Certificate Authorities (CAs) and digital certificates

Securing Digital Communications

- An electronic document used to prove the ownership of a public key.

- Also known as a public key certificate, is used to cryptographically link ownership of a public key with the entity that owns it. Digital certificates are for sharing public keys to be used for encryption and authentication.

Types of Digital Certificates

- **SSL/TLS Certificates**: Used to secure websites and online transactions.
- **Email Certificates**: Secure email communications.
- **Client Certificates:** Authenticate individual users.

Certificate Authorities (CAs)

A CA is a trusted organization that issues digital certificates.

Role

Verification: Authenticate the identity of entities (individuals, organizations) before issuing a certificate.

Issuance: Create and distribute certificates.

Revocation: Manage a Certificate Revocation List (CRL) to invalidate compromised certificates.

Hierarchy

Root CAs: The top-level CAs whose certificates are self-signed and trusted universally.

Intermediate CAs: Subordinate CAs that derive their authority from Root CAs.

Public Key Infrastructure (PKI)

A framework that manages digital certificates and public-key encryption.

CA: As described above.

Registration Authority (RA): Assists the CA by verifying the identity of entities requesting certificates.

Certificate Repository: A database where certificates and CRLs are stored.

Certificate Revocation List (CRL): A list of certificates that have been revoked before their expiration date.

PKI Users: Entities that use and rely on the certificates for secure communication.

The Process of Issuing a Certificate

Request: An entity requests a certificate from a CA.

Verification: The CA, often with the help of an RA, verifies the entity's identity.

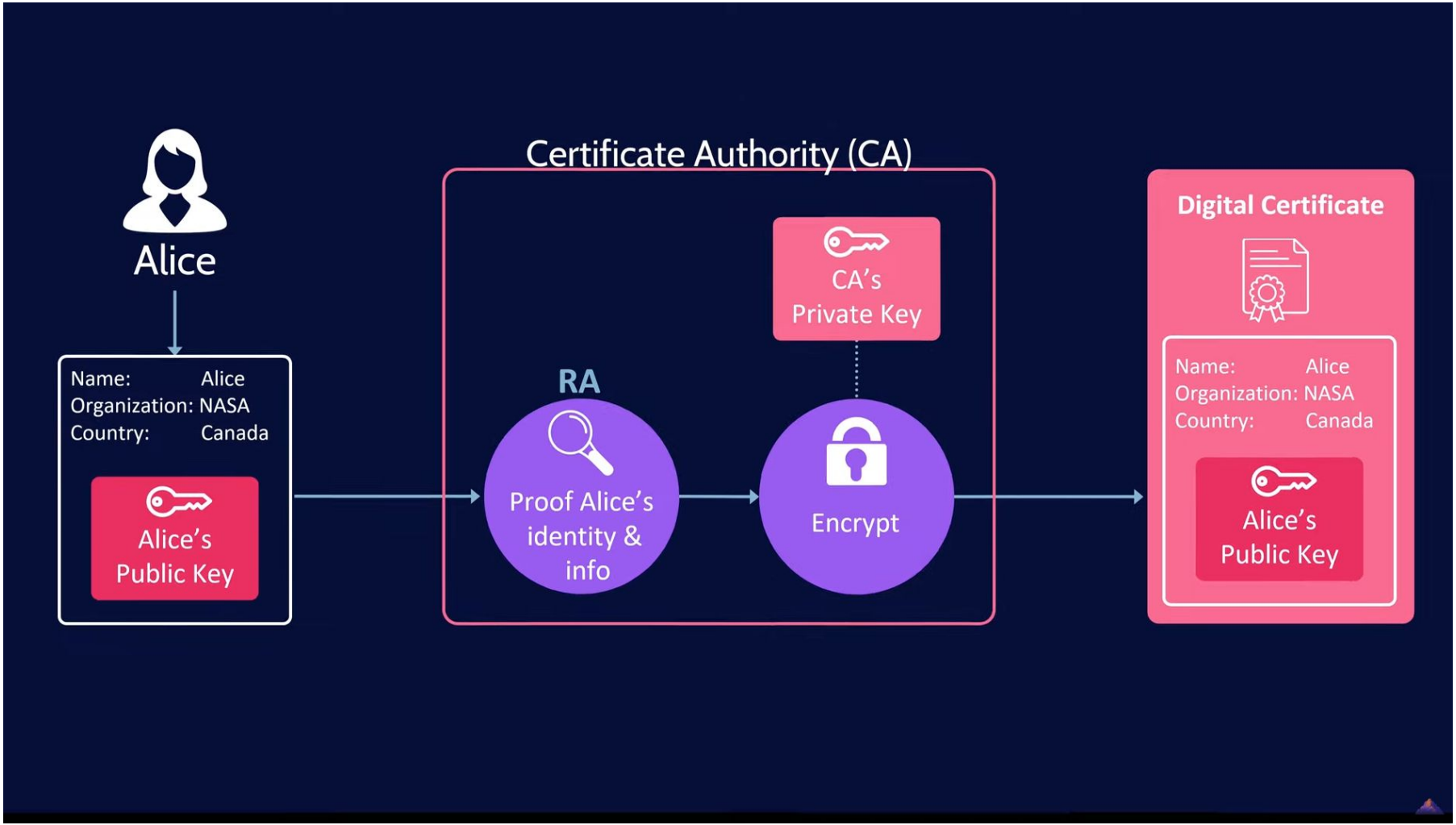
Issuance: Upon successful verification, the CA issues the certificate and digitally signs it.

Installation: The entity installs the certificate on their server or device.

Usage: The certificate is used to establish secure connections or authenticate software.

Components

- **Public Key**: The key that is shared publicly for encryption.
- **Owner Information**: Details about the owner, such as name and address.
- **Digital Signature**: Issued by a trusted entity to verify authenticity.
- **Validity Period**: Specifies the time frame in which the certificate is valid.
- **Certificate Serial Number**: A unique number assigned to each certificate.
- **Issuing CA**: The Certificate Authority that issued the certificate.


Alice
Name: Alice
Organization: NASA
Country: Canada
Alice's Public Key
Certificate Authority (CA)
CA's Private Key
RA
Proof Alice's identity & info
Encrypt
Digital Certificate
Name: Alice
Organization: NASA
Country: Canada
Alice's Public Key

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: A0B85CD0 (0xA0B85CD0)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=Example Corp, O=Example Organization, C=US
        Validity:
            Not Before: May 31 12:00:00 2023 GMT
            Not After : May 31 12:00:00 2025 GMT
        Subject: CN=www.example.com, O=Example Organization, C=US
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public-Key: (2048 bit)
            Modulus:
                00:83:6b:5c:30:0d:aa:44:db:35:77:2f:a7:5a:44:
                56:6b:bb:47:9b:4d:13:46:a1:9f:1e:16:72:1b:ee:
                c9:3b:9b:9b:42:54:cb:3a:5e:34:cf:5b:e7:5b:5e:
                63:2e:33:75:75:e3:7e:a2:78:32:18:69:94:ff:12:
                f1:9c:24:45:bd:52:34:9d:62:83:54:3d:35:16:63:
                62:6c:de:e4:56:70:64:34:63:10:6b:dd:97:45:a1:
                ef:54:1c:77:de:6d:b8:1b:0e:4d:cd:5c:a4:70:cf:
                13:ee:22:82:38:38:6d:76:0a:57:7d:8d:13:df:b4:
                5e:6a:92:49:14:bc:ae:ad:b3
            Exponent: 65537 (0x10001)
    Signature Algorithm: sha256WithRSAEncryption
         9b:61:9a:65:63:b2:67:0d:4b:97:44:0d:22:5d:2b:79:b2:4c:
         2e:ec:8f:23:9c:0a:58:53:bd:6f:57:af:4a:1c:c7:1f:e2:35:
         b7:53:e1:2f:2d:3d:47:9f:1c:39:1a:e2:43:4d:2e:39:ff:68:
         d5:29:9a:4e:0f:b3:68:43:af:32:3f:e1:9c:62:18:c1:82:9e:
```

Trust and Security

Trust Chain: Users trust Root CAs, and by extension, they trust certificates issued by Intermediate CAs.

Browser Trust Store: Web browsers and operating systems maintain a list of trusted Root CAs.

Certificate Pinning: A security mechanism to prevent attacks by associating a host with their expected public key.

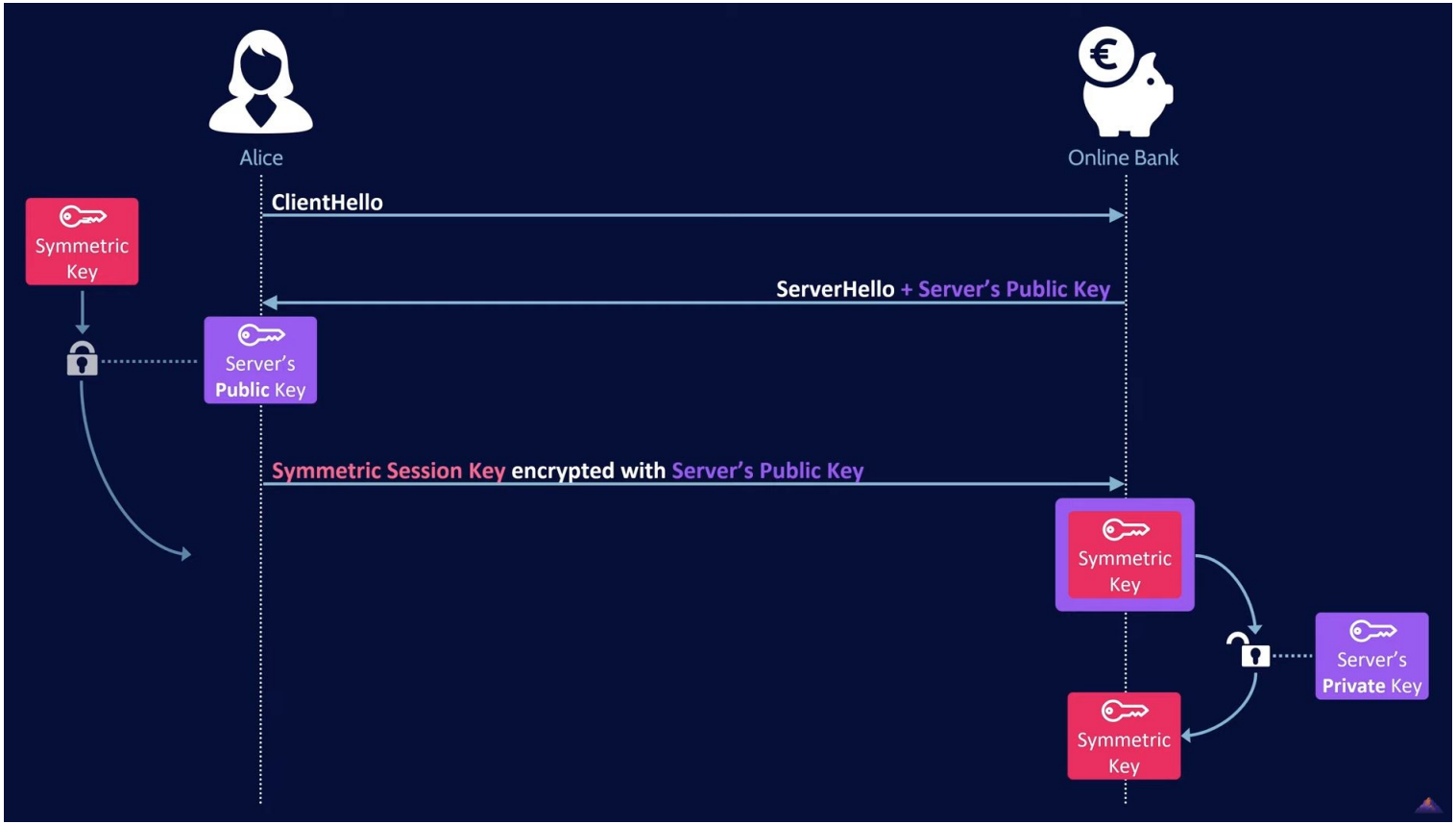
Online Certificate Status Protocol (OCSP): A protocol used to check the revocation status of a digital certificate.

Common Attacks and Mitigations

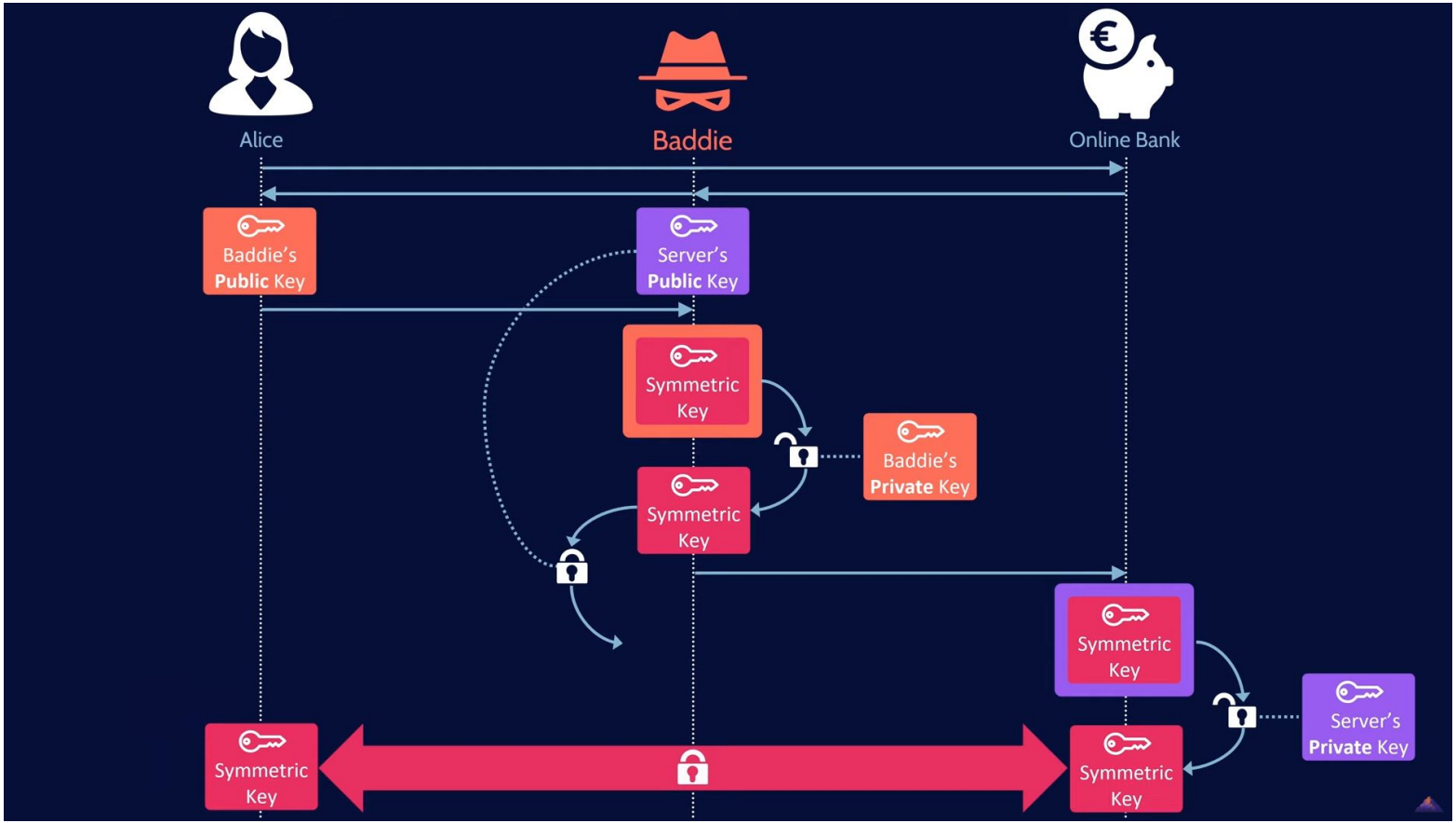
Man-in-the-Middle (MITM) Attacks: Intercepting and altering communications. Mitigation includes using valid and trusted certificates.

Phishing and Fake Certificates: Fraudulent websites presenting fake certificates. Mitigation involves user awareness and advanced browser warnings.

MITM Attacks



continued…….


Alice
Baddie
Online Bank
Baddie's Public Key
Server's Public Key
Symmetric Key
Baddie's Private Key
Symmetric Key
Symmetric Key
Server's Private Key
Symmetric Key
Symmetric Key

continued…….


Alice
Baddie
Online Bank
Digital Certificate
Name: Baddie
Organization: Evil Inc.
Country: Darkweb
Baddie's Public Key
Digital Certificate
Name: Server
Organization: Bank
Country: USA
Server's Public Key

conclusion

Digital certificates and CAs are critical for ensuring secure and trusted digital communications.

Thank you!!!!