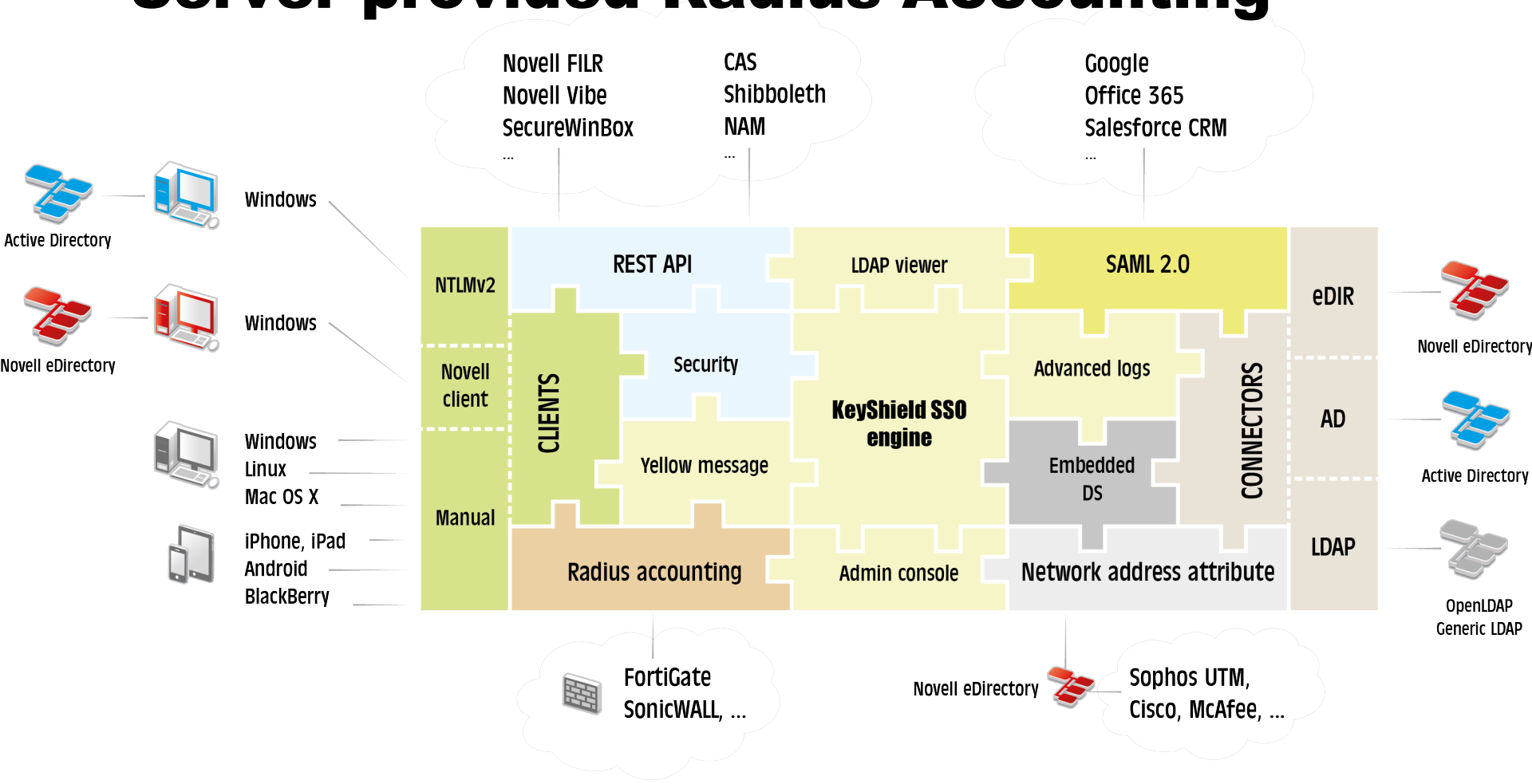
* Oftenly fails due to non-standard connection abort

KeyShield SSO customized

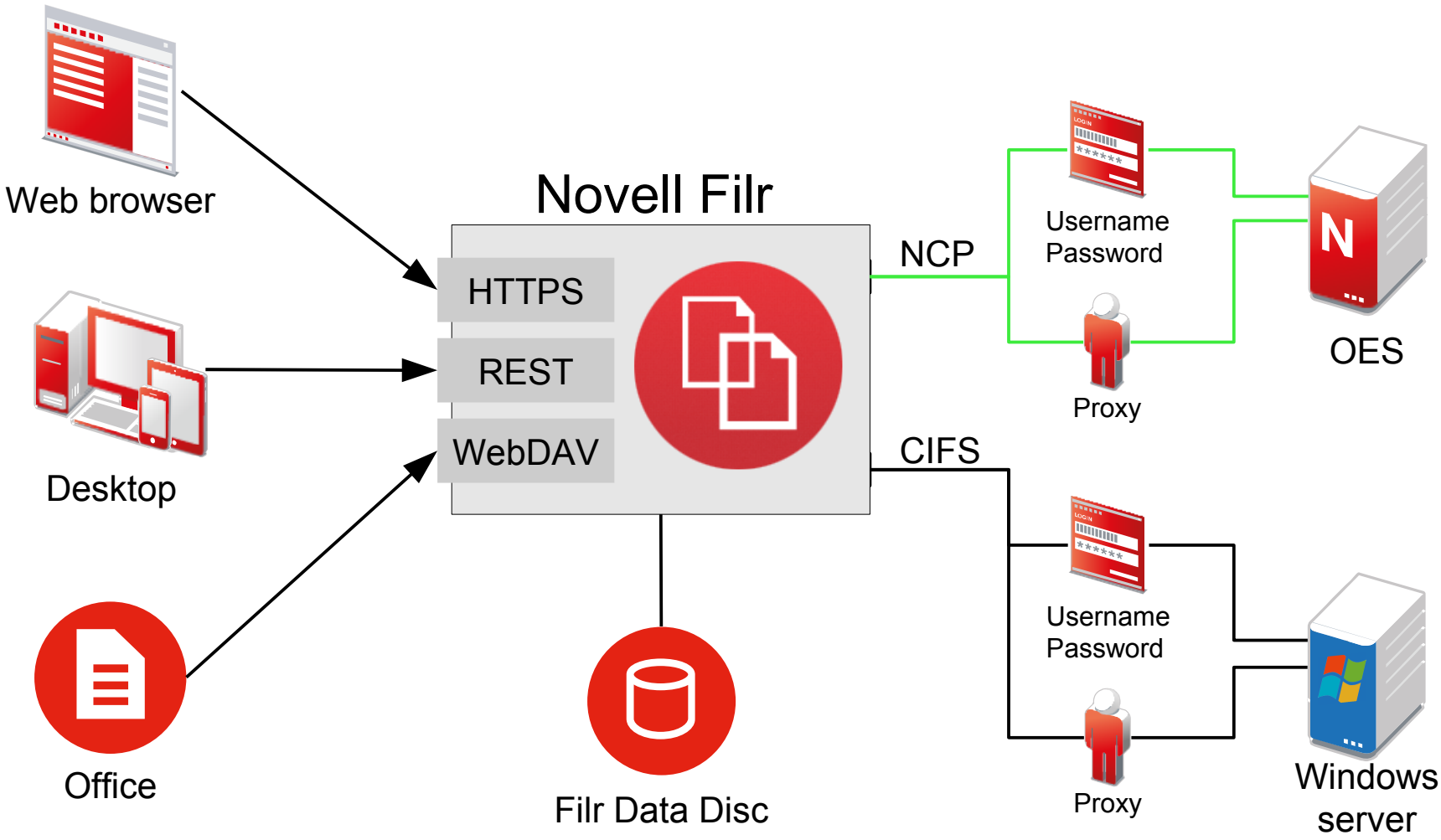


* 100% Reliable, no Ghost IP Addresses

Server provided Radius Accounting

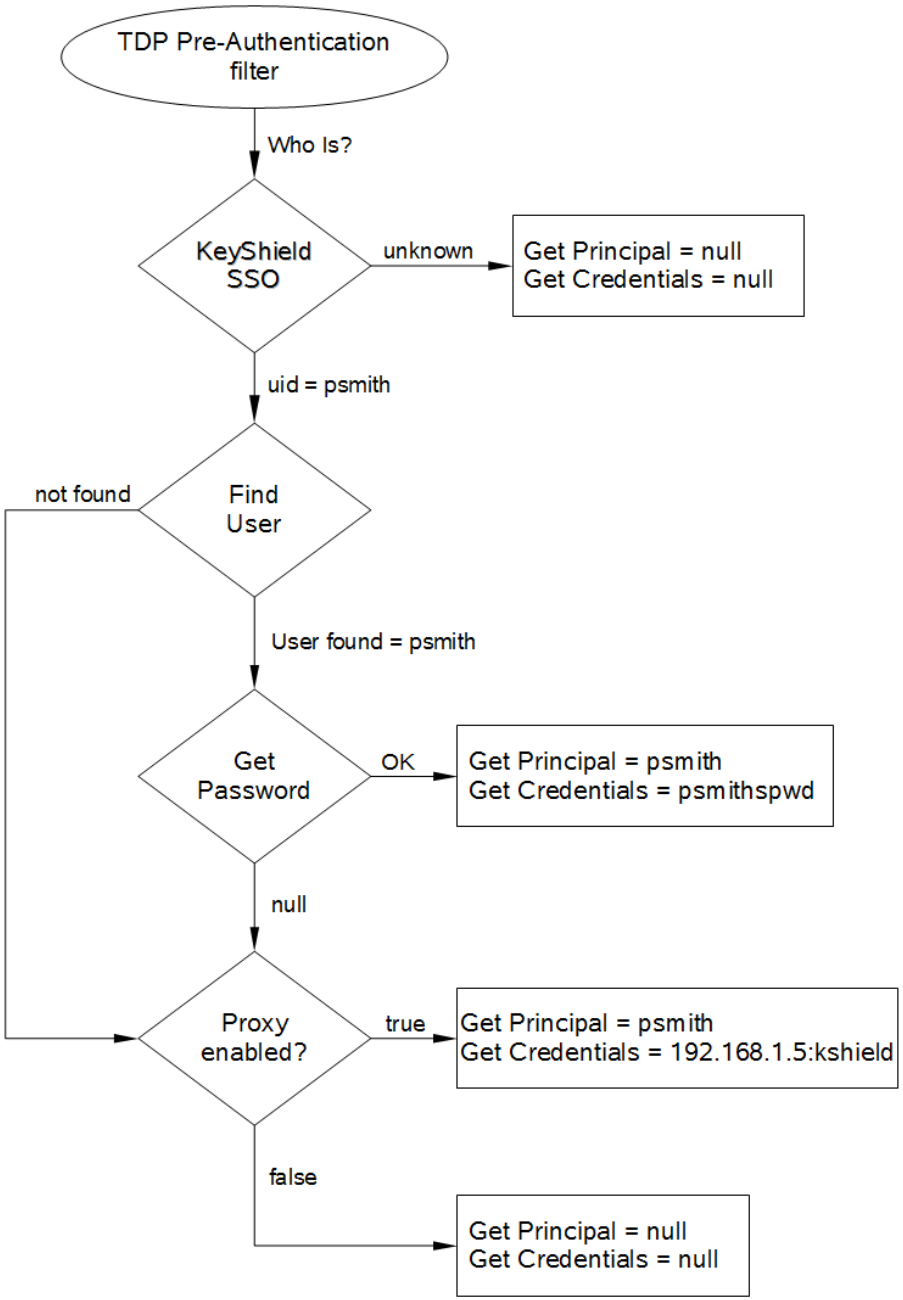


KeyShield SSO



TDP

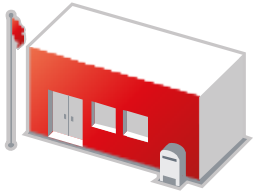
KeyShield SSO



TDP

KeyShield SSO

GW POA



KeyShield SSO Client

WebAccess

KeyShield SSO server

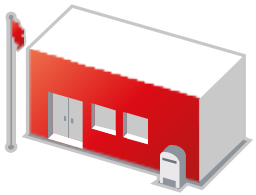
Web browser

GroupWise is not the easy one for SSO, because it uses backend authentication and winning proprietary protocols

TDP

KeyShield SSO

GW POA



KeyShield SSO Client

WebAccess

1

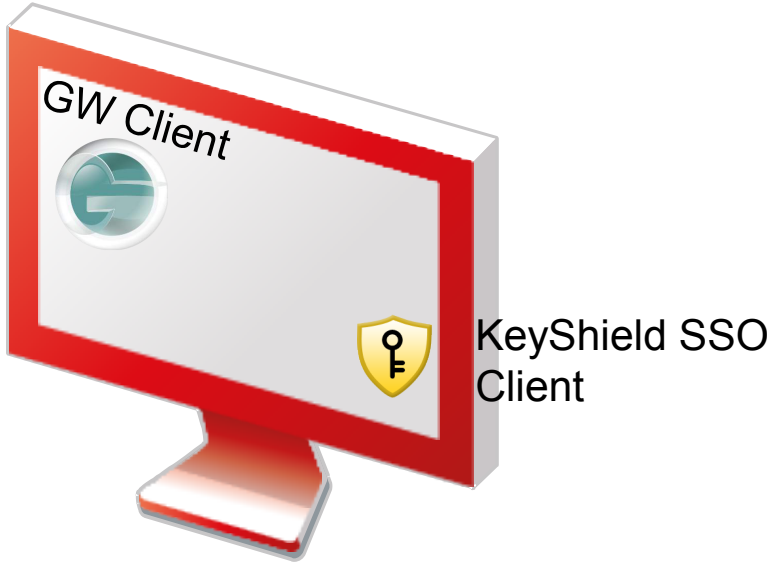
Web browser

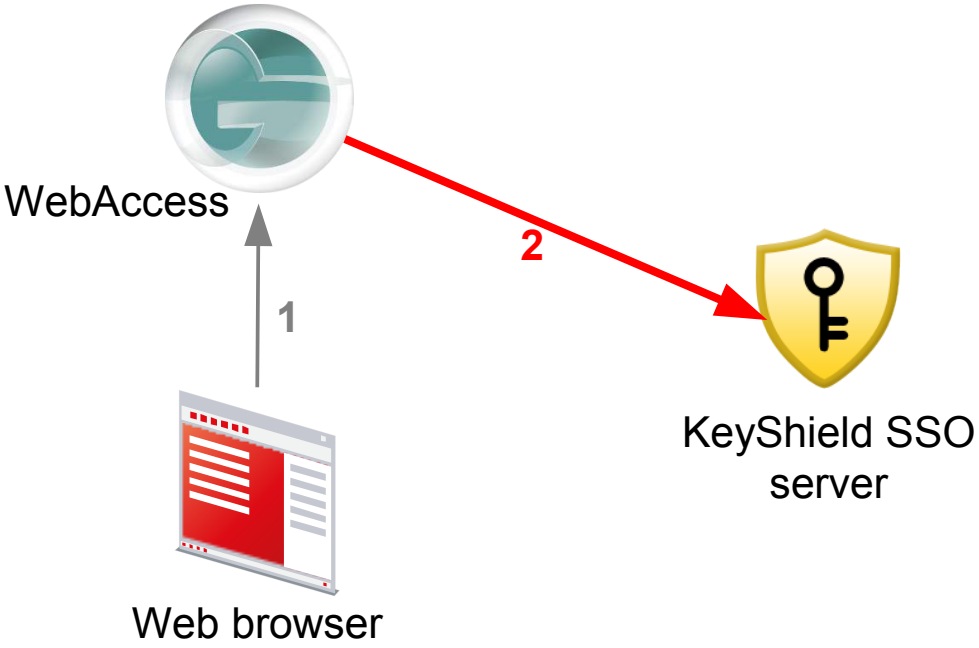
KeyShield SSO server

Browser is knocking the door without valid session

TDP

KeyShield SSO

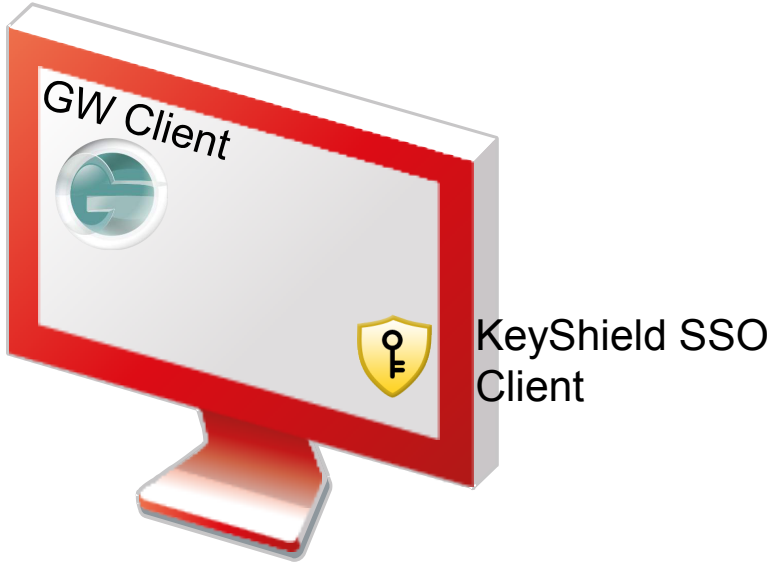


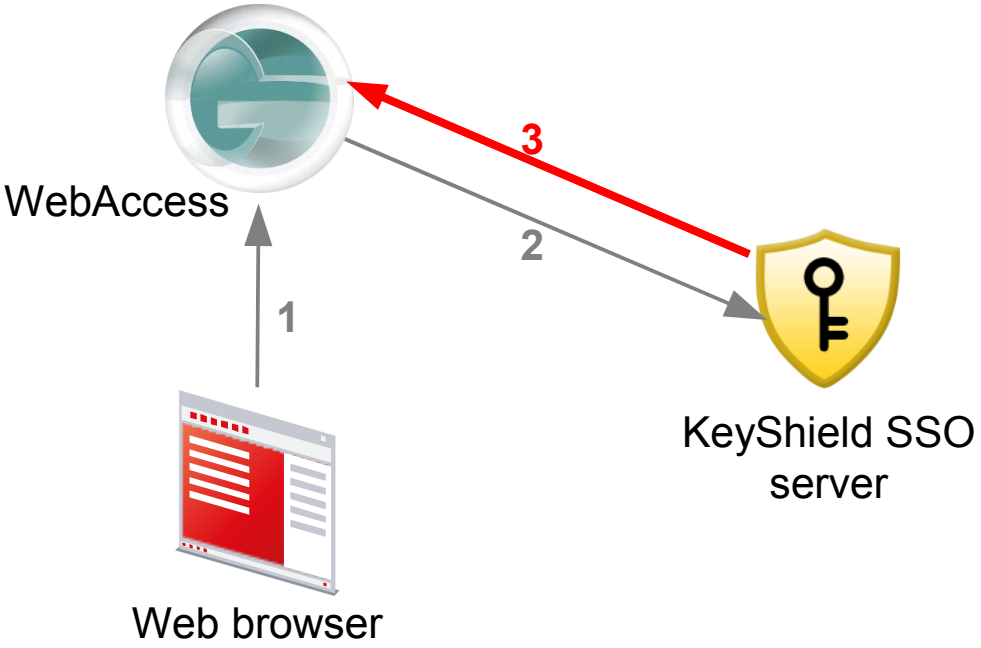


WebAccess asks KeyShield SSO server for user's ID certificate.

TDP

KeyShield SSO

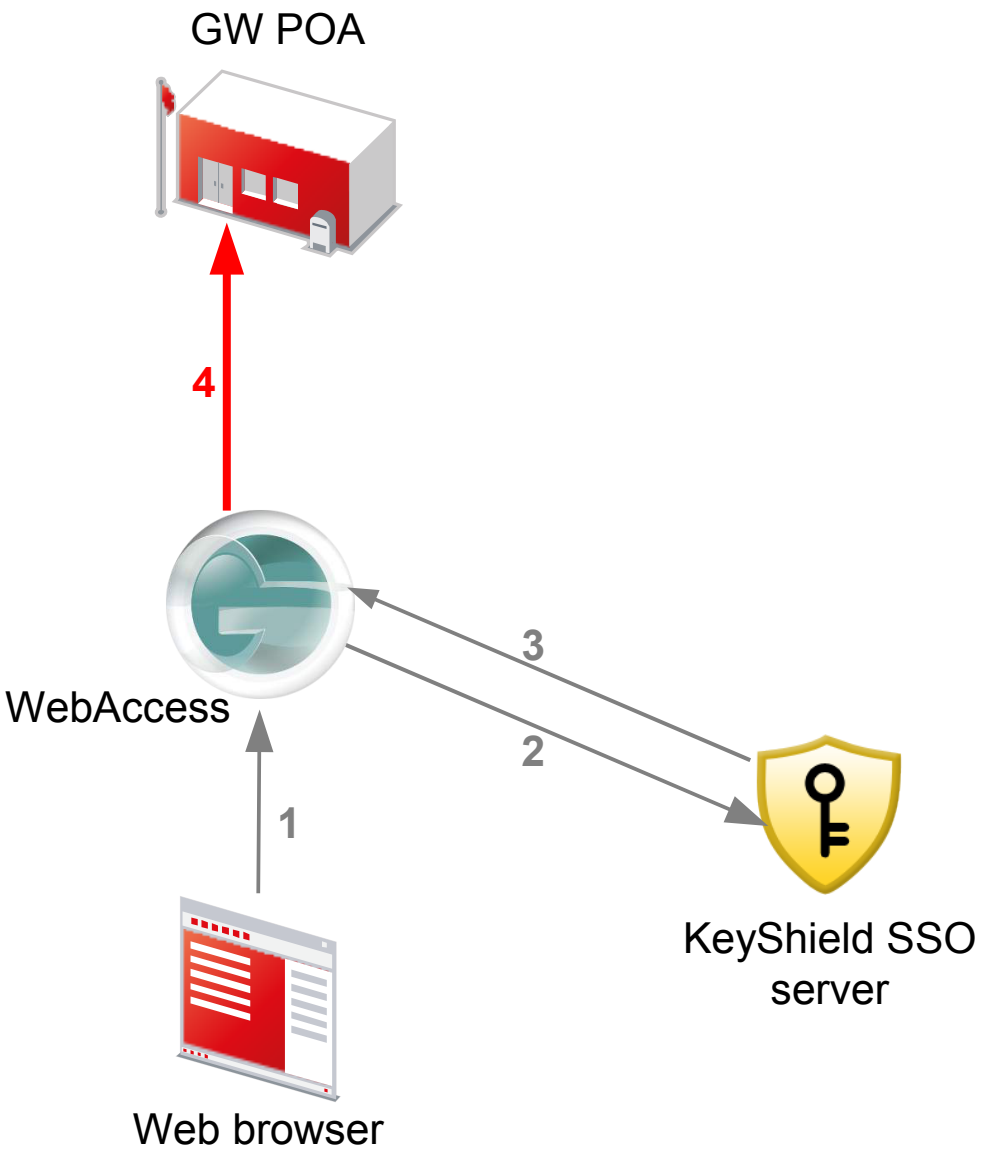


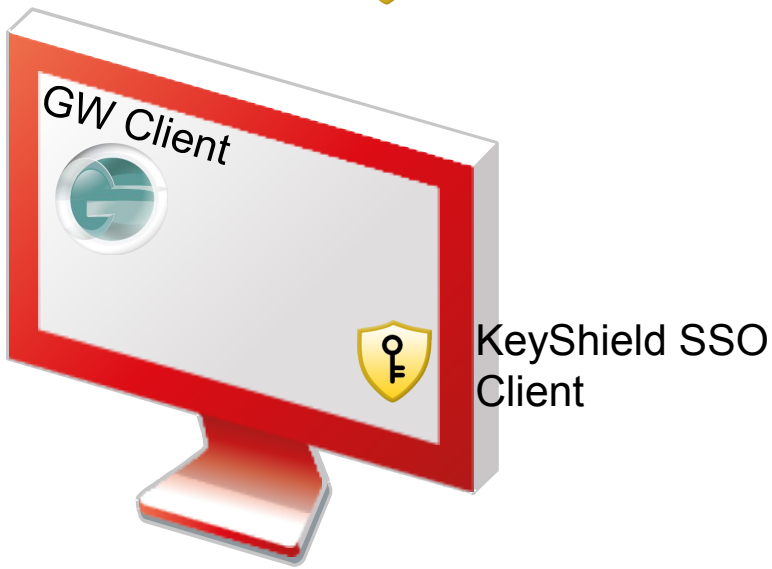


If the response is - user is not known, then standard authentication dialog is used. Otherwise the certificate says, who is the user – email, GUID, FDN

TDP

KeyShield SSO

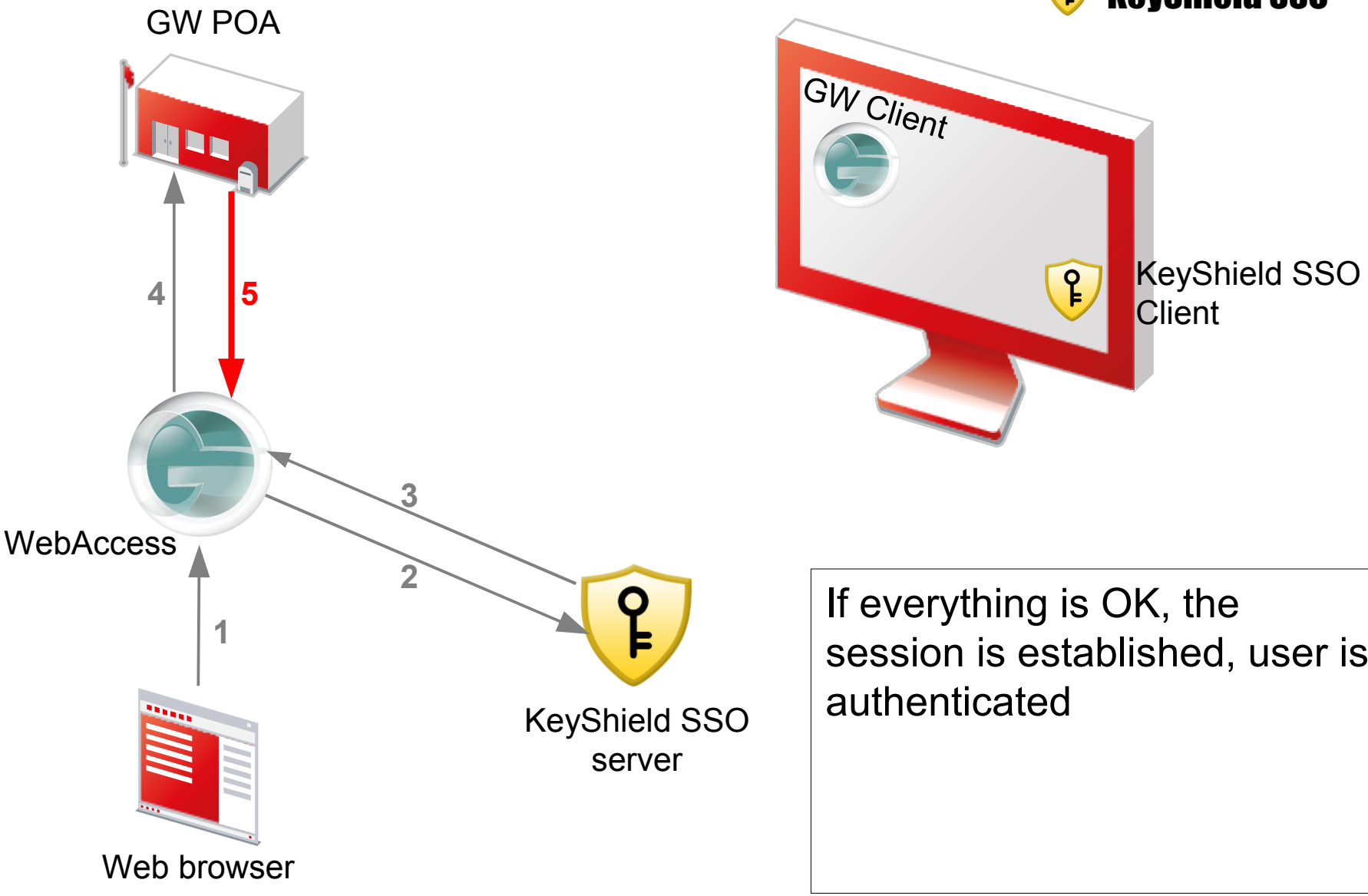




WebAccess send the certificate to POA. POA checks signature, validity and looks for the user

TDP

KeyShield SSO

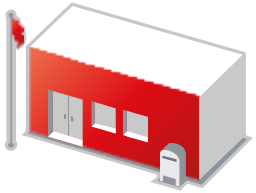


If everything is OK, the session is established, user is authenticated

TDP

KeyShield SSO

GW POA



KeyShield SSO Client

WebAccess

KeyShield SSO server

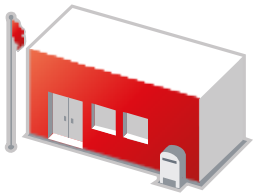
Web browser

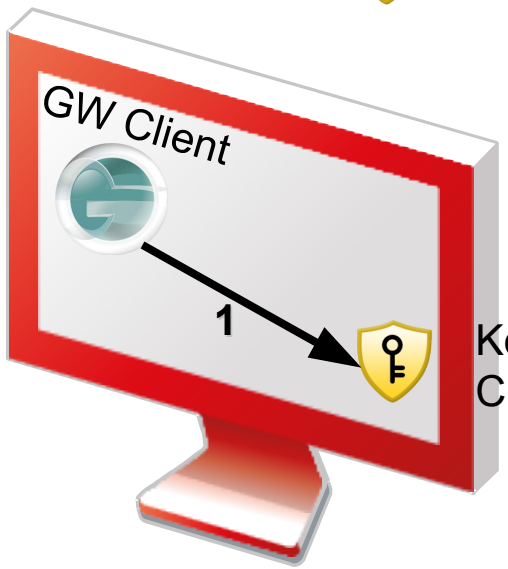
GroupWise client for Windows uses the infrastructure provided by KeyShield SSO client for Windows

TDP

KeyShield SSO

GW POA





KeyShield SSO Client

WebAccess

KeyShield SSO server

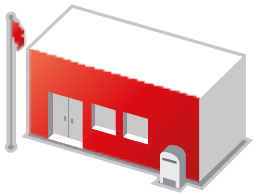
Web browser

GW Client checks presence of KeyShield SSO, then status. If the user is authenticated, GW client requests the certificate

TDP

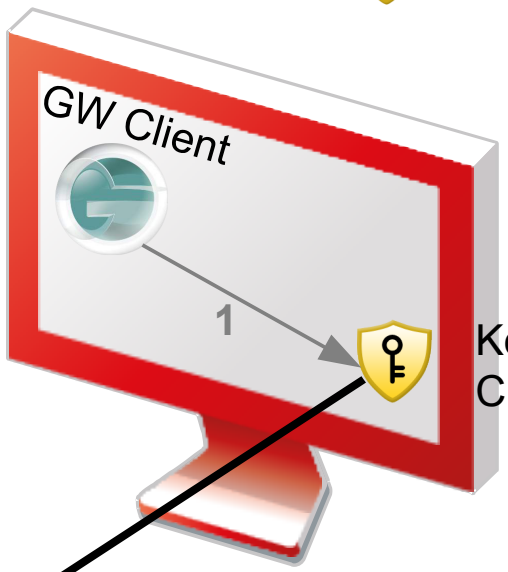
KeyShield SSO

GW POA



WebAccess

Web browser



KeyShield SSO Client

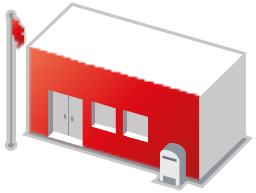
KeyShield SSO server

KeyShield SSO client uses existing secured connection to the server and requests the certificate

TDP

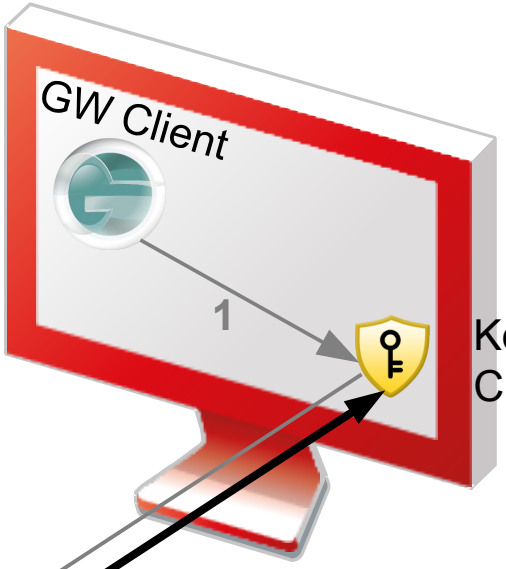
KeyShield SSO

GW POA



WebAccess

Web browser



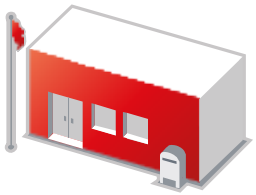
KeyShield SSO
server

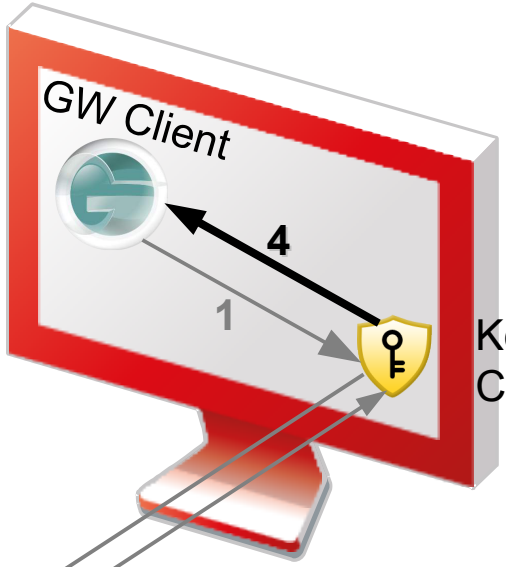
The certificate is delivered to KeyShield SSO client

TDP

KeyShield SSO

GW POA





KeyShield SSO Client

WebAccess

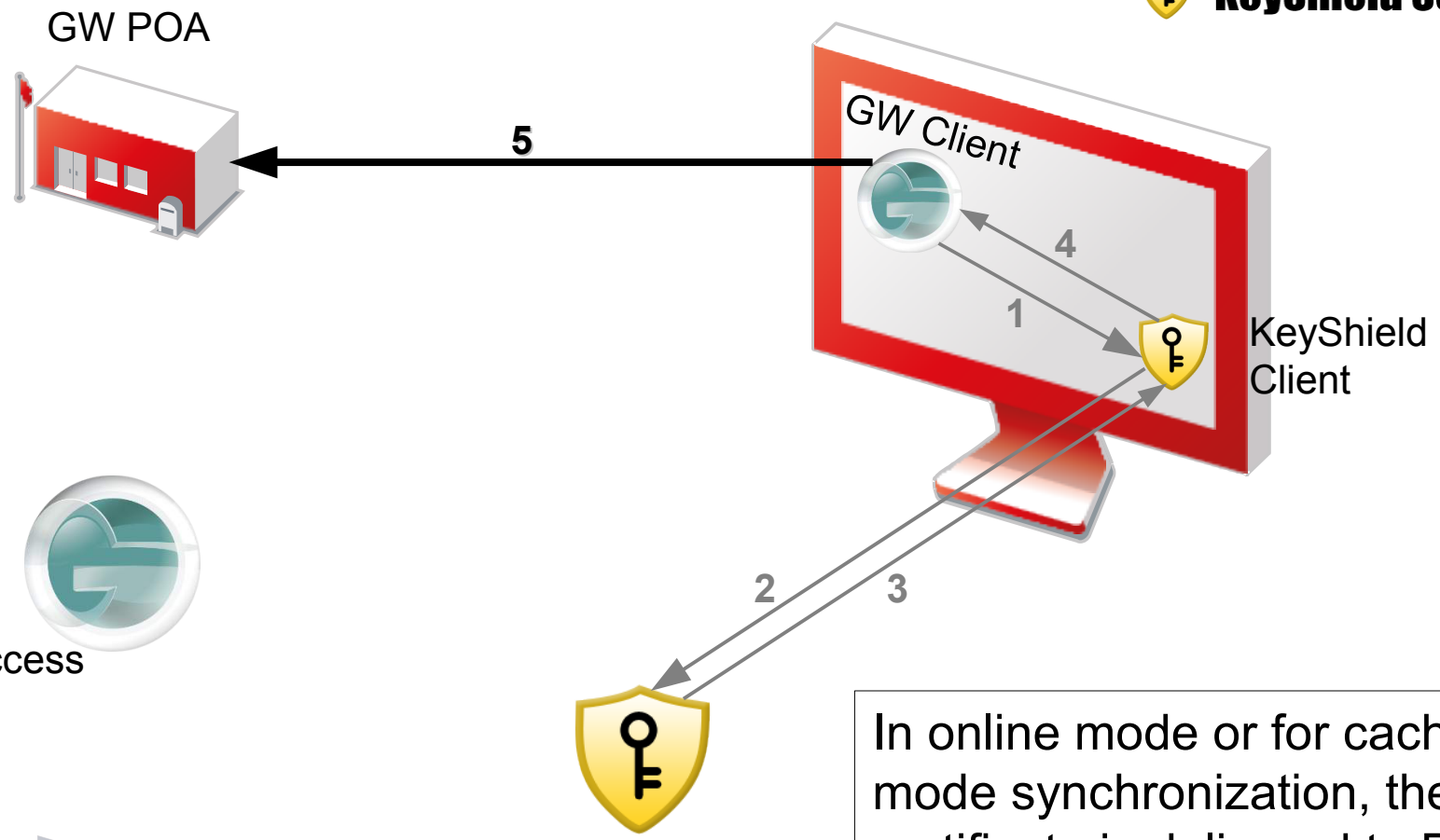
KeyShield SSO server

Web browser

And then passed locally to GroupWise client. If the client is in the cache mode, the certificate is evaluated locally with use of CA certificate synchronised from PO

TDP

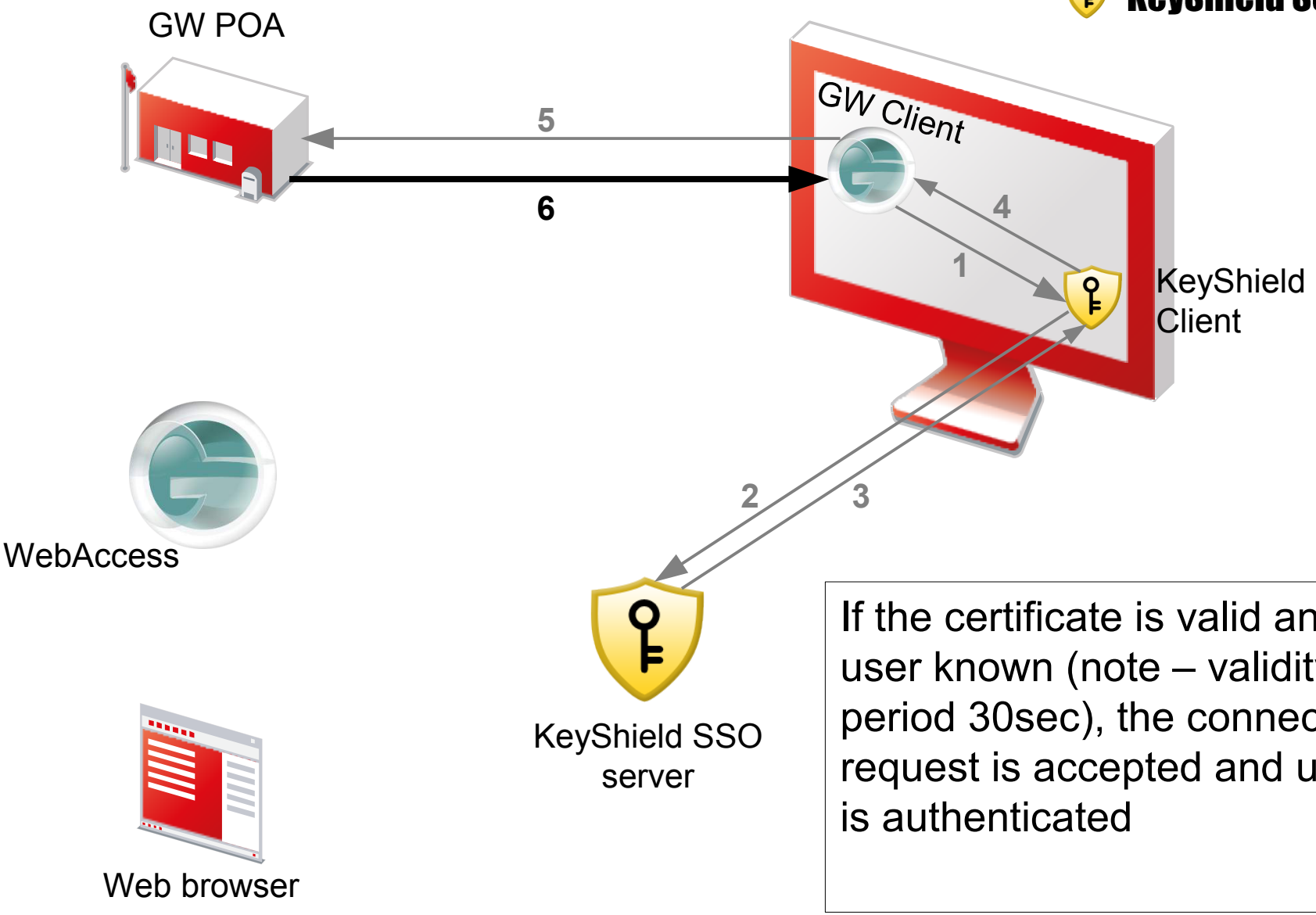
KeyShield SSO



In online mode or for cache mode synchronization, the certificate is delivered to POA instead of username/password

TDP

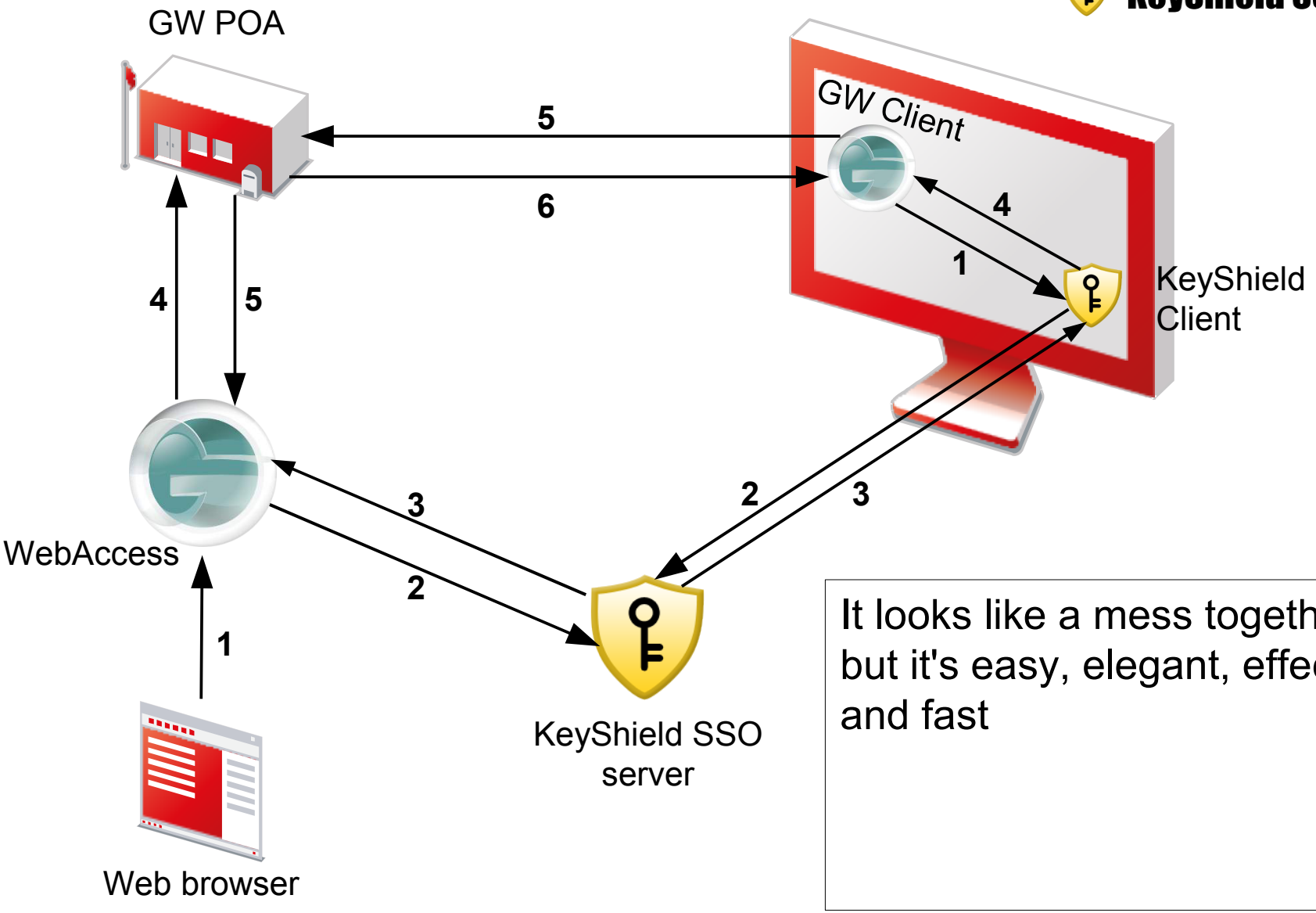
KeyShield SSO



If the certificate is valid and user known (note – validity period 30sec), the connection request is accepted and user is authenticated

TDP

KeyShield SSO



It looks like a mess together but it's easy, elegant, effective and fast

TDP

ČZU

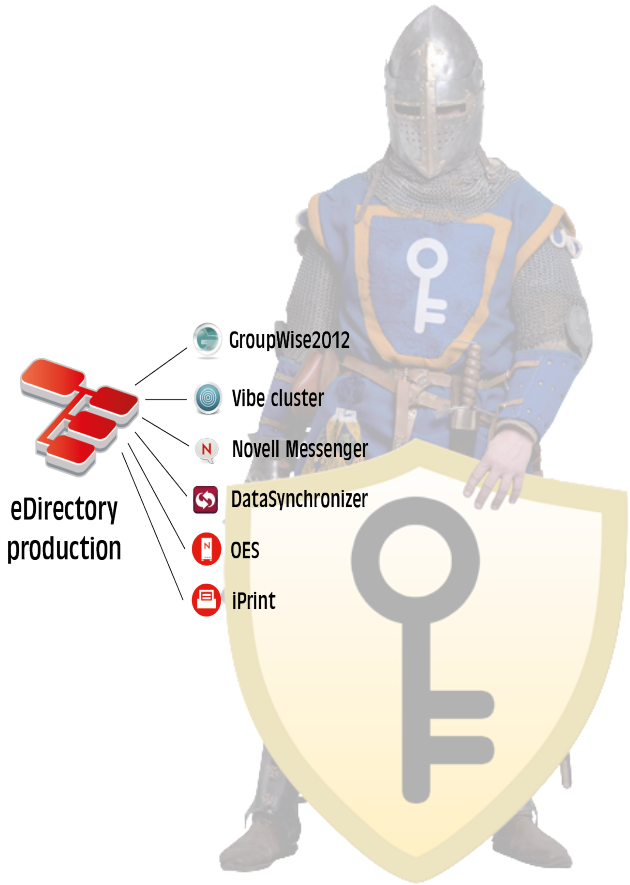
KeyShield SSO

eDirectory
production

TDP

ČZU

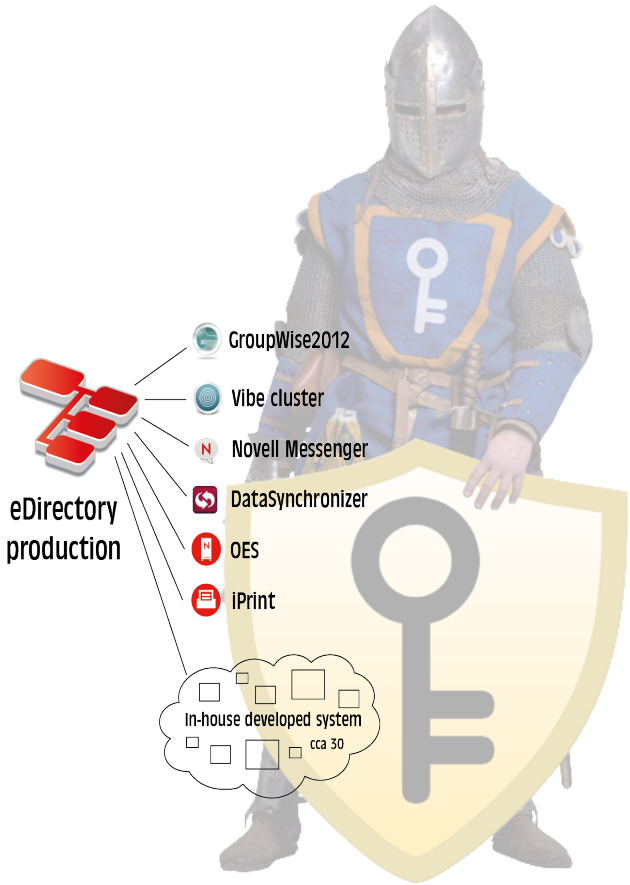
KeyShield SSO



TDP

ČZU

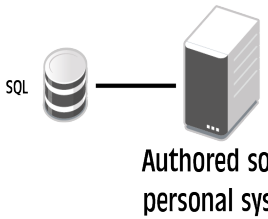
KeyShield SSO

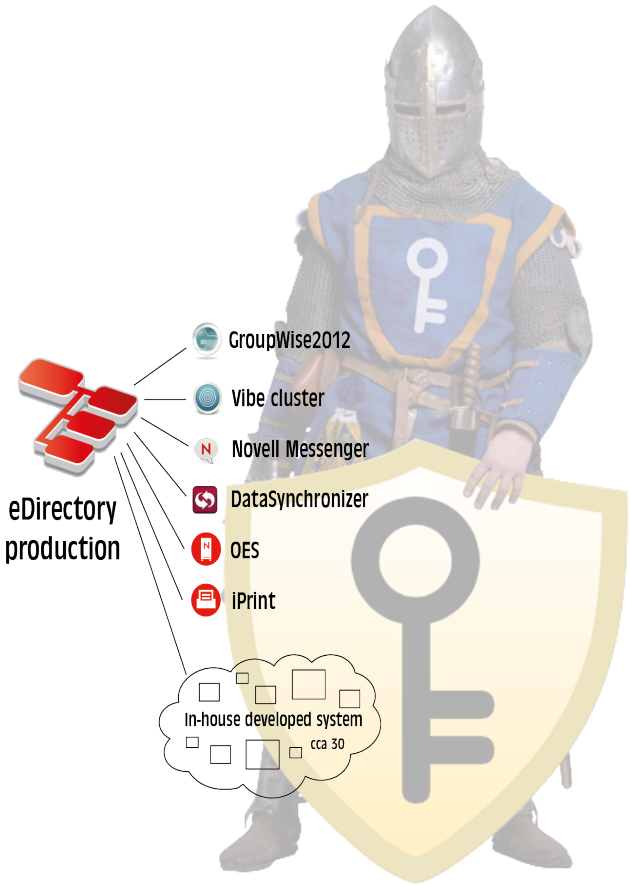


TDP

ČZU

KeyShield SSO

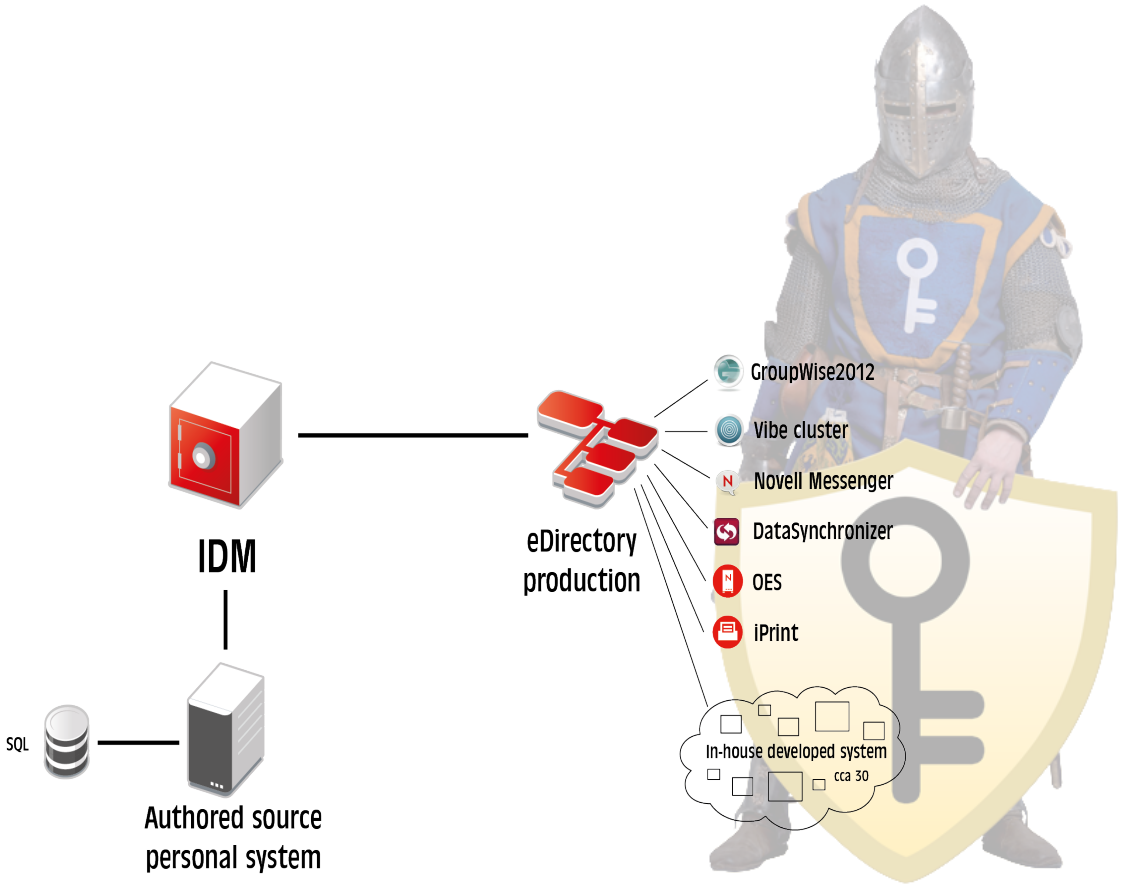




TDP

KeyShield SSO

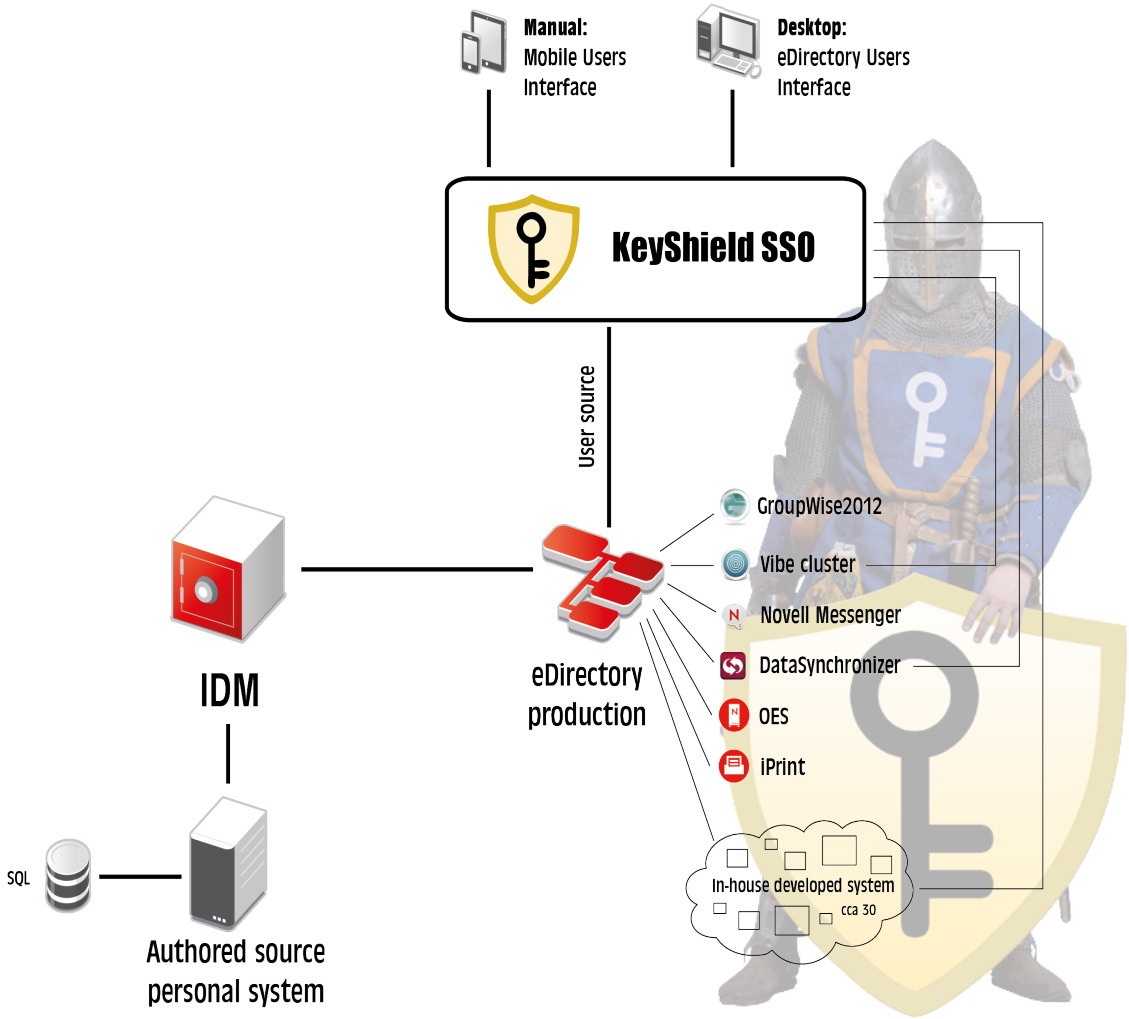
ČZU



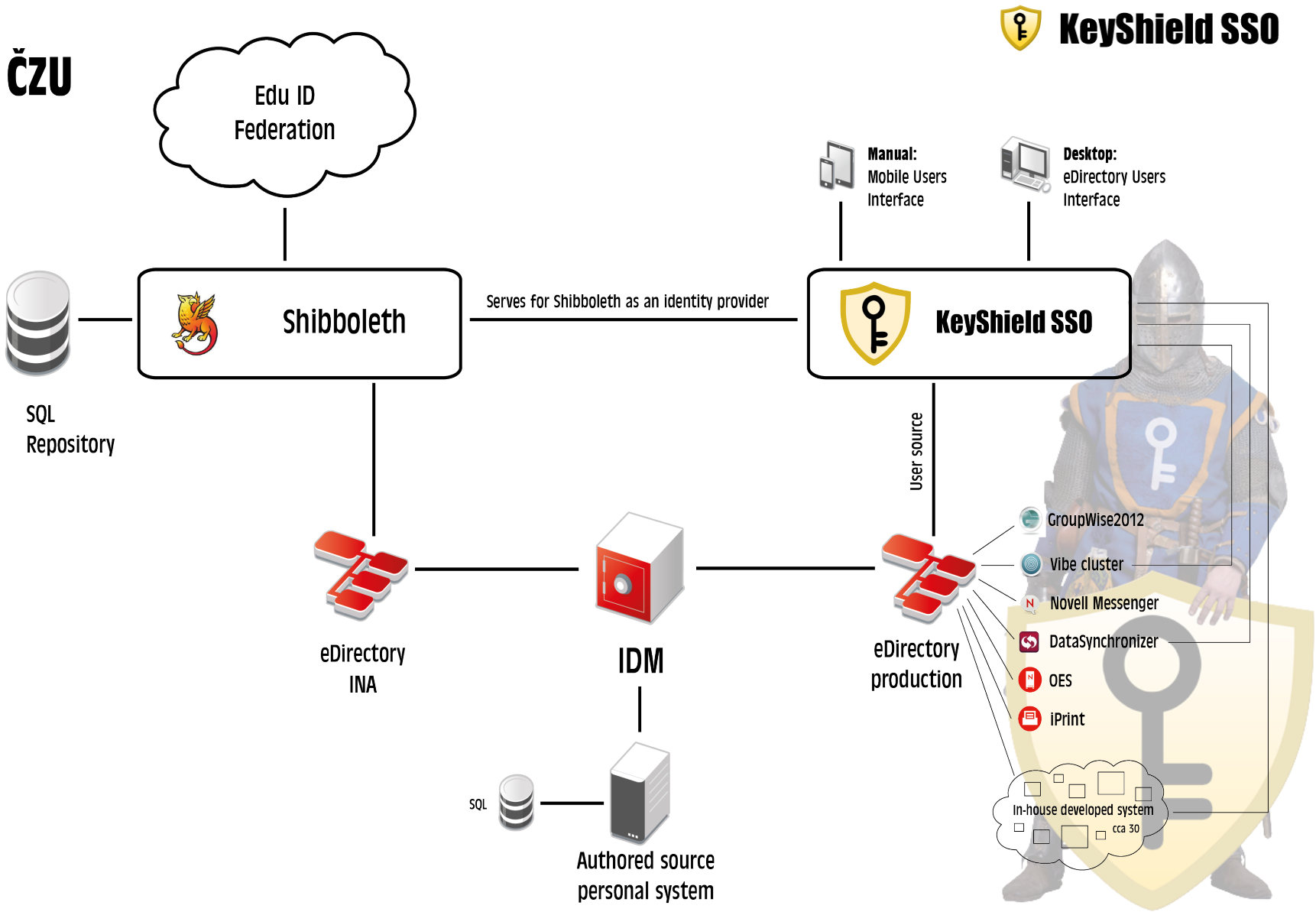
TDP

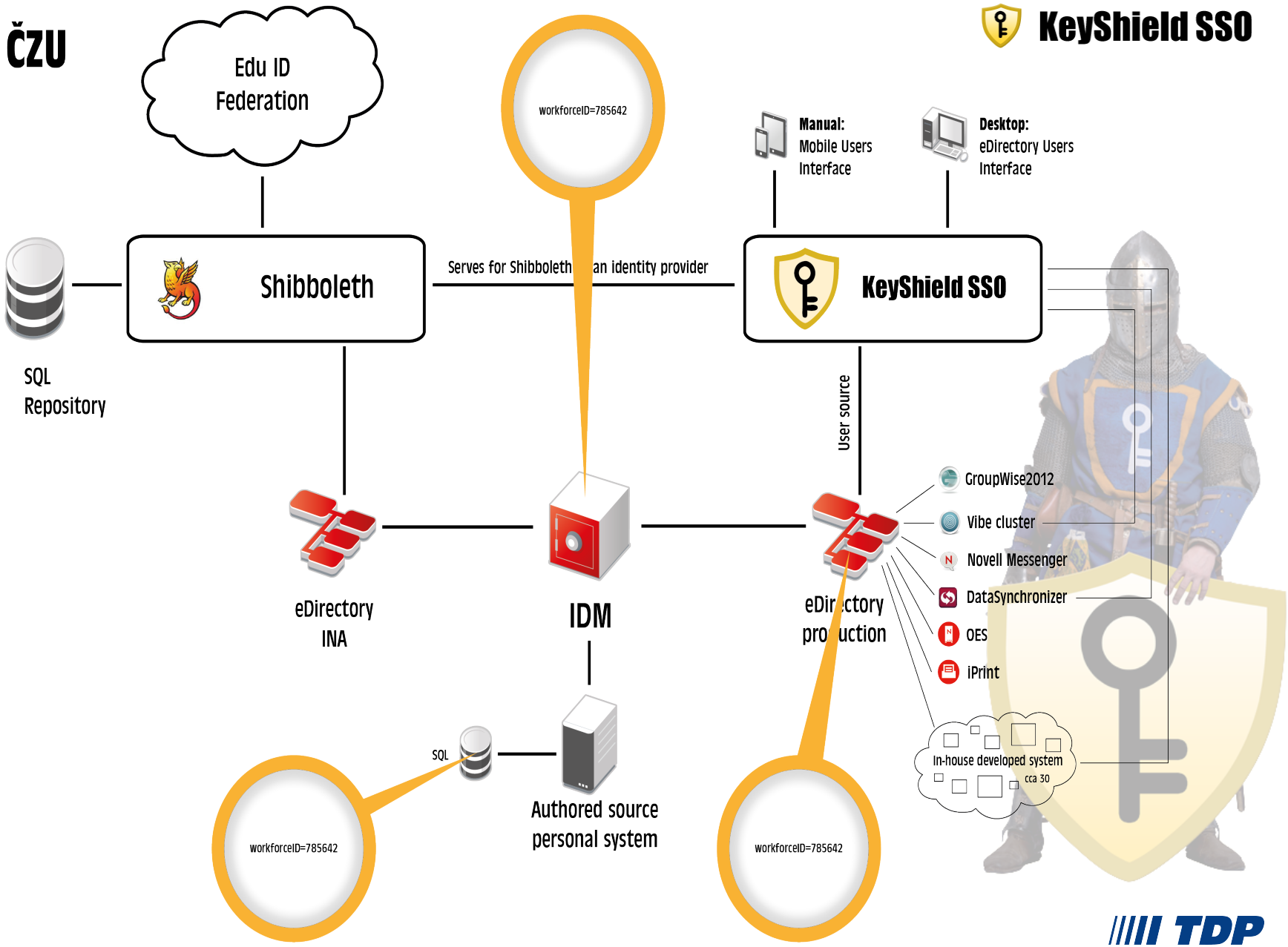
KeyShield SSO

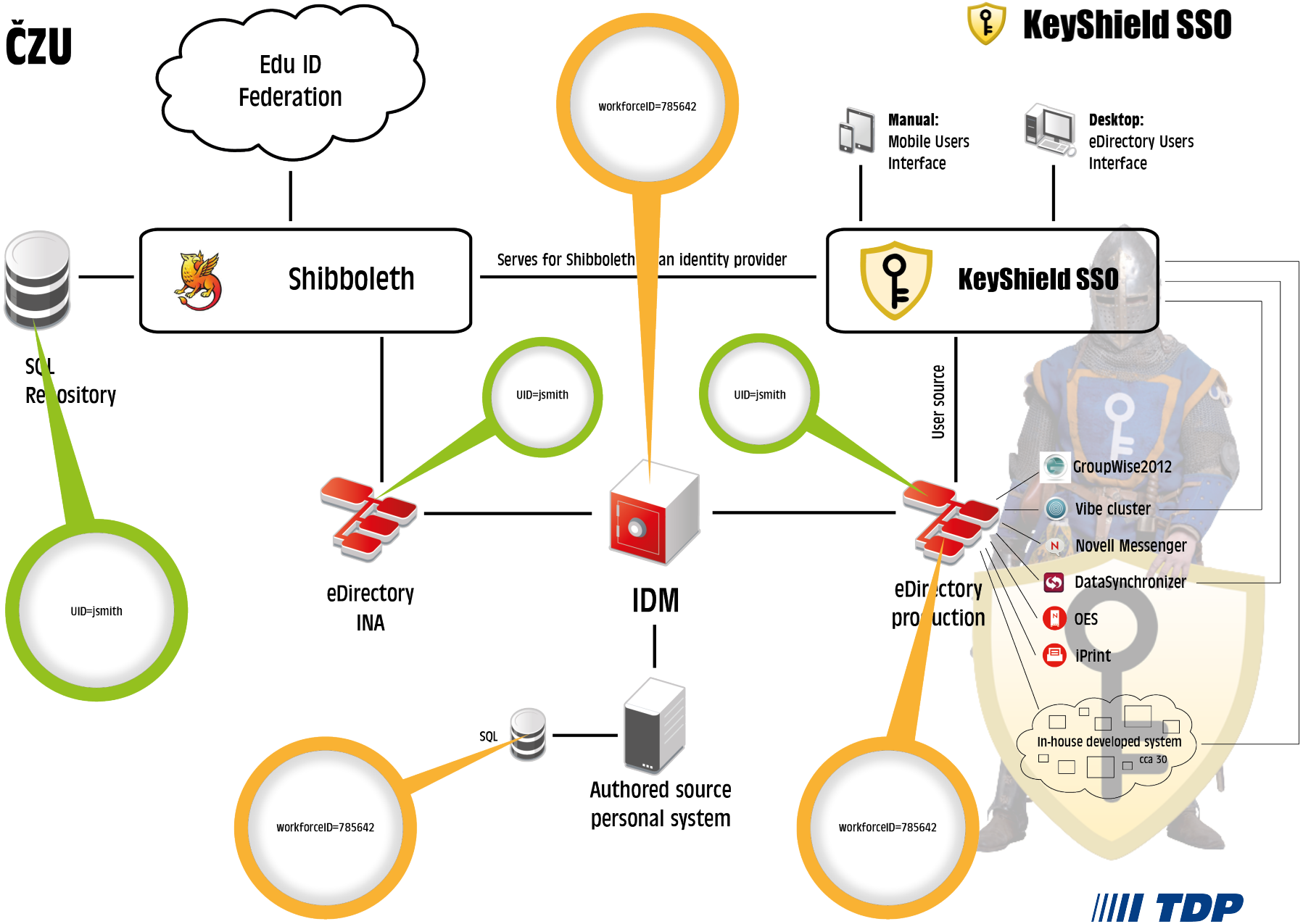
ČZU



TDP


ČZU
KeyShield SSO
Edu ID
Federation
Manual:
Mobile Users
Interface
Desktop:
eDirectory Users
Interface
Shibboleth
Serves for Shibboleth as an identity provider
KeyShield SSO
SQL
Repository
User source
eDirectory
INA
IDM
eDirectory
production
GroupWise2012
Vibe cluster
Novell Messenger
DataSynchronizer
OES
iPrint
In-house developed system
cca 30
SQL
Authored source
personal system
TDP


ČZU
KeyShield SSO
Edu ID
Federation
workforceID=785642
Manual:
Mobile Users
Interface
Desktop:
eDirectory Users
Interface
Shibboleth
Serves for Shibboleth an identity provider
KeyShield SSO
SQL
Repository
User source
GroupWise2012
Vibe cluster
Novell Messenger
DataSynchronizer
OES
iPrint
In-house developed system
cca 30
eDirectory
INA
IDM
eDirectory
production
SQL
Authored source
personal system
workforceID=785642
workforceID=785642
TDP

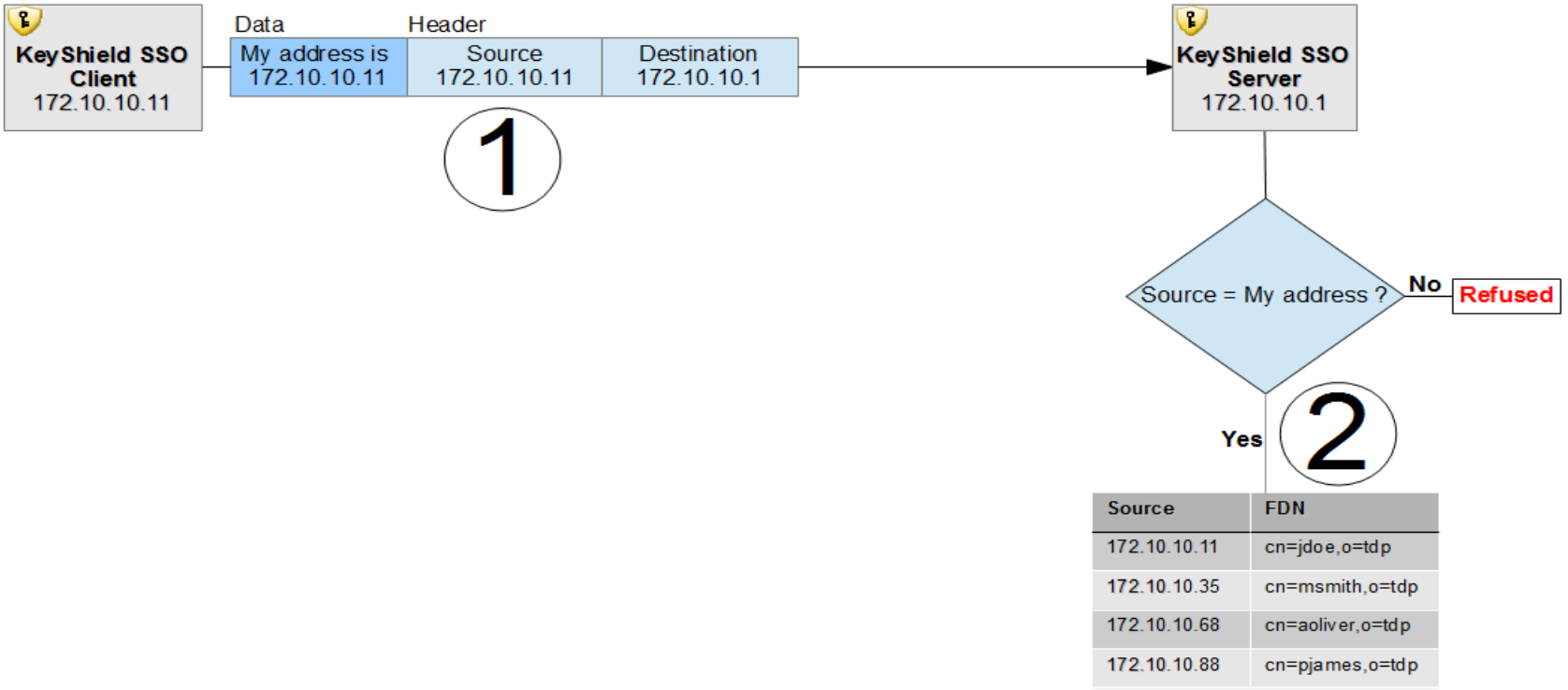

ČZU
KeyShield SSO
Edu ID
Federation
workforceID=785642
Manual:
Mobile Users
Interface
Desktop:
eDirectory Users
Interface
Shibboleth
Serves for Shibboleth an identity provider
KeyShield SSO
SQL
Repository
UID=jsmith
UID=jsmith
UID=jsmith
User source
eDirectory
INA
IDM
eDirectory
production
GroupWise2012
Vibe cluster
Novell Messenger
DataSynchronizer
OES
iPrint
In-house developed system
cca 30
SQL
Authored source
personal system
workforceID=785642
workforceID=785642
TDP

KeyShield SSO

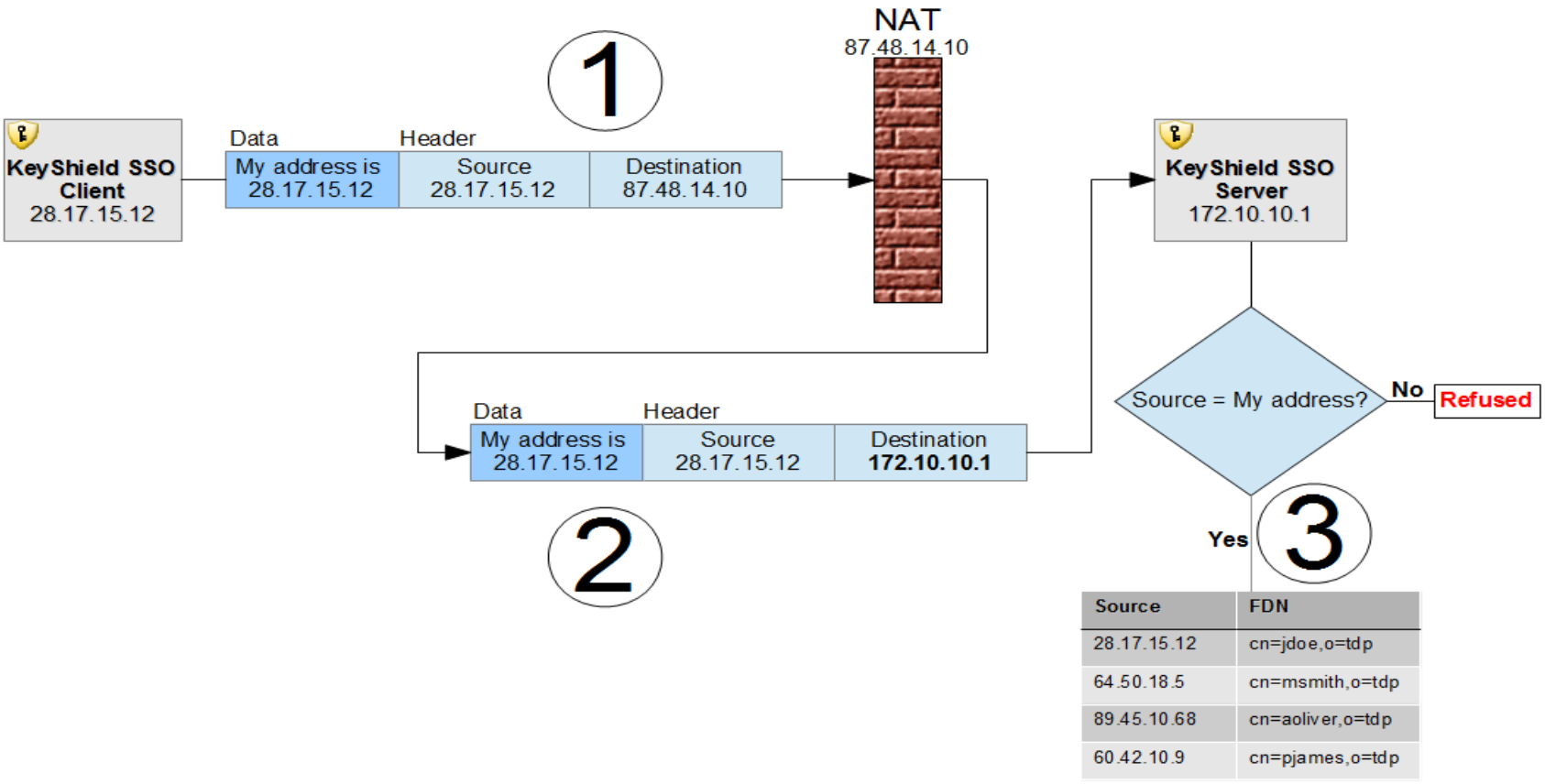
Q/A

vsamsa@tdp.cz

KeyShield SSO - LAN

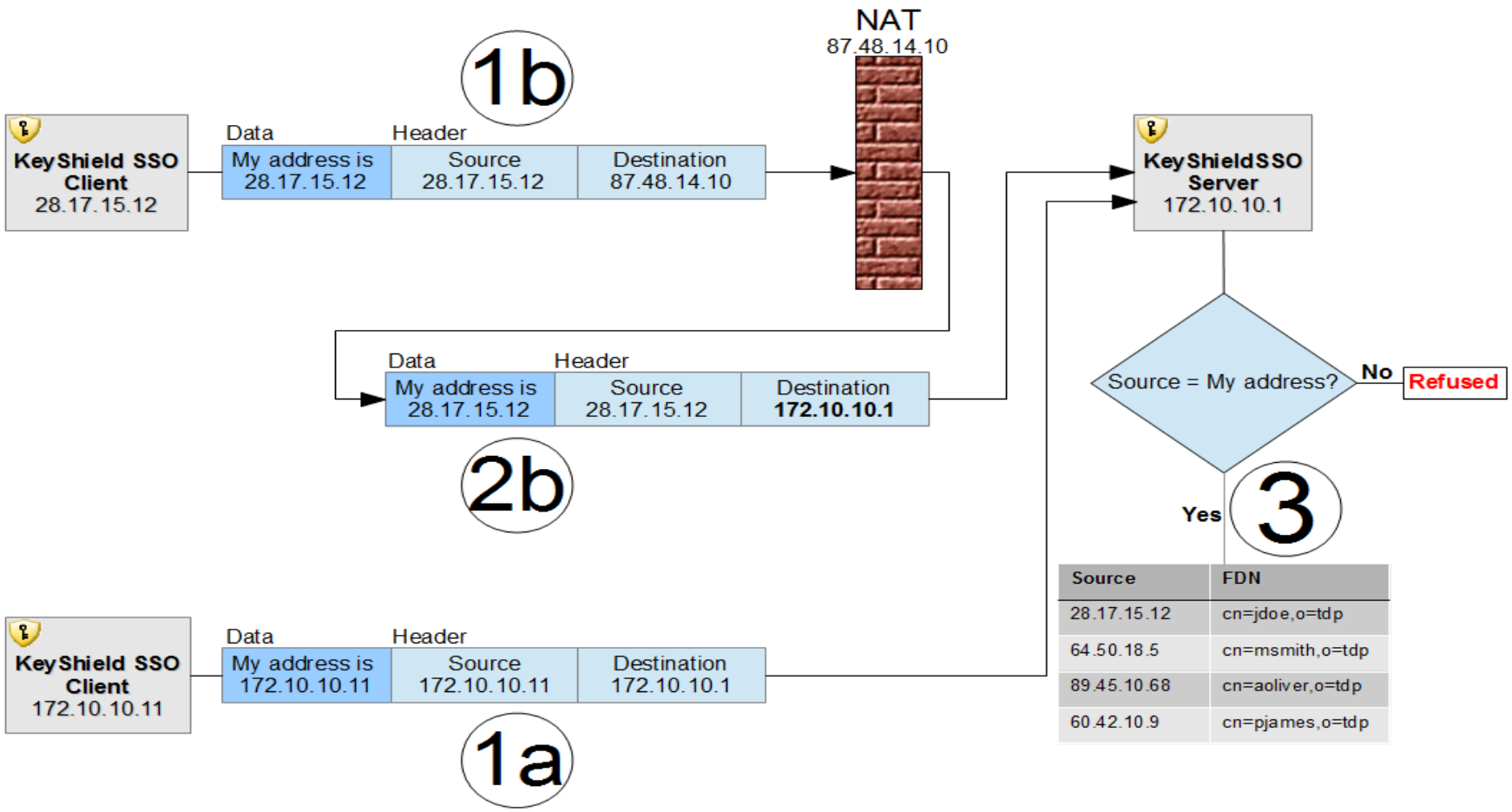


KeyShield SSO – server behind NAT

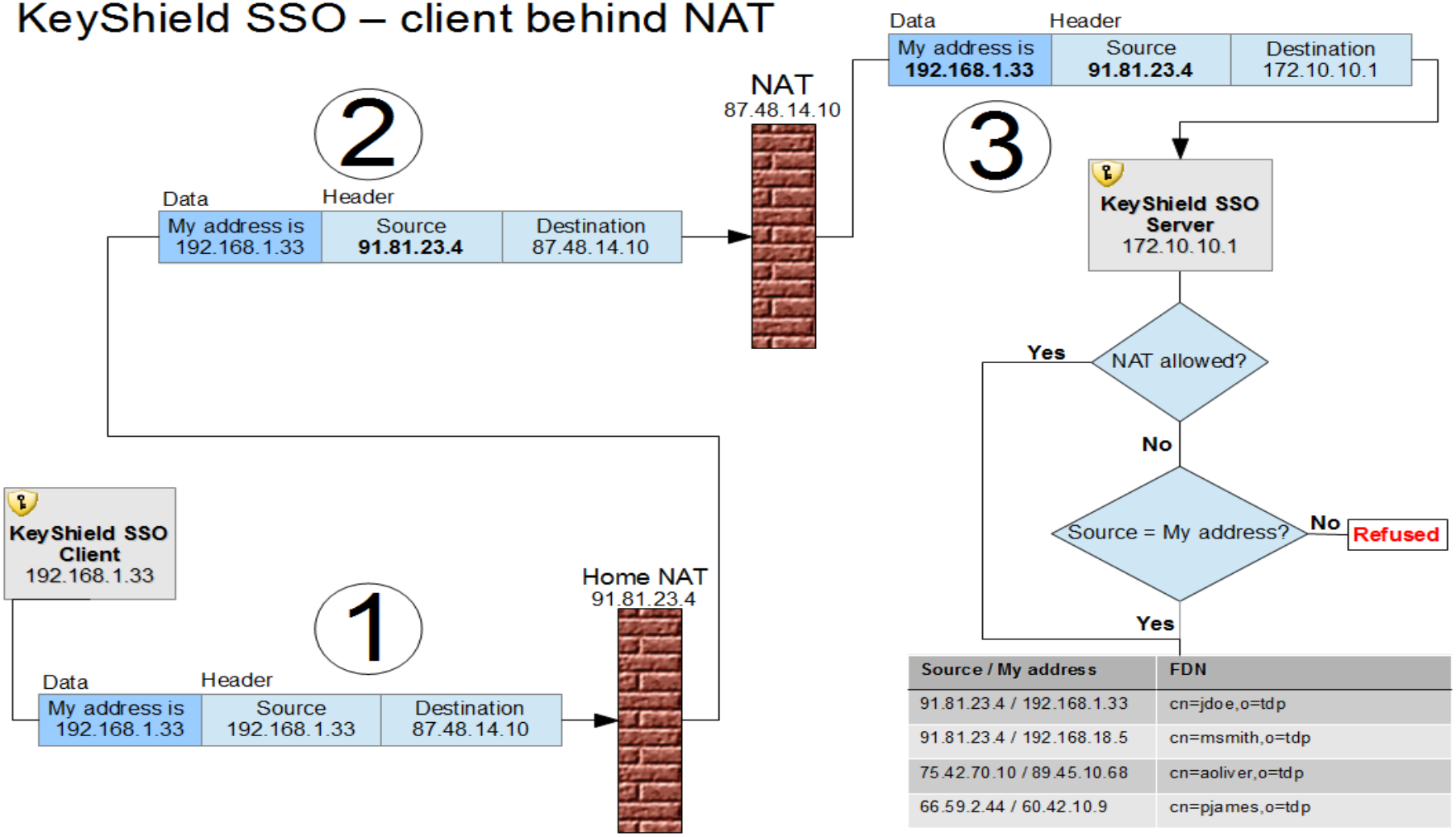


Source	FDN
28.17.15.12	cn=jdoe,o=tdp
64.50.18.5	cn=msmith,o=tdp
89.45.10.68	cn=aoliver,o=tdp
60.42.10.9	cn=pjames,o=tdp

KeyShield SSO – server in LAN and behind NAT



KeyShield SSO – client behind NAT



Source / My address	FDN
91.81.23.4 / 192.168.1.33	cn=jdoe,o=tdp
91.81.23.4 / 192.168.18.5	cn=msmith,o=tdp
75.42.70.10 / 89.45.10.68	cn=aoliver,o=tdp
66.59.2.44 / 60.42.10.9	cn=pjames,o=tdp