WEB SECURITY

CODE FELLOWS

401 .NET CORE

HTTPS

Privacy

Integrity

Identification

Privacy	No unauthorized parties can eavesdrop
Integrity:	The state of your data is not changed during data transfer Man in the Middle attacks
Identification	Who is sending the Data? Digital Signatures Certificate Authoriteis

ENCRYPTION

- What is Encryption?
- What is Decryption?
- Keys still required

SYMMETRIC KEY ALGORITHM

- One key to both encrypt and decrypt
- Not easy to share
- Anyone with the key can decrypt

ASYMMETRIC KEY ALGORITHM

2 keys

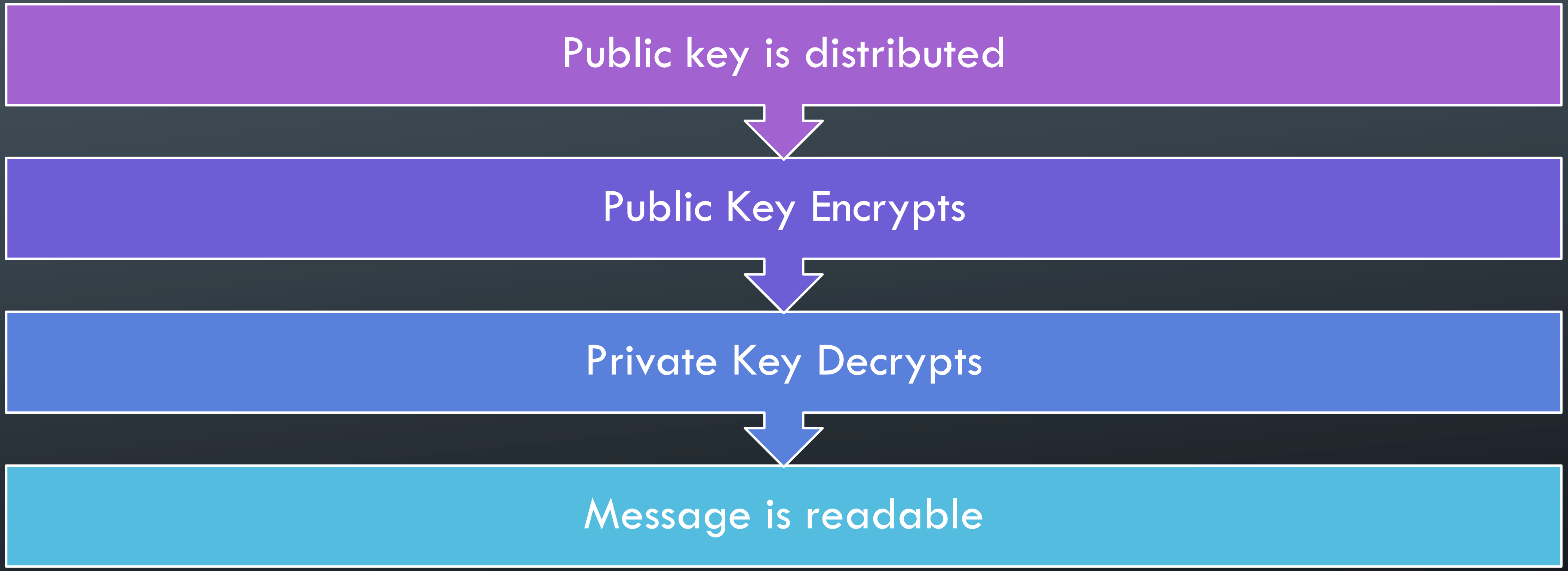
1 public – share with your friends

1 private – keep yourself

Keys work together

Only the holder of private key can decrypt

DATA FLOW



Public key is distributed

Public Key Encrypts

Private Key Decrypts

Message is readable

ADVANTAGES OF ASYMMETRIC KEYS

Privacy – No one else can read the data

Identification – only the owner has the private key. Guarantee the person is who they say they are

Integrity – state doesn't change

3 WAY HANDSHAKE

CLIENT SAYS HELLO

SERVER SAYS HELLO

SECURE CONNECTION IS ESTABLISHED

HTTPS VS SSL VS TLS

HTTPs

- HyperText Transfer Protocol
- S stands for Secure
- Create an HTTPS connection by sending data with SSL/TLS

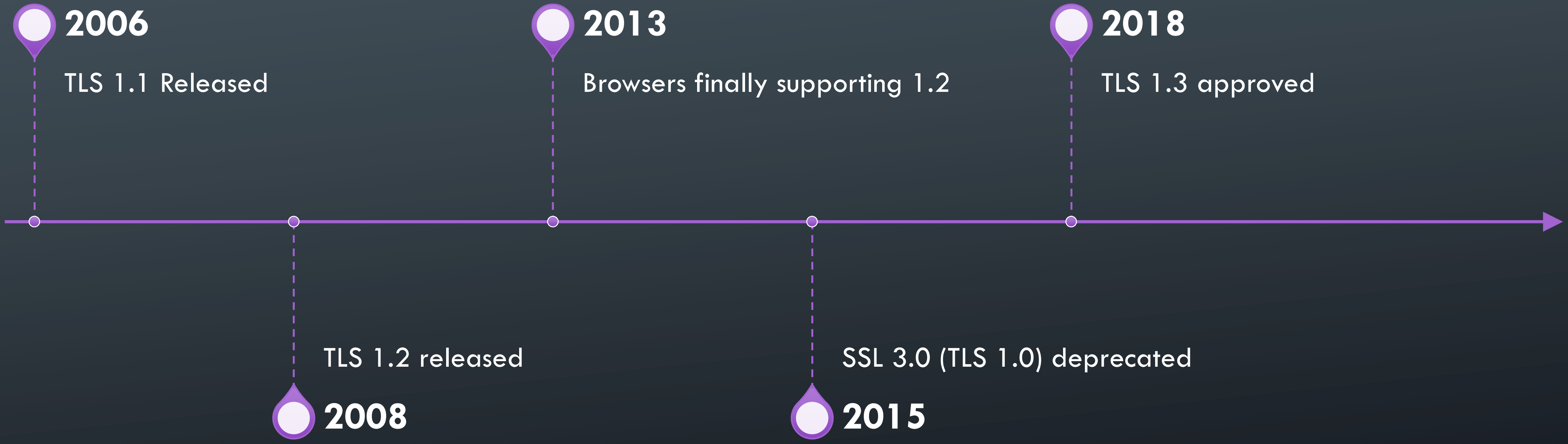
SSL

- Secure Socket Layer
- Super duper old (1995 version 3.0)
- IETF (Internet Engineering Task Force) upgraded it to TLS (SSL 3.1) in 1999

TLS

- Transport Layer Security
- Currently on 1.3 (as of March 2018)
- 1.2 still recommended (as of Summer 2018)

TLS TIMELINE



2006

TLS 1.1 Released

2008

TLS 1.2 released

2013

Browsers finally supporting 1.2

2015

SSL 3.0 (TLS 1.0) deprecated

2018

TLS 1.3 approved

CERTIFICATE AUTHORITIES

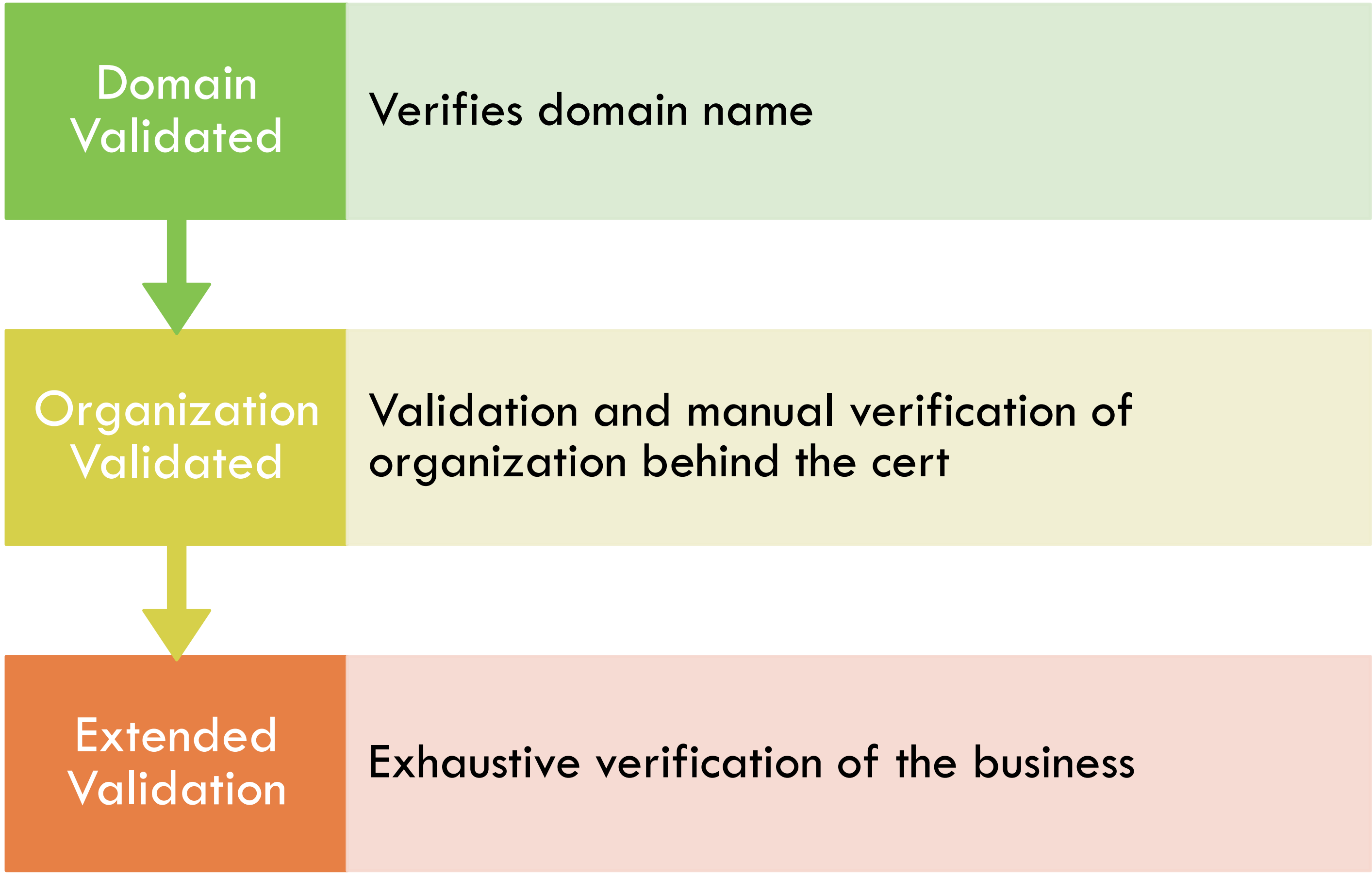
3rd party organization objectives

1. Issue Certificates
2. Confirm identities of cert owners
3. Provide proof a cert is valid

Examples:

Let's Encrypt
GoDaddy
DigiCert
Symantec

TYPES OF CERTIFICATES



Domain Validated

Verifies domain name

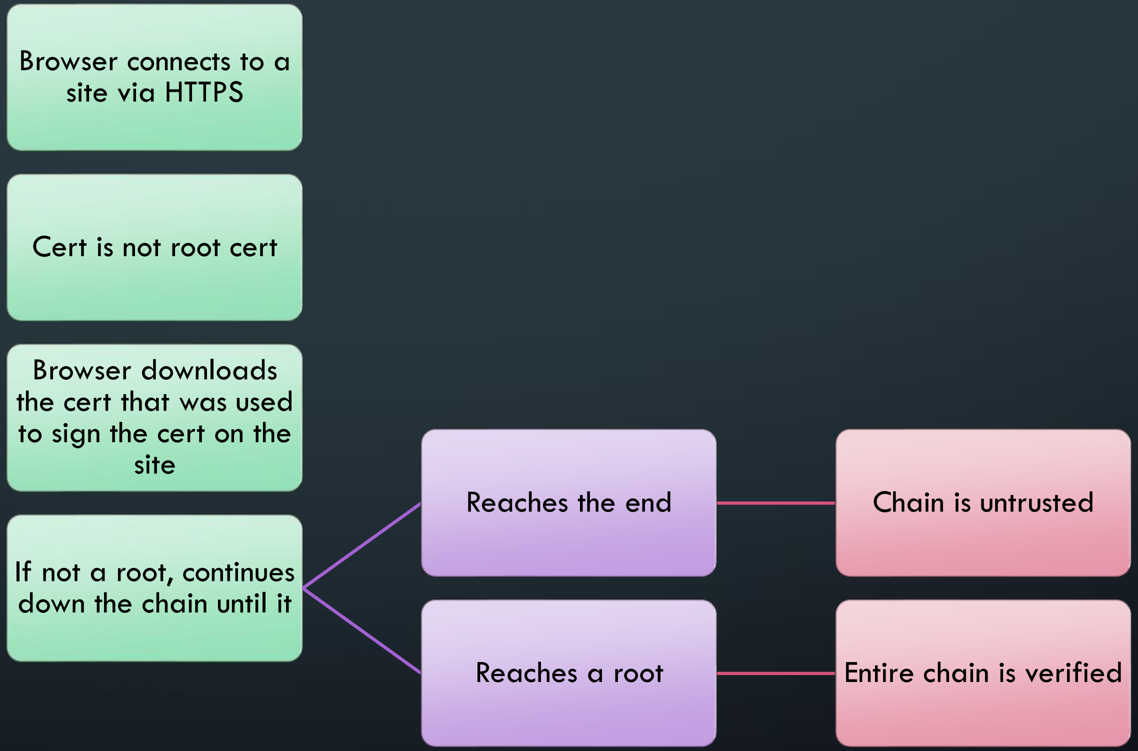
Organization Validated

Validation and manual verification of organization behind the cert

Extended Validation

Exhaustive verification of the business

VALIDATION PROCESS



Browser connects to a site via HTTPS

Cert is not root cert

Browser downloads the cert that was used to sign the cert on the site

If not a root, continues down the chain until it

Reaches the end

Chain is untrusted

Reaches a root

Entire chain is verified

SELF SIGNED CERTIFICATES

- You create it yourself
- Only good for intranets and testing sites

BREAK