Security Workshop 2013 – Improving Security in a Hacker's World

Workshop

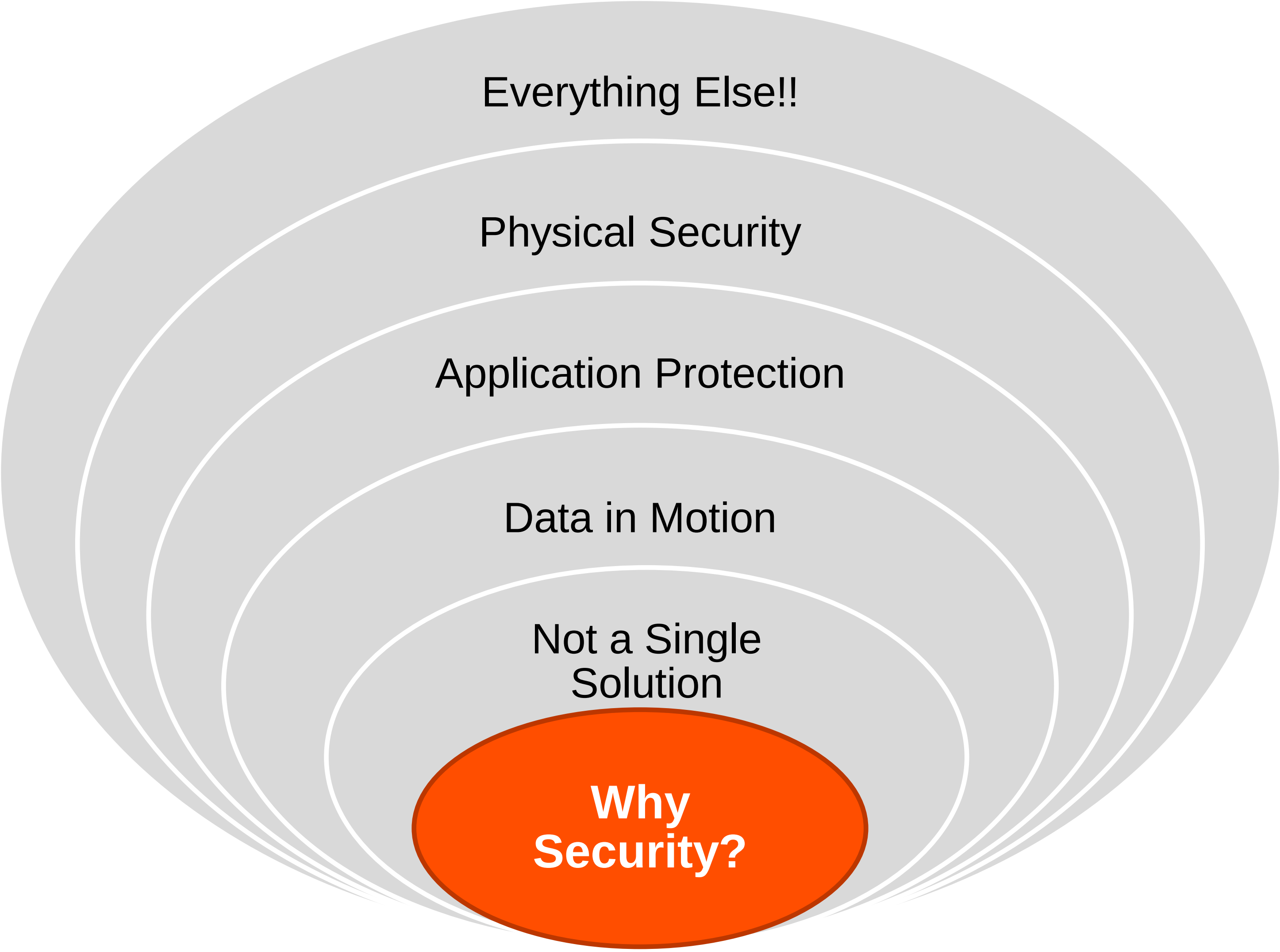
Steve, Roy, Rob, Brian, Peter
Progress Software
Today

PROGRESS EXCHANGE 2013
DISCOVER. DEVELOP. DELIVER.

Agenda and Timeframes

Topic	Type	Presenter	Approx. Length (Minutes)
Introductions / Opening	Lecture	Brian Bowman	10
A Wide Open World	Lab		10
Data In Motion	Lecture	Steve Boucher	15
Enabling SSL	Lab		15
Application Protection	Lecture	Rob Marshall	15
Client Principle	Lab		30
External Security	Lecture	Brian Bowman & Roy Ellis	10
LDAP Authentication	Lab		15
Physical Security	Lecture	Brian & Roy	10
TDE	Lab		15
Misc. Topics	Lecture	Rob & Brian	10
Tying it all together	Lecture	Peter Judge	30

Agenda



Everything Else!!

Physical Security

Application Protection

Data in Motion

Not a Single Solution

Why Security?

Lab # 1 – Introduction to Security

Why Security?

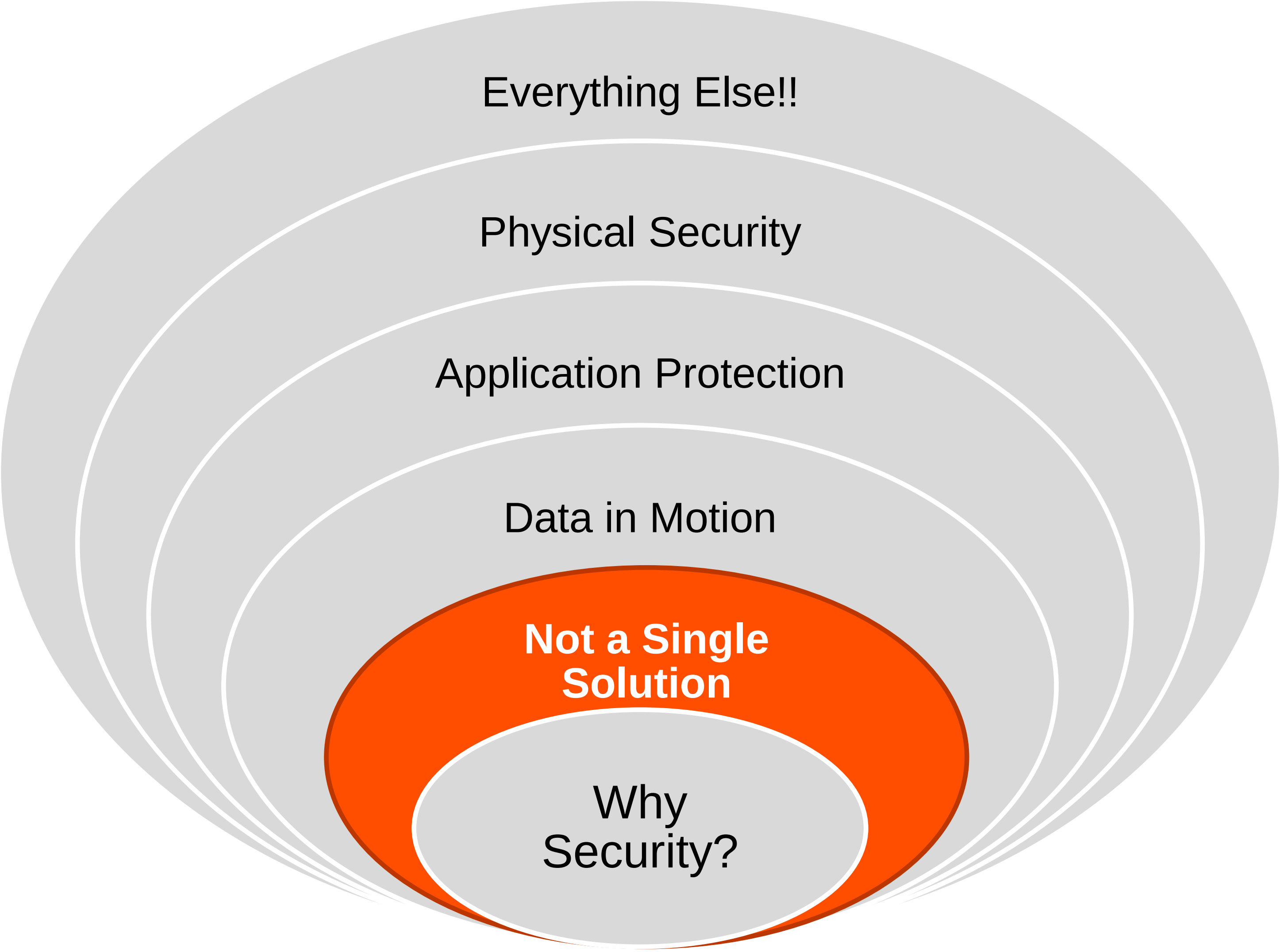
- The need to provide **Security** for data continues to increase
- Affects many Market segments
  - Finance
  - Retail
  - Healthcare and more
- Governments have enacted legislation to enforce **Compliance** of data
- Protecting intellectual property (i.e. your application code)
- Mobile computing greatly increases security risks
  - Laptops with sensitive data
  - Mobile devices (phones and tablets) with passwords stored on them

Compliance Legislation Examples

- Payment Card Industry (PCI)
- Health Insurance Portability & Accountability Act (HIPPA)
- Sarbanes-Oxley Act (SOX)
- Public company accounting reform and investor protection
- European Union Data Protection Directive

“Must Have” Conformance to do Business

Agenda



Everything Else!!

Physical Security

Application Protection

Data in Motion

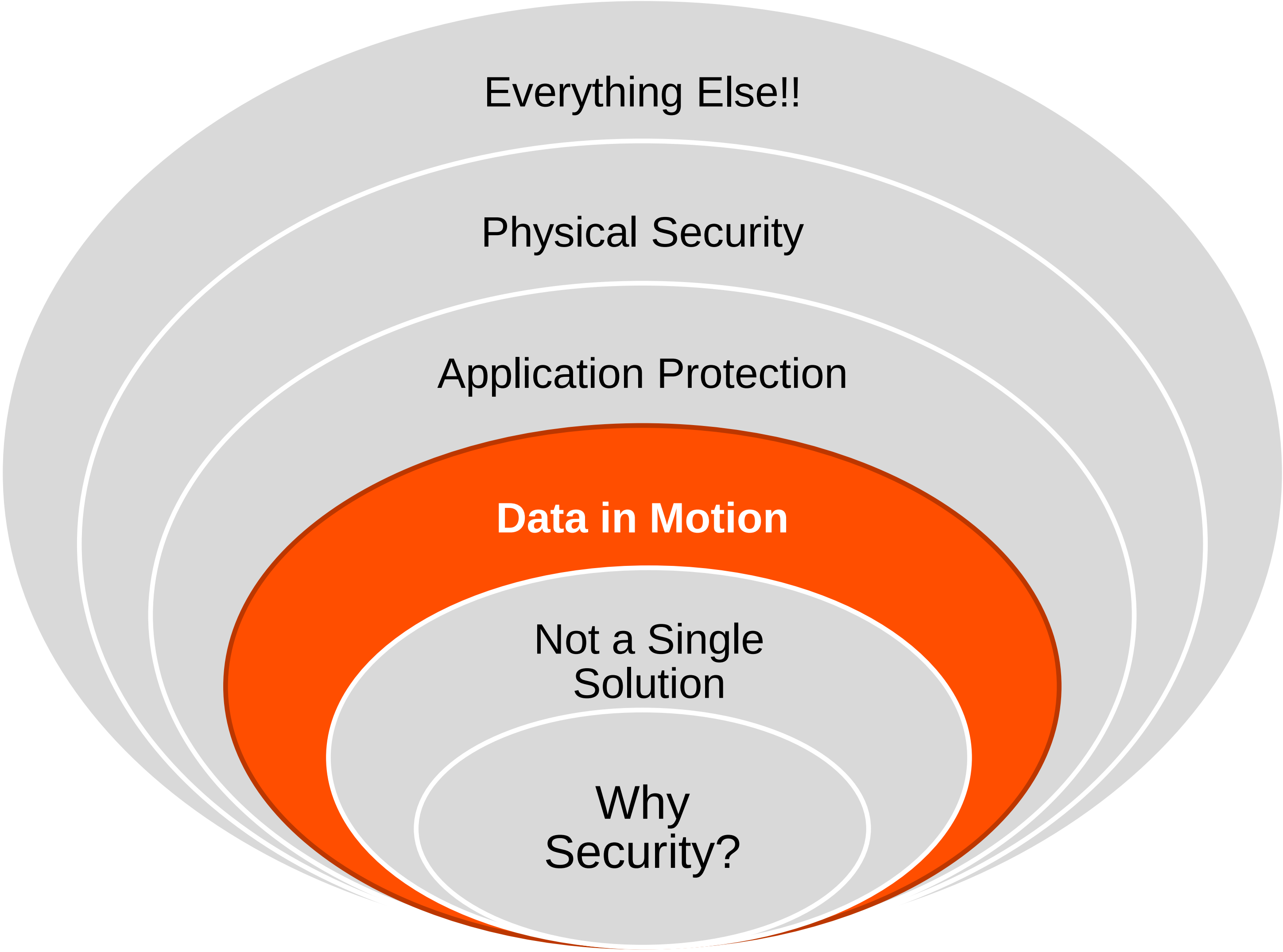
Not a Single Solution

Why Security?

Security is Not a Solution…

- Security is not a solution, but a process
  - Requires a set of defined goals and exclusions
  - Requires monitoring
  - Requires updating as technology and system access evolve
- Protecting vital data via security is a multiple step approach using:
  - Environment
  - Process
  - Hardware
  - Software

Agenda



Everything Else!!

Physical Security

Application Protection

Data in Motion

Not a Single Solution

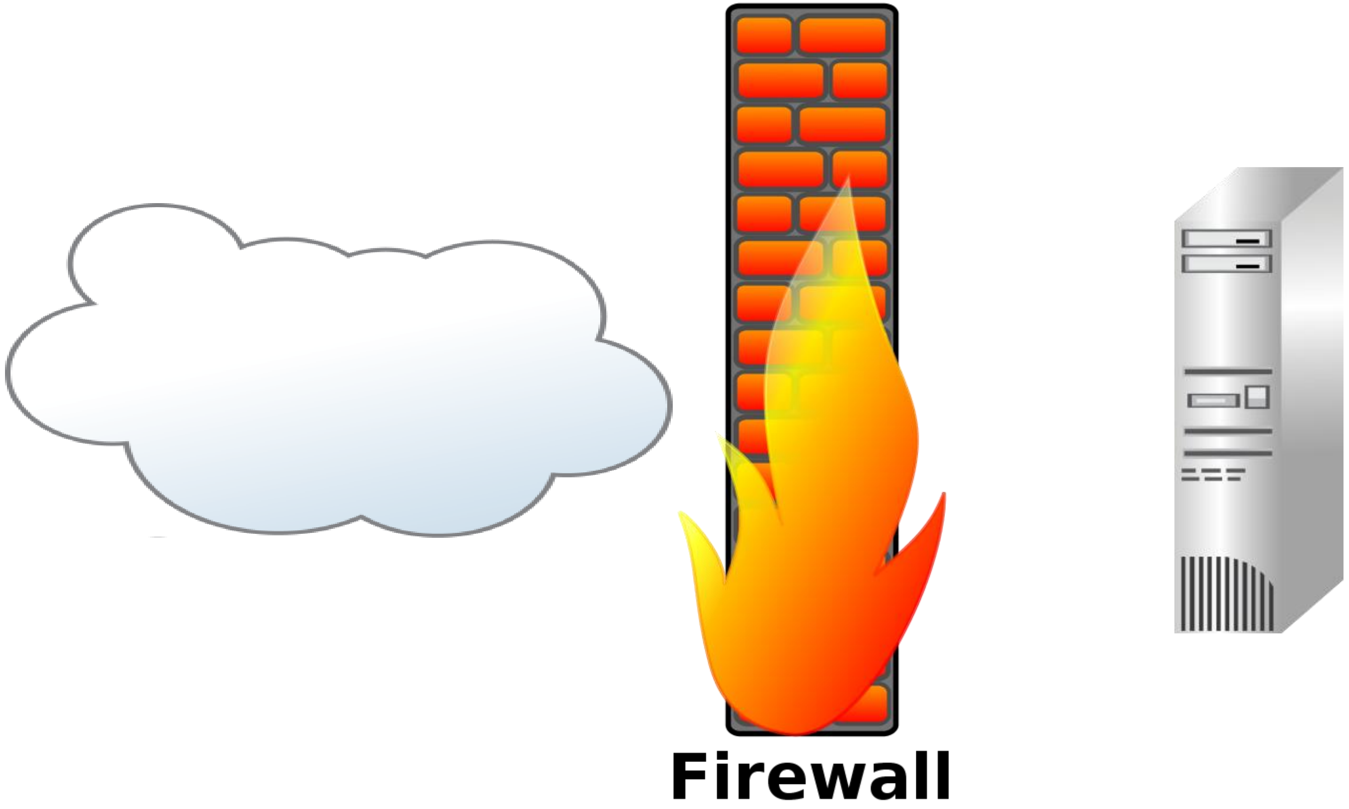
Why Security?

Data in Motion

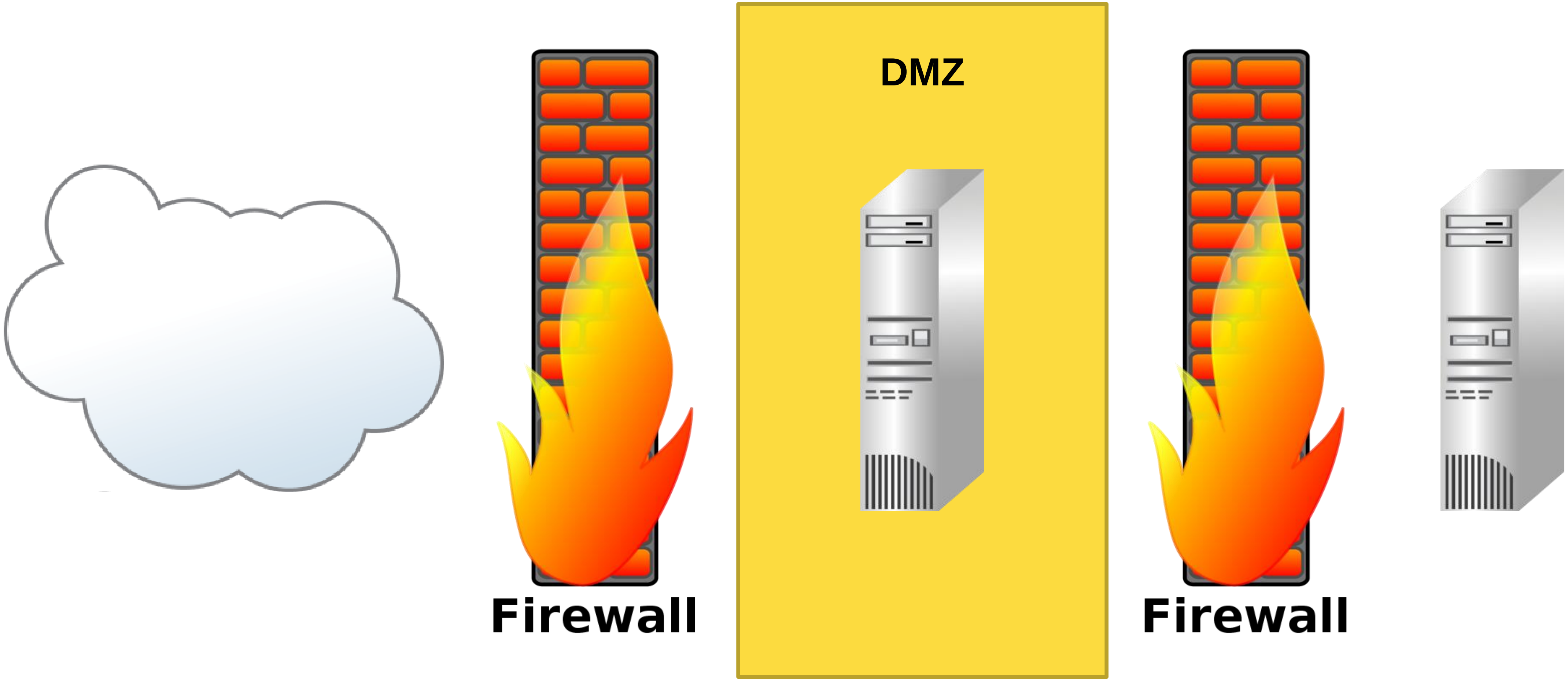
- Internet
- Firewall/DMZ configuration
- Network Security
- Quick Notes

The Internet

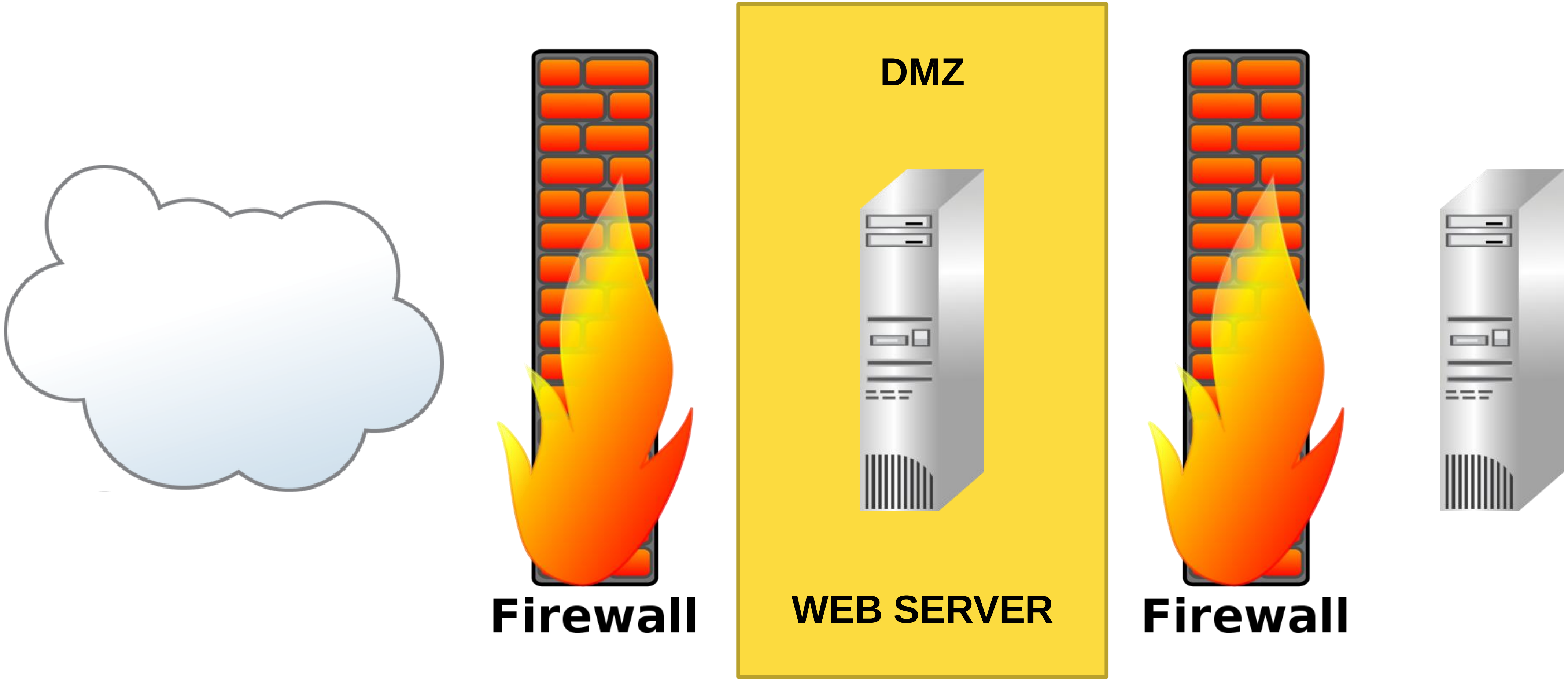
The Internet



The Internet



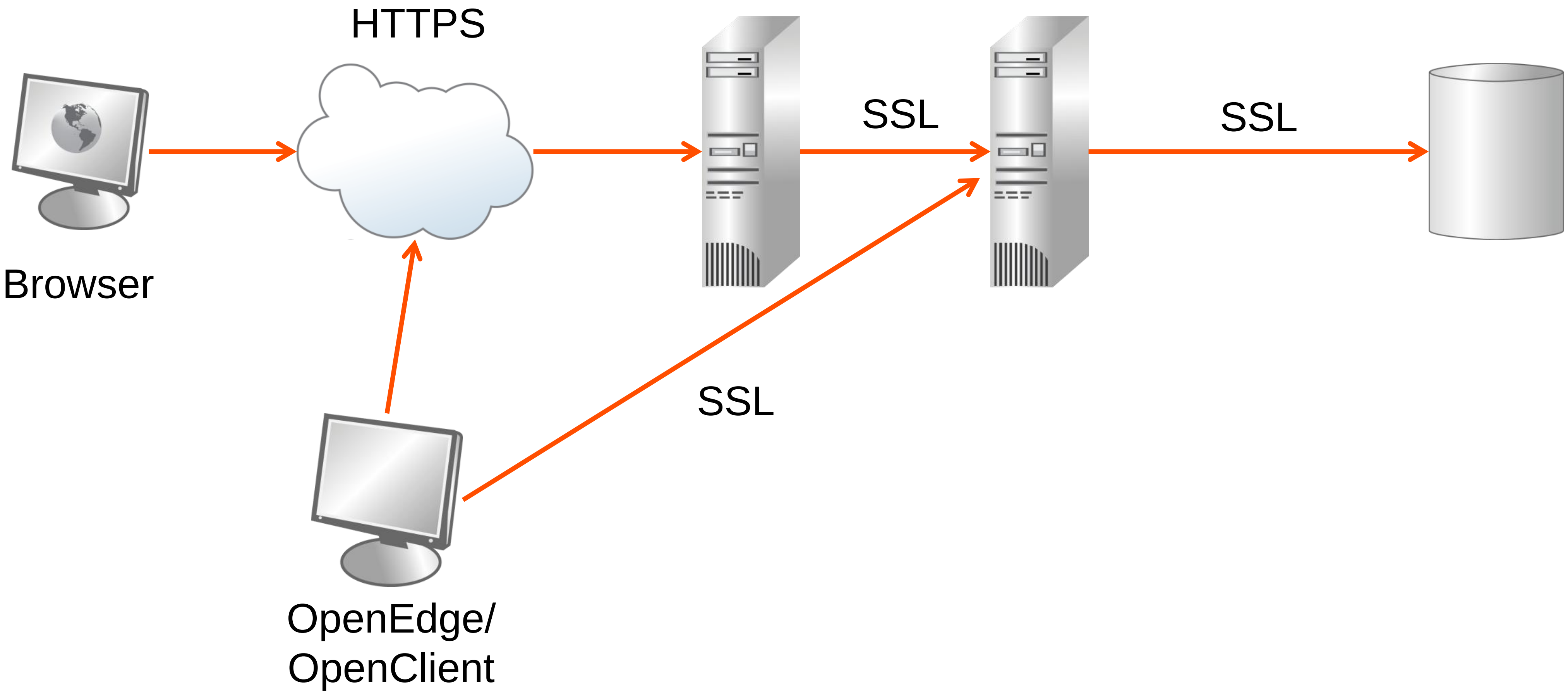
The Internet



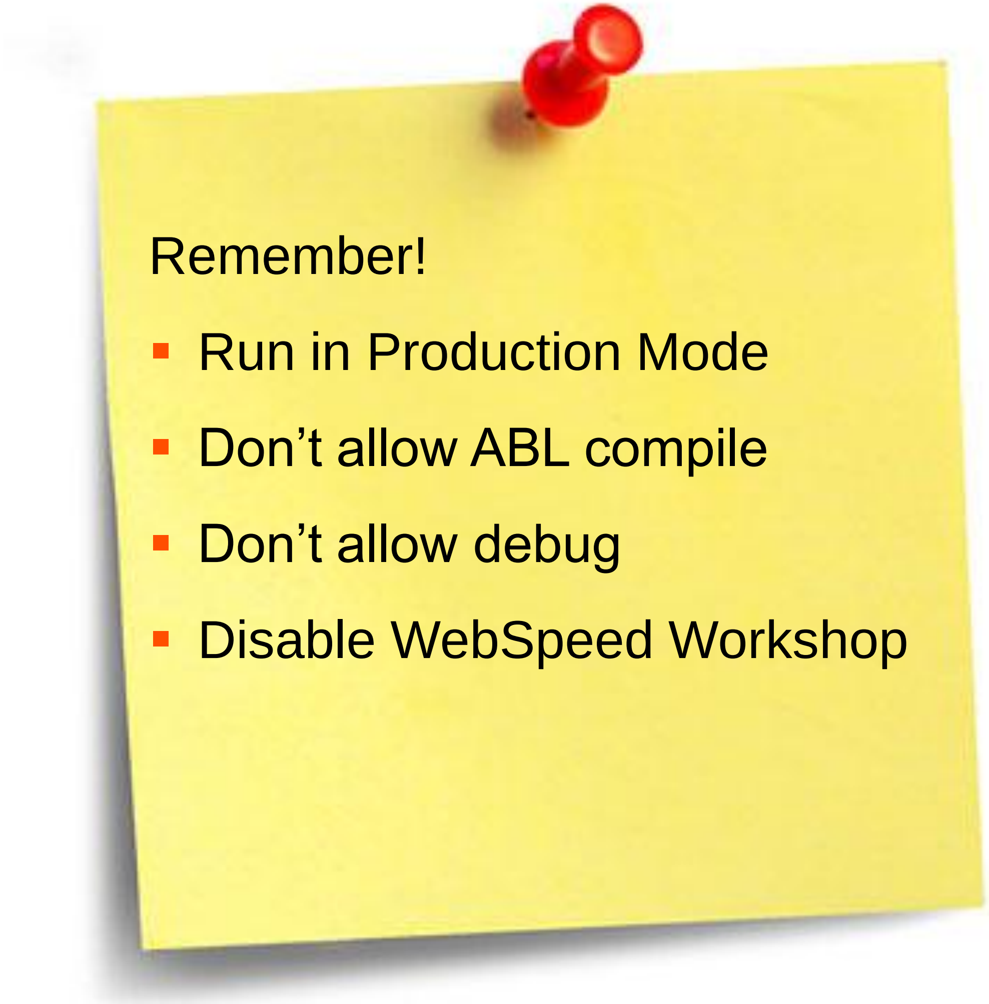
Network Security

- HTTPS
  - For web communication
  - Part of the Web Server
- SSL
  - For web communication from client to AppServer
  - Needed elsewhere?
    - It’s your setup
    - It’s your call
- Performance latency?
  - Using HTTPS/SSL will cause performance degradation
  - Only encrypt information that is sensitive
    - Use different AppServers w/SSL for sensitive data

The Internet and Intranet

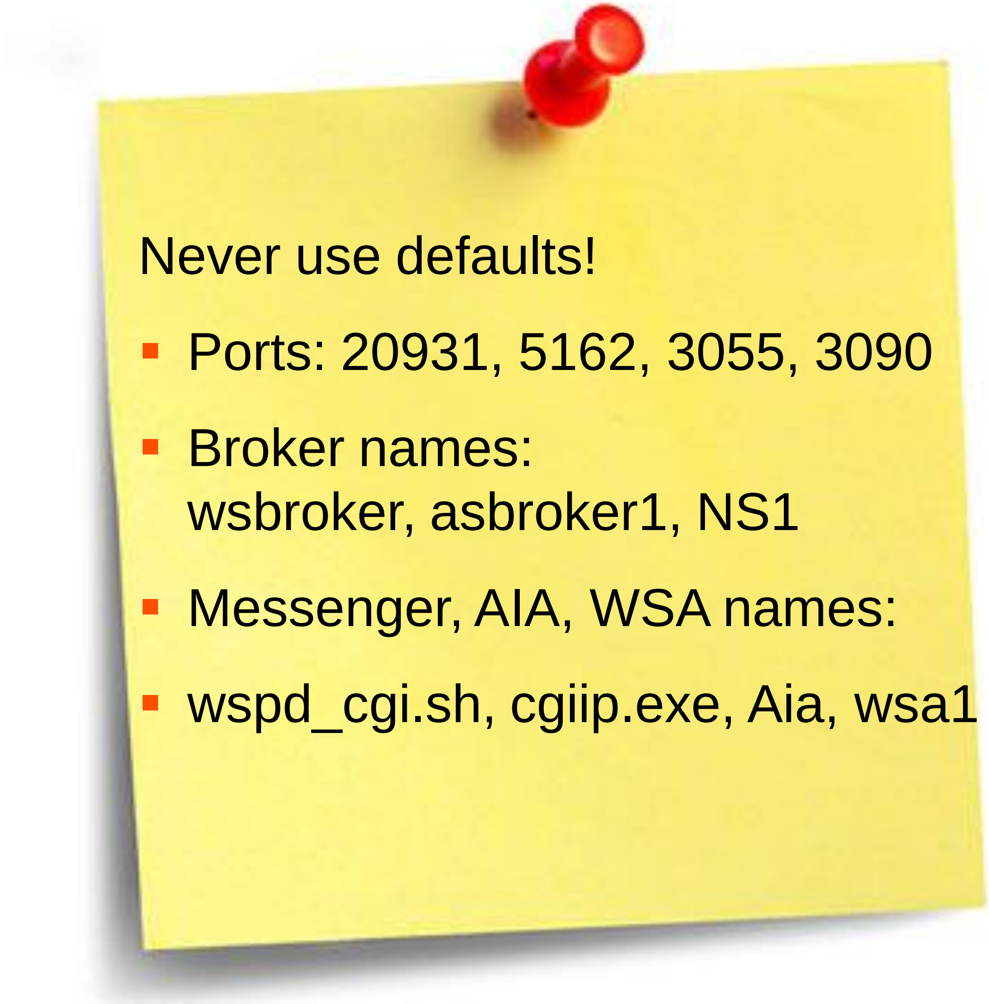


Quick Notes



Remember!

- Run in Production Mode
- Don’t allow ABL compile
- Don’t allow debug
- Disable WebSpeed Workshop

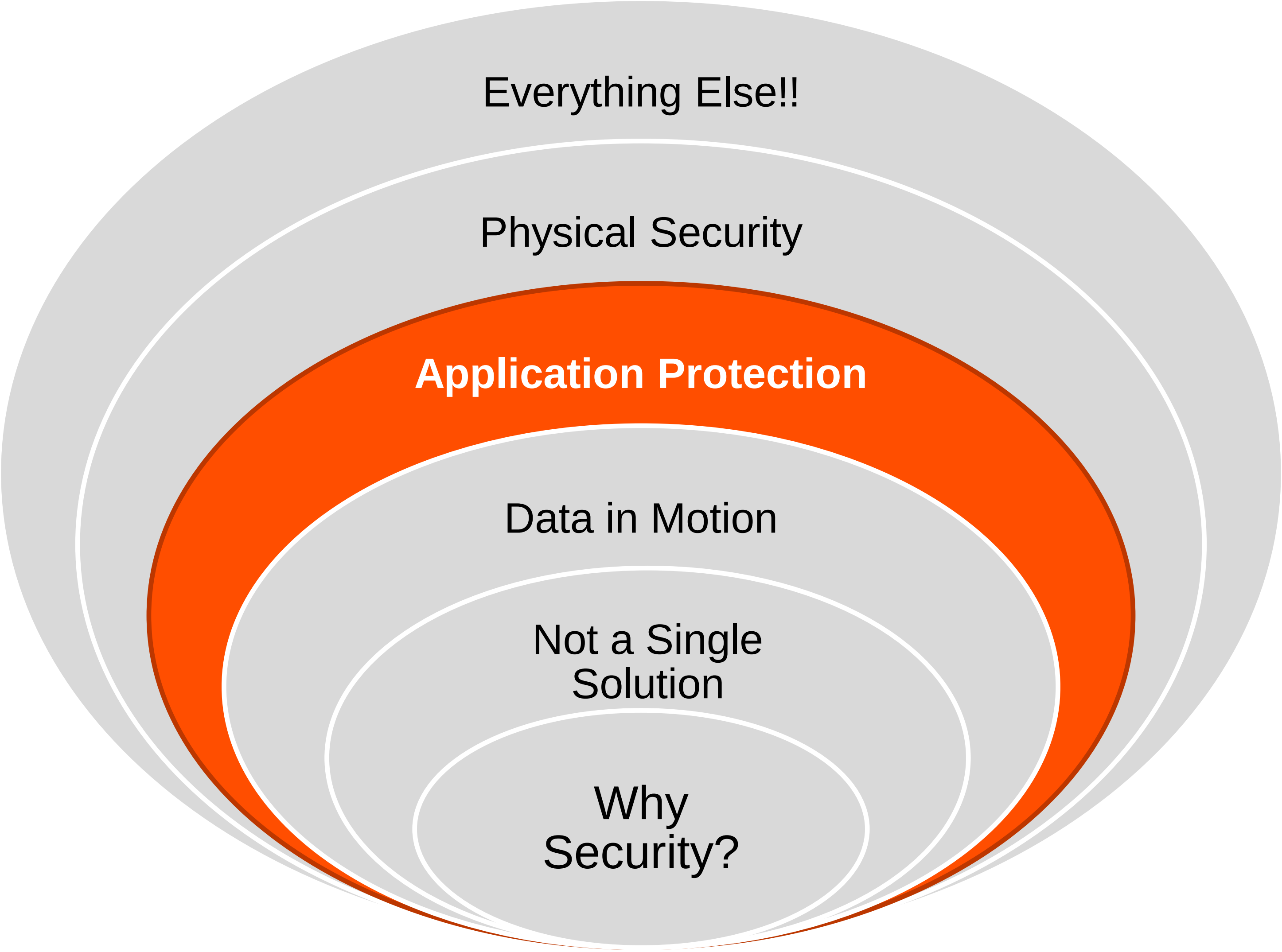


Never use defaults!

- Ports: 20931, 5162, 3055, 3090
- Broker names:
  wsbroker, asbroker1, NS1
- Messenger, AIA, WSA names:
- wspd_cgi.sh, cgiip.exe, Aia, wsa1

Lab # 2 – Enabling SSL

Agenda


Everything Else!!

Physical Security

Application Protection

Data in Motion

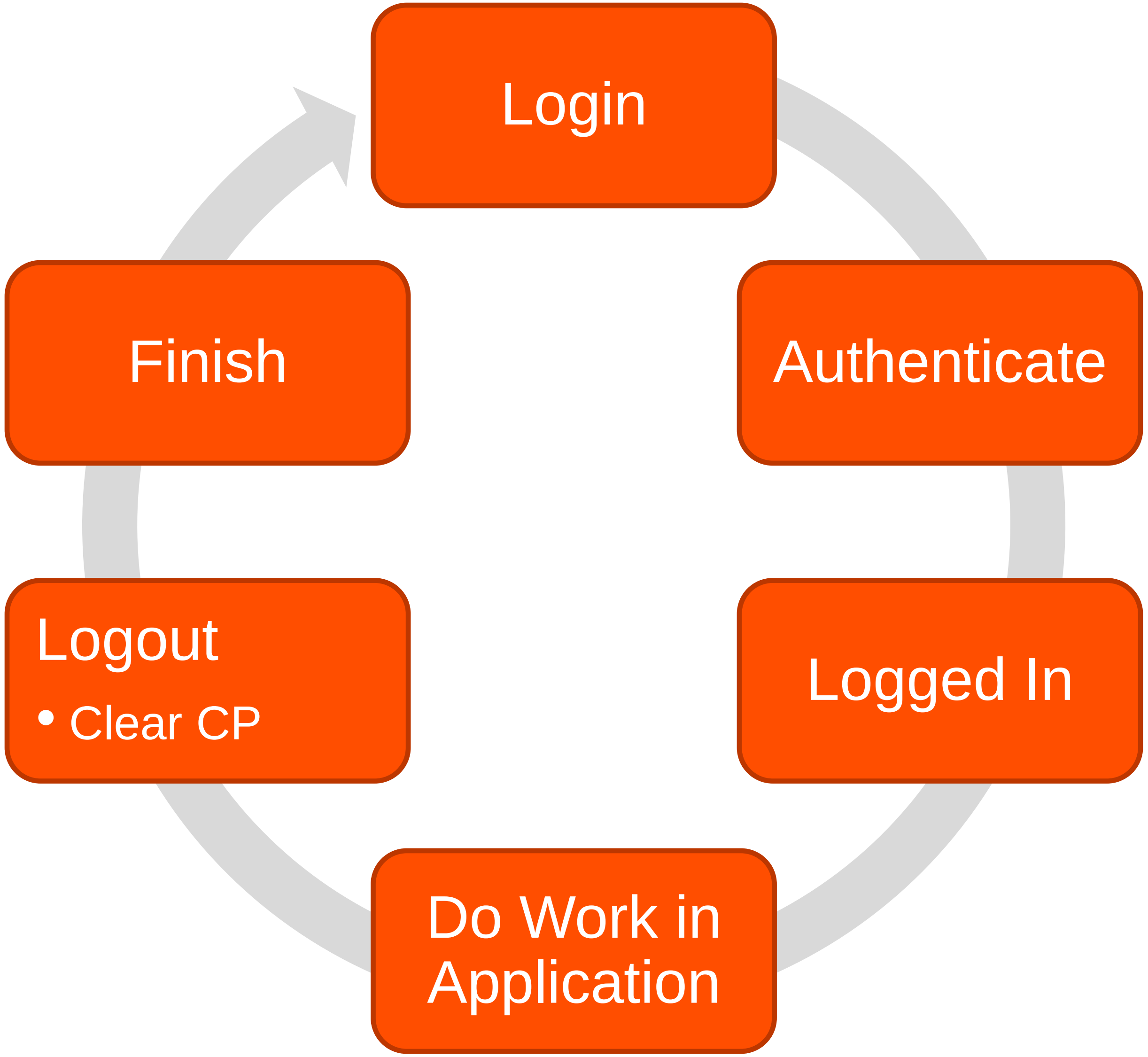
Not a Single Solution

Why Security?

Application Protection

- ABL Client Principal
- 3rd Party Authentication

The Basic Client Principal



Login

Authenticate

Logged In

Do Work in Application

Logout

- Clear CP

Finish

The Basic Client Principal

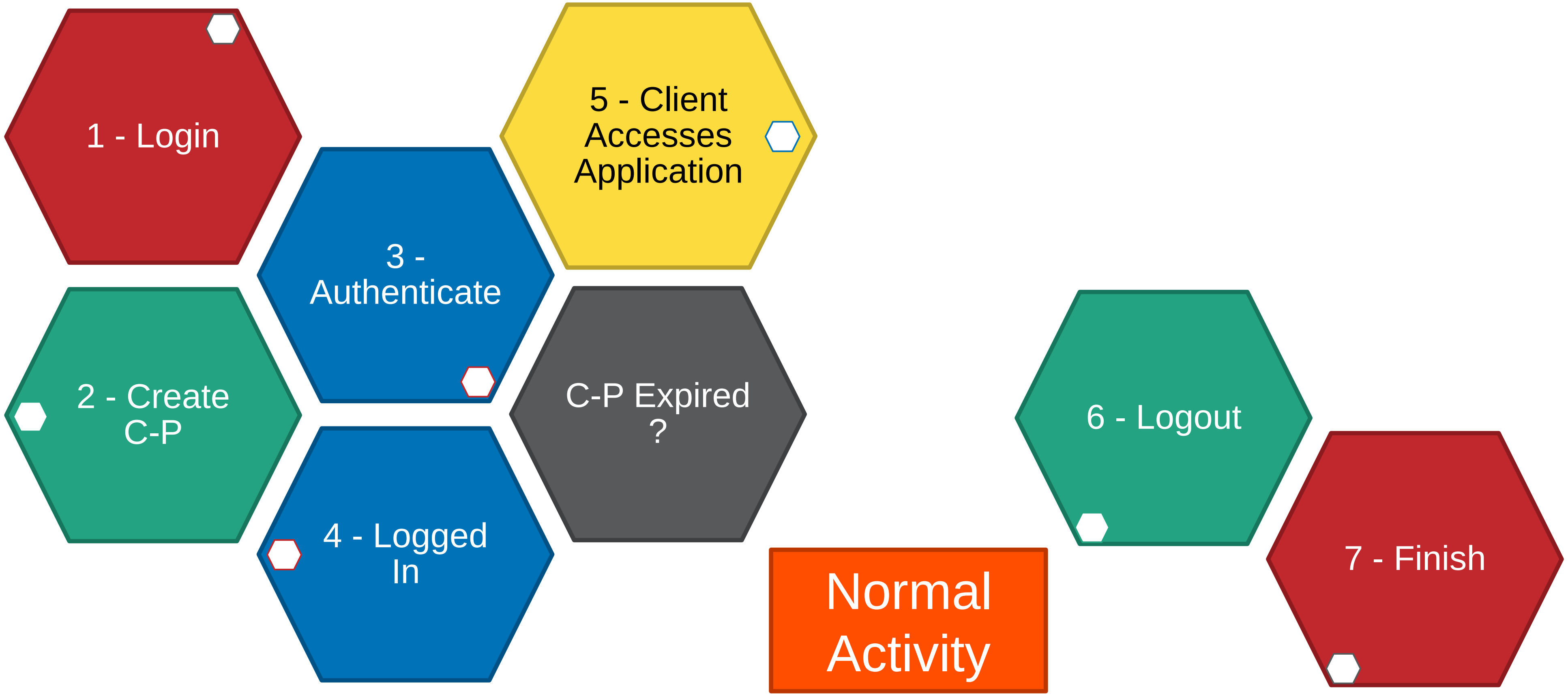
What is needed:

- DEFINE VARIABLE hClientPrincipal   AS HANDLE NO-UNDO.
- CREATE CLIENT-PRINCIPAL hClientPrincipal.
- hClientPrincipal:INITIALIZE(‘rmarshal@progress.com’).
- hClientPrincipal:SEAL(‘bedford’).

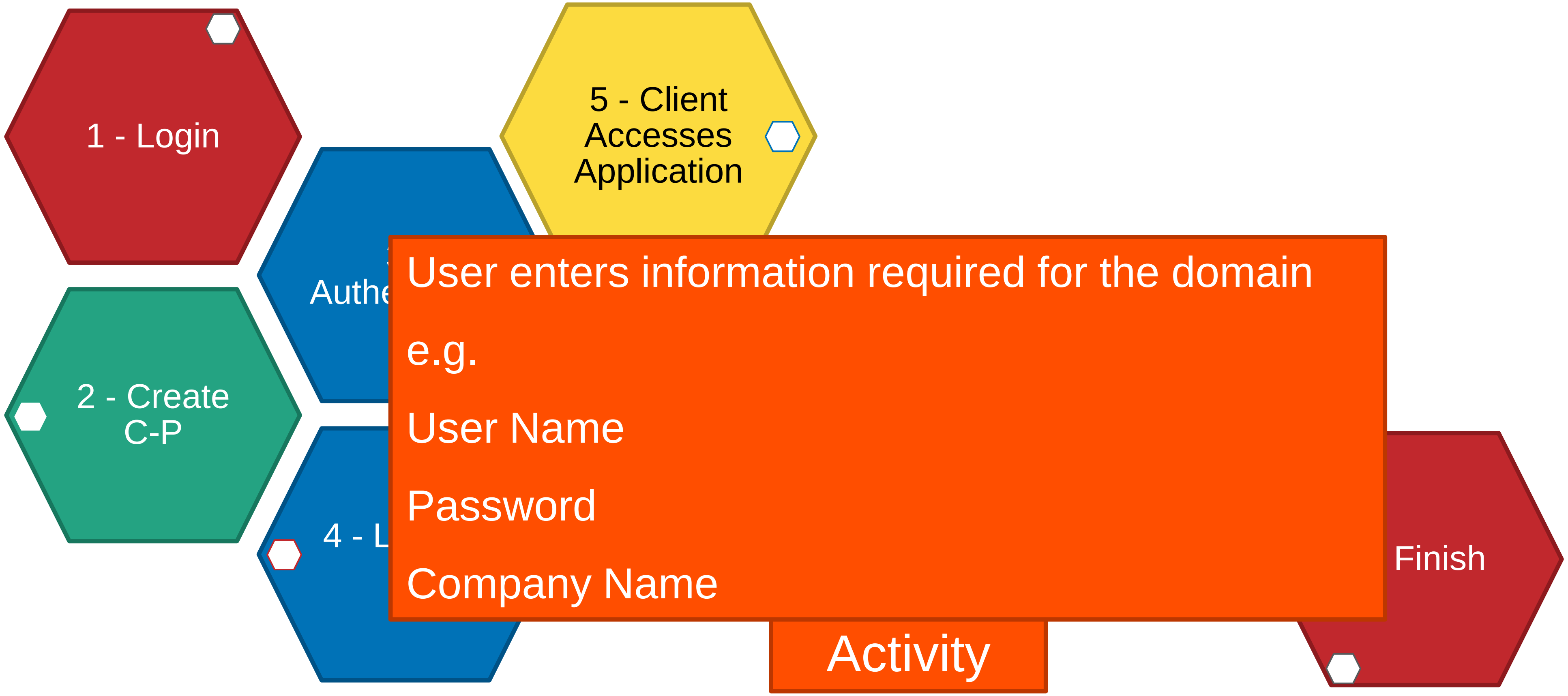
Basic Client Principal Authentication

- Authentication is not just verifying that you can login
- Authentication needs to have an expiry

Basic Client Principal Authentication



Basic Client Principal Authentication



User enters information required for the domain

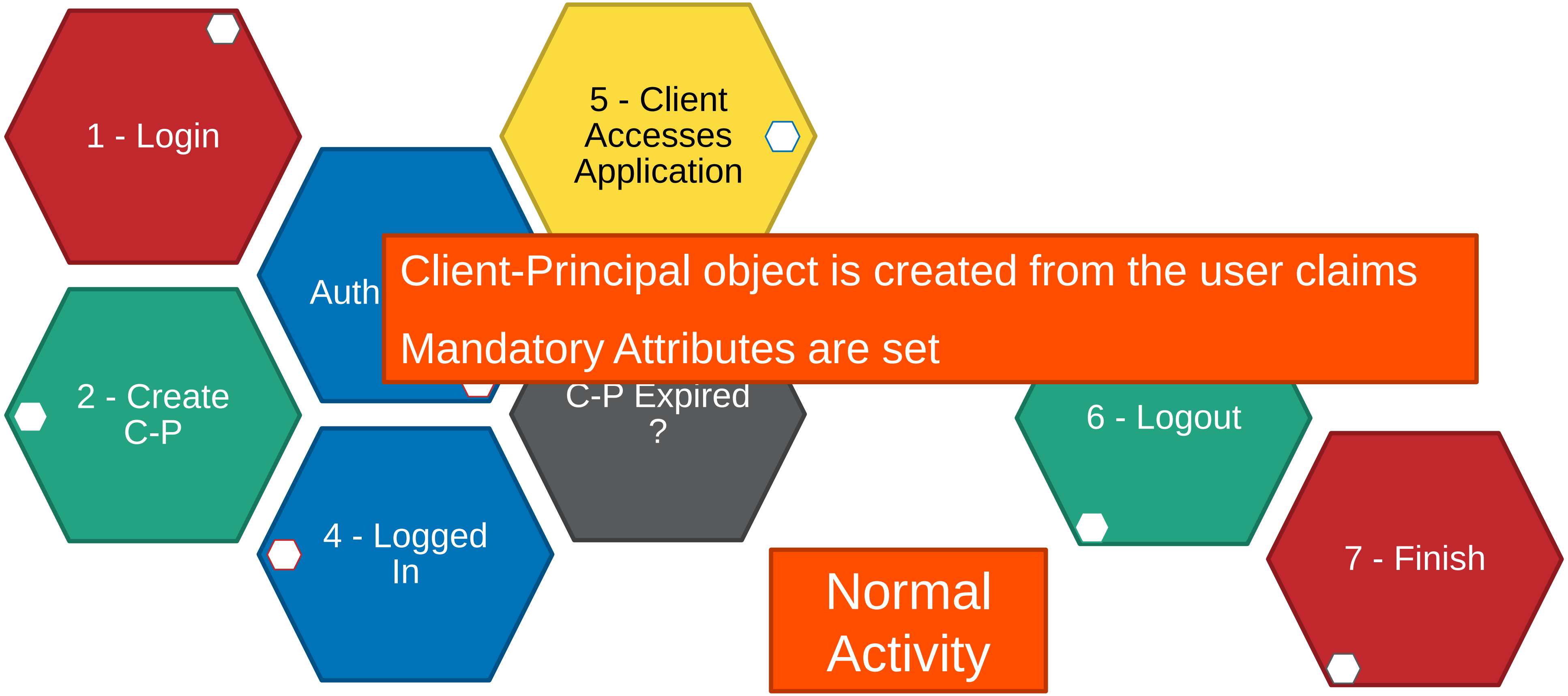
e.g.

User Name

Password

Company Name

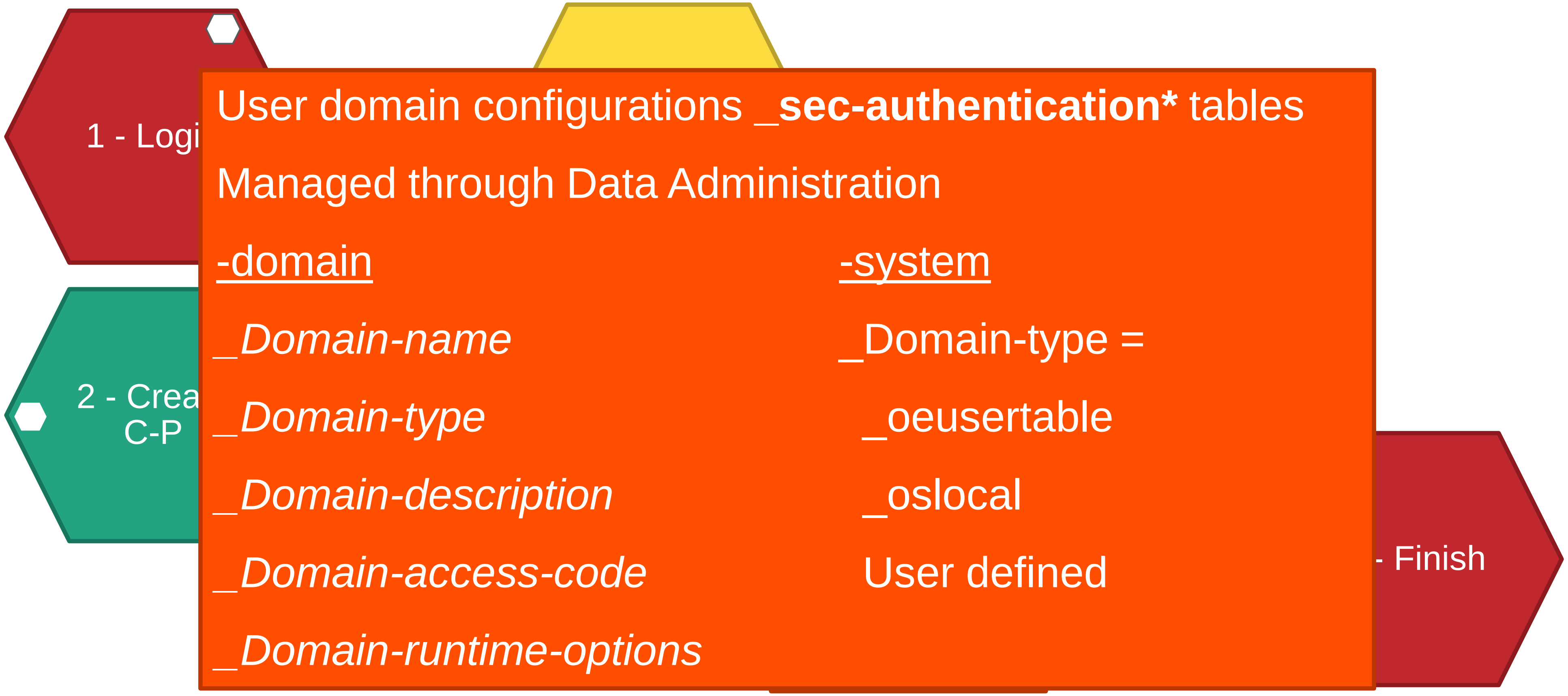
Basic Client Principal Authentication



Client-Principal object is created from the user claims

Mandatory Attributes are set

Basic Client Principal Authentication



User domain configurations _**sec-authentication*** tables

Managed through Data Administration

-domain

_Domain-name

_Domain-type

_Domain-description

_Domain-access-code

_Domain-runtime-options

-system

_Domain-type =

_oeusertable

_oslocal

User defined

Application Authentication

- ABL Client-Principal
  - Current and future OpenEdge products rely on Client-Principal (multi-tenancy, auditing)
  - A cryptographically “sealed” security token
  - Container for authenticated credentials
    - User, password, domain info, etc.
  - Once sealed the client-principal is read-only
  - Can be used by all ABL application components
    - ABL Session, DB connection
- Some 3rd party authentication recommendations
  - LDAP
  - Active Directories
  - Kerberos
  - Multi-Factor Authentication
  - **Require complex passwords!**

Securing Your Application

- Protect your intellectual property (application code)
  - Employ encryption (file or file system level)
  - Utilize O/S and user access limitation
- The basics of runtime
  - DBAuthkey (RCODEKEY)- ensure code running against the DB was compiled to use that DB
  - Runtime table and column access controls
  - Operating system file security settings, etc.

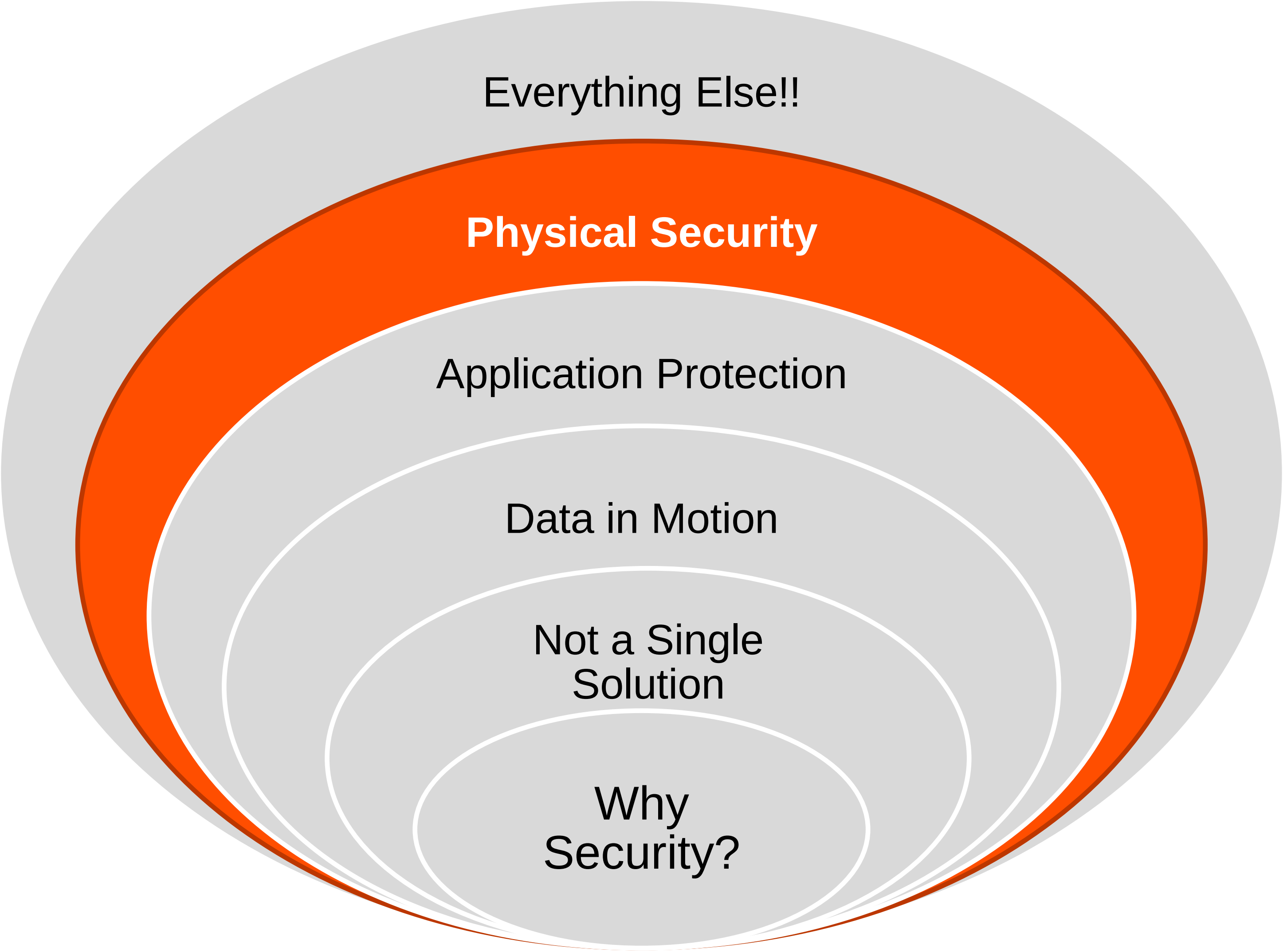
Lab # 3 – Client Principal Programming

ABL Accessing LDAP

- AuthWP.zip is available on Communities
  - The code is not perfect
  - But it is a great place to start!
  - http://communities.progress.com/pcom/docs/DOC-45878
    - AuthWP.zip
    - LDAPAuthenticationWP.doc
- We will be using Apache Directory Studio
  - It has a developer IDE for easy use (not what you will see in production)
  - Shows you what you need to change in the sample code

Lab # 4 – LDAP Integration

Agenda



Everything Else!!

Physical Security

Application Protection

Data in Motion

Not a Single Solution

Why Security?

Physical Security

- Physical Security
- Transparent Data Encryption

The Real Physical Aspect

- Limit access to your building
- Discourage “tailgating”
- Second level security on your Server Room

Process Security

- Security Policies
- Monitoring tools
- Secure installations (protect code and db)

User Security

- Lock, timeout/lock unattended machines
- Control expired user accounts and files

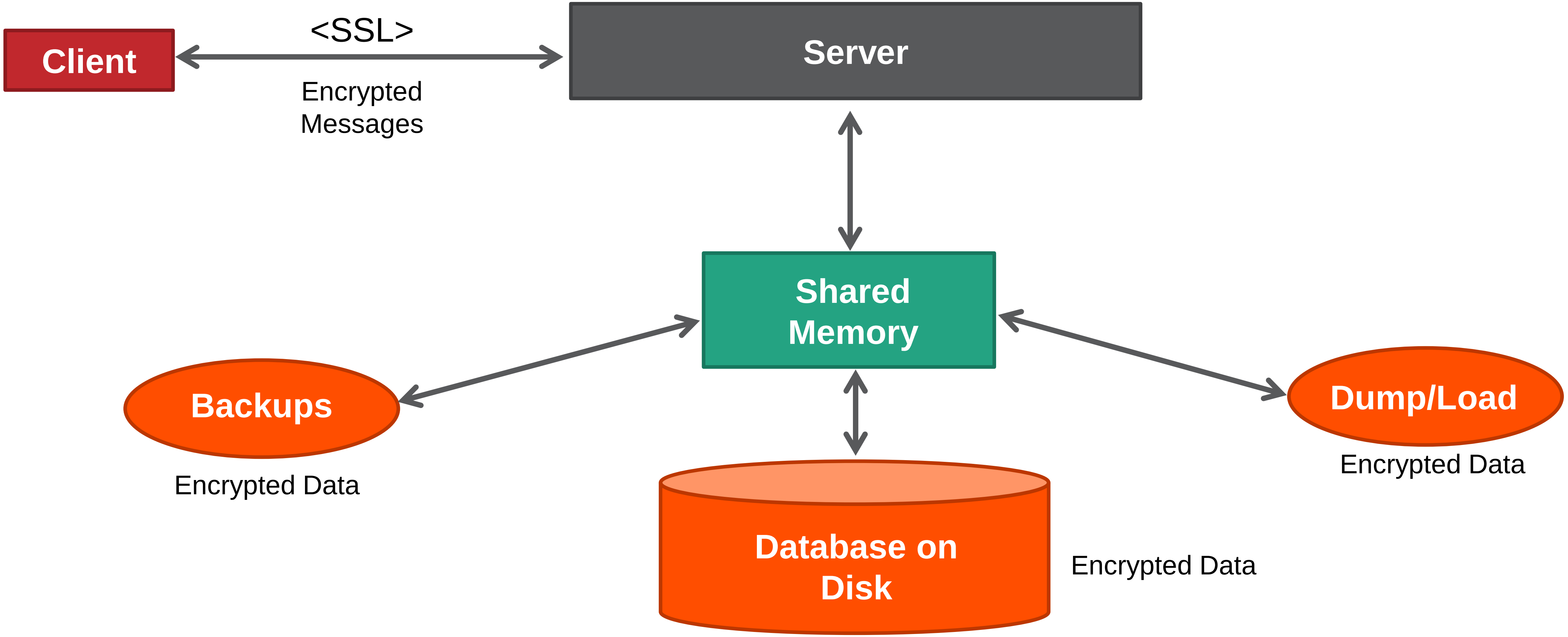
System Security

- Don’t forget O/S security!
- Directory & File Permissions
- User Permissions
- Separation of Responsibilities

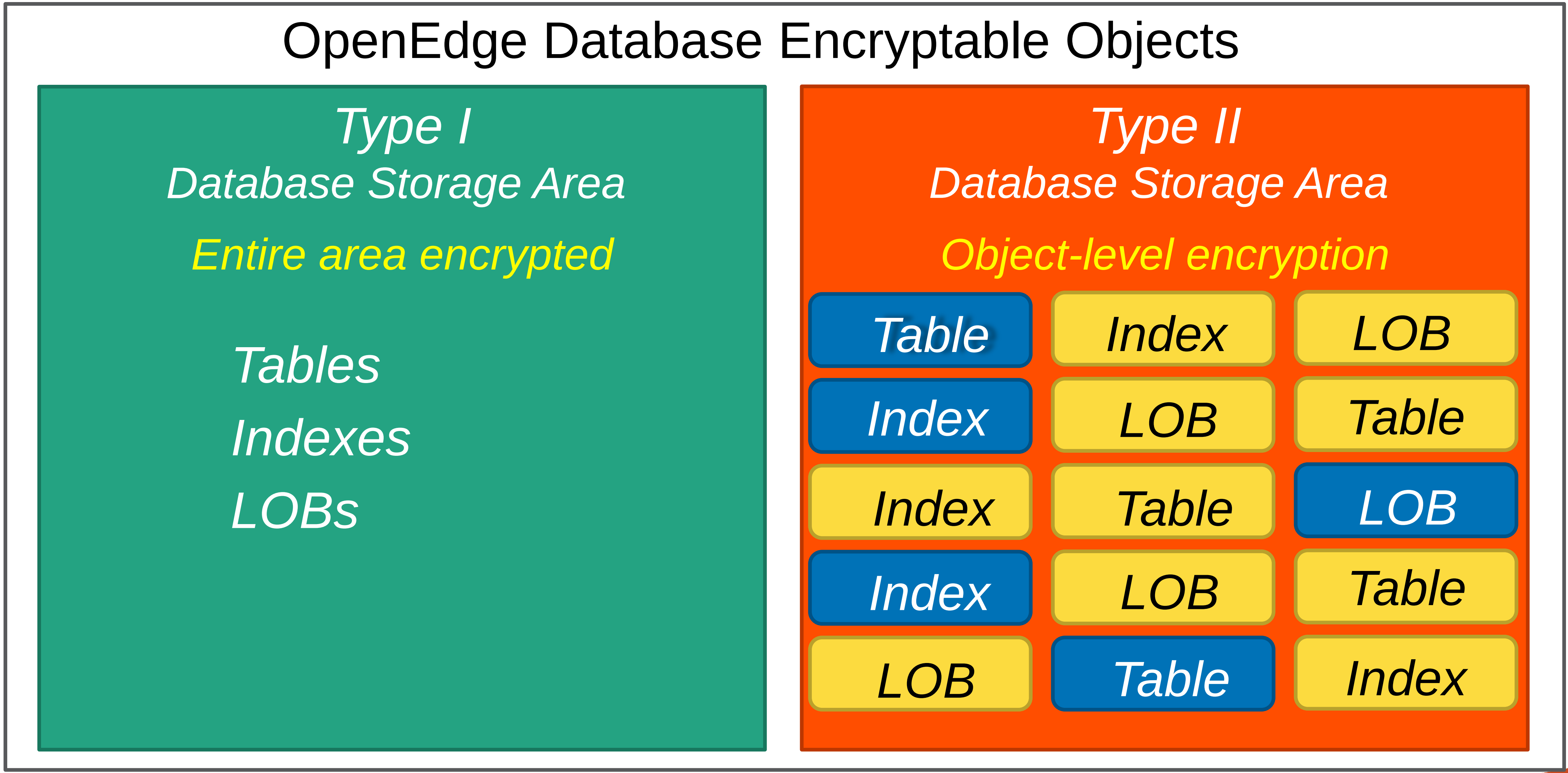
OpenEdge 10.2B Transparent Data Encryption

- Option for Enterprise Database: At-Rest Data Encryption
  - Data secure on-disk, backup, and binary dump
  - Data is unencrypted In-Memory = (up to) normal speed
- Secure Key Store and Key Management
  - Change keys on-line
- Policies control use of utilities
- Industry standard encryptions
  - AES, DES, triple DES, etc.
- Encrypt “on the fly”
  - As data changes or
  - As an online process
- **No application changes for TDE!**

Securing Your Data – A High Level View…



Securing Your Data



OpenEdge Database Encryptable Objects

Type I
Database Storage Area

Entire area encrypted

Tables
Indexes
LOBs

Type II
Database Storage Area

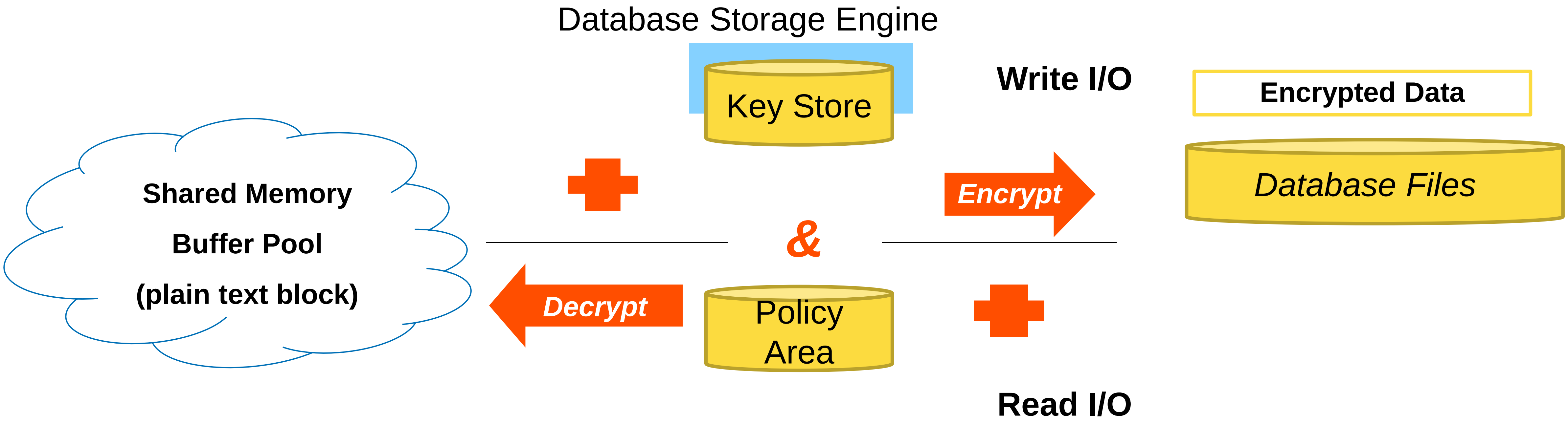
Object-level encryption

Table	*Index*	*LOB*
Index	*LOB*	*Table*
Index	*Table*	*LOB*
Index	*LOB*	*Table*
LOB	*Table*	*Index*

Database Key Store

- Independent and Secure Entity
  - Not part of the database
  - One for each encrypted database
  - Managed by the DB Administrator (a separate and distinct role)
- Stores DB Master Key (DMK)
  - Each TDE-enabled database has one unique DMK- required to connect to the DB (via a passphrase)
  - Only one database is accessible if the DMK is compromised
- Each DB Object Has One or More Unique Virtual Data Encryption Keys
  - Generated by the key store service based on the DMK- no DBA action required
  - If key is cracked, intruder only has access to that one database object
  - Ability to change keys online

How Does It Work?



- Key Store
  - Database Master Key (DMK)
  - DMK Admin/User Passphrase
  - Manual/Automatic Authentication on DB start
- Encryption Policy Area
  - Encryption Policies - What (object) & how (cipher)

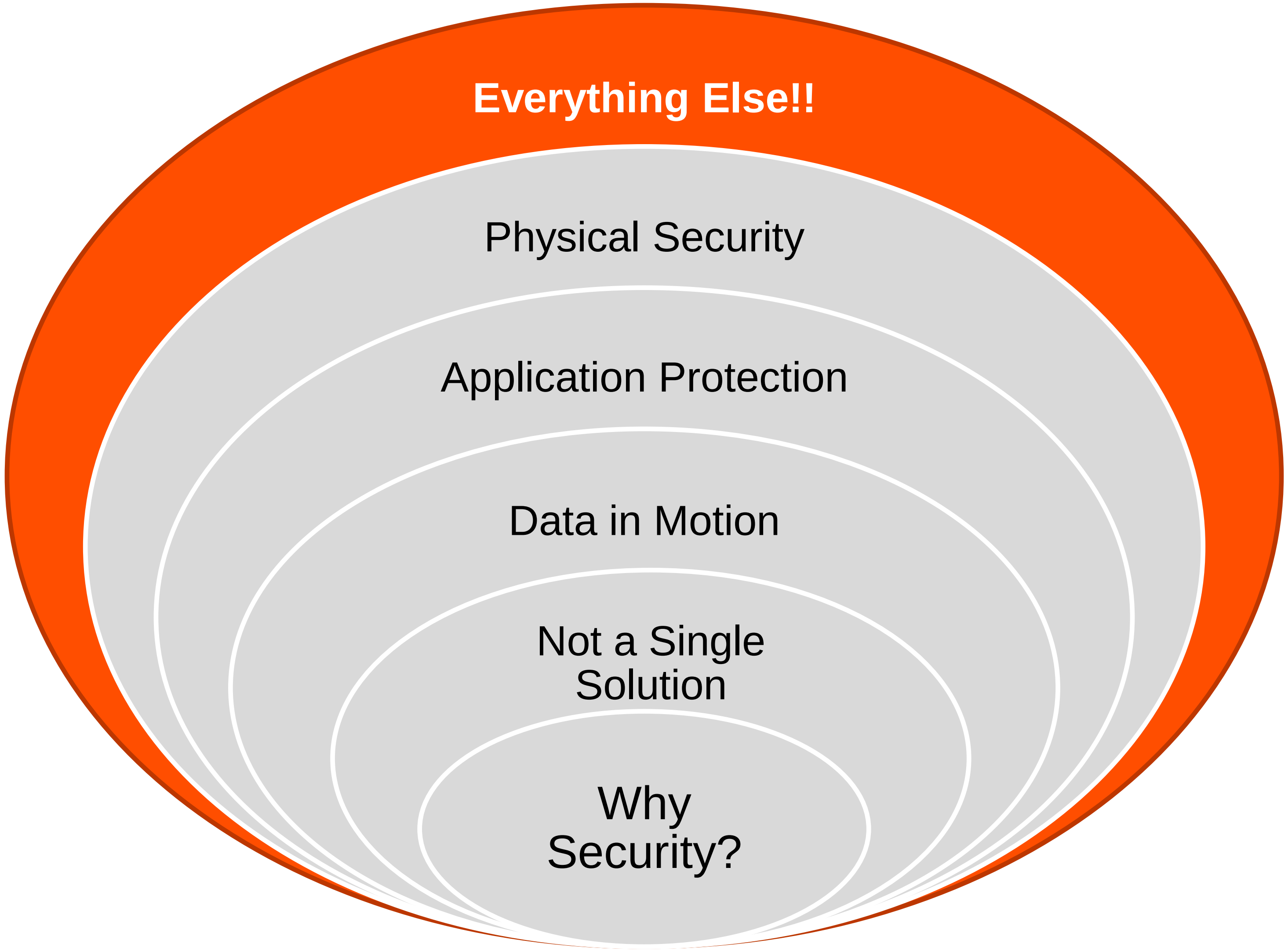
Why TDE from OpenEdge?

- Easy to use
  - **No Application changes needed for TDE!**
  - Add Encryption Policy Area, Enable, Add Policies, Encrypt!
- Protects data even when not in database
  - Data encrypted in backup files
  - Data encrypted in binary dump files
- Very fast performance
  - Little to no performance impact!

"We always try to improve our performance and get things to run faster. We tested a fully encrypted database and there was ***only a 4% decrease in performance*** *versus an unencrypted database. We tested that with alternative data pools, we actually* ***gained back almost 2% of that*** *initial performance degradation. We believe with additional fine tuning the performance will continue to improve." (A TDE user)*

Lab # 5 – Transparent Data Encryption (TDE)

Agenda



Everything Else!!

Physical Security

Application Protection

Data in Motion

Not a Single Solution

Why Security?

Miscellaneous

- Disaster Recovery
- Management
- Multi-Tenancy

Securing Your Data

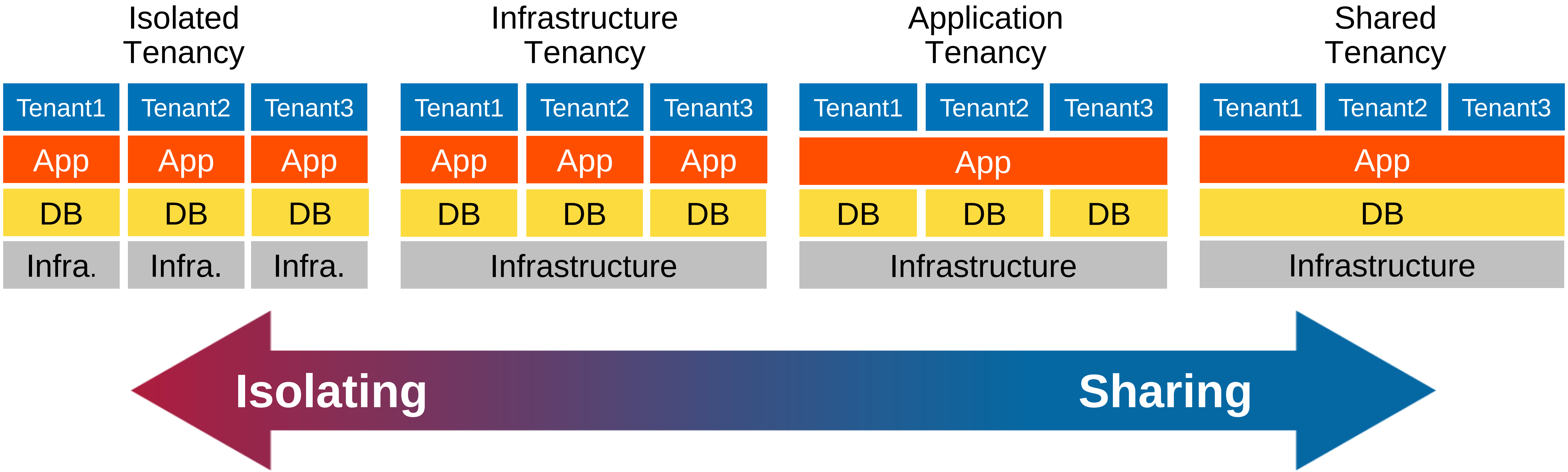
Other considerations…

- Disaster Recovery
  - Securing your data from catastrophic loss (soft and hard failures)
  - Off-site backup storage
  - Cloud storage is quickly growing in popularity
- Database Replication & Replication Plus
  - Replicate to up to 2 databases at the same time
  - Quick failover to backup databases
  - Some customers have on-premise DB and Cloud Replication

Securely Managing Your Application

- OpenEdge Explorer and OpenEdge Management
  - Has its own user authentication
- The AdminServer has security settings
  - “Require Username” and “Admin Groups”
- Separation of Development and Production
  - The internal developer threat to your production system
  - Different machines, networks, ports, everything
- Keep your operating system up-to-date
  - Download and install critical system updates
  - Install and configure system firewall

Multi-Tenancy – Securing Tenant Data



Isolated Tenancy

Tenant1 | Tenant2 | Tenant3
App | App | App
DB | DB | DB
Infra. | Infra. | Infra.

Infrastructure Tenancy

Tenant1 | Tenant2 | Tenant3
App | App | App
DB | DB | DB
Infrastructure

Application Tenancy

Tenant1 | Tenant2 | Tenant3
App
DB | DB | DB
Infrastructure

Shared Tenancy

Tenant1 | Tenant2 | Tenant3
App
DB
Infrastructure

Easier customization, security
Simpler throttling control
Target dissimilar customers
No transformation

Better economy of scale
Simpler management
Target like-customers
Least cost to serve

ODBC / JDBC Security

- By default there are 2 accounts with DBA rights
  - The account that originally CREATED the database
  - The sysprogress account (not enabled by default)
- Best practices are to create a DBA user and NOT USE the root/sysprogress account
- You can use any SQL tool of choice to connect to the OpenEdge database, for purposes of the labs we will use the command line tool sqlexp (SQL Explorer)
- Security rights can be changed while the database is online.

ODBC / JDBC Security

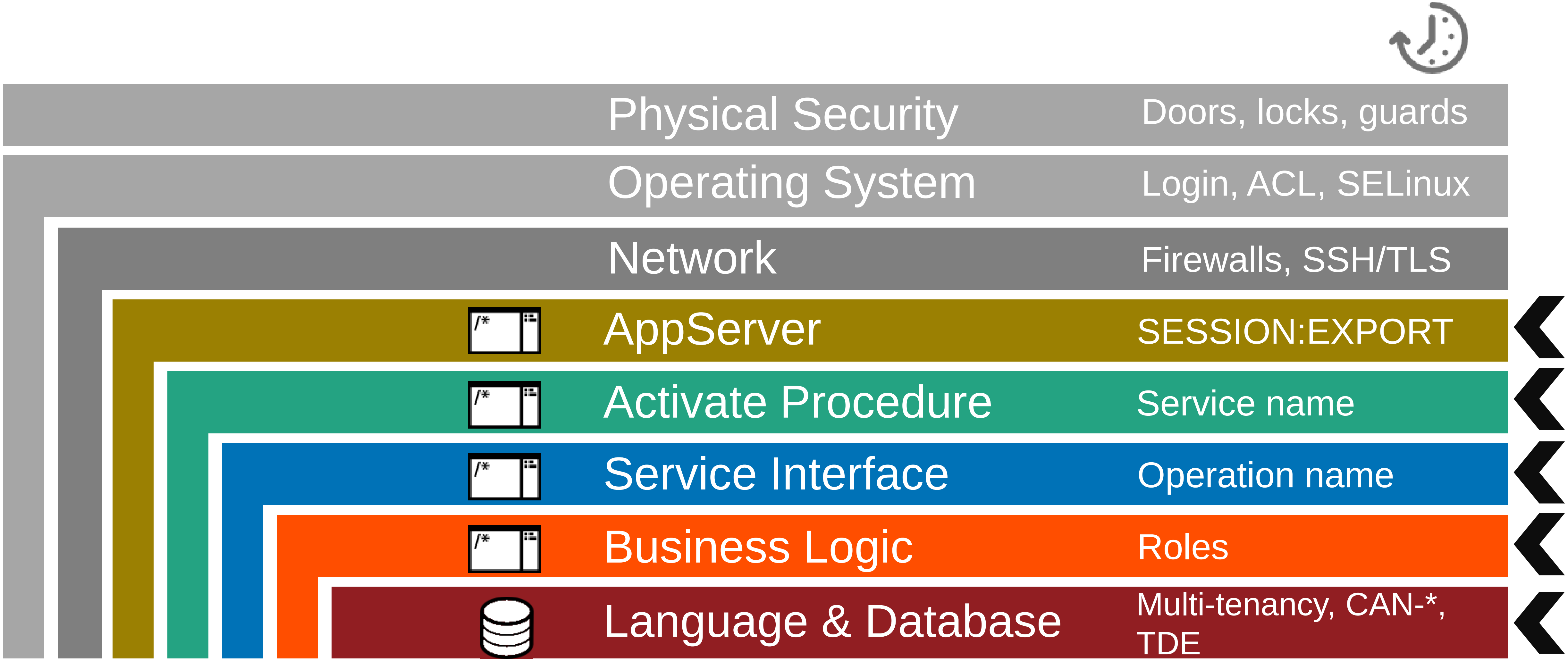
- It is a good idea to have separate brokers for SQL vs ABL clients
- When creating new SQL users, the ONLY thing they have rights to is the catalog (look at the db schema information)
- Remember that any ABL triggers WILL NOT FIRE when data is changed via SQL
- Give users access to only what they need and remember what database they are going against (you cannot change data on a replication target)
- Keep all SQL scripts in your source control

Lab # 6 – Optional Lab - ODBC / JDBC

Tying It All Together

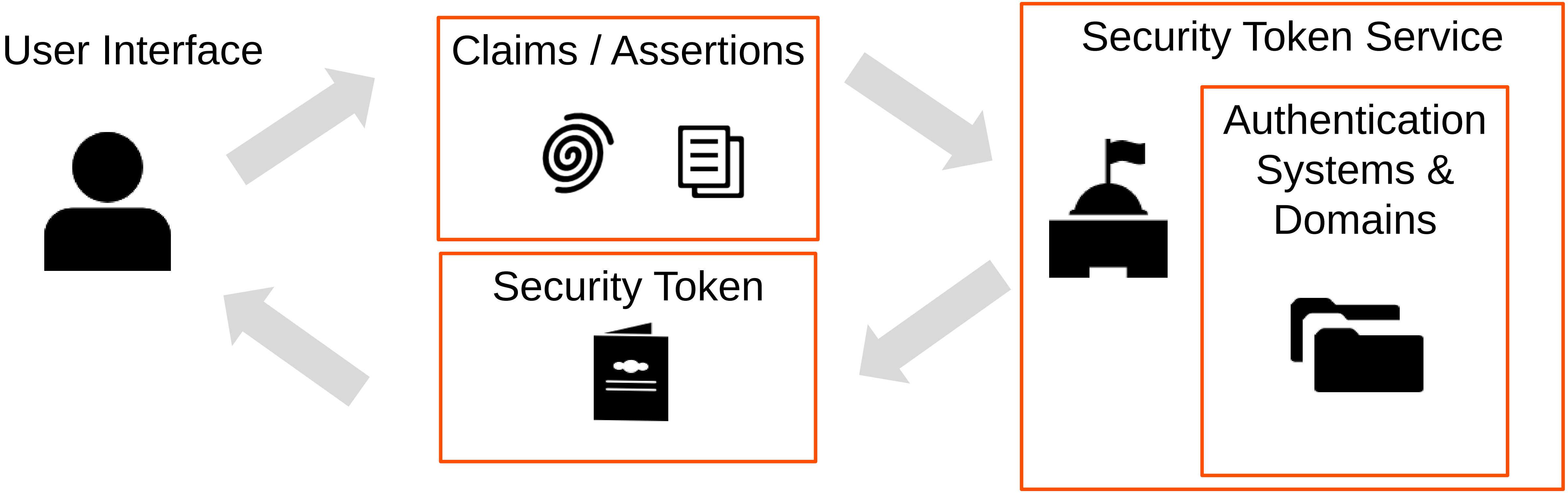
- Client Principal and Application Theory (Peter Judge)

Defense in Depth



Physical Security	Doors, locks, guards
Operating System	Login, ACL, SELinux
Network	Firewalls, SSH/TLS
AppServer	SESSION:EXPORT
Activate Procedure	Service name
Service Interface	Operation name
Business Logic	Roles
Language & Database	Multi-tenancy, CAN-*, TDE

Application Flow: Login



User Interface

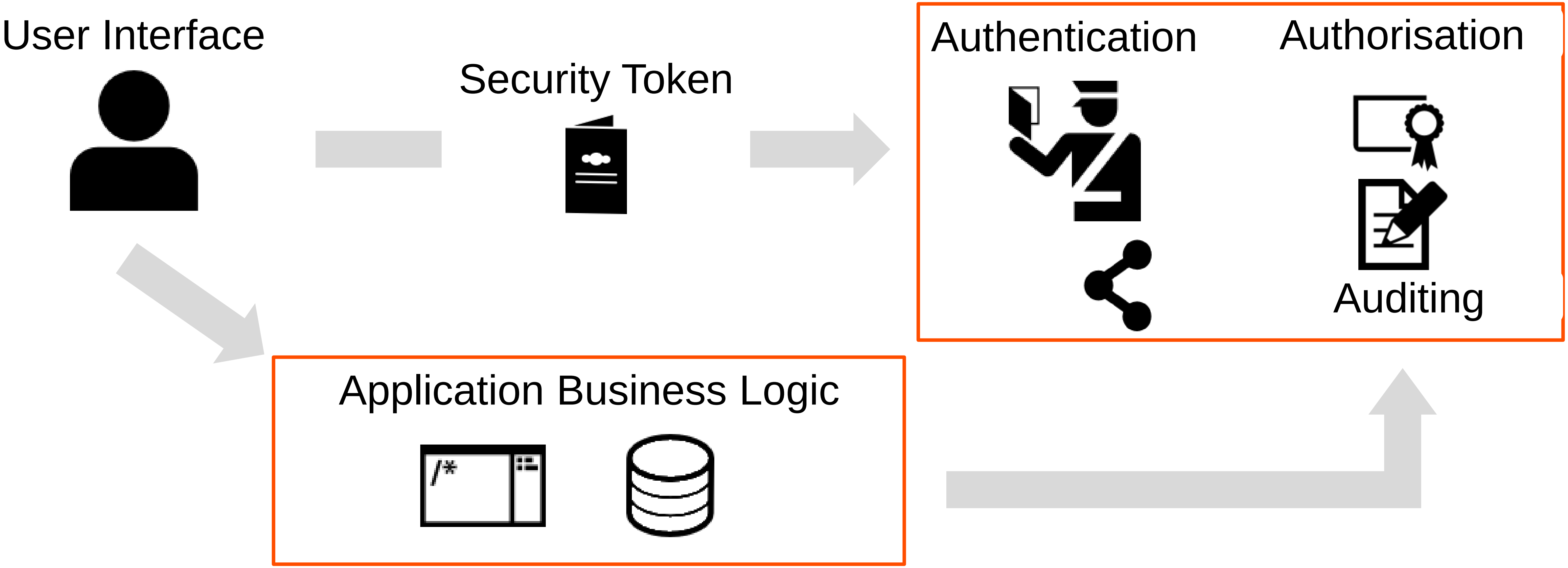
Claims / Assertions

Security Token

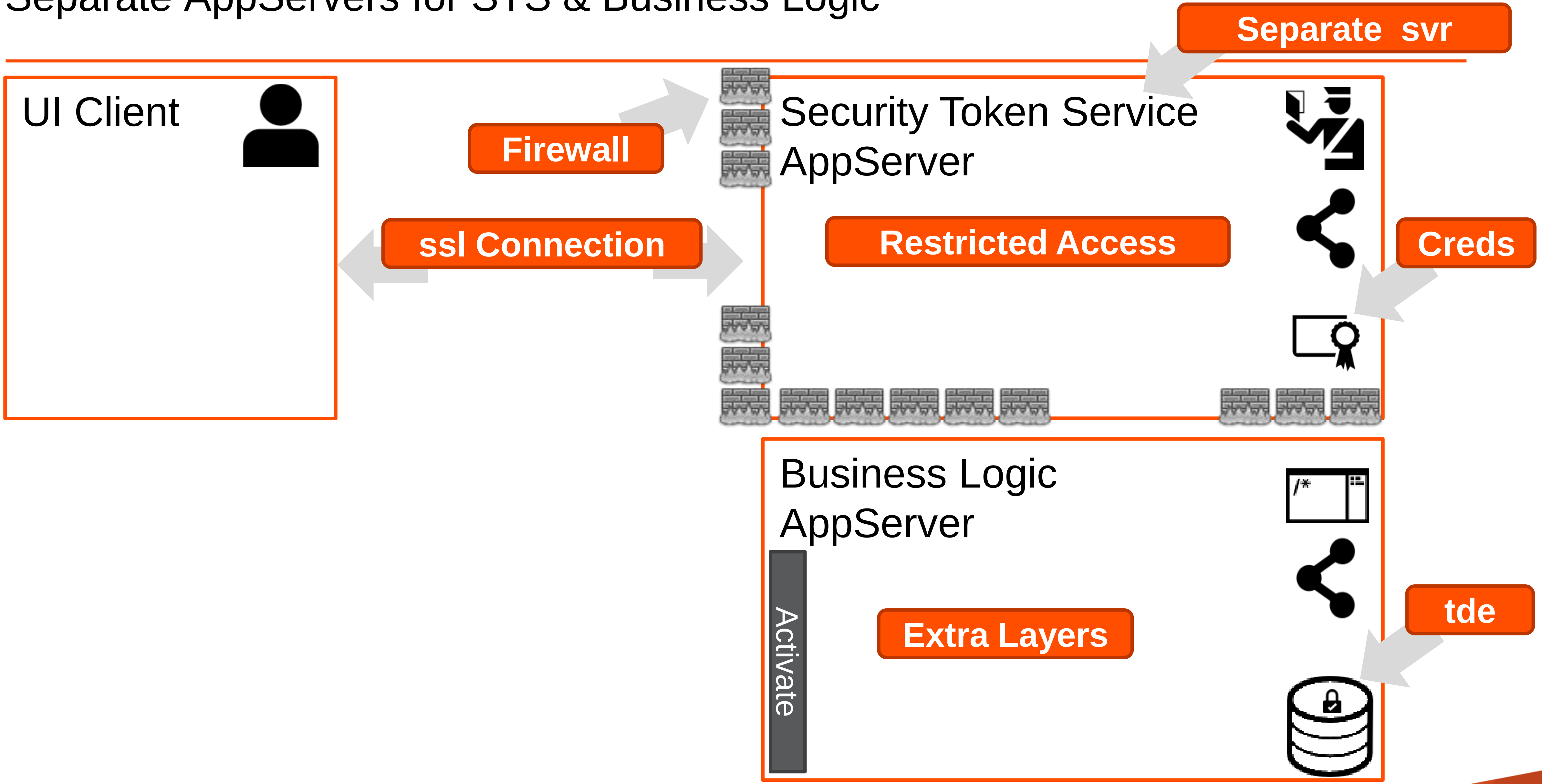
Security Token Service

Authentication Systems & Domains

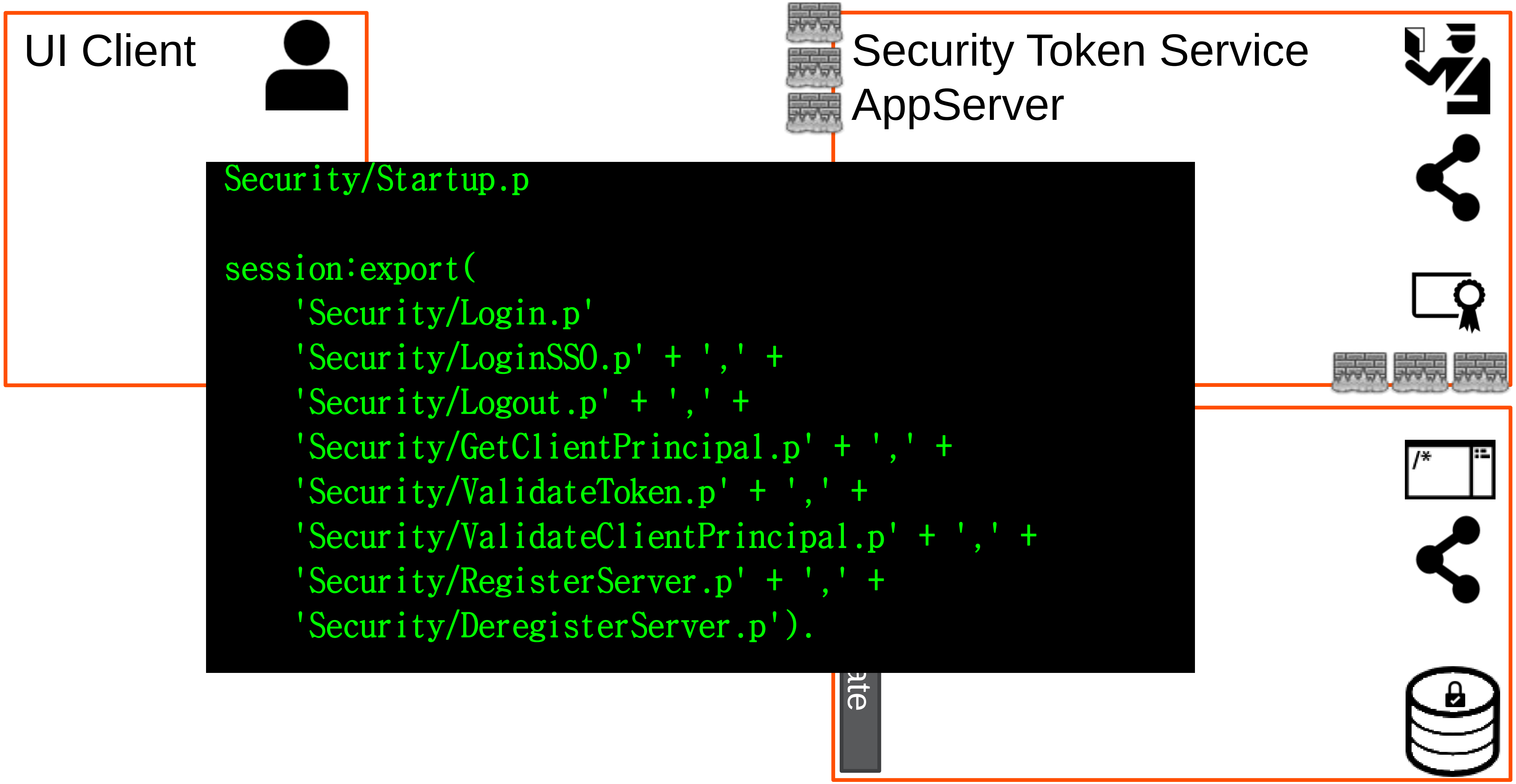
Application Flow: Business Logic



Separate AppServers for STS & Business Logic

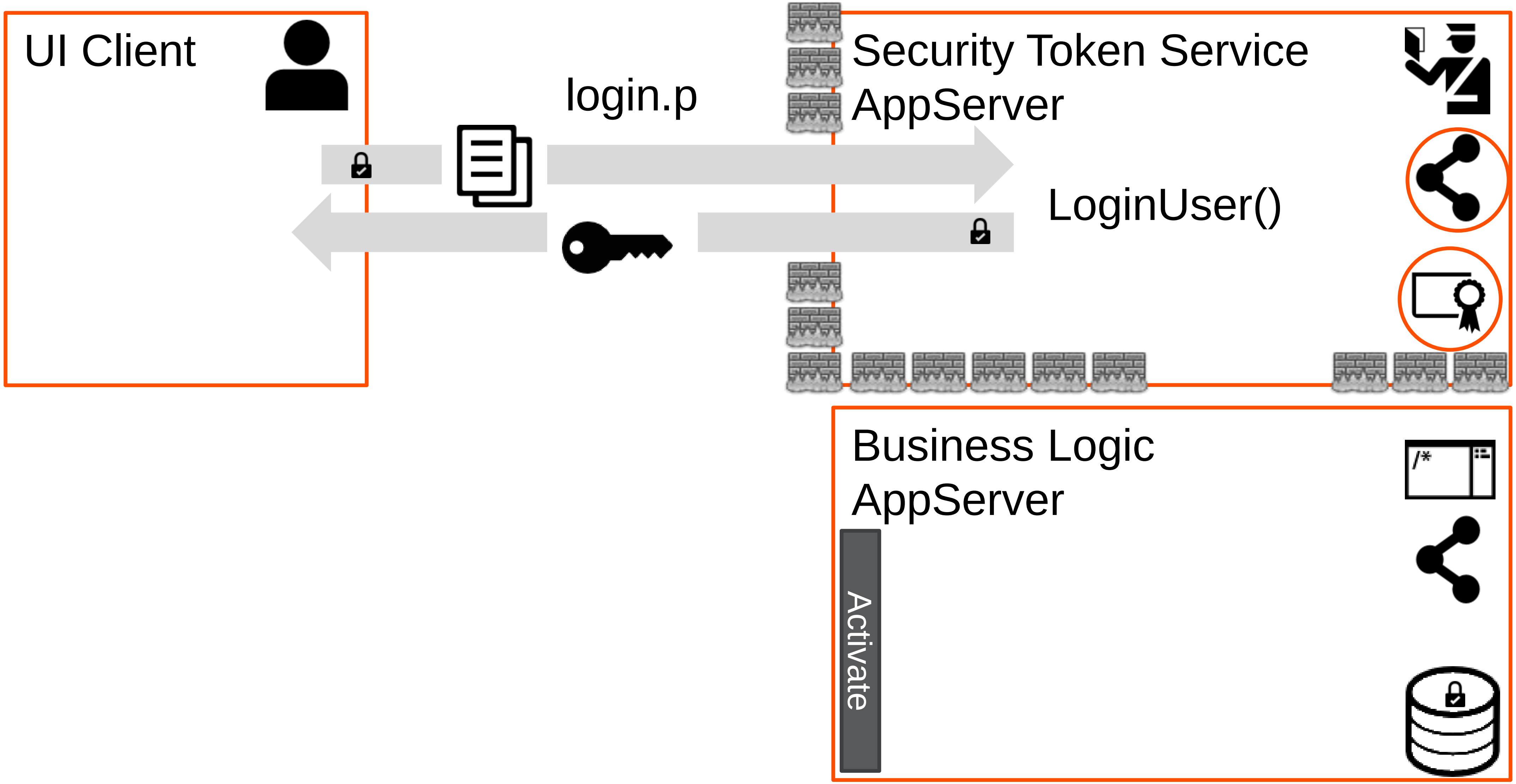


Separate AppServers for STS & Business Logic

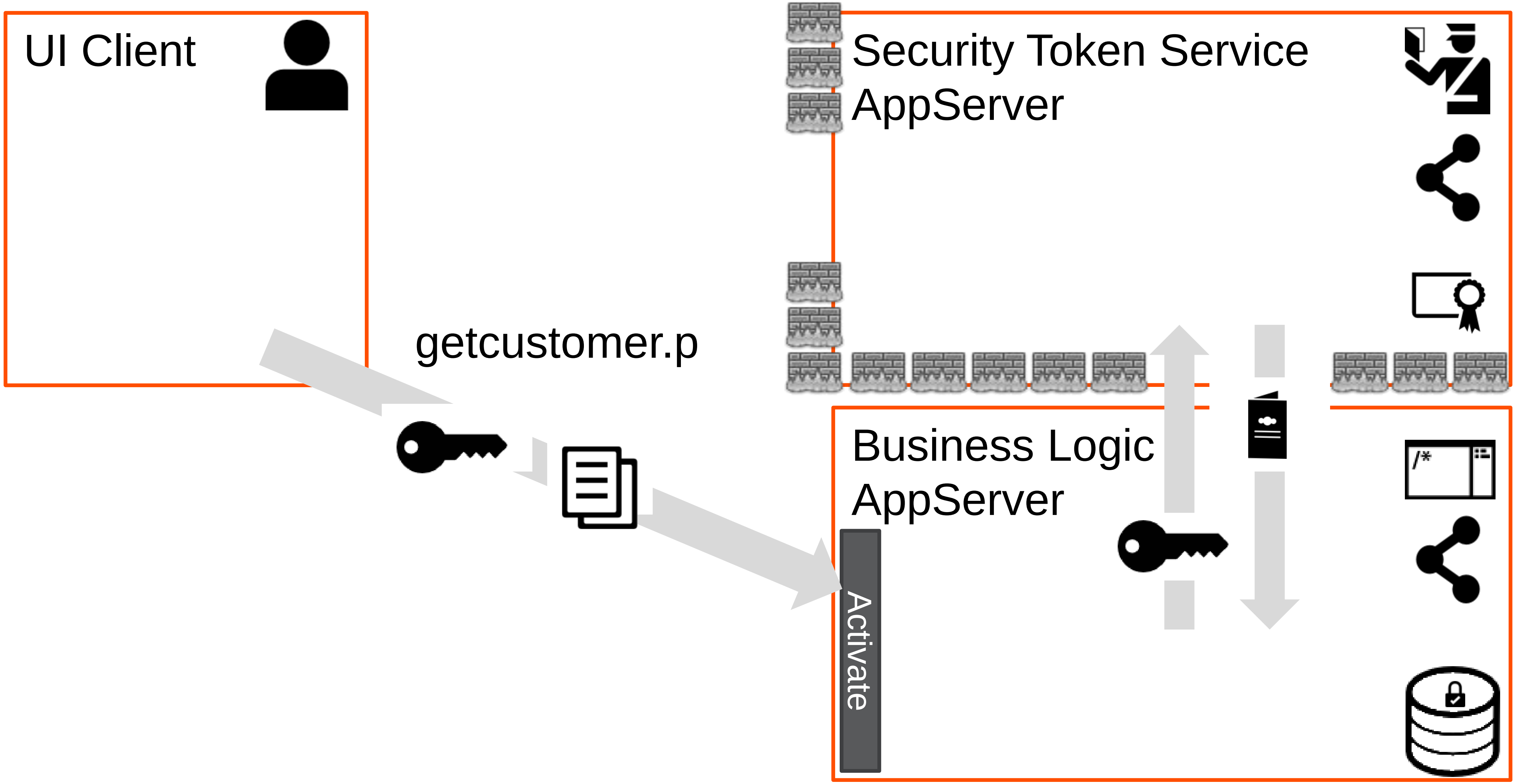


```
Security/Startup.p

session:export(
    'Security/Login.p'
    'Security/LoginSSO.p' + ',' +
    'Security/Logout.p' + ',' +
    'Security/GetClientPrincipal.p' + ',' +
    'Security/ValidateToken.p' + ',' +
    'Security/ValidateClientPrincipal.p' + ',' +
    'Security/RegisterServer.p' + ',' +
    'Security/DeregisterServer.p').
```

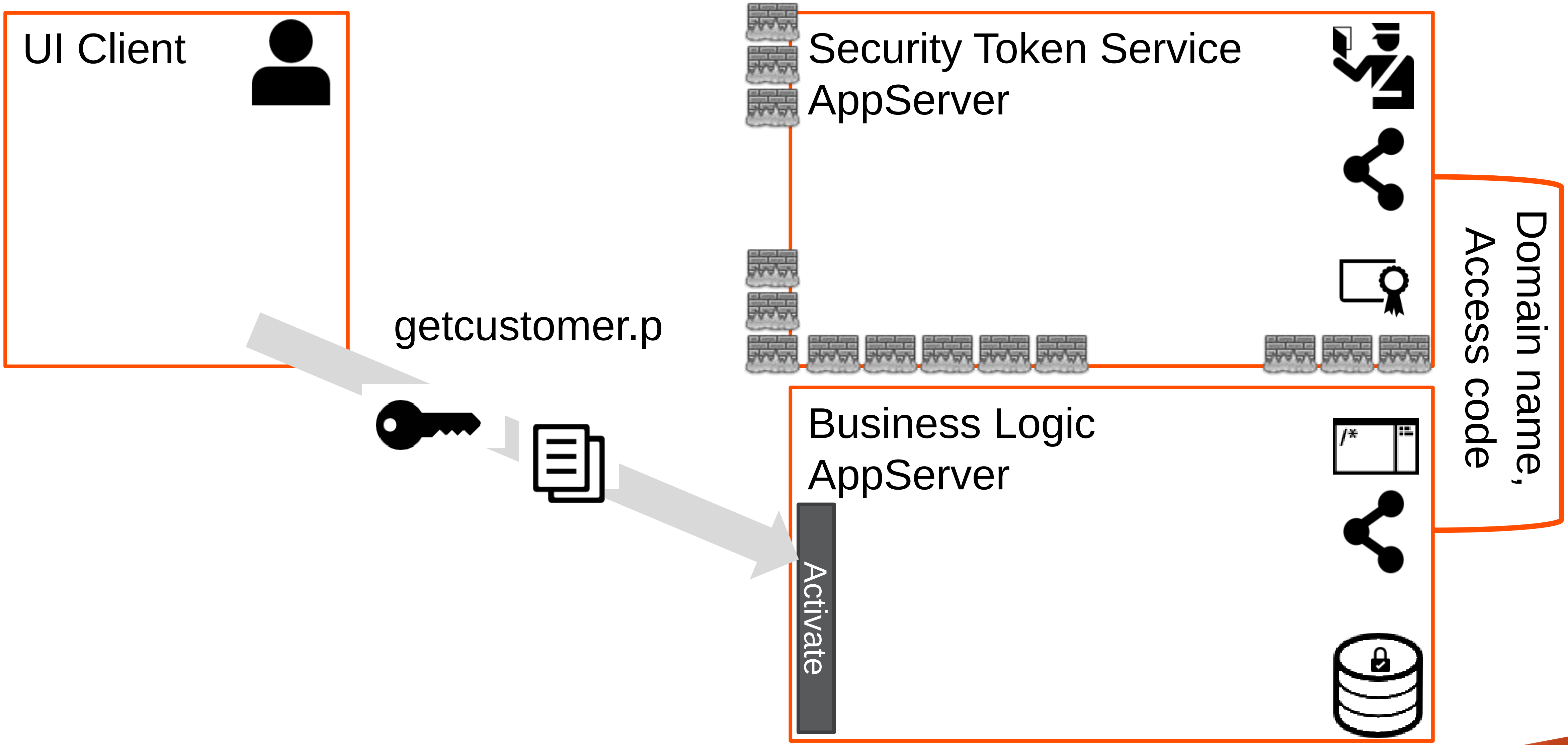
Separate AppServers for STS & Business Logic



Separate AppServers for STS & Business Logic



Separate AppServers for STS & Business Logic



_sec-authentication-system & -domain

Security Token Service

```
create _sec-authentication-system.
_Domain-type                  = 'DBTABLE-Identity'.
_PAM-plug-in                  = true.
_PAM-callback-procedure       =
         'IdentityTableAuthenticate.p'.
```

Business Logic Service

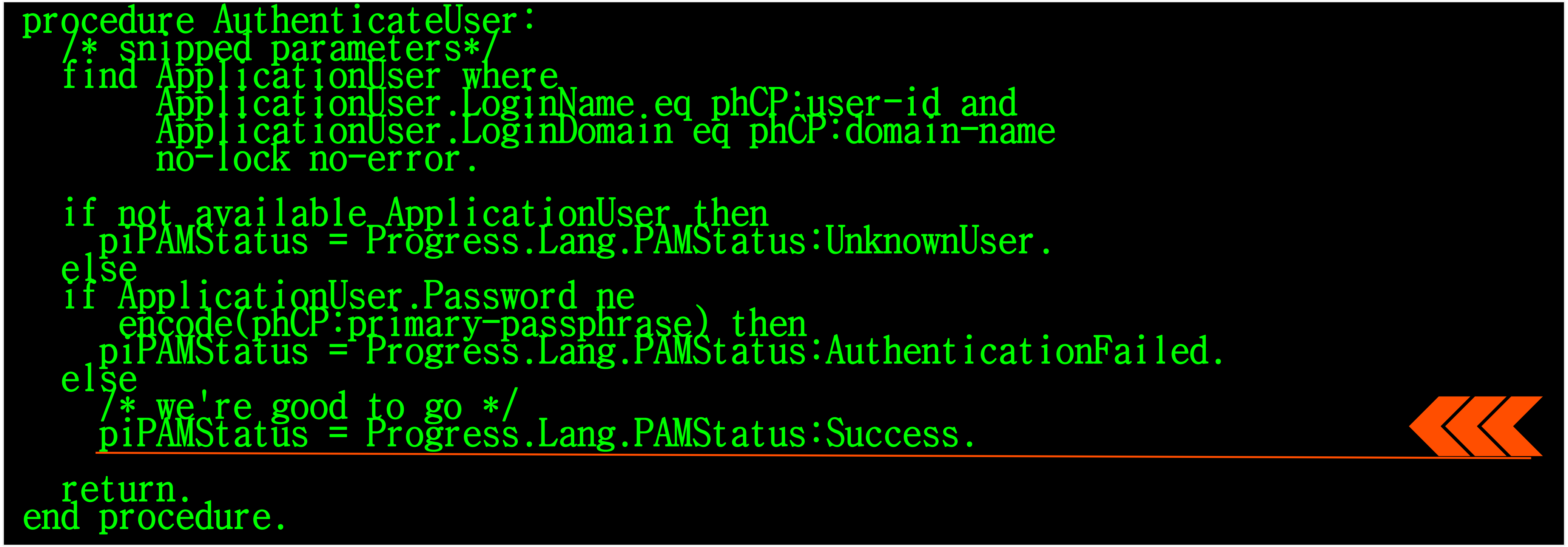
```
create _sec-authentication-system.
_Domain-type                  = 'DBTABLE-Identity'.
_PAM-plug-in                  = true.
_PAM-callback-procedure       =
         'noLoginAuthenticate.p'.
```

Common

```
create _sec-authentication-domain.
_Domain-name        = 'employee'.
_Domain-type        = 'DBTABLE-Identity'.
_Domain-access-code = audit-policy:encrypt-audit-mac-key(
                      ‘s00perSecr1tK3y4EMPLOYEE').
_Domain-enabled     = true.
```

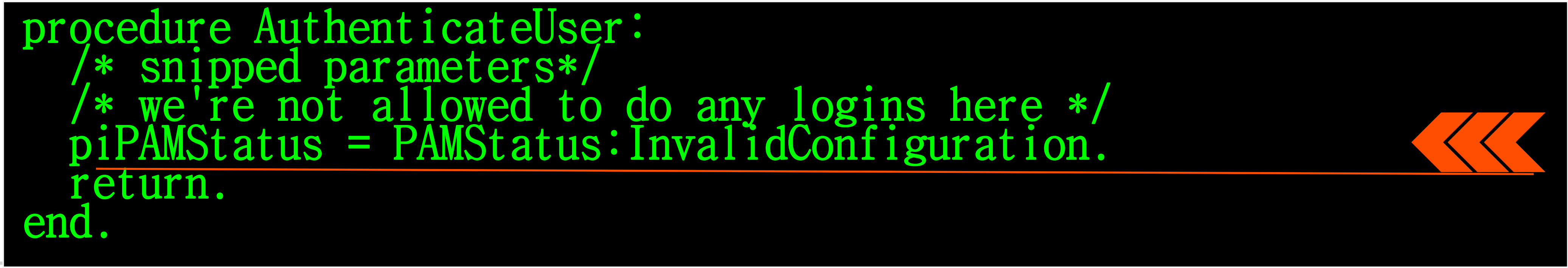
_PAM-callback-procedure

Security Token Service



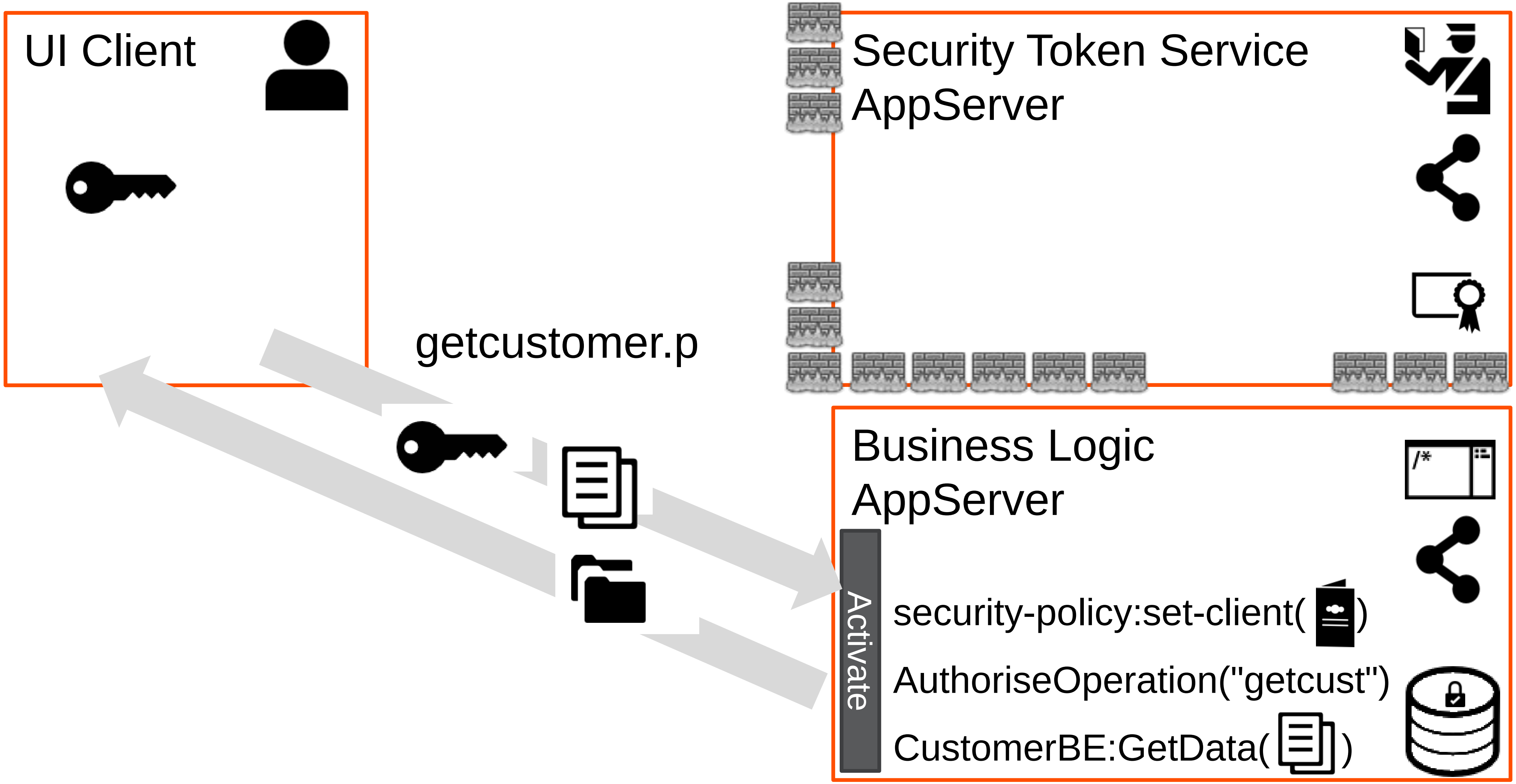
```
procedure AuthenticateUser:
  /* snipped parameters*/
  find ApplicationUser where
          ApplicationUser.LoginName eq phCP:user-id and
          ApplicationUser.LoginDomain eq phCP:domain-name
          no-lock no-error.

  if not available ApplicationUser then
    piPAMStatus = Progress.Lang.PAMStatus:UnknownUser.
  else
  if ApplicationUser.Password ne
     encode(phCP:primary-passphrase) then
    piPAMStatus = Progress.Lang.PAMStatus:AuthenticationFailed.
  else
    /* we're good to go */
    piPAMStatus = Progress.Lang.PAMStatus:Success.

  return.
end procedure.
```

Business Logic Service



```
procedure AuthenticateUser:
  /* snipped parameters*/
  /* we're not allowed to do any logins here */
  piPAMStatus = PAMStatus:InvalidConfiguration.
  return.
end.
```

Separate AppServers for STS & Business Logic



UI Client

Security Token Service AppServer

getcustomer.p

Business Logic AppServer

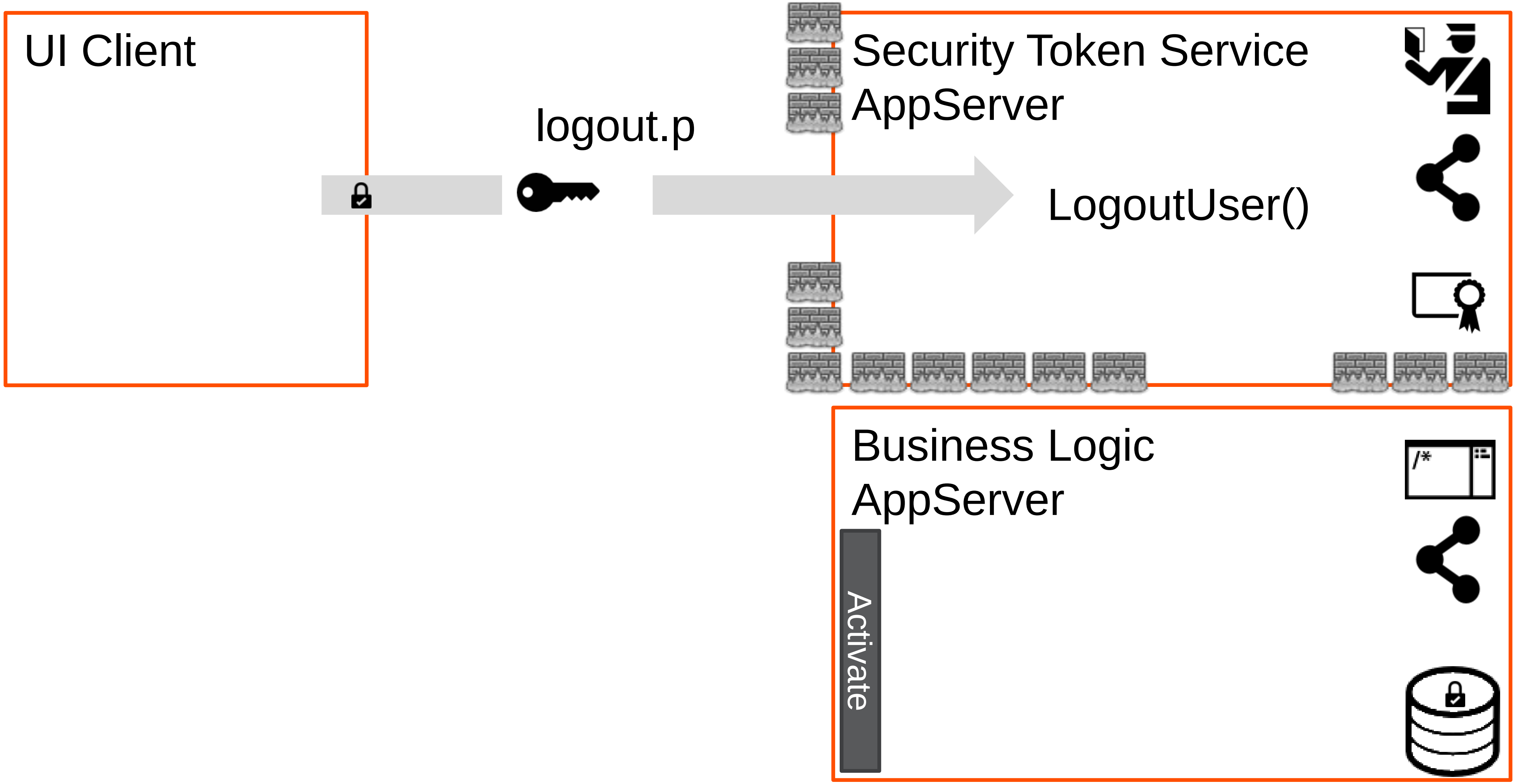
Activate

security-policy:set-client( )

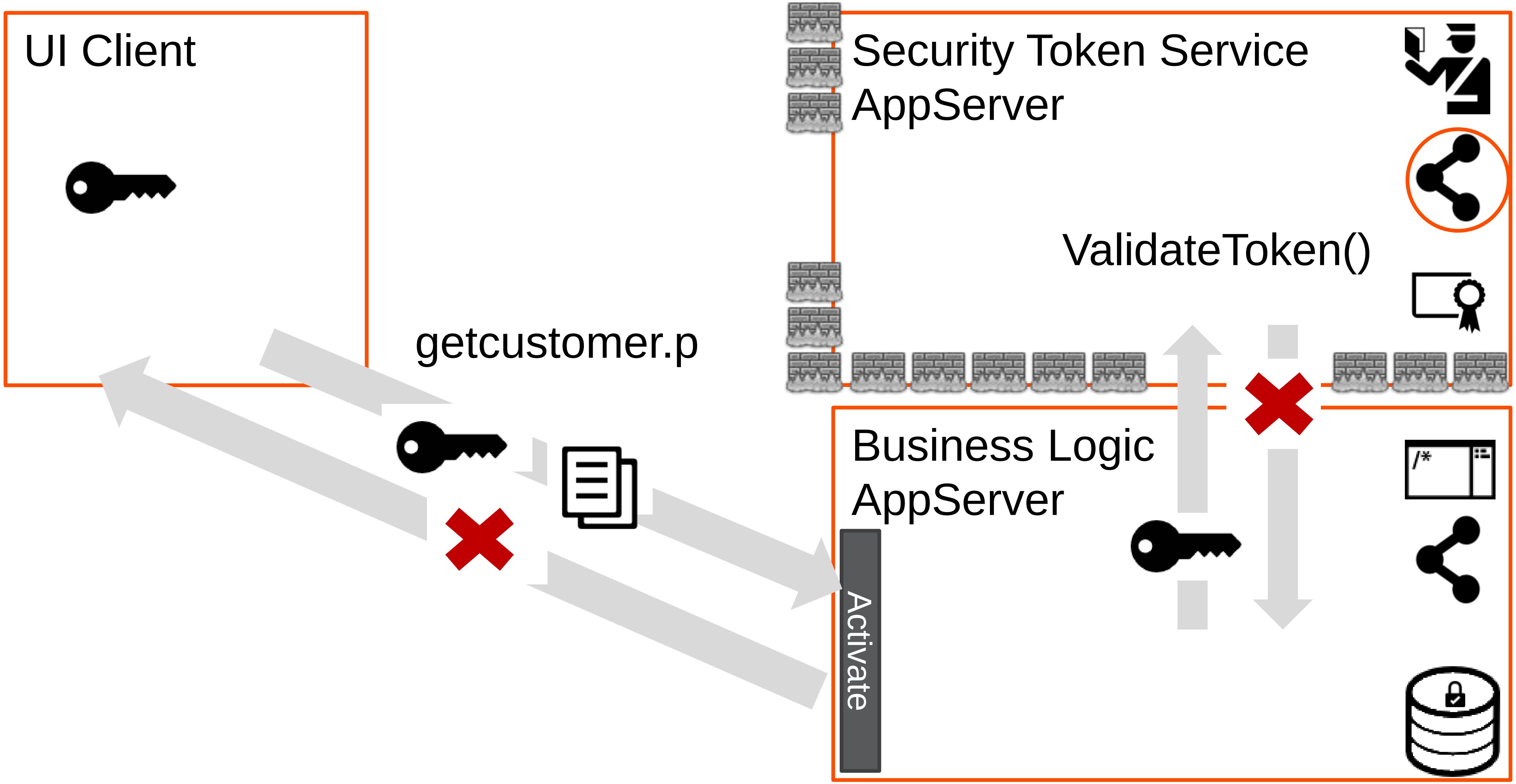
AuthoriseOperation("getcust")

CustomerBE:GetData( )

Separate AppServers for STS & Business Logic



Separate AppServers for STS & Business Logic



Application Security Principles

Applications must have security designed in. Some proven application security principles

1. Identify and secure the weakest link
2. Practice defense in depth
3. Be reluctant to trust
4. Remember that hiding secrets is hard
5. Follow the principle of least privilege
6. Fail and recover securely
7. Compartmentalize
8. Keep it simple, stupid
9. Keep trust to yourself
10. Assume nothing

Gary McGraw's 10 steps to secure software

Lather, Rinse, Repeat

- Think of security as a continuous improvement project.
  You are never done!
- Keep informed of the latest security tools and threats
- Progress will continue to give you tools to help secure your Application and valuable data
- Want more information on any of the topics in this presentation?
  - Look in the briefcase available after this this talk
  - Go to http://communities.progress.com

Summary

- Security is a complex issue that is constantly changing
- There are many options for you to choose from –
  today you experience some options
- Start Simple, identify what is important, and don’t stop evolving…

PROGRESS

Reference Materials

- http://directory.apache.org/studio/ - Apache Directory Studio
- http://www.nirsoft.net/utils/smsniff.html - Smart Sniffer
- http://www.openldap.org/ - OpenLDAP
- http://communities.progress.com/pcom/docs/DOC-45878 - AuthWP.zip for LDAP
- http://communities.progress.com/pcom/docs/DOC-106849 - Security Webinar Briefcase
- http://news.cnet.com/2008-1082-276319.html - 10 Steps to Secure Software

Other Exchange Security Sessions

Identity Management Basics (Part 1)	Peter Judge
Coding with Identity Management & Security (Part 2)	Peter Judge
Transparent Data Encryption	Doug Vanek
Introduction to Multi-tenancy	Gus Bjorklund
Security and Session Management with Mobile Devices	Mike Jacobs & Wayne Henshaw