Writing the Code

Edward Curren

@edwardcurren http://www.edwardcurren.com

Overview

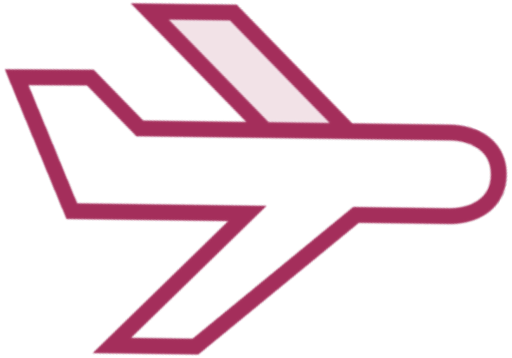
Setup a Certificate Authority

Create Key Pairs

Create Certificates

Encrypt and Decrypt Data

Sign Data and Validate Data Signatures



Before the Code

- The Project
- The ‘Trust Us’ Certificate Authority
- The Data Structures

The Project

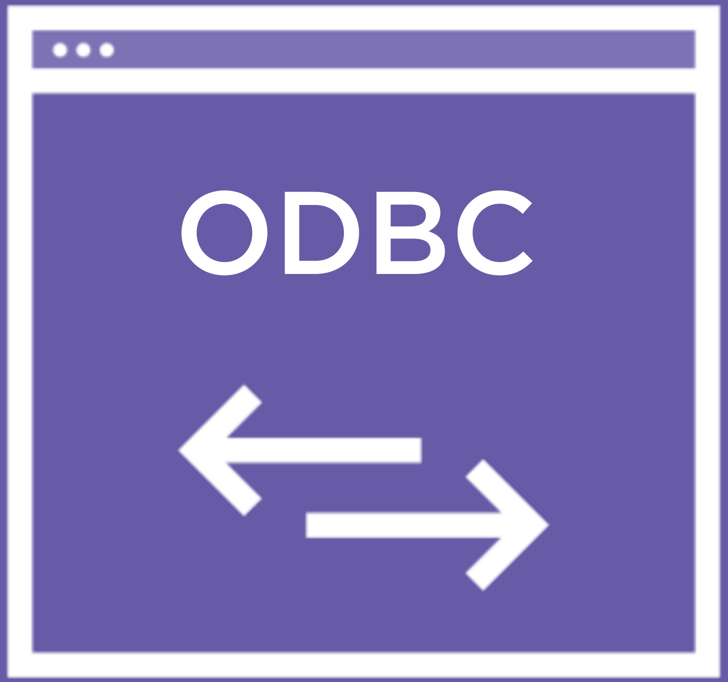
The Project

Trust Us Certificate Authority

Pluralsight.TrustUs.Certificate.Authority

Cryptlib

- Explicit configuration definition to understand implementation of concepts.
- Simple API



You may use any database and any ODBC driver that you prefer, however the Data Source Name (DSN) must be named “TrustUs”

The Project

Trust Us Certificate Authority

Pluralsight.TrustUs.Certificate.Authority

Duck Airlines Application

Pluralsight.DuckAirlines.Cryptography

Bouncy Castle

Eases implementation and improves understanding of the code

Large Code Base

The project has a lot of code in there already so that you have sample code to play with as keep exploring asymmetric cryptography.

Blank Methods

These are the methods that we are going to write together in this project

Trust Us Certificate Authority

Providing reputable X.509 certificate services to
the global community

Root Certificate Authority

- Keystore File Name
- Certificate Request File Name
- Certificate File Name
- Key Label
- Private Key Password
- Distinguished Name

Key Pairs

Key Configuration

Key Pairs

- Keystore File Name
- Certificate Request File Name
- Certificate File Name
- Key Label
- Private Key Password
- Distinguished Name

Key Configuration

- Country
- State or Province
- Locality
- Organization
- Organizational Unit
- Common Name

Distinguished Name

Signing Certificates

Certificate Configuration

- Signing Key File Name
- Signing Key Label
- Signing Key Password

Key Pairs

Key Configuration

Distinguished Name

CA Setup

Certificate Authority Configuration

- Certificate Store File Path
- Certificate Store ODBC Name
- Certificate Store URL
- Revocation List URL
- Online Certificate Status Protocol (OCSP) URL

Signing Certificates

Certificate Configuration

Key Pairs

Key Configuration

Distinguished Name

CA Setup	Certificate Authority Configuration	
Signing Certificates	Certificate Configuration	
Key Pairs	Key Configuration	Distinguished Name

Demo

Writing the Certificate Authority code first

- More complex compared to Duck Airlines application

Not a prerequisite for the rest of the code

- Can go through the rest of the code first then come back and watch this

C# vs C

C#

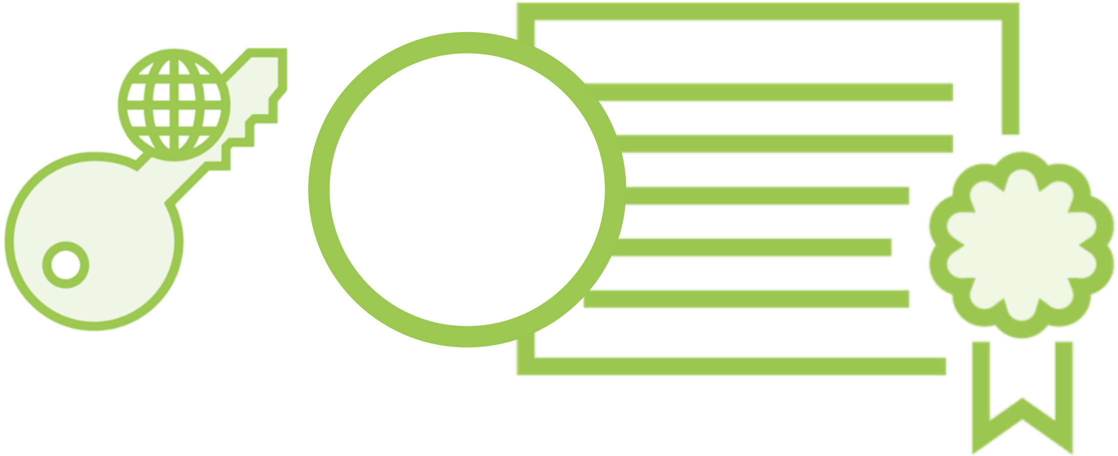
C# code is compiled into an intermediate language that runs within the Common Language Runtime (CLR).

The CLR handles all resource allocation and cleanup.

C

C is a low-level language that compiles directly into machine code.

Allocation and cleanup of resources must be done by the code.



Four Responsibilities of a PKI

Authentication

Integrity

Confidentiality

Non-Repudiation

RFC 5280 Certificate Policy Rules

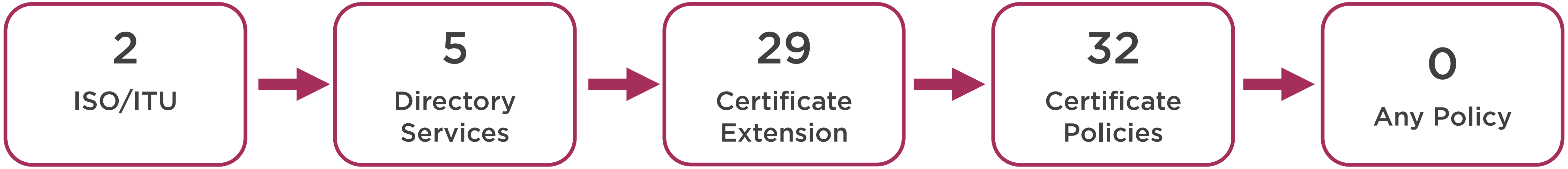
Certificate Policies extension must appear in all certificates in the chain except root certificate.

Certificate policy OID presented in leaf certificate must be valid for entire certification path.

If Certificate Policies extension is missing in the CA certificate, no explicit certificate policies are allowed below that CA certificate.

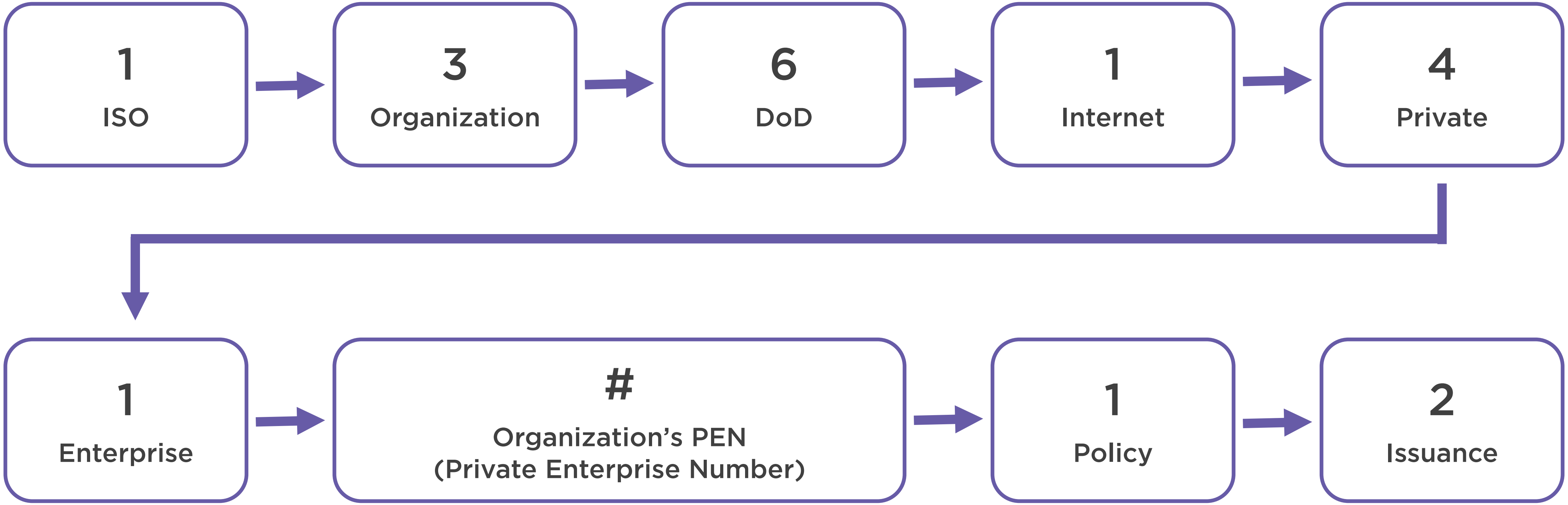
Certificate Policy OIDs

Generic Certificate Policy OID



Certificate Policy OIDs

Organization Certificate Policy OID

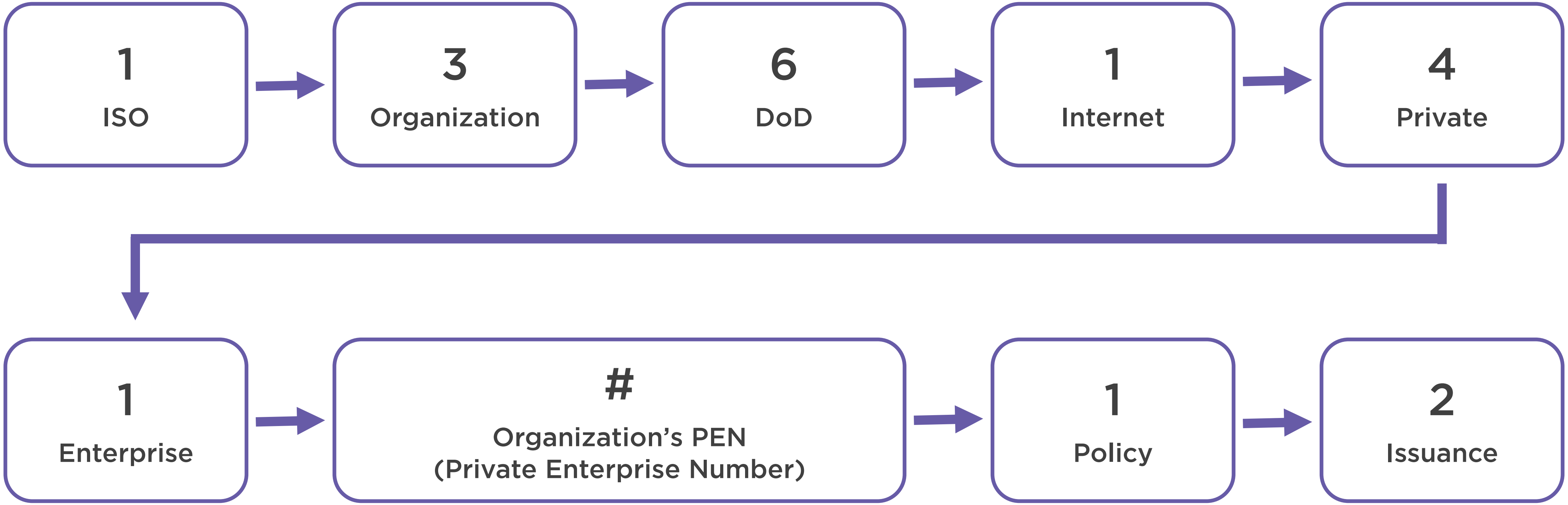


Private Enterprise Number (PEN)

To have a PEN assigned to you, fill out this IANA form: https://pen.iana.org/pen/PenApplication.page

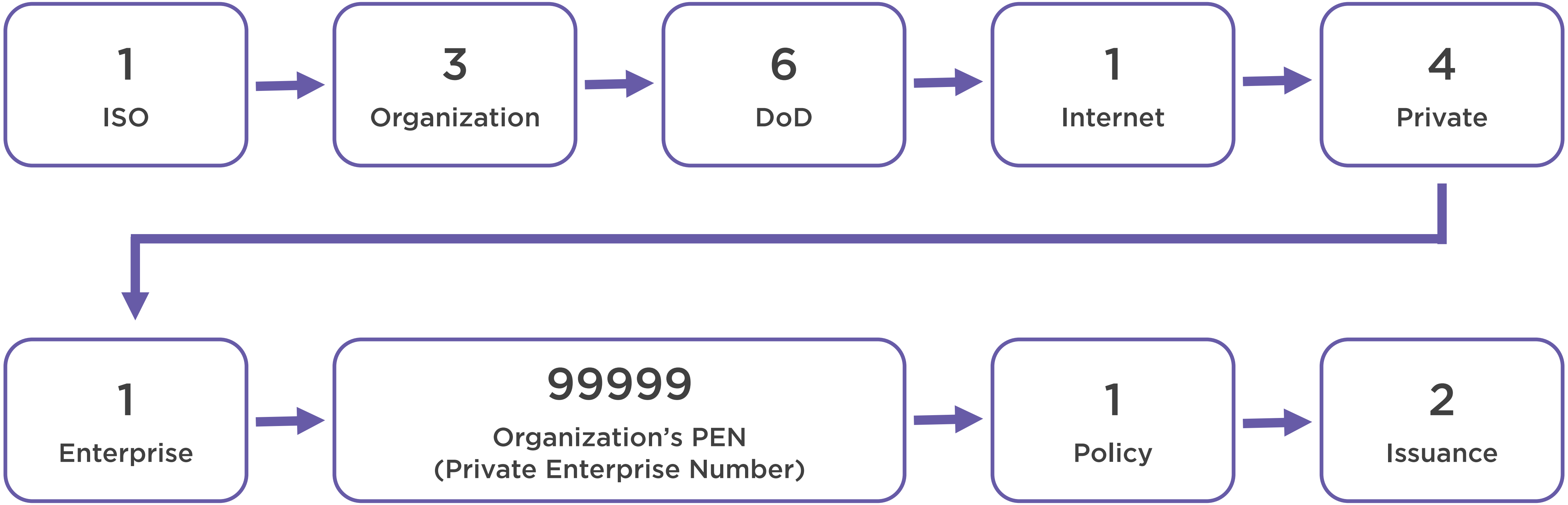
Certificate Policy OIDs

Organization Certificate Policy OID



Certificate Policy OIDs

Organization Certificate Policy OID



1.3.6.1.4.1.99999.1.2

.1	Issuance Policy for North America
.2	Issuance Policy for Asia
.3	Issuance Policy for Europe
.4	Issuance Policy for South America

Certificates have long lifecycle

- Identity validation
- Issuance
- Potential expiration or revocation

Need to know the lifecycle state of the certificate

Cryptlib / ODBC

Using an ODBC connection allows Cryptlib to be database agnostic.

Issuing a Certificate in Cryptlib

Cryptlib has 3 steps to issue a certificate from a certificate signing request

Submit the CSR

Issue the Certificate

Export to CER file

“We hit the ground every time”

The Situation Onboard Flight 657

Secure communications have established

“Chicken Armageddon” officially downgraded to “Chicken Faux-Pas”

Cryptographic Library

Using Bouncy Castle library for ease of writing the project code

Bouncy Castle documentation: http://www.bouncycastle.org/csharp/

Cryptographic Library

Cryptlib’s encryption and signature implementation is complex

Full separation of concerns

ASN: Abstract Syntax Notation

A standard interface description language for defining data structures that can be serialized and deserialized in a cross-platform way.

ASN1 Encoding

DER

Distinguished Encoding Rules

BER

Basic Encoding Rules

Coming Up

Encryption / Decryption

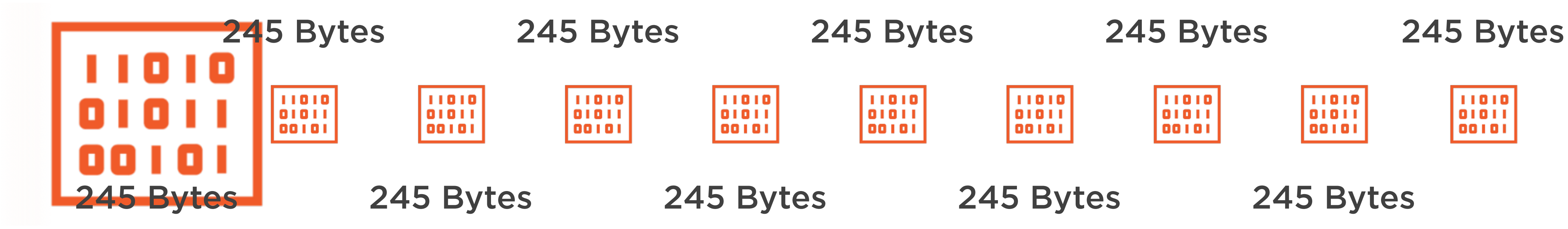
Signature / Validation

Later On

Full scale run of our application

≡ 2048

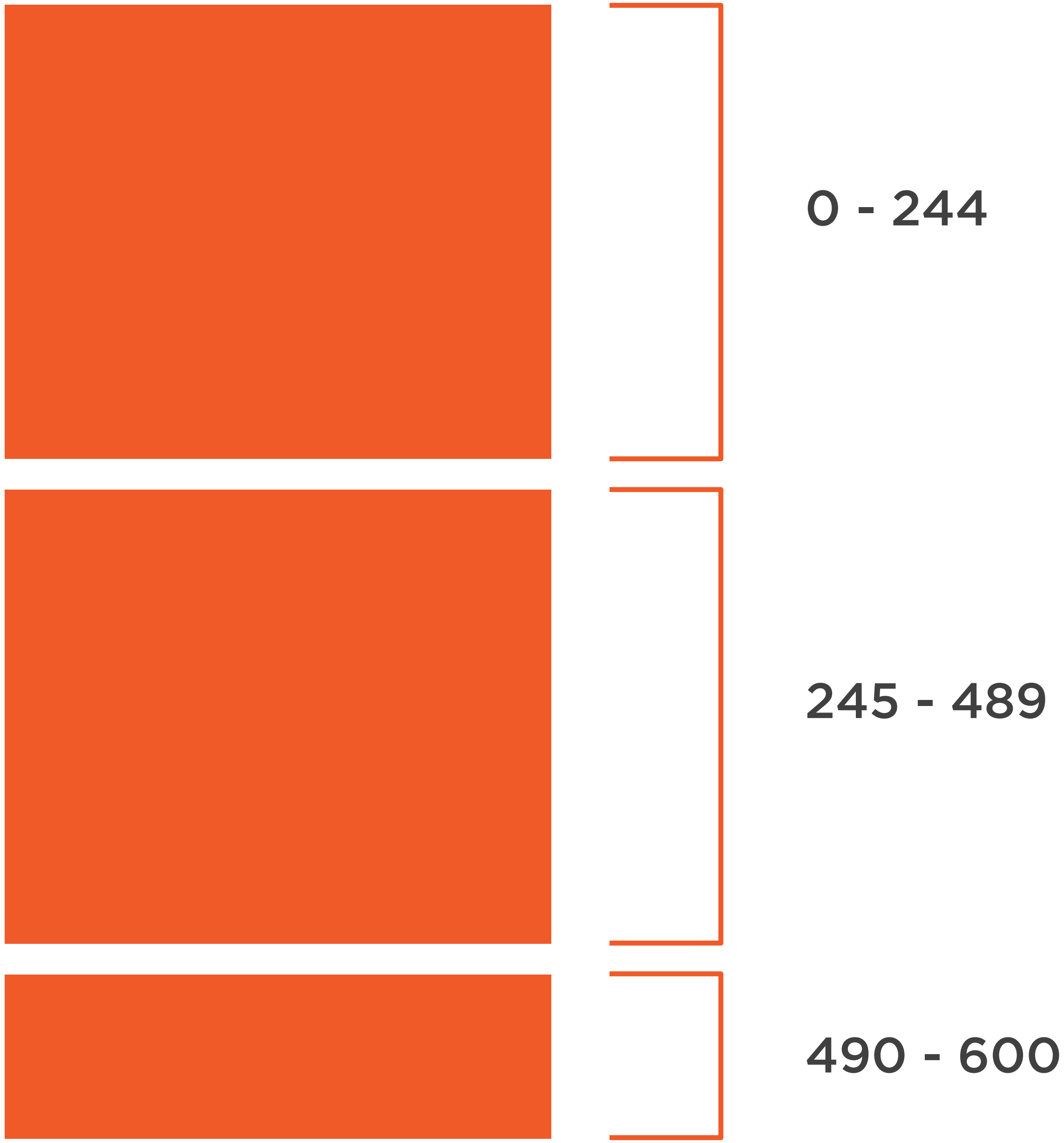
≡ 245



245 Bytes 245 Bytes 245 Bytes 245 Bytes 245 Bytes

245 Bytes 245 Bytes 245 Bytes 245 Bytes 245 Bytes

600 Bytes



0 - 244

245 - 489

490 - 600

Updates

@edwardcurren

http://www.duckairlines.com