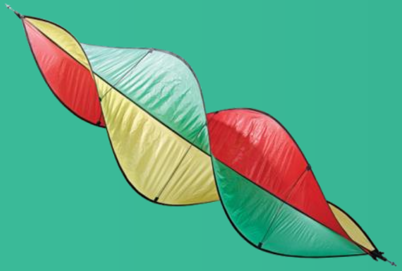
KU LEUVEN

TECHNOLOGIECAMPUS GENT

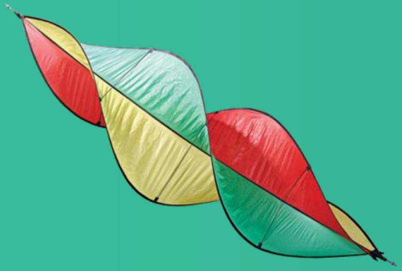


Seminar: Secure Remote Access over VPN

Ing. Vincent Raes
Onderzoeker MSEC

Program

8h30	**Reception with coffee and breakfast (Room C1T1)**	
9h00	**Theory: Secure remote access over VPN (Room C1T1)** *Public-Key Infrastructure/secure communication/user authentication/VPN* Vincent Raes (KU Leuven - MSEC)	
10h00	**Coffee break (Room C1T1)**	
10h20	**Hands-on: Secure remote access with pfSense (Room C1T1)** Configuring pfSense as router and firewall Tijl Deneut (Howest)	
12h00	**Lunch (Room cafeteria)**	
	Two parallel sessions	
	group 1	**group 2**
13h00	**Demonstration: Secure remote access over VPN (Room G120)** *eWON/Siemens Scalance S623* Vincent Raes (KU Leuven - MSEC)	**Demonstration: Secure remote access over VPN (Room G101)** *Cisco Catalyst 3560X/mGuard RS4000* Tijl Deneut (Howest), Thibaut Demasure (Ugent)
14h45	**Coffee break (Room G120)**	
15h00	**Demonstration: Secure remote access over VPN (Room G101)** *Cisco Catalyst 3560X/mGuard RS4000* Tijl Deneut (Howest), Thibaut Demasure (Ugent)	**Demonstration: Secure remote access over VPN (Room G120)** *eWON/Siemens Scalance S623* Vincent Raes (KU Leuven - MSEC)



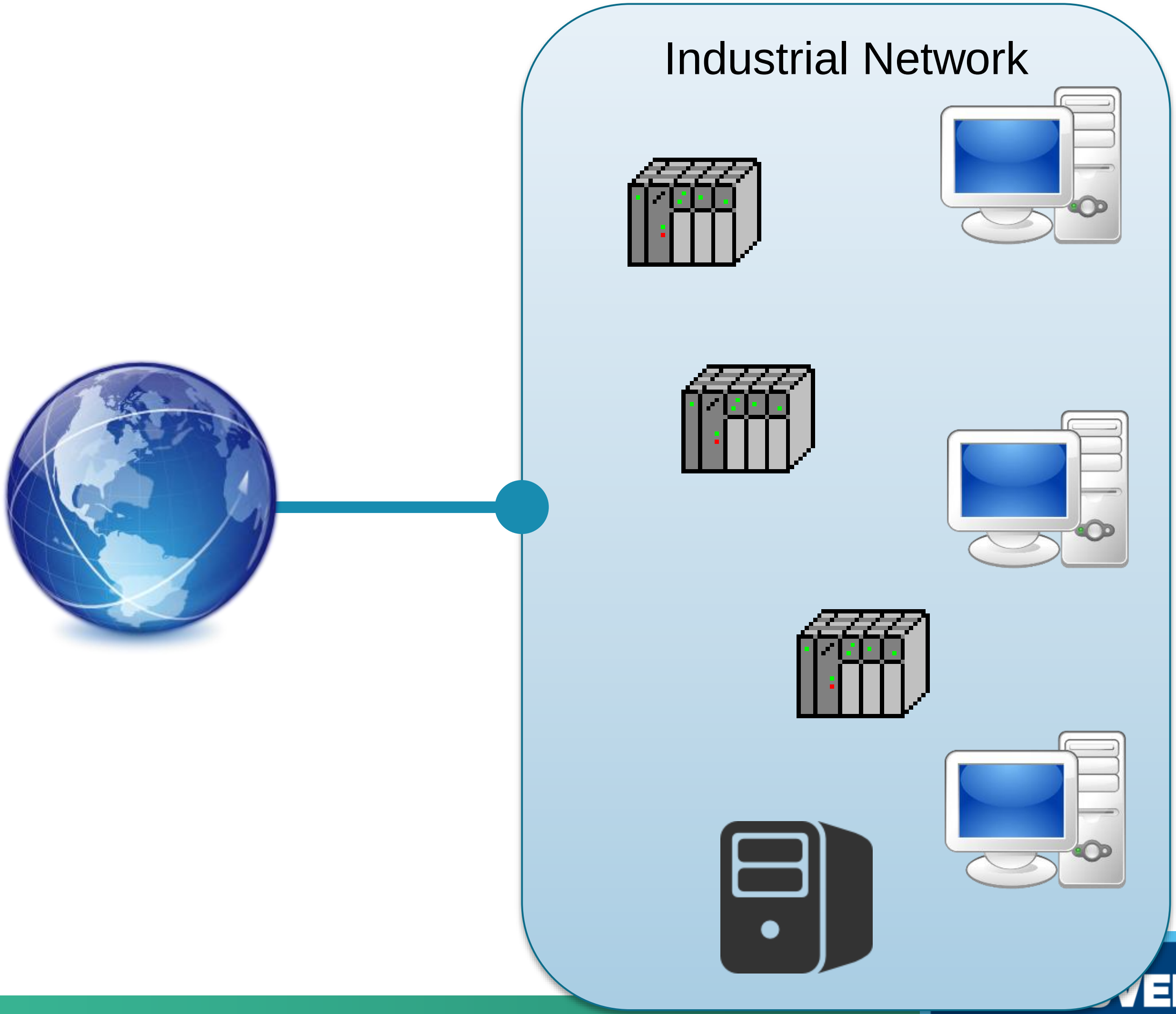
Theoretical Background

Overview

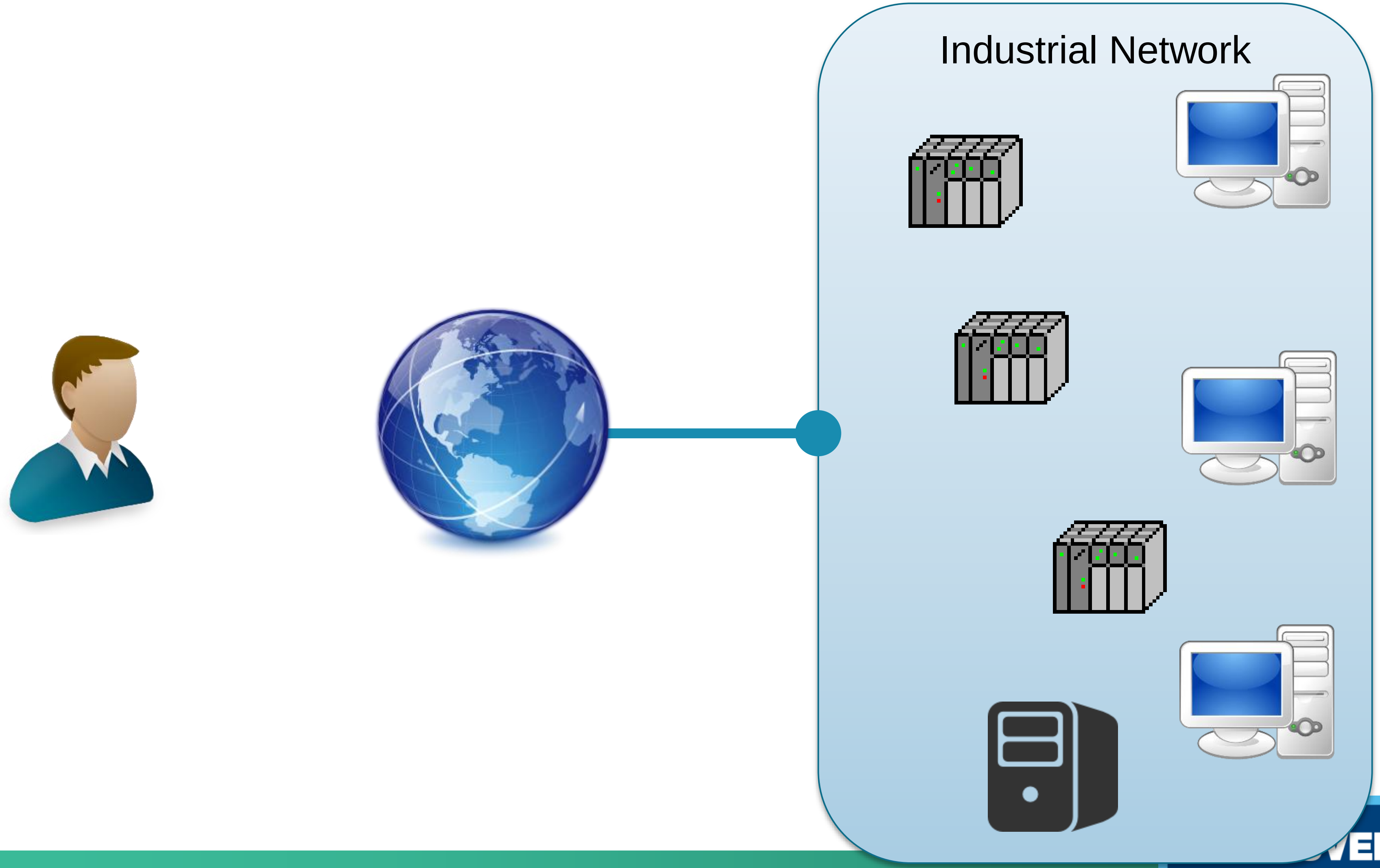
- Introduction
- Public Key Infrastructure
- Realizing Secure Communication
- User Authentication
- Virtual Private Network
  - IPsec
  - OpenVPN
- Industrial VPN Routers

Introduction

Introduction

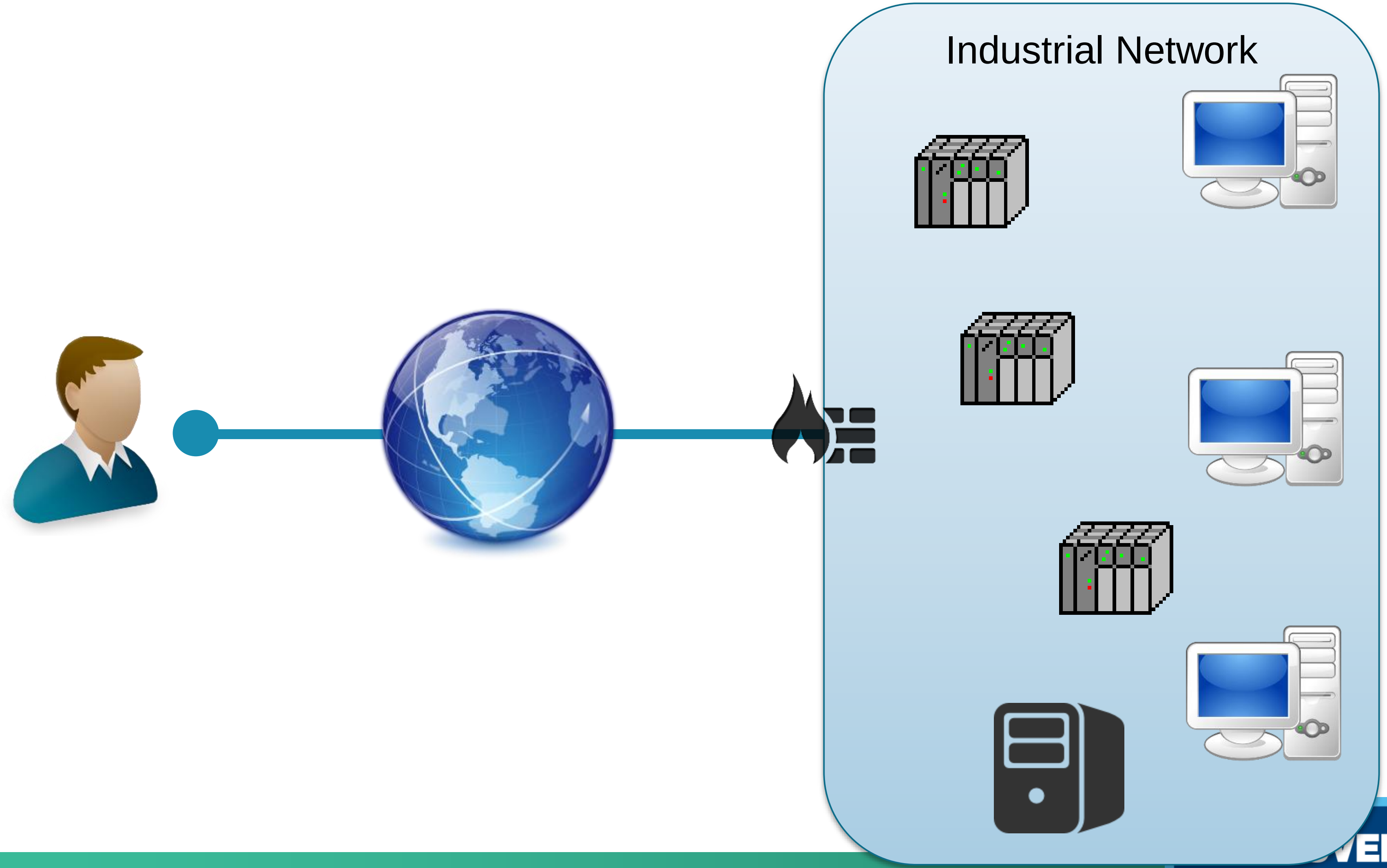


Introduction

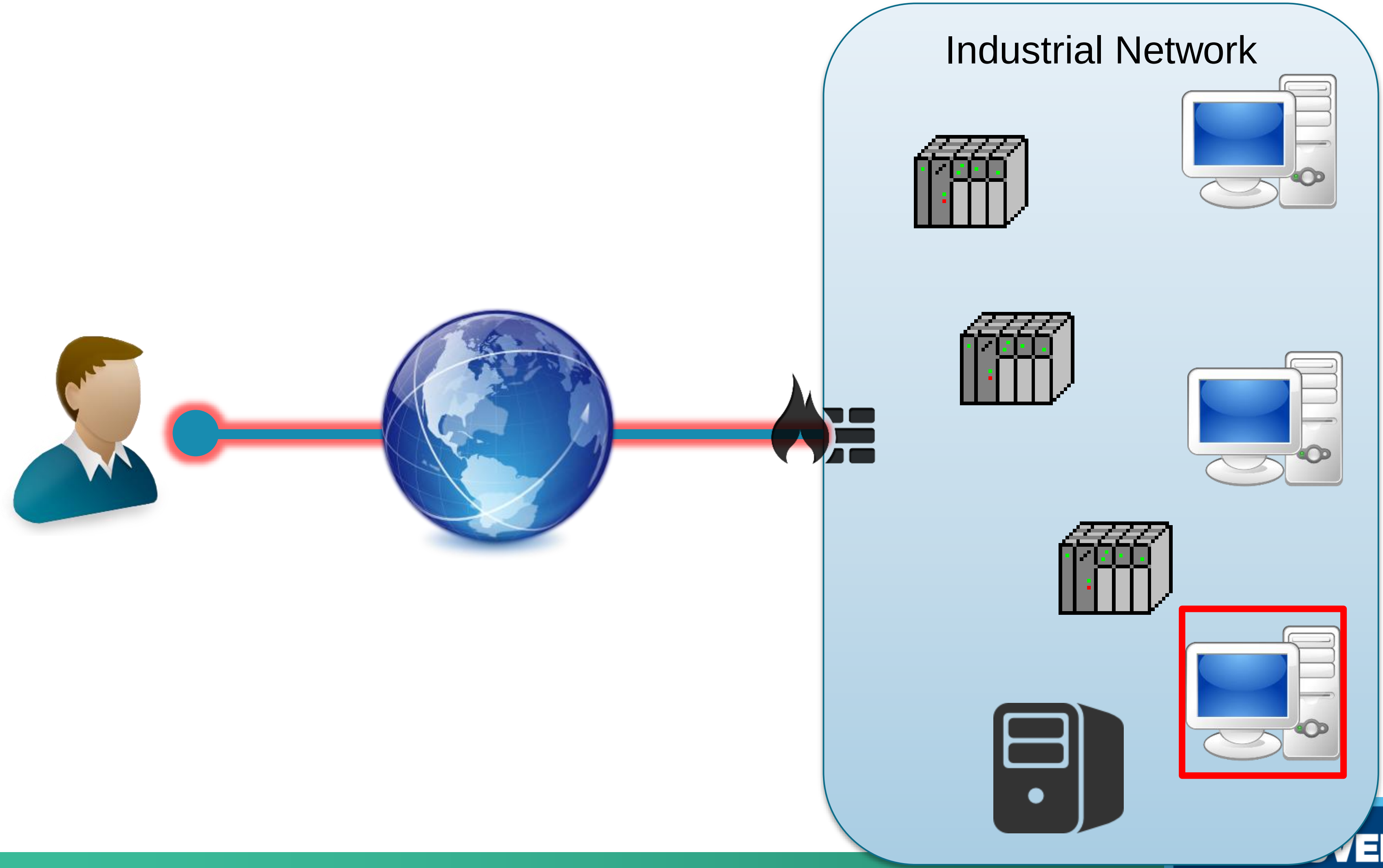


Industrial Network

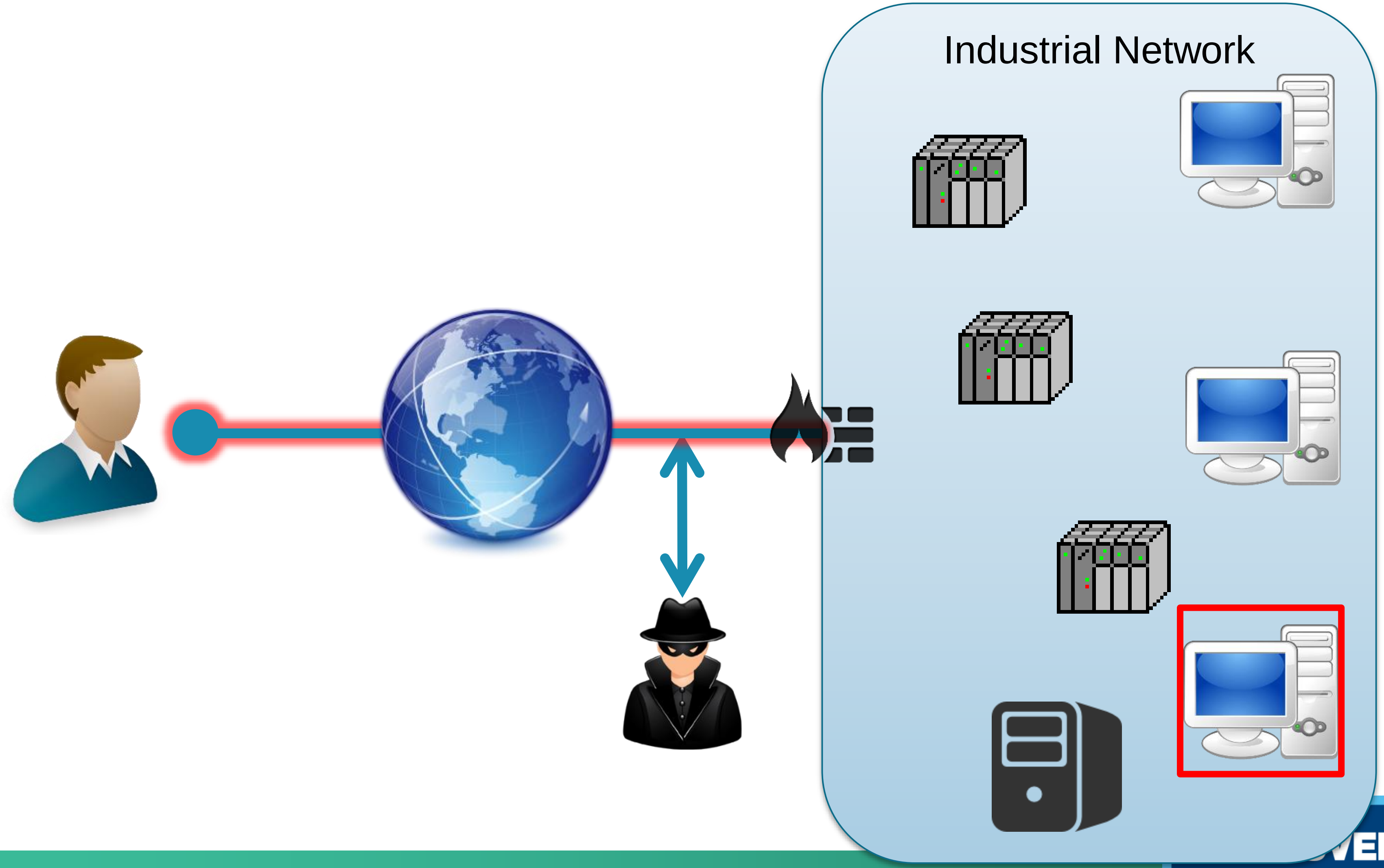
Introduction



Introduction

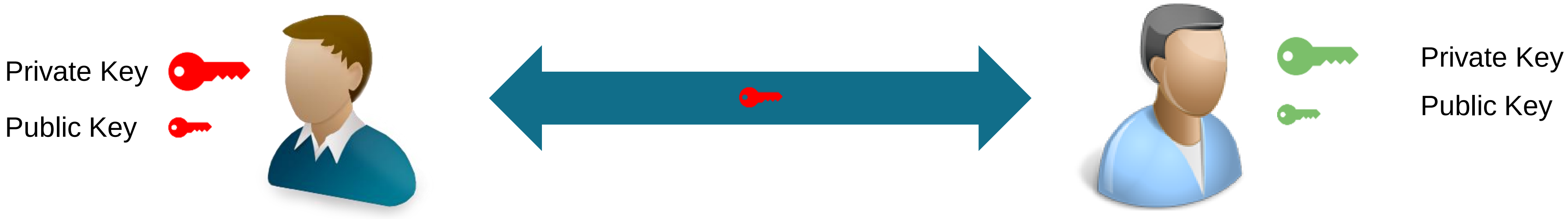


Introduction



Public Key Infrastructure

Public-Key Cryptography



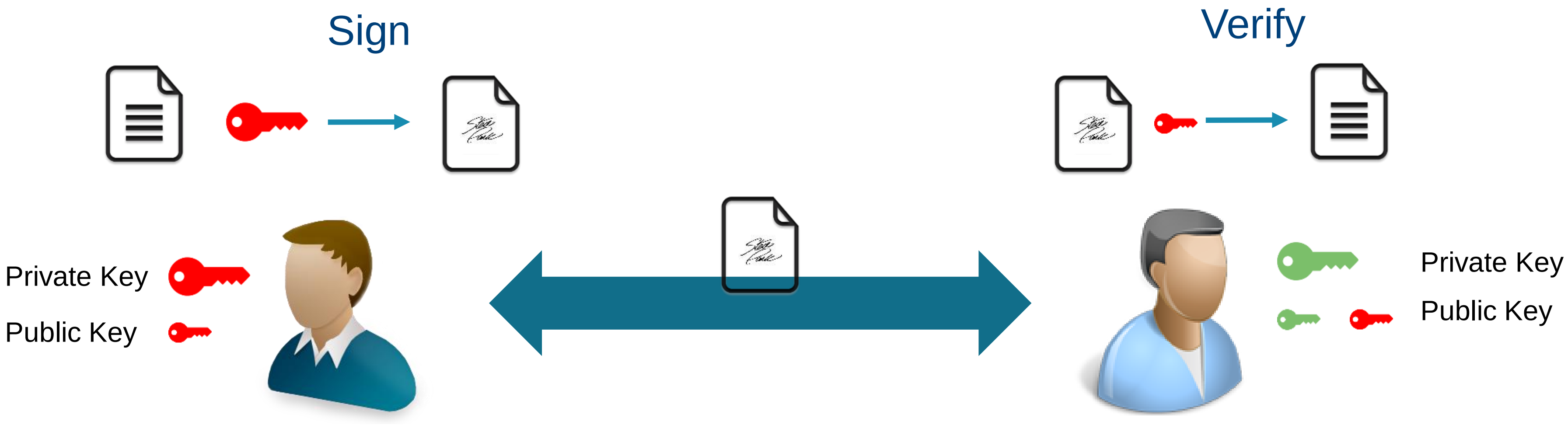
Private Key

Public Key

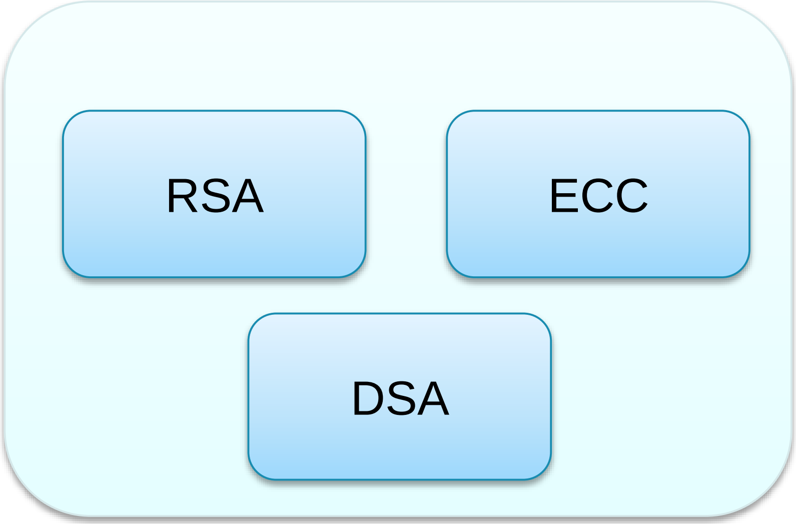
Private Key

Public Key

Public-Key Cryptography



Public-Key Cryptography



RSA

ECC

DSA

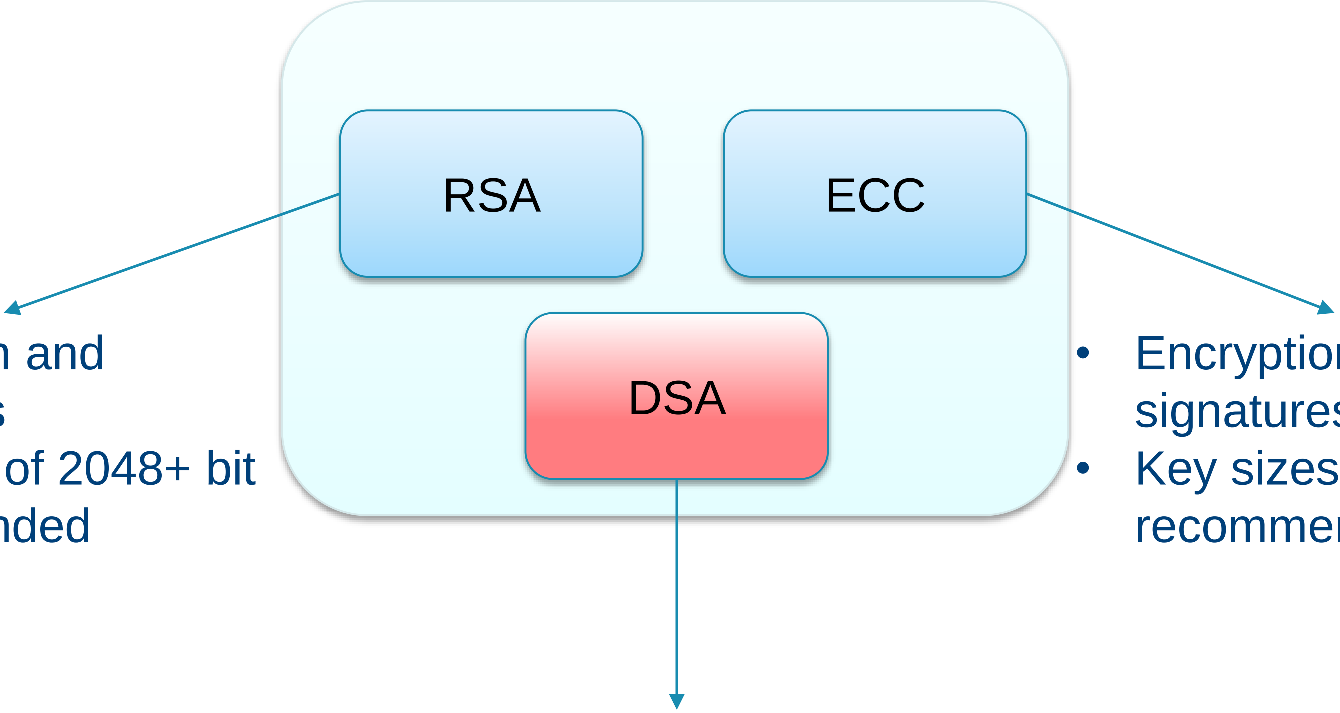
Private Key

Public Key

Private Key

Public Key

Public-Key Cryptography



RSA:

- Encryption and signatures
- Key sizes of 2048+ bit recommended

ECC:

- Encryption and signatures
- Key sizes of 224+ bit recommended

DSA:

- Signatures only
- Needs a one-time random value
- Key sizes of 2048+ bit recommended

http://www.cryptopp.com/wiki/Security_Level

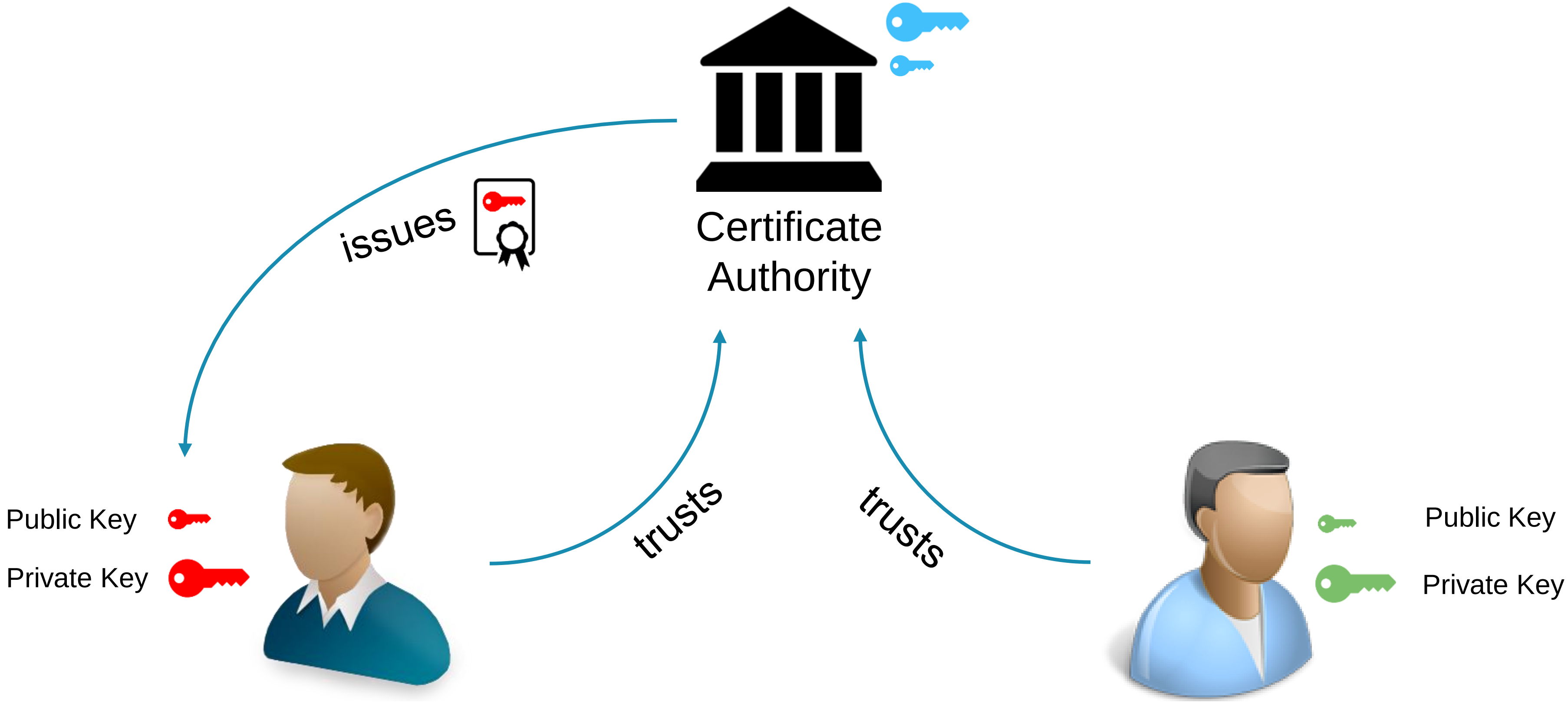
http://www.keylength.com/en/4/

Public-Key Cryptography

- Issue with Public-Key Cryptography

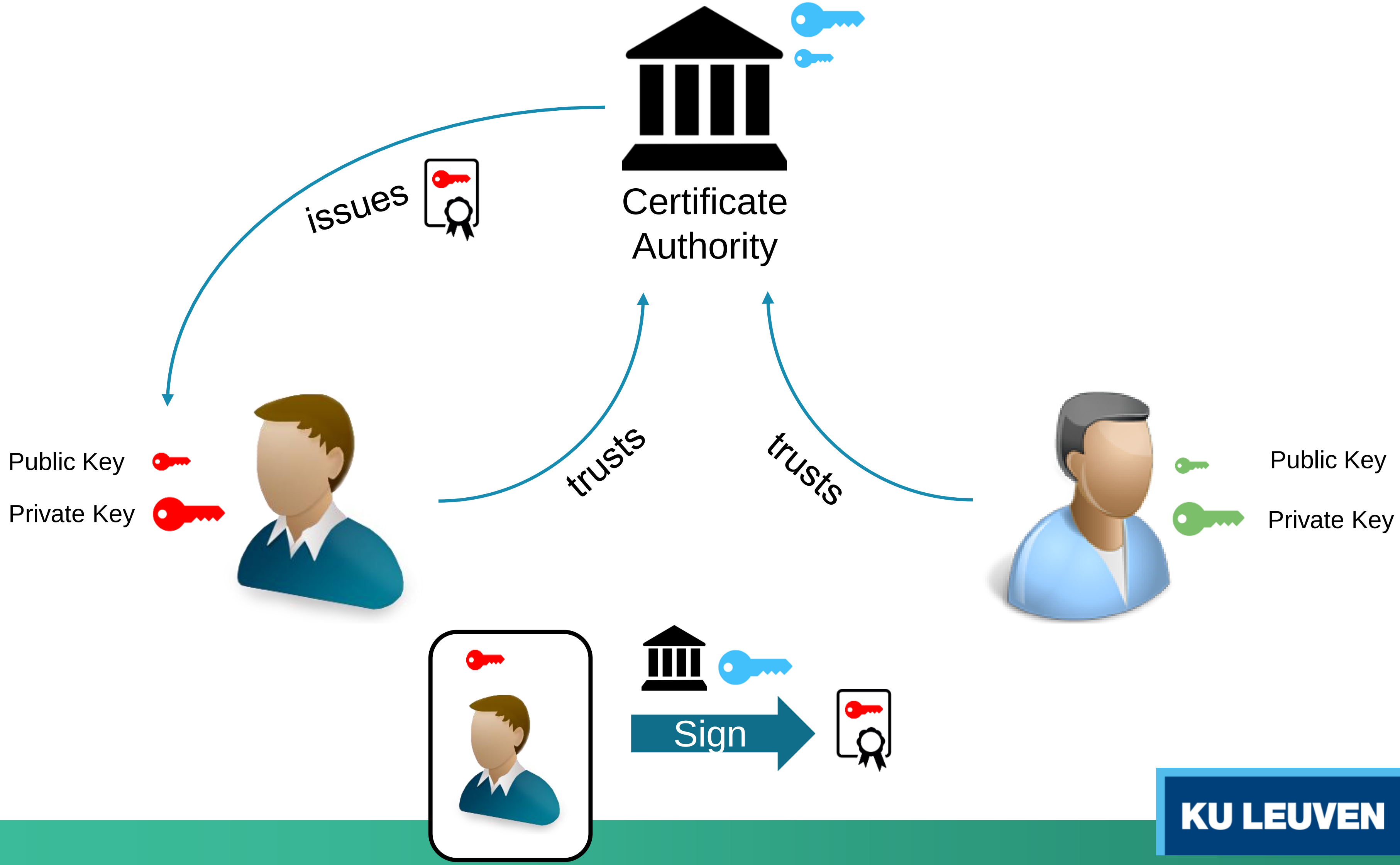
➔ Public-Key Infrastructure

Public Key Infrastructure

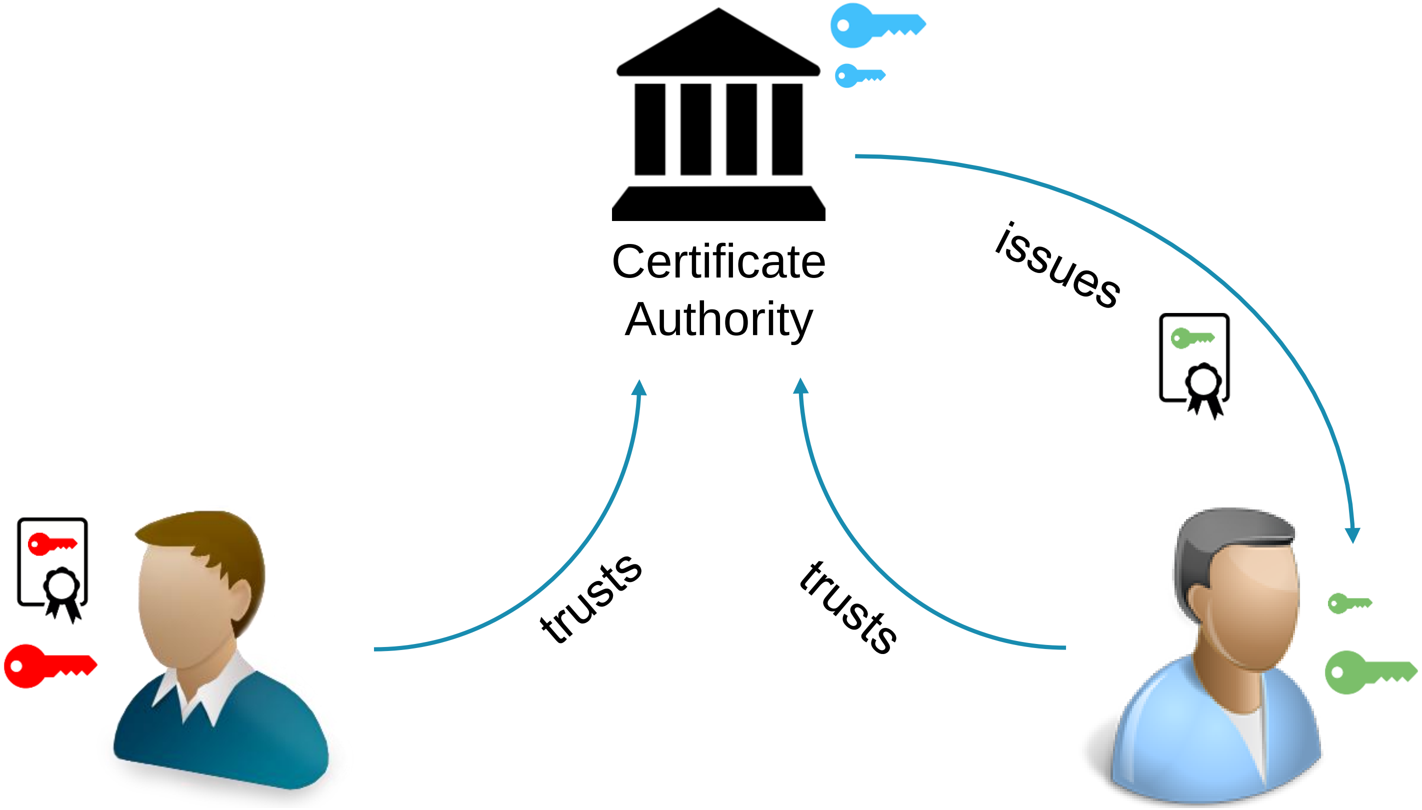


KU LEUVEN

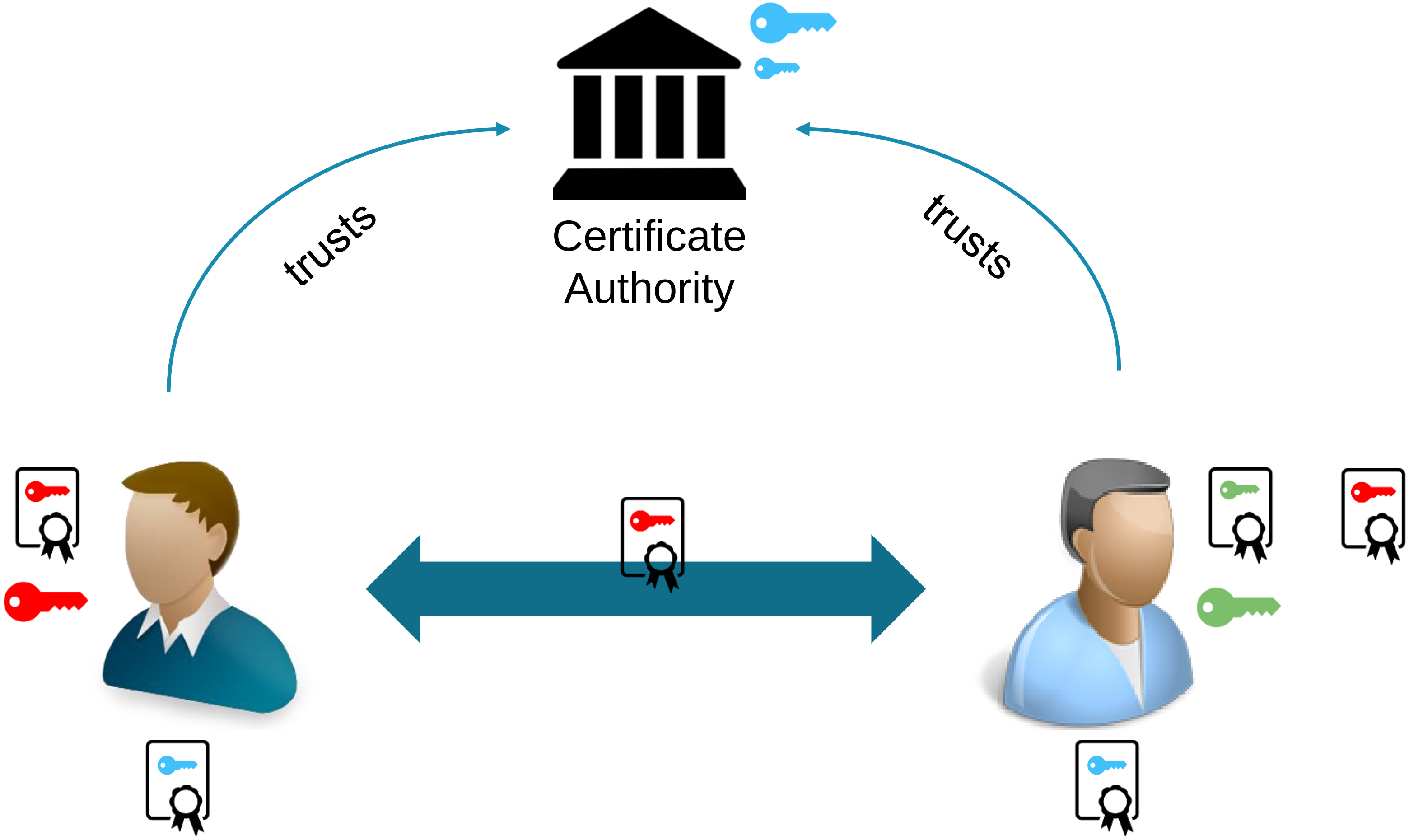
Public Key Infrastructure



Public Key Infrastructure



Public Key Infrastructure



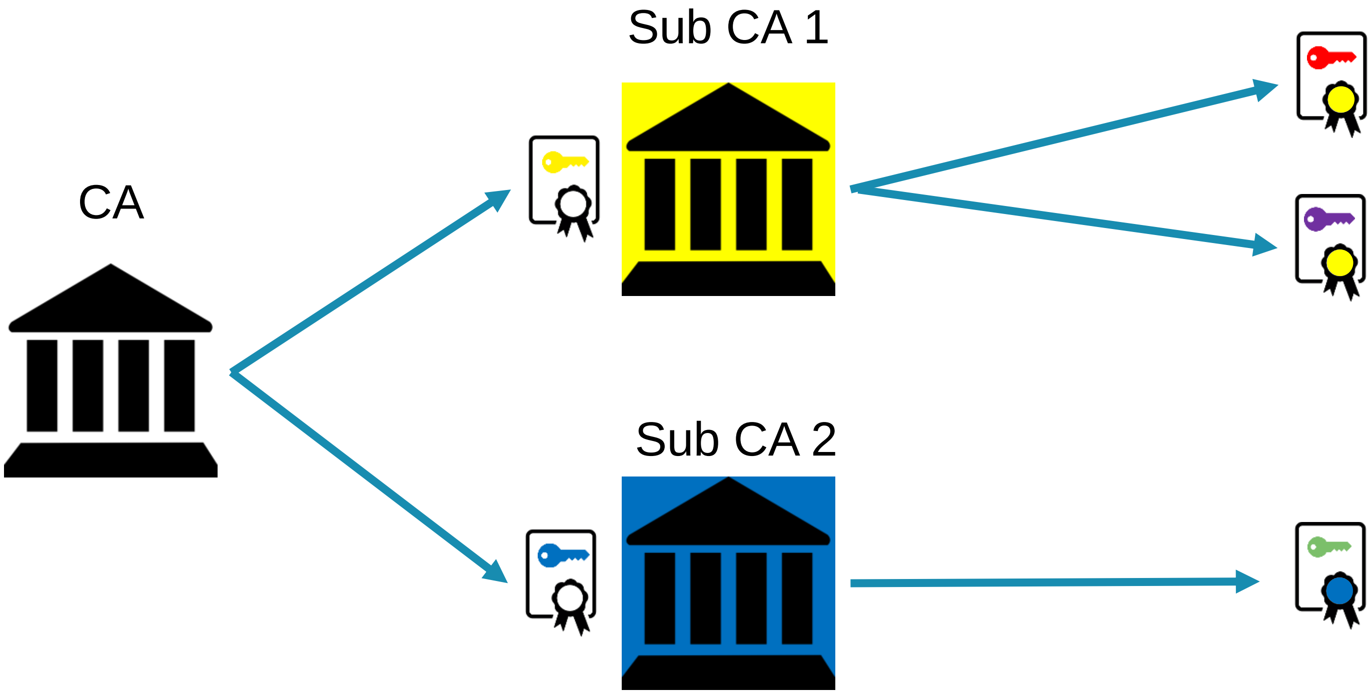
Public Key Certificates

A digital certificate is a digitally signed statement that binds a public key held by an entity to a set of information that identifies the holder of the corresponding key

X.509 Certificate
Version
Serial number
Algorithm ID
Issuer
Validity Not Before Not After
Subject
Subject Public Key Info Public Key Algorithm Subject Public Key
Extensions (Optional)
Certificate Signature Algorithm
Certificate Signature

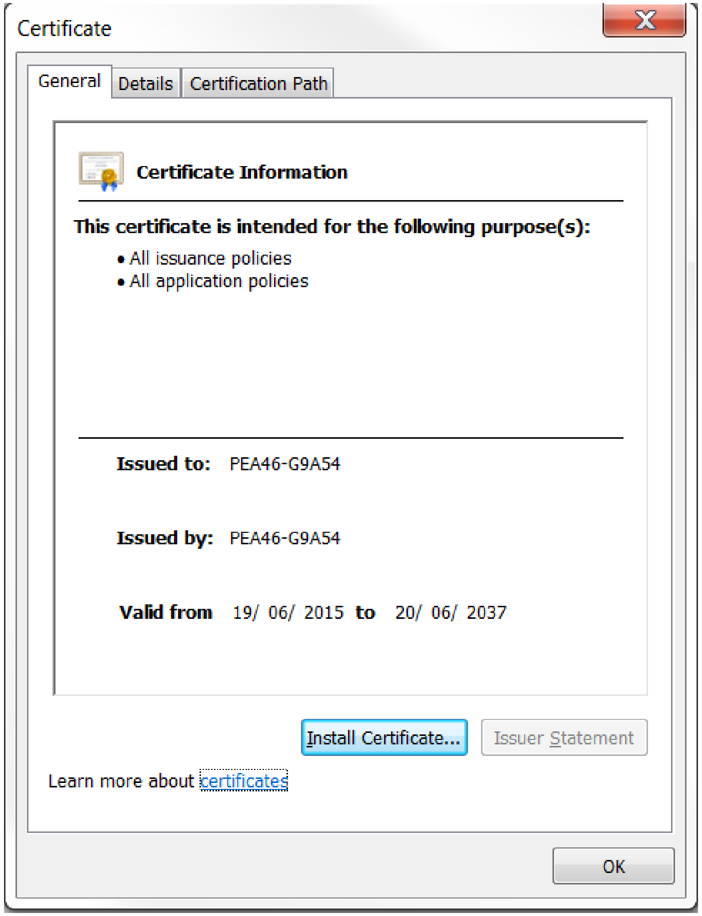
Public Key Certificates

- Certificate Chains



Public Key Certificates

- Certificate Creation
  - ○ Self-Signed Certificate
    - Subject = Issuer
    - Public Key = Issuer Public Key
    - Often used by certificate authorities
      ➔ Pre-installed certificates



Certificate

Certificate Information

This certificate is intended for the following purpose(s):

- All issuance policies
- All application policies

Issued to: PEA46-G9A54

Issued by: PEA46-G9A54

Valid from 19/ 06/ 2015 **to** 20/ 06/ 2037

Learn more about certificates

KU LEUVEN

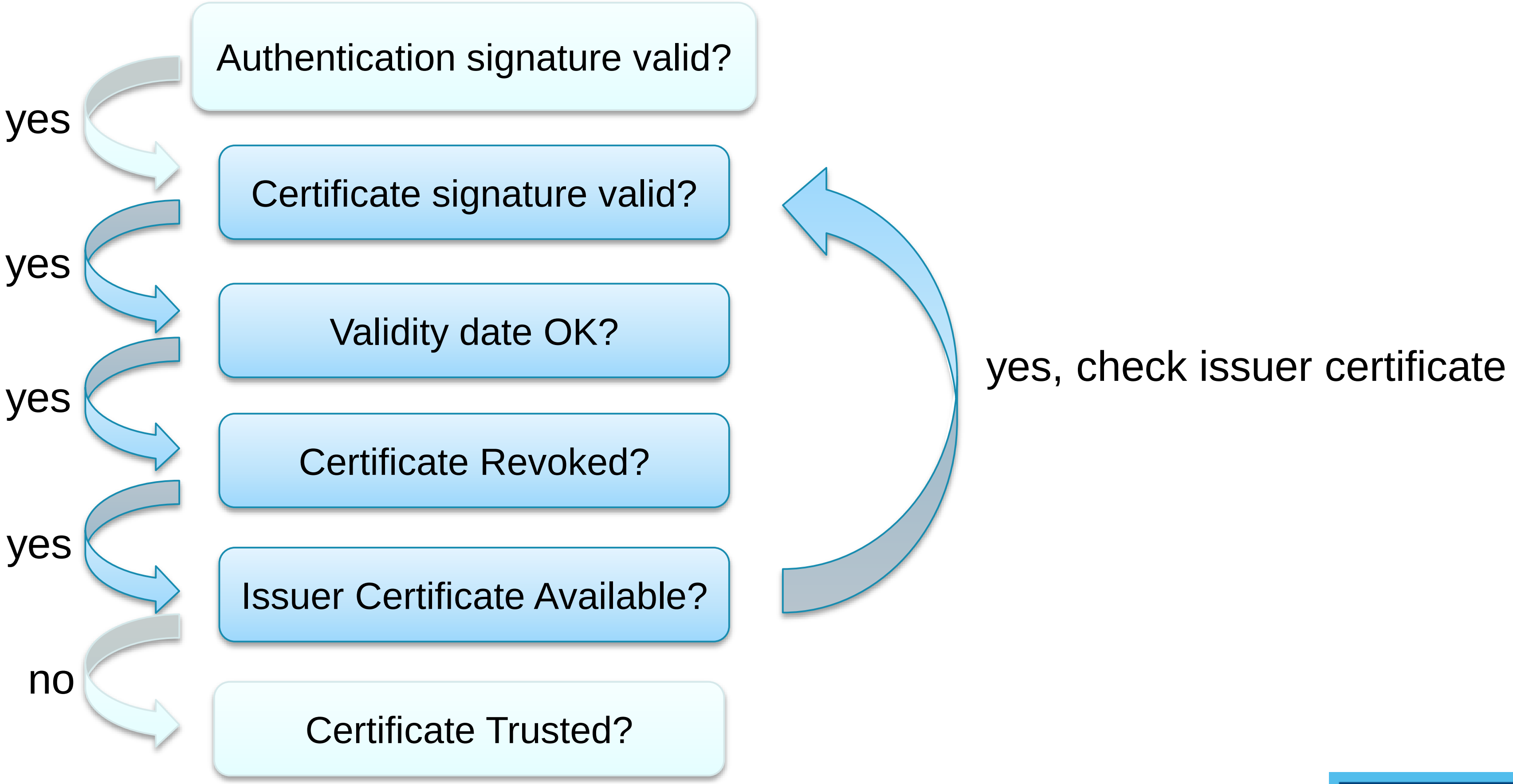
Public Key Certificates

- Certificate Revocation
  - Certificates expire after validity period

    ➔ What if certificate is compromised before it expired?
  - CAs publish Certificate Revocation List
    - Blacklist of certificate serial numbers
    - Short lifetime
    - Issued on regular periodic basis

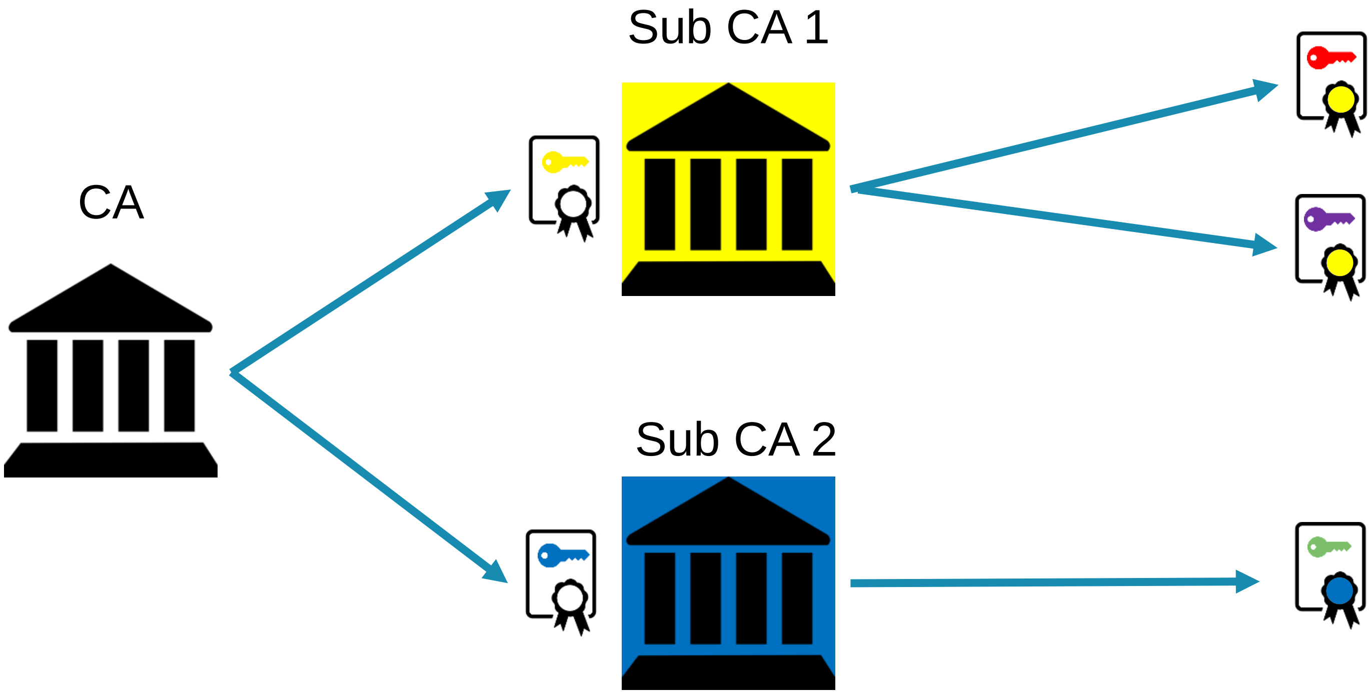
Public Key Certificates

- Certificate Validation


Authentication signature valid?
yes
Certificate signature valid?
yes
Validity date OK?
yes
Certificate Revoked?
yes
Issuer Certificate Available?
no
Certificate Trusted?
yes, check issuer certificate

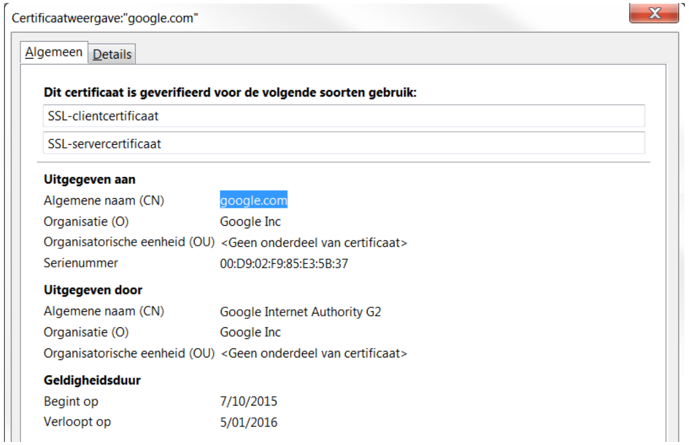
Public Key Certificates

- Certificate Validation



Public Key Certificates

- Certificate Validation



Certificaatweergave:"google.com"

Dit certificaat is geverifieerd voor de volgende soorten gebruik:

SSL-clientcertificaat

SSL-servercertificaat

Uitgegeven aan

Algemene naam (CN)	google.com
Organisatie (O)	Google Inc
Organisatorische eenheid (OU)	<Geen onderdeel van certificaat>
Serienummer	00:D9:02:F9:85:E3:5B:37

Uitgegeven door

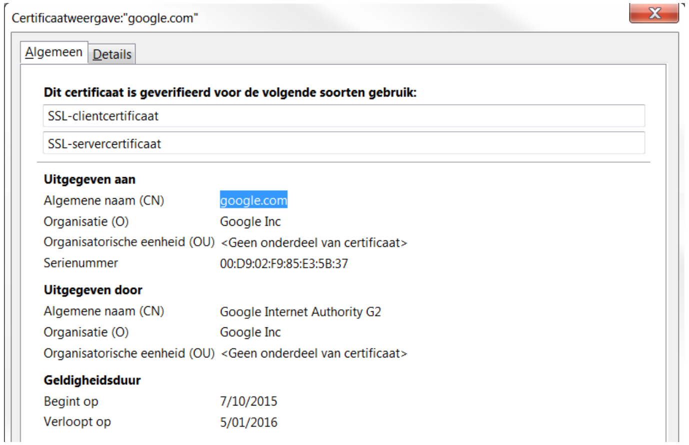
Algemene naam (CN)	Google Internet Authority G2
Organisatie (O)	Google Inc
Organisatorische eenheid (OU)	<Geen onderdeel van certificaat>

Geldigheidsduur

Begint op	7/10/2015
Verloopt op	5/01/2016

Public Key Certificates

- Certificate Validation



Certificaatweergave:"google.com"

Dit certificaat is geverifieerd voor de volgende soorten gebruik:

SSL-clientcertificaat

SSL-servercertificaat

Uitgegeven aan

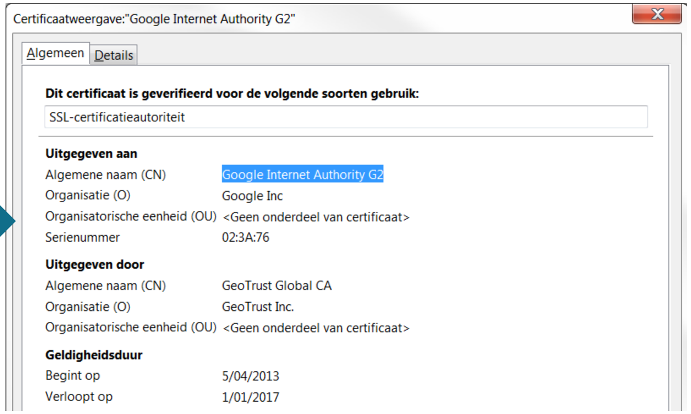
Algemene naam (CN)	google.com
Organisatie (O)	Google Inc
Organisatorische eenheid (OU)	<Geen onderdeel van certificaat>
Serienummer	00:D9:02:F9:85:E3:5B:37

Uitgegeven door

Algemene naam (CN)	Google Internet Authority G2
Organisatie (O)	Google Inc
Organisatorische eenheid (OU)	<Geen onderdeel van certificaat>

Geldigheidsduur

Begint op	7/10/2015
Verloopt op	5/01/2016



Certificaatweergave:"Google Internet Authority G2"

Dit certificaat is geverifieerd voor de volgende soorten gebruik:

SSL-certificatieautoriteit

Uitgegeven aan

Algemene naam (CN)	Google Internet Authority G2
Organisatie (O)	Google Inc
Organisatorische eenheid (OU)	<Geen onderdeel van certificaat>
Serienummer	02:3A:76

Uitgegeven door

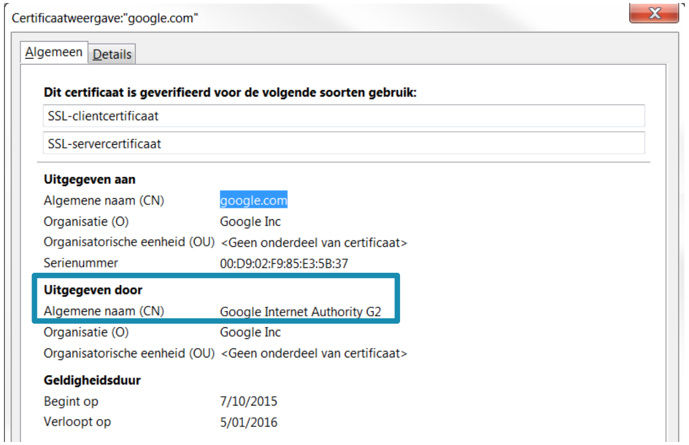
Algemene naam (CN)	GeoTrust Global CA
Organisatie (O)	GeoTrust Inc.
Organisatorische eenheid (OU)	<Geen onderdeel van certificaat>

Geldigheidsduur

Begint op	5/04/2013
Verloopt op	1/01/2017

Public Key Certificates

- Certificate Validation



Certificaatweergave:"google.com"

Dit certificaat is geverifieerd voor de volgende soorten gebruik:

SSL-clientcertificaat

SSL-servercertificaat

Uitgegeven aan

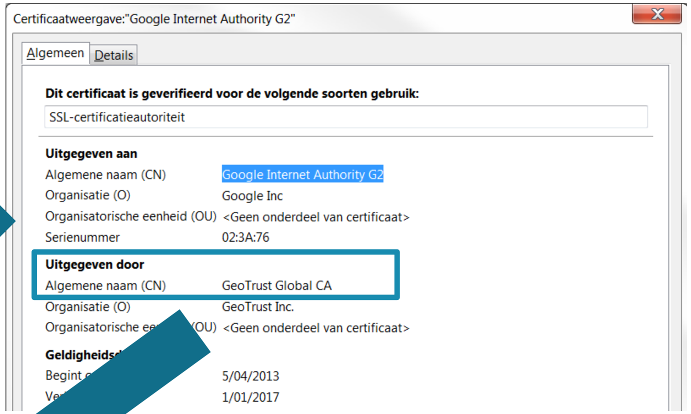
Algemene naam (CN)	google.com
Organisatie (O)	Google Inc
Organisatorische eenheid (OU)	<Geen onderdeel van certificaat>
Serienummer	00:D9:02:F9:85:E3:5B:37

Uitgegeven door

Algemene naam (CN)	Google Internet Authority G2
Organisatie (O)	Google Inc
Organisatorische eenheid (OU)	<Geen onderdeel van certificaat>

Geldigheidsduur

Begint op	7/10/2015
Verloopt op	5/01/2016



Certificaatweergave:"Google Internet Authority G2"

Dit certificaat is geverifieerd voor de volgende soorten gebruik:

SSL-certificatieautoriteit

Uitgegeven aan

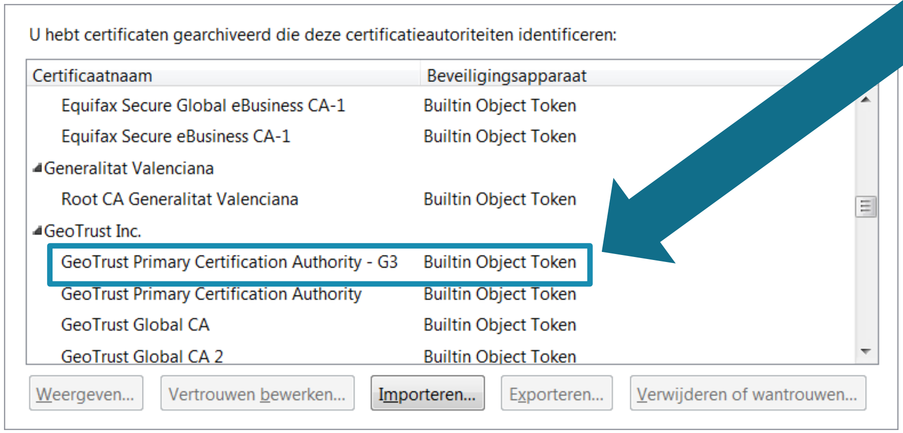
Algemene naam (CN)	Google Internet Authority G2
Organisatie (O)	Google Inc
Organisatorische eenheid (OU)	<Geen onderdeel van certificaat>
Serienummer	02:3A:76

Uitgegeven door

Algemene naam (CN)	GeoTrust Global CA
Organisatie (O)	GeoTrust Inc.
Organisatorische ee (OU)	<Geen onderdeel van certificaat>

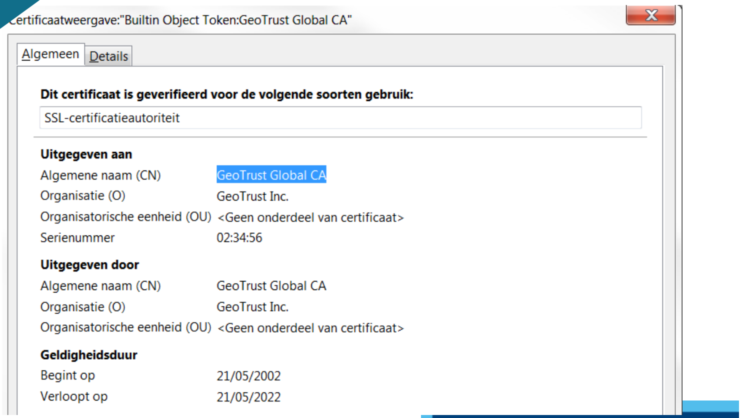
Geldigheids

Begint o	5/04/2013
Ve	1/01/2017



U hebt certificaten gearchiveerd die deze certificatieautoriteiten identificeren:

Certificaatnaam	Beveiligingsapparaat
Equifax Secure Global eBusiness CA-1	Builtin Object Token
Equifax Secure eBusiness CA-1	Builtin Object Token
◢Generalitat Valenciana	
Root CA Generalitat Valenciana	Builtin Object Token
◢GeoTrust Inc.	
GeoTrust Primary Certification Authority - G3	Builtin Object Token
GeoTrust Primary Certification Authority	Builtin Object Token
GeoTrust Global CA	Builtin Object Token
GeoTrust Global CA 2	Builtin Object Token



Certificaatweergave:"Builtin Object Token:GeoTrust Global CA"

Dit certificaat is geverifieerd voor de volgende soorten gebruik:

SSL-certificatieautoriteit

Uitgegeven aan

Algemene naam (CN)	GeoTrust Global CA
Organisatie (O)	GeoTrust Inc.
Organisatorische eenheid (OU)	<Geen onderdeel van certificaat>
Serienummer	02:34:56

Uitgegeven door

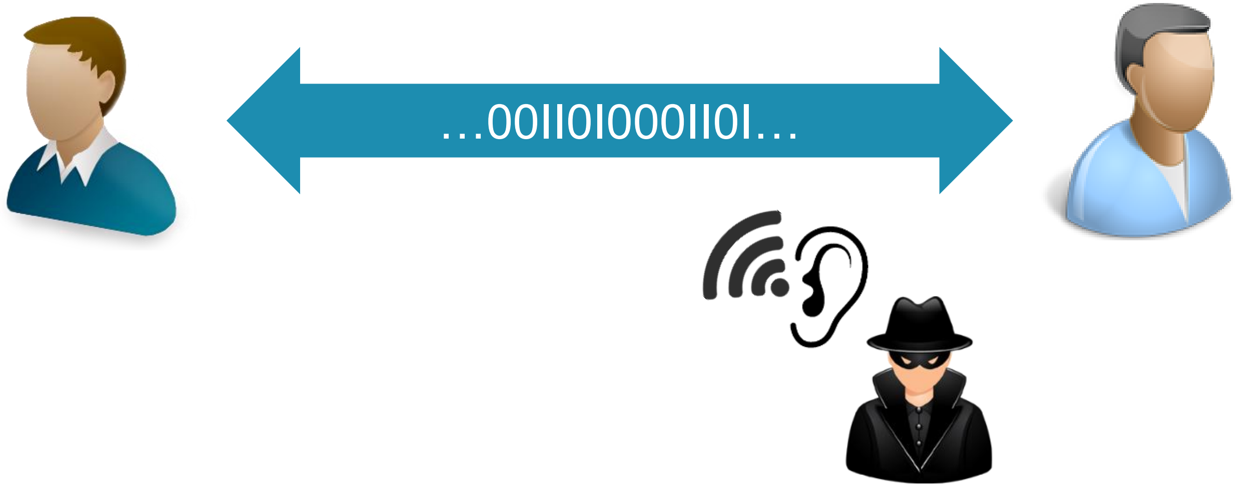
Algemene naam (CN)	GeoTrust Global CA
Organisatie (O)	GeoTrust Inc.
Organisatorische eenheid (OU)	<Geen onderdeel van certificaat>

Geldigheidsduur

Begint op	21/05/2002
Verloopt op	21/05/2022

Realizing Secure Communication

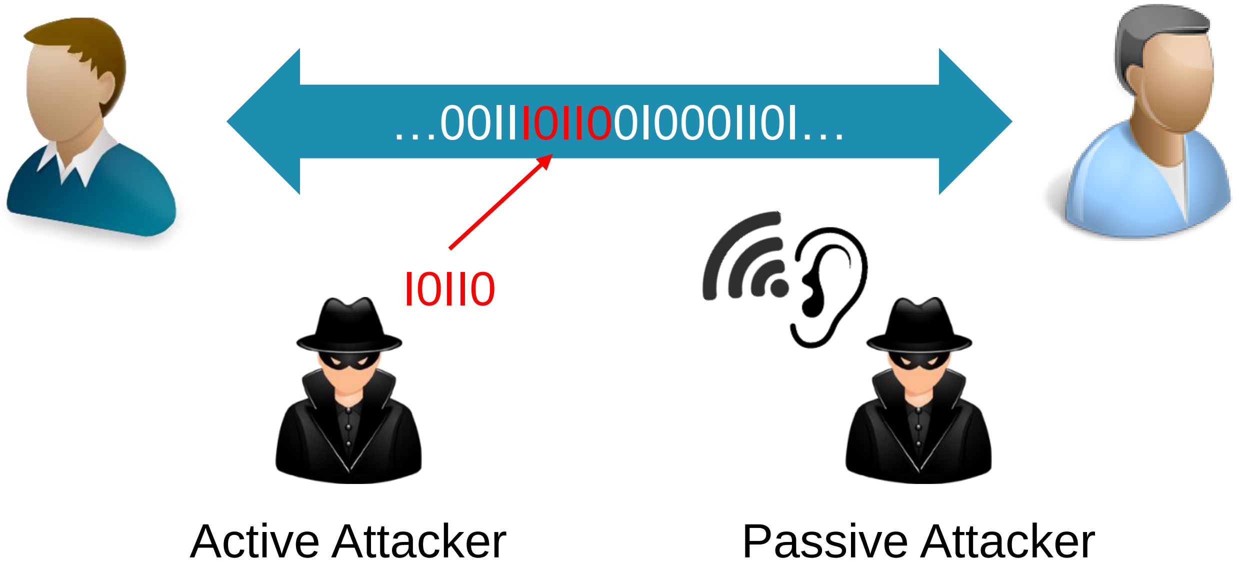
Secure Communication Properties



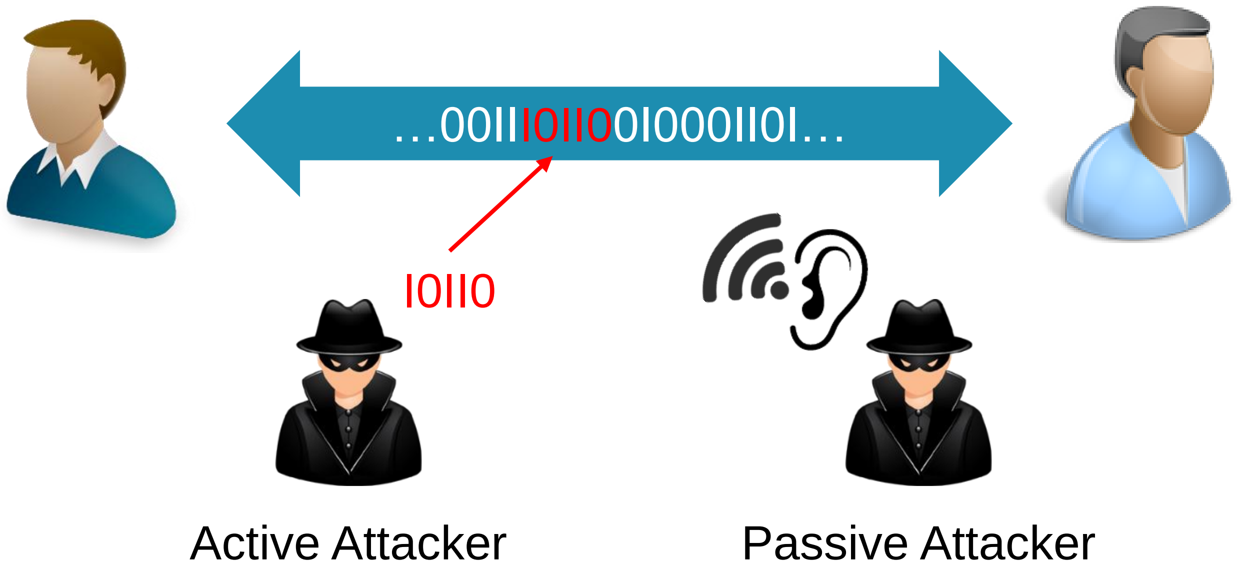
…00II0I000II0I…

Passive Attacker

Secure Communication Properties

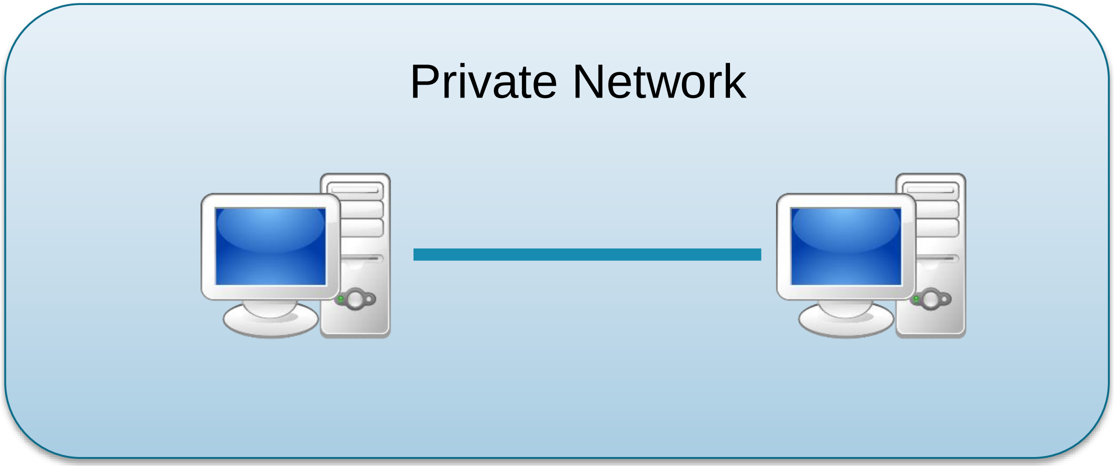


Secure Communication Properties



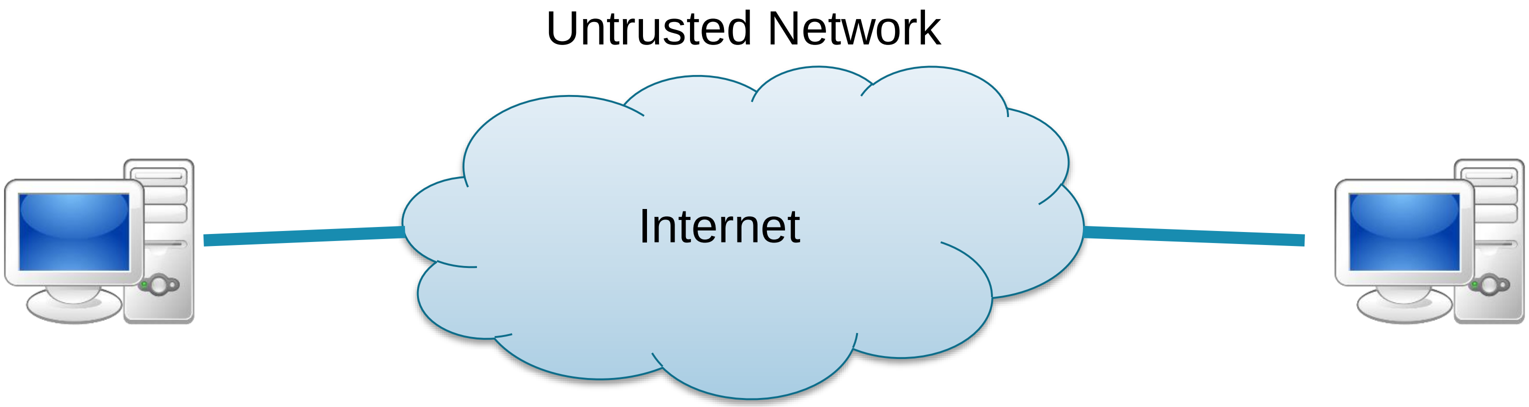
- Desired security properties
  - Message confidentiality
  - Message authentication

Secure Communication Properties



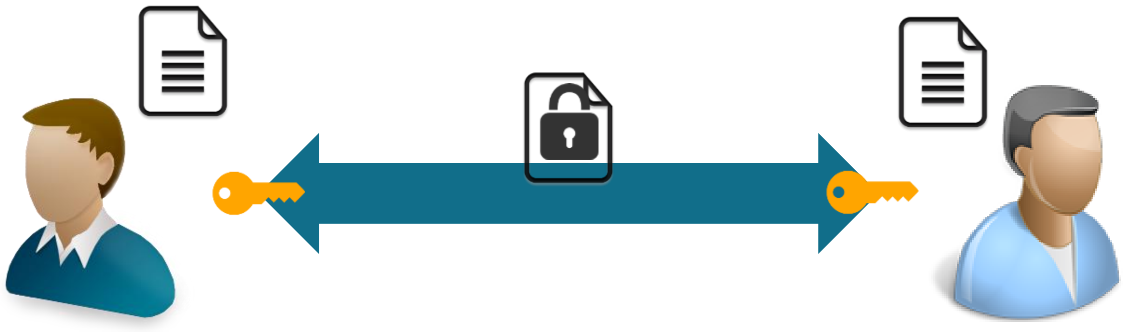
- Message Confidentiality ✓
- Message Authentication ✓

Secure Communication Properties

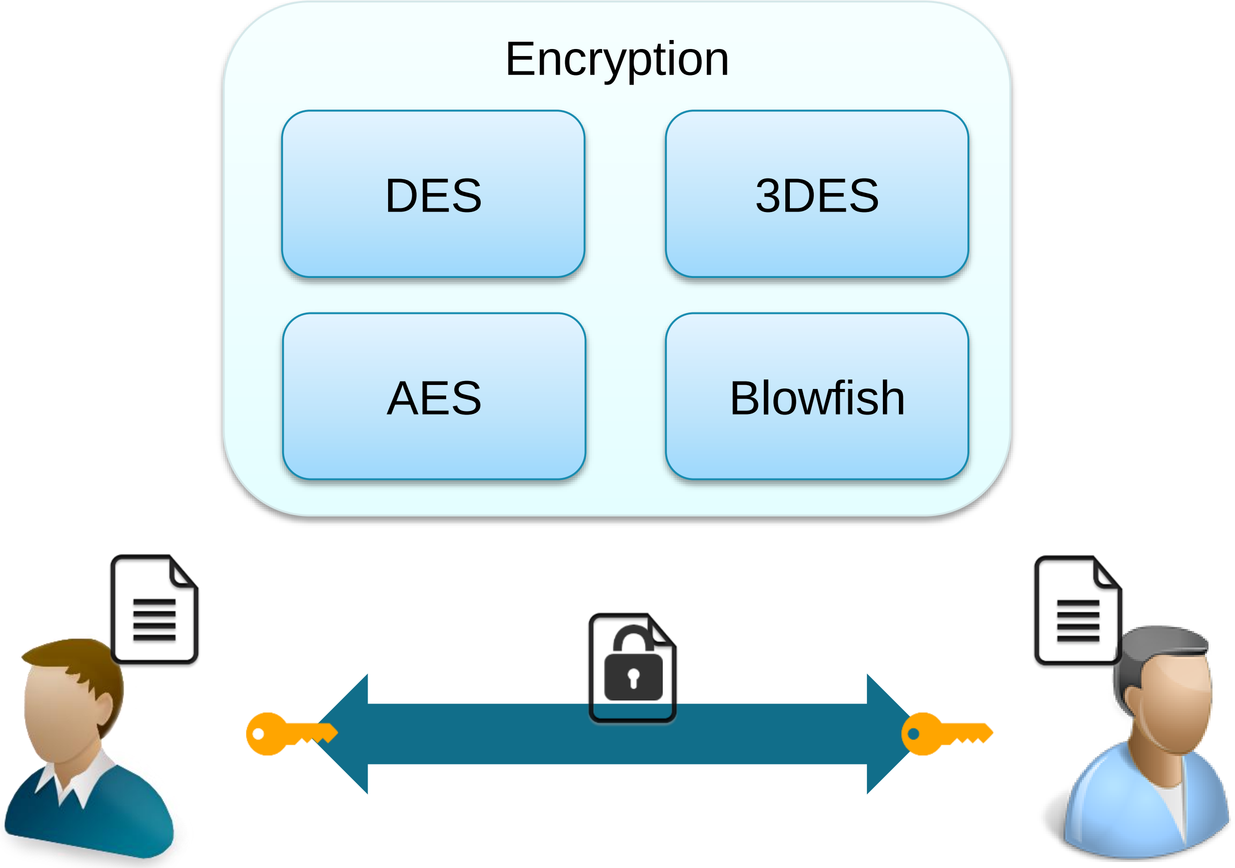


- Message Confidentiality ✗
- Message Authentication ✗

Message Confidentiality



Message Confidentiality



Encryption

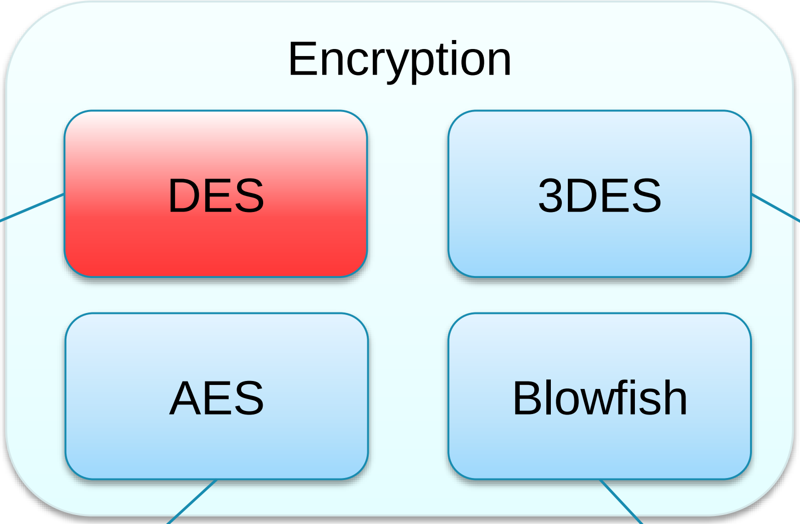
DES

3DES

AES

Blowfish

Message Confidentiality



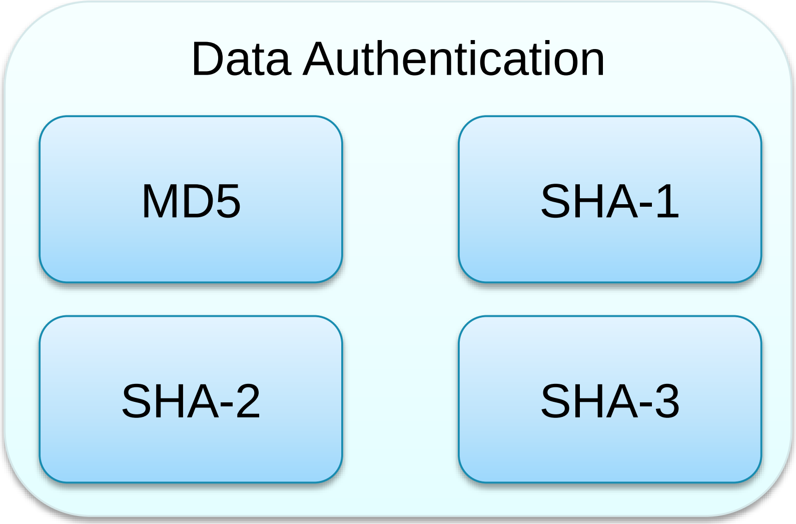
- Old standard
- Not secure due to key size of 56 bits
- Efficient hardware

- Cascades 3 instances of DES
- Secure with key size of 112 bit
- Efficient hardware

- Current standard
- Secure with key sizes of 128, 192 or 256 bits
- Efficient hardware and software

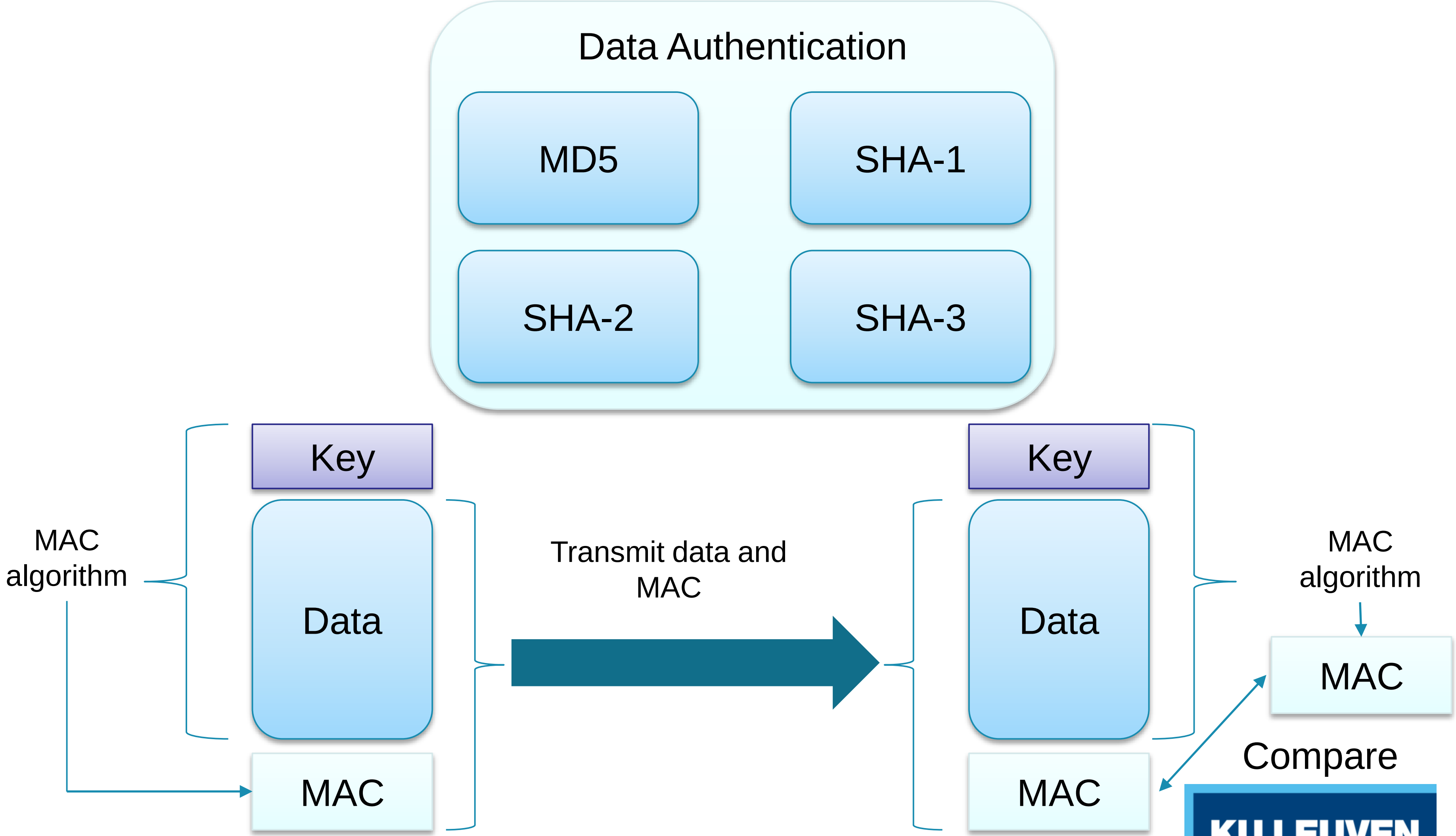
- Key sizes variable between 32 and 448 bits
- Efficient software

Message Authentication

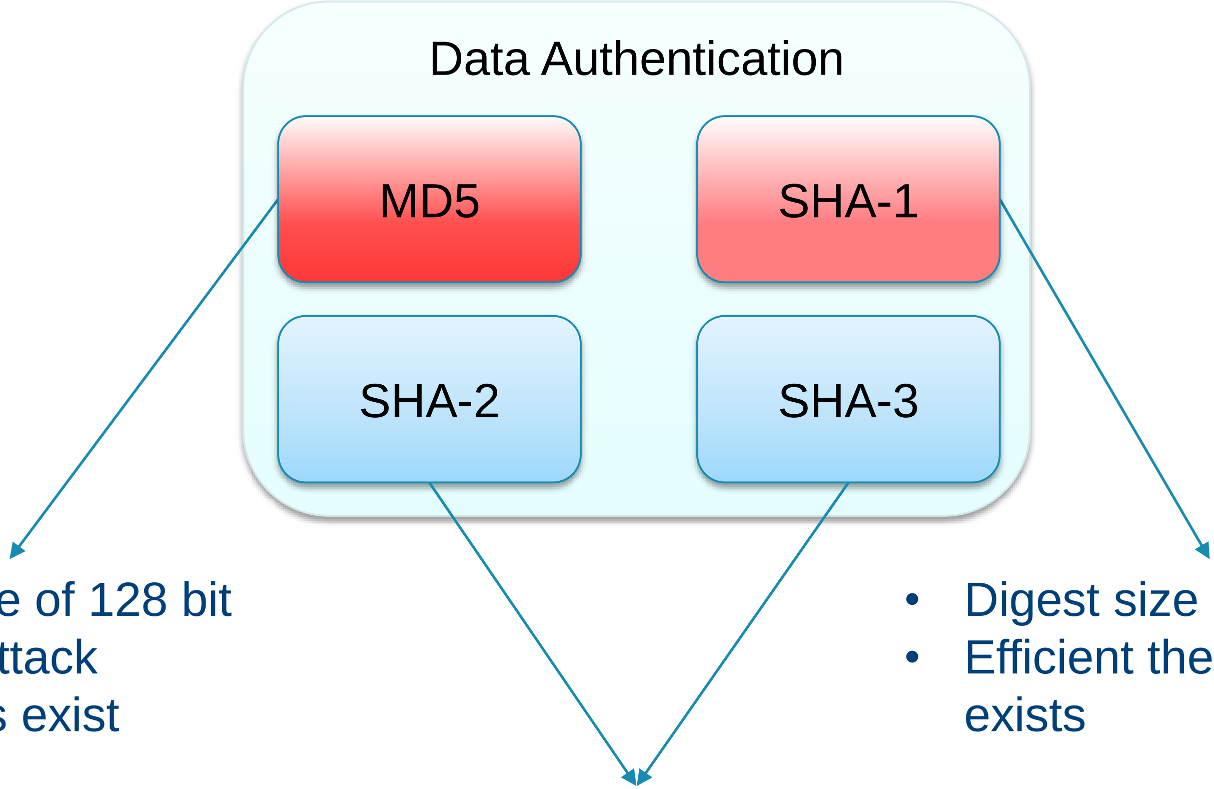


- Hash function that maps data of arbitrary size to fixed size
- Practically impossible to invert
- Used to assure integrity and to provide authenticity

Message Authentication



Message Authentication



- Digest size of 128 bit
- Efficient attack algorithms exist

- Digest size of 160 bit
- Efficient theoretical attack exists

- Digest size of 224, 256, 384, 512bit
- Secure
- Not often implemented

Session Key Establishment

- Secure communication between two parties
  - Symmetric cryptography
    - ➔ Session key?

Session Key Establishment

- Goal:
  - Set up a shared secret in a dynamic on-demand manner

- Properties:
  - Both parties learn the value of the session key
  - No other parties know the value of the session key
  - Unilateral or mutal authentication
  - Both parties are ensured the key is freshly generated

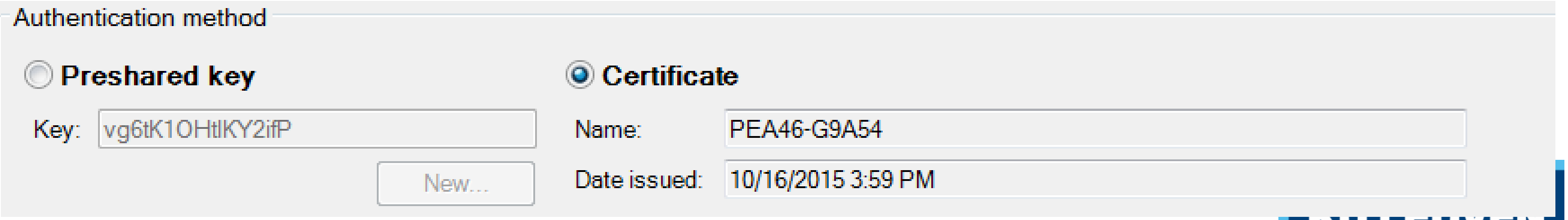
Session Key Establishment

- Possible solutions:
  - Pre-shared keys (PSK)

    "A pre-shared key is a shared secret which was previously shared between the two parties using some secure channel before it needs to be used"

  - Public-key infrastructure (PKI)

    "A PKI is an arrangement that binds public keys with respective user identities by means of a certificate"



Authentication method

○ **Preshared key**

Key: vg6tK1OHtlKY2ifP

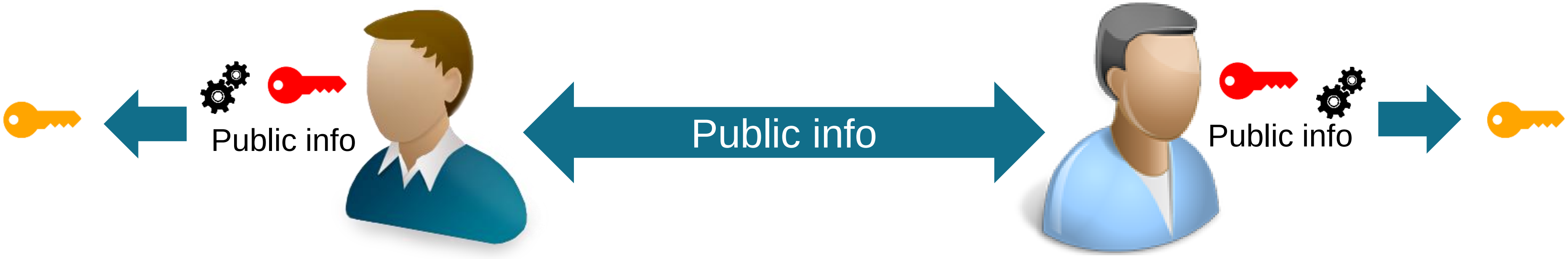
● **Certificate**

Name: PEA46-G9A54

Date issued: 10/16/2015 3:59 PM

Session Key Establishment

- Pre-shared Key



“A pre-shared key is a shared secret which was previously shared between the two parties using some secure channel before it needs to be used”

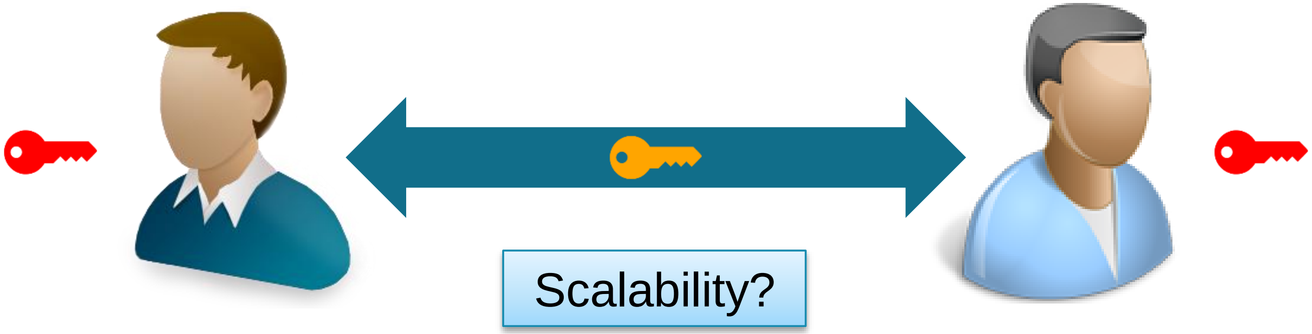
Session Key Establishment

- Pre-shared Key
  - 🔑 required to generate 🔑
  - Both parties know the identity of the other party that holds 🔑

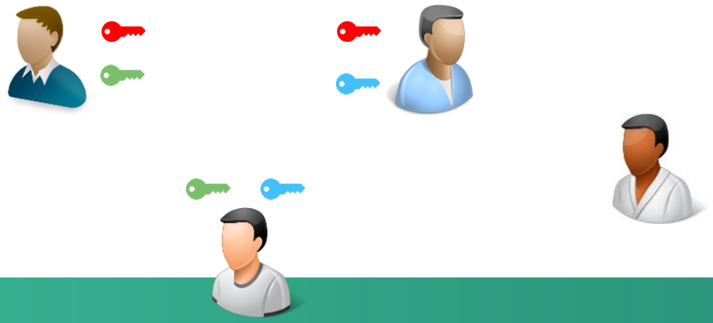
“A pre-shared key is a shared secret which was previously shared between the two parties using some secure channel before it needs to be used”

Session Key Establishment

- Pre-shared Key
  - 🔑 required to generate 🔑
  - Both parties know the identity of the other party that holds 🔑



Scalability?



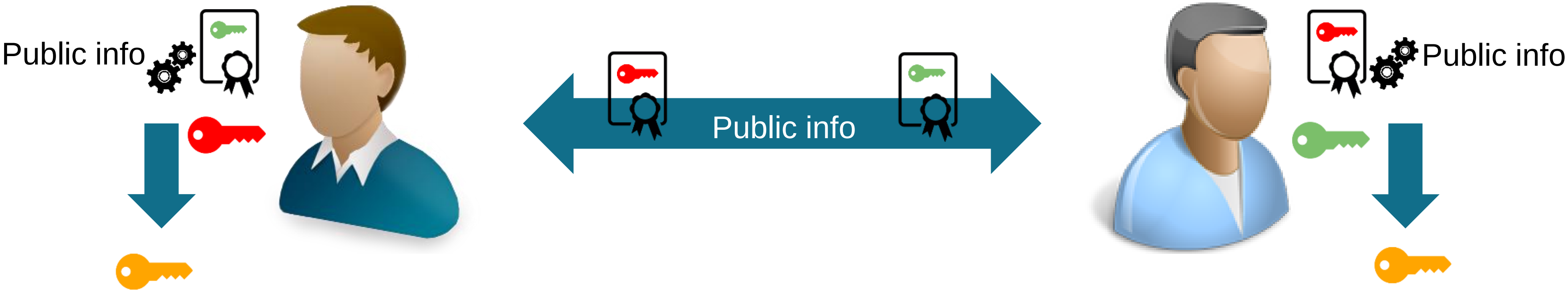
Session Key Establishment

- Pre-shared Key
- Public Key Infrastructure

> "A PKI is an arrangement that binds public keys with respective user identities by means of a certificate"

Session Key Establishment

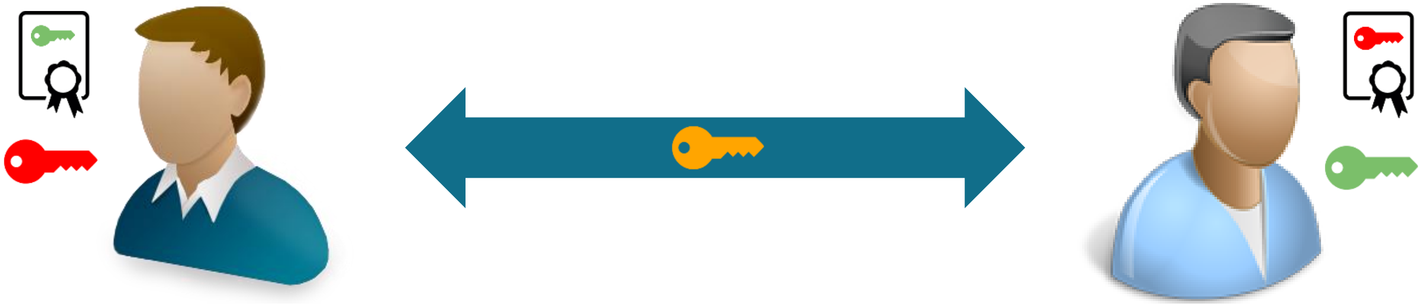
- Pre-shared Key
- Public Key Infrastructure



“A PKI is an arrangement that binds public keys with respective user identities by means of a certificate”

Session Key Establishment

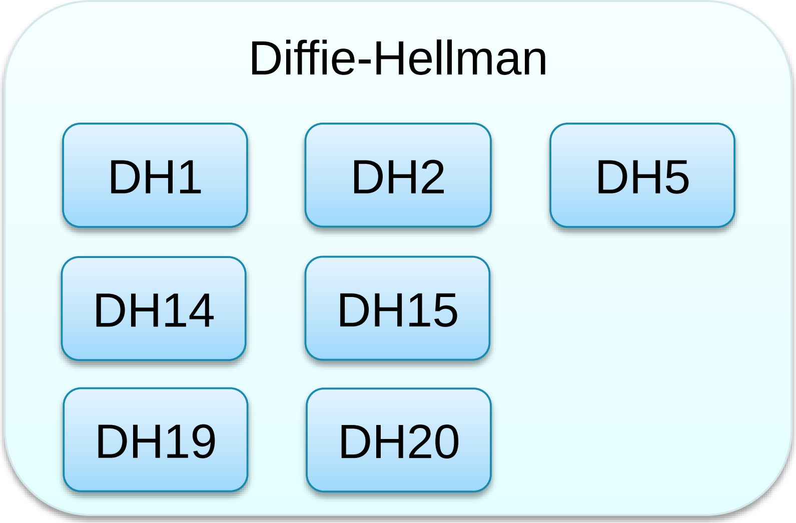
- Pre-shared Key
- Public Key Infrastructure
  - 🔑 can only be generated if possession of 🔑 or 🔑
  - Identity of owners of 🔑 and 🔑 is certified in 📜 📜



> “A PKI is an arrangement that binds public keys with respective user identities by means of a certificate”

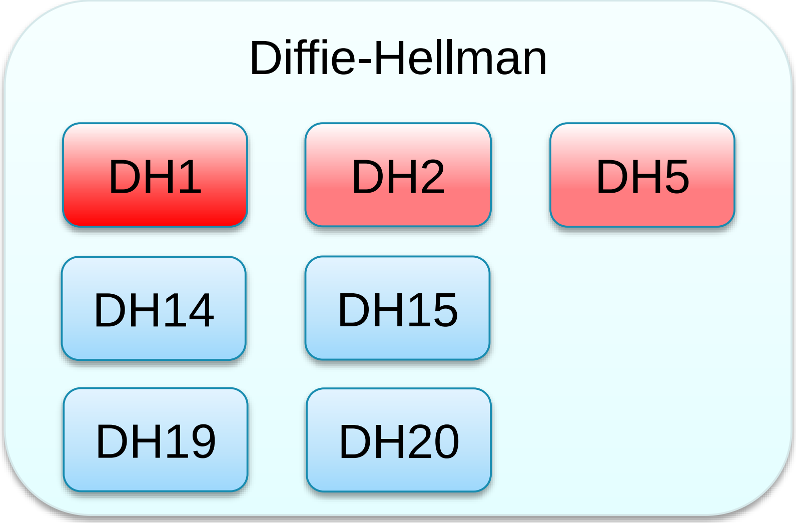
Session Key Establishment

- Pre-shared Key
- Public Key Infrastructure



Session Key Establishment

- Pre-shared Key
- Public Key Infrastructure



Diffie-Hellman

DH1 DH2 DH5

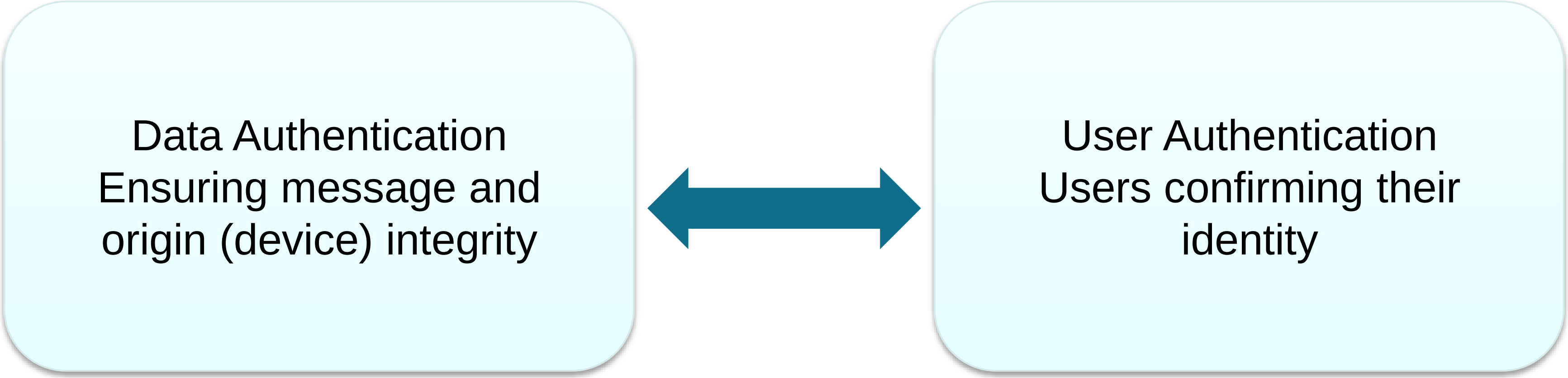
DH14 DH15

DH19 DH20

  - DH group
    - Key size
    - Session key establishment algorithm (RSA/ECC based)
  - Higher groups are more secure
  - Lower groups are faster

User Authentication

User Authentication



Data Authentication
Ensuring message and origin (device) integrity

User Authentication
Users confirming their identity

- Certificates
- Preshared Key
- Data authentication algorithms

- Username/password
- PIN codes
- Biometric scans

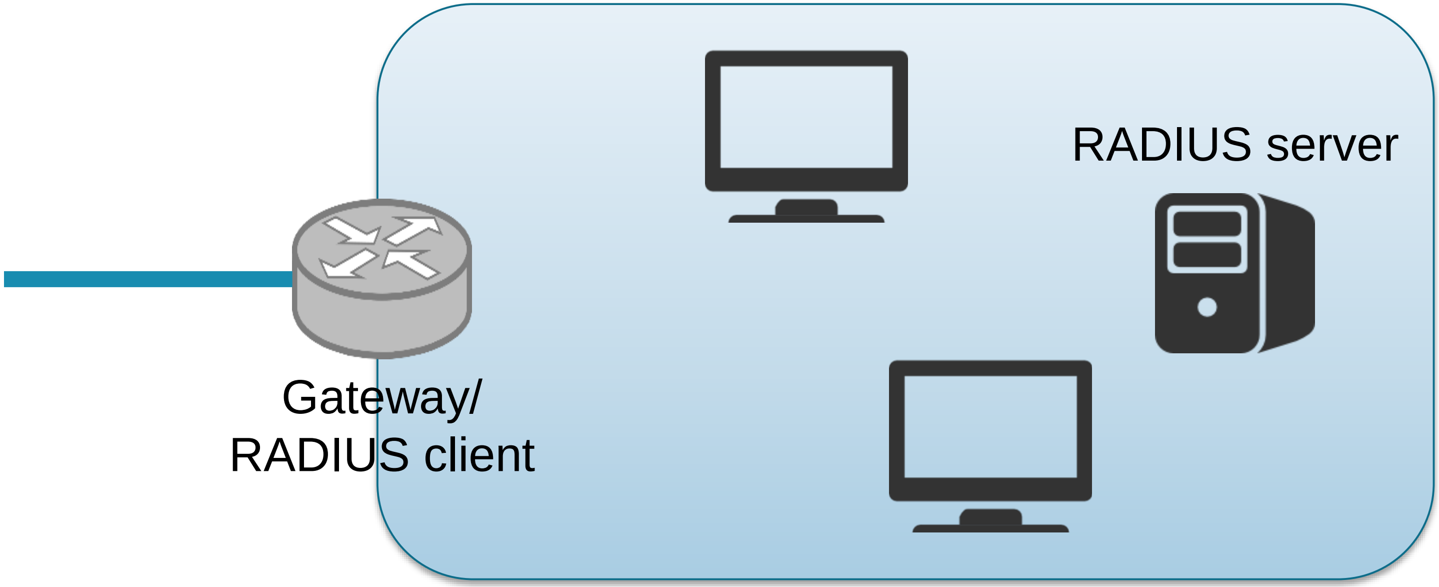
User Authentication

- Where to handle user authentication?
  - On-device
  - Authentication Server

- Advantages of Authentication Server
  - Centralized user administration
  - Comfort
  - Scalability

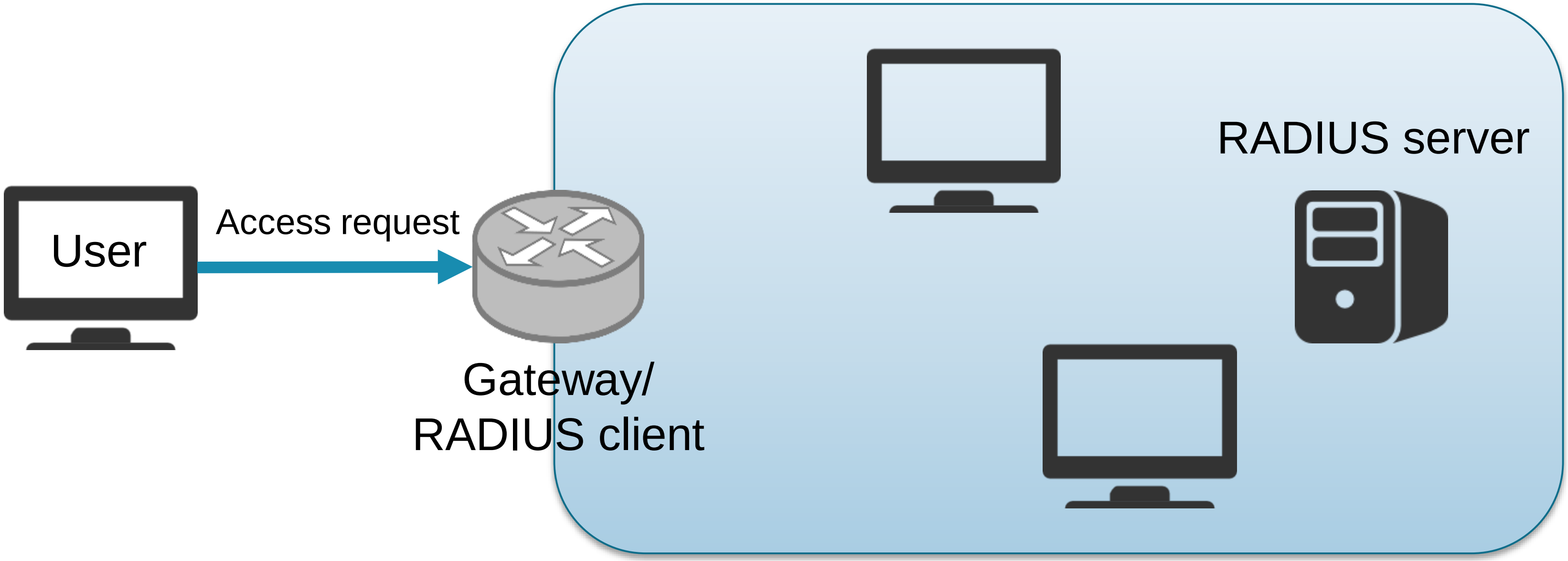
RADIUS

- Authentication, Authorization and Accounting protocol
- Client/server protocol



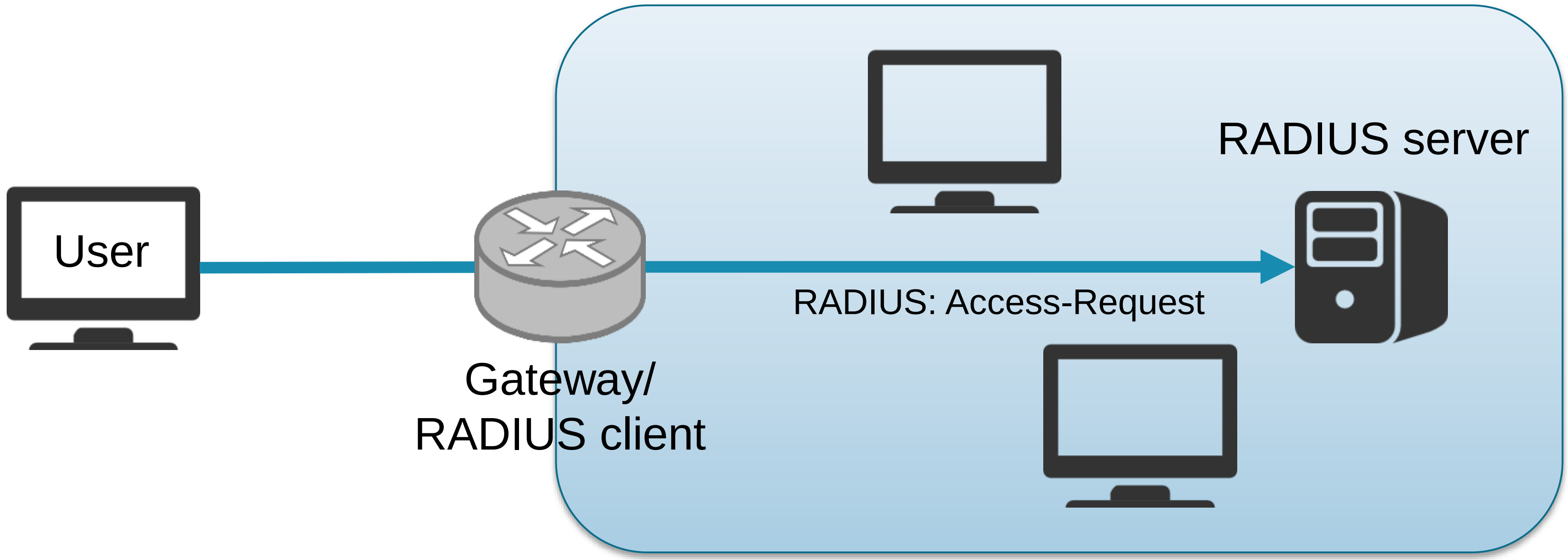
RADIUS

- Authentication and Authorization



RADIUS

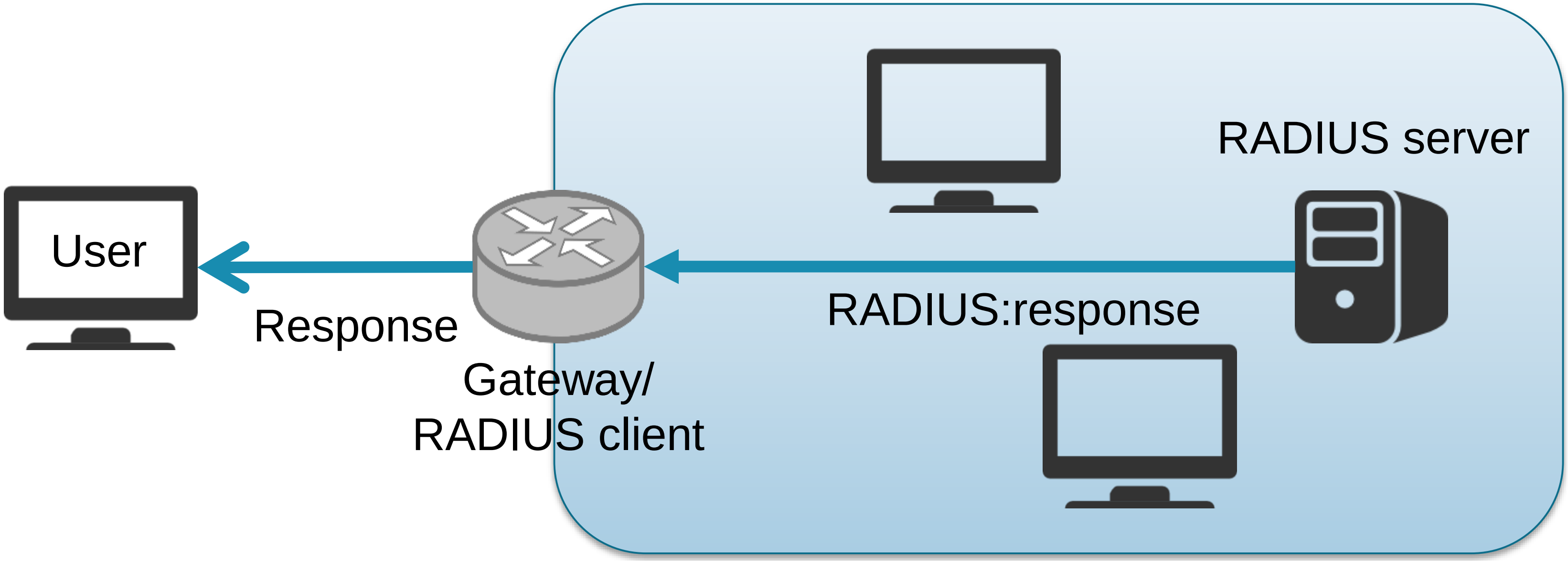
- Authentication and Authorization



- RADIUS:Access-Request includes:
  - User information (eg: Name)
  - User credentials (Password, certificate, …)
    Encrypted with shared secret

RADIUS

- Authentication and Authorization



- Possible responses
  - Access Reject
  - Access Challenge
  - Access Accept

RADIUS

- Open source RADIUS servers

FreeRADIUS

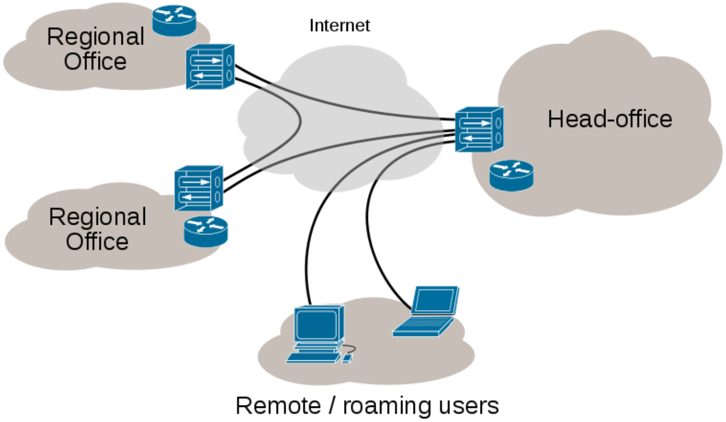
The world's most popular RADIUS Server

NPS Server

Virtual Private Network

Virtual Private Network

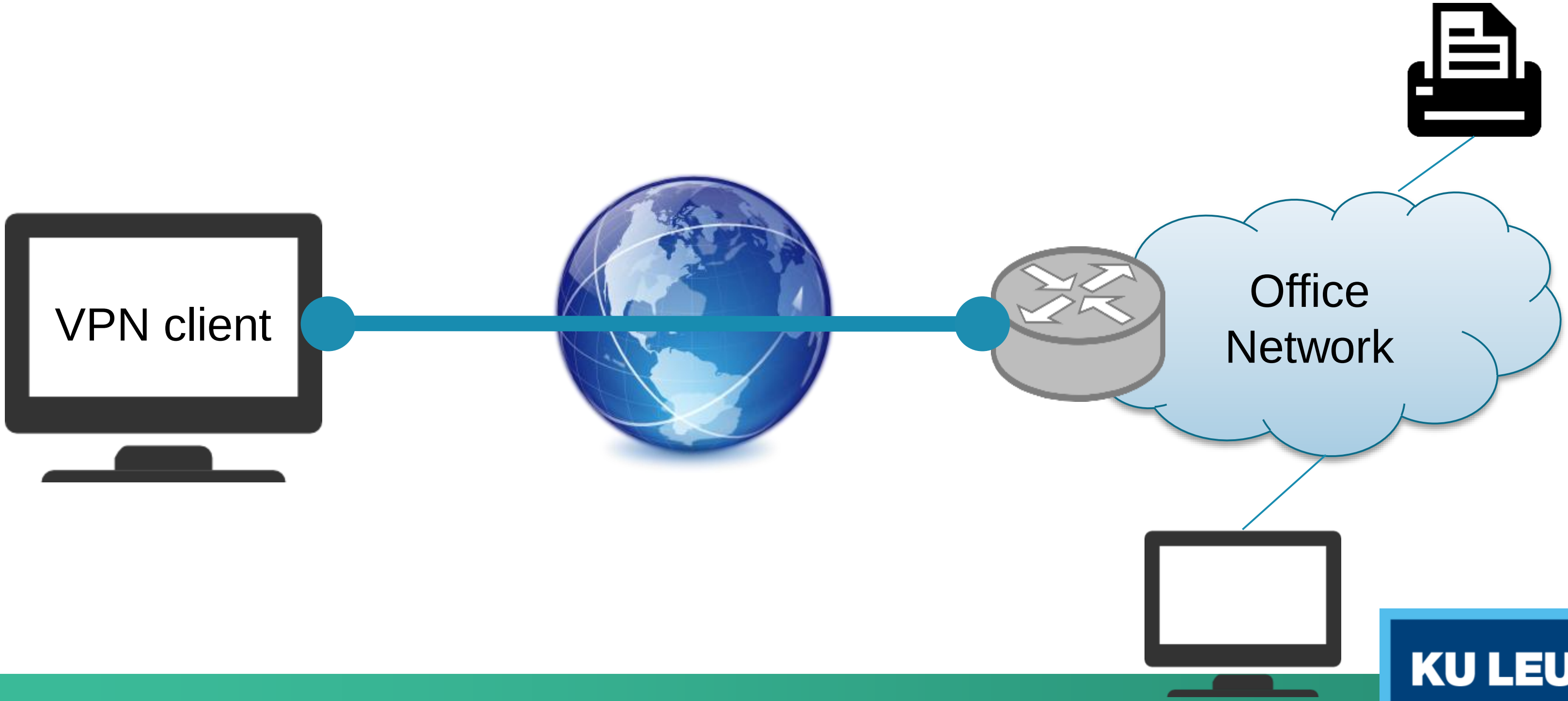
- Extends a private network across a public network (e.g. the Internet)



- Allows a user to access remote network resources as if they were within the private network

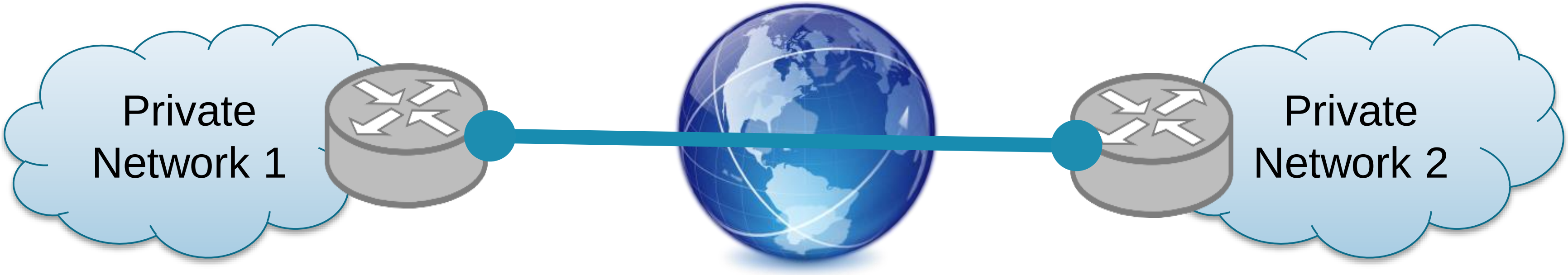
Virtual Private Network

- Two setups
  - Remote Access
    - Remote access to resources in a private network over the Internet



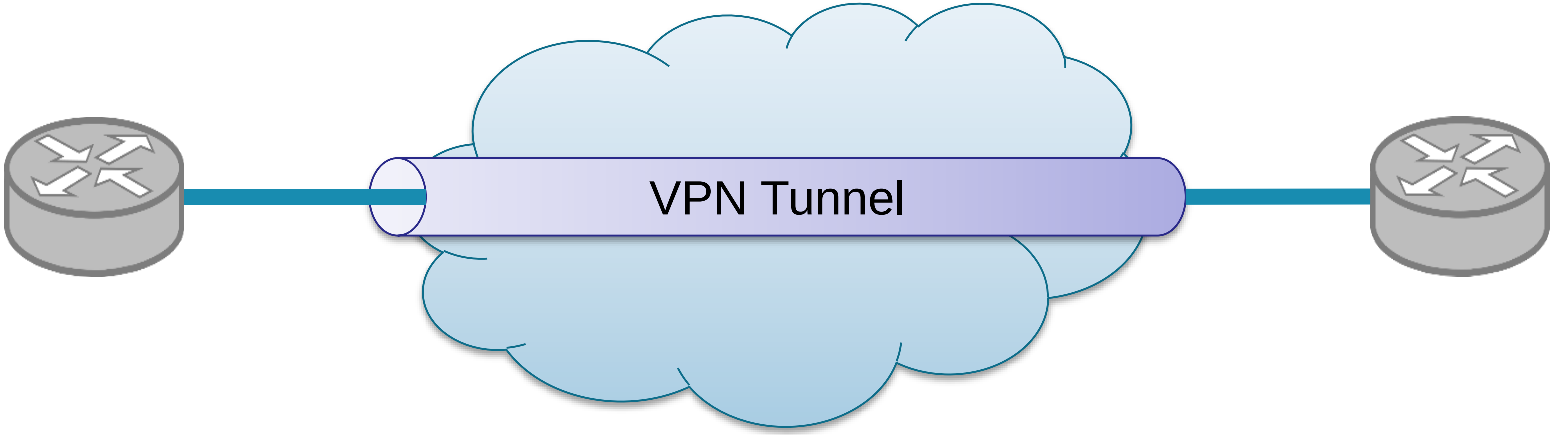
Virtual Private Network

- Two setups
  - Remote Access
  - Site-to-Site
    - Connecting two networks over the Internet



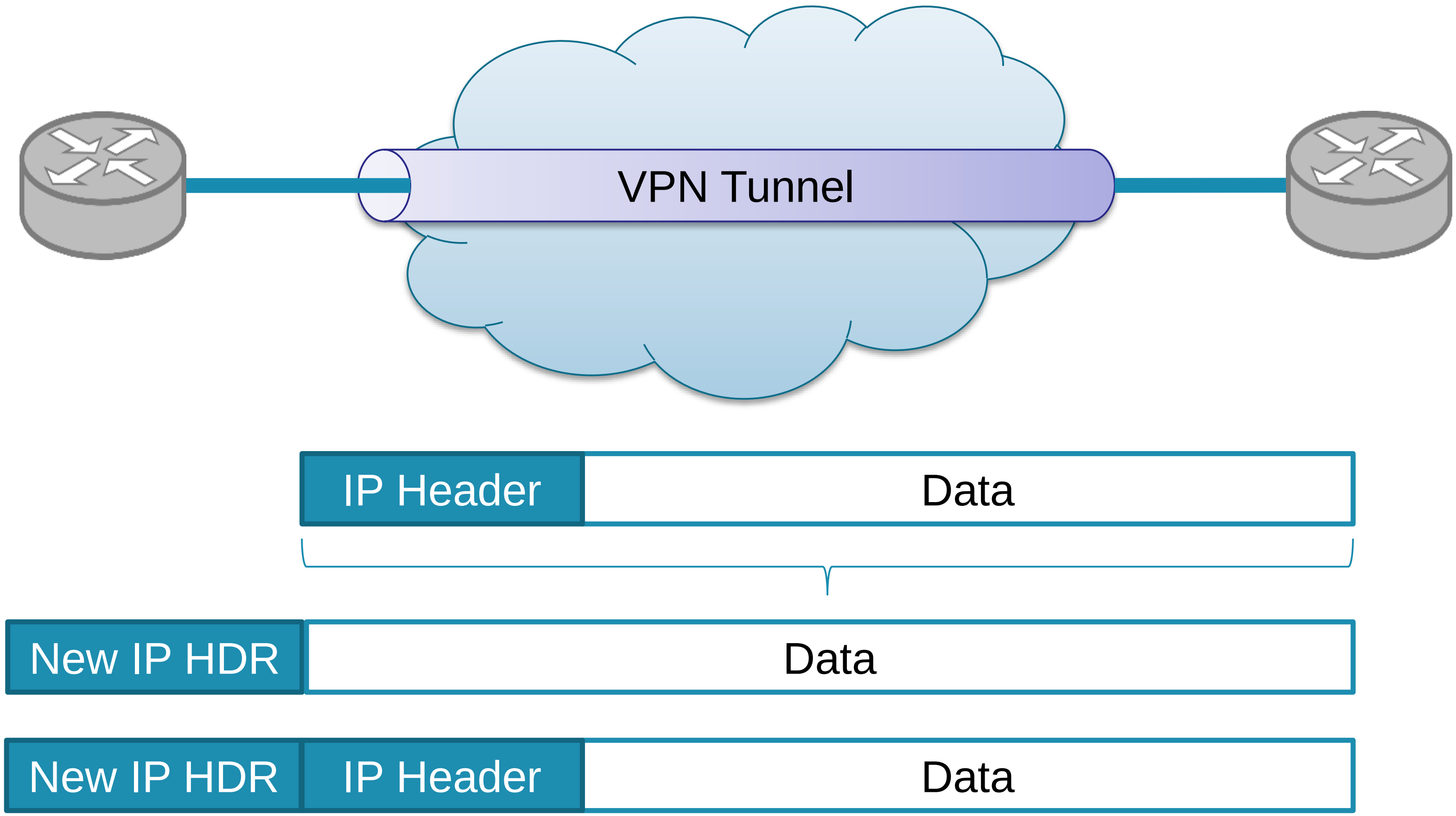
Virtual Private Network

- Tunneling



Virtual Private Network

- Tunneling



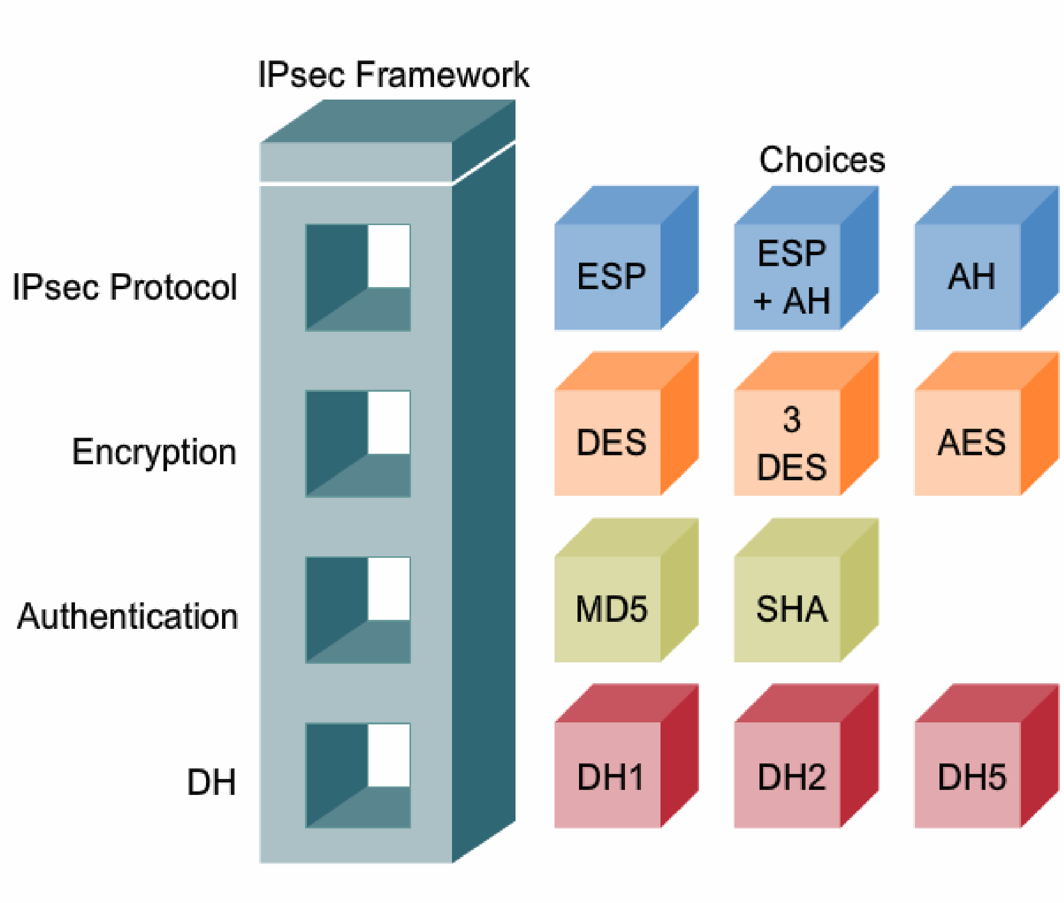
Virtual Private Network

	IPsec	OPENVPN™
Background	• RFC standarization	• Open source solution ○ Based on SSL/TLS
Encryption	• Standardised IPsec Protocol	• OpenSSL
Ports	• Fixed ports ○ UDP 500 ○ UDP 50 ○ UDP 1701 ○ UDP 4500	• Configurable ports ○ UDP ○ TCP ○ TCP 443: to bypass firewalls

IPsec

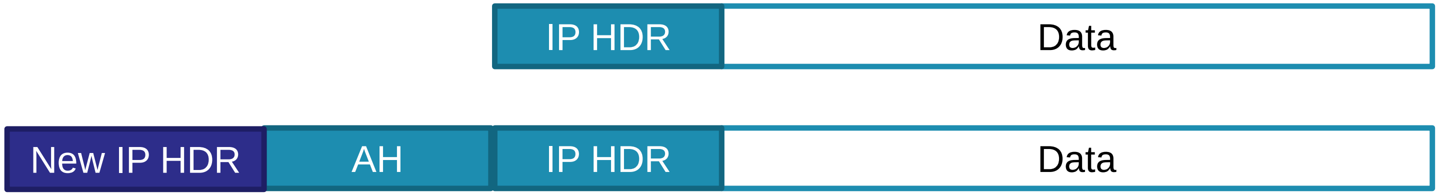
- Security Association
  - Relationship between multiple entities
  - Describes what security services used to communicate
    - Encryption algorithms
    - Authentication algorithms

IPsec


IPsec Framework
Choices
IPsec Protocol
Encryption
Authentication
DH
ESP
ESP + AH
AH
DES
3 DES
AES
MD5
SHA
DH1
DH2
DH5

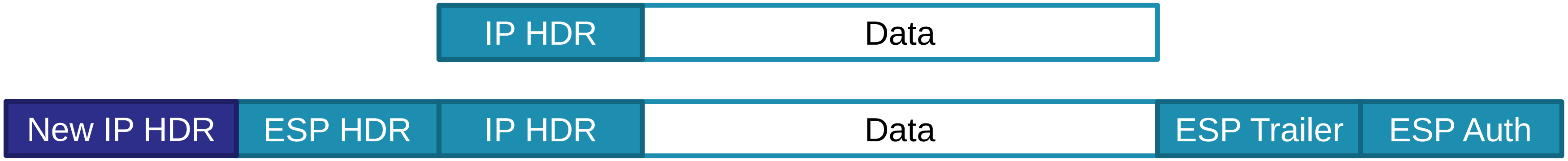
IPsec

- IPsec Protocol
  - AH: Authentication Header



Garantees connectionless integrity and data origin

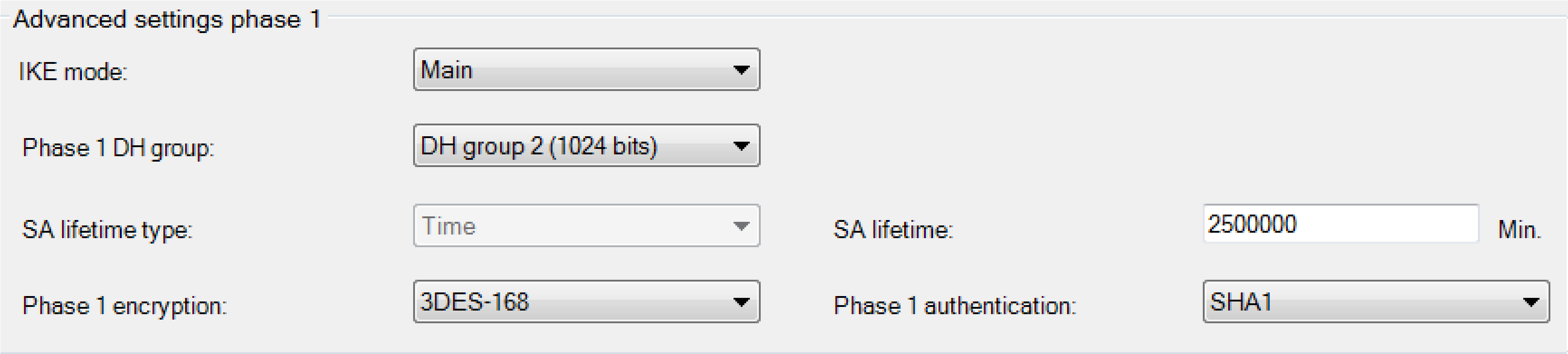
  - ESP: Encapsulating Security Payload



Provides Authenticity, Integrity and Confidentialy for packets

IPsec

- Internet Key Exchange
  - Phase 1



Advanced settings phase 1

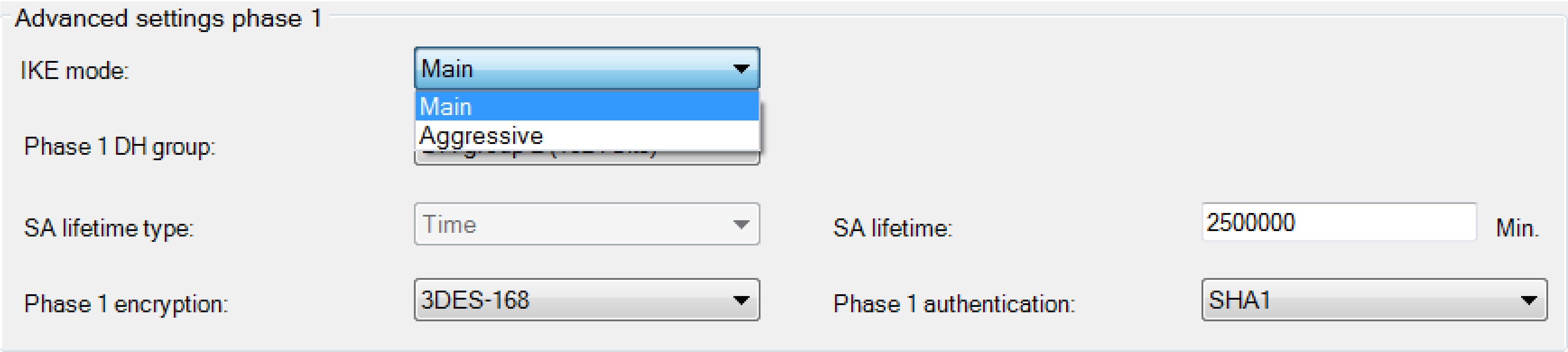
IKE mode:	Main		
Phase 1 DH group:	DH group 2 (1024 bits)		
SA lifetime type:	Time	SA lifetime:	2500000 Min.
Phase 1 encryption:	3DES-168	Phase 1 authentication:	SHA1

SA exchange
Agree on algorithms to use during communiation

DH key exchange
A shared secret is generated using Diffie-Hellman

IPsec

- Internet Key Exchange
  - Phase 1



Advanced settings phase 1

IKE mode: Main

Main
Aggressive

Phase 1 DH group:

SA lifetime type: Time

SA lifetime: 2500000 Min.

Phase 1 encryption: 3DES-168

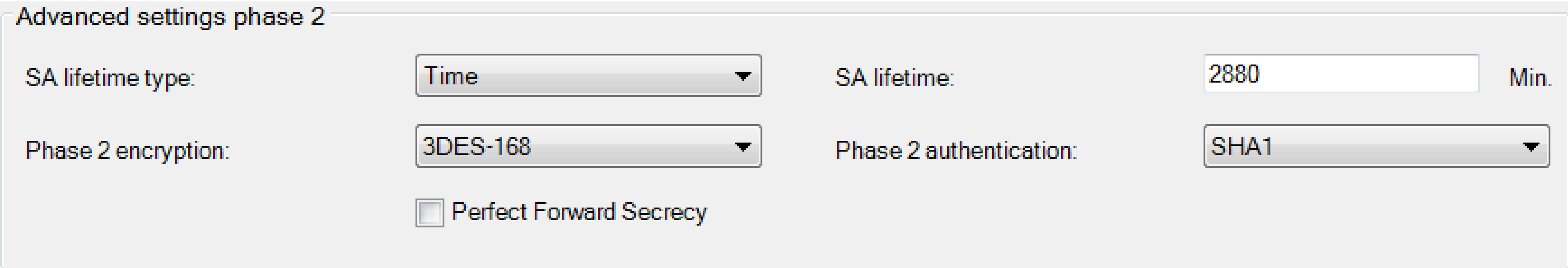
Phase 1 authentication: SHA1

Main mode
Slow
3 Exchanges
Identity encrypted

Aggressive mode
Fast
1 Exchange
Identity exposed

IPsec

- Internet Key Exchange
  - Phase 2



Advanced settings phase 2

SA lifetime type: Time

SA lifetime: 2880 Min.

Phase 2 encryption: 3DES-168

Phase 2 authentication: SHA1

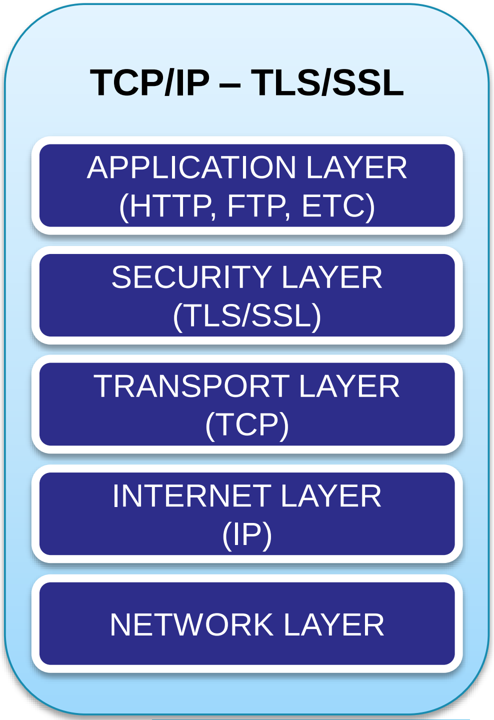
□ Perfect Forward Secrecy

- Use secure channel from Phase 1 to establish IPsec Security Associations
- Perfect Forward Secrecy

  ➔ Compromise of a single key permits access only to data protected by that single key

OpenVPN

- Based on SSL/TLS
- Intermediate layer between Transport and Application
- Two phases:
  - Handshake
    - Client and/or server authentication
    - Establish cryptographic keys and parameters
  - Secure exchange of information



OpenVPN

OpenSSL

➔All ciphers in the OpenSSL package can be used (DES, 3DES, AES, RSA)

- Several ways of authentication
  - Preshared-keys
  - Certificates
  - Username/password

Devices

Devices

PHOENIX CONTACT

SIEMENS

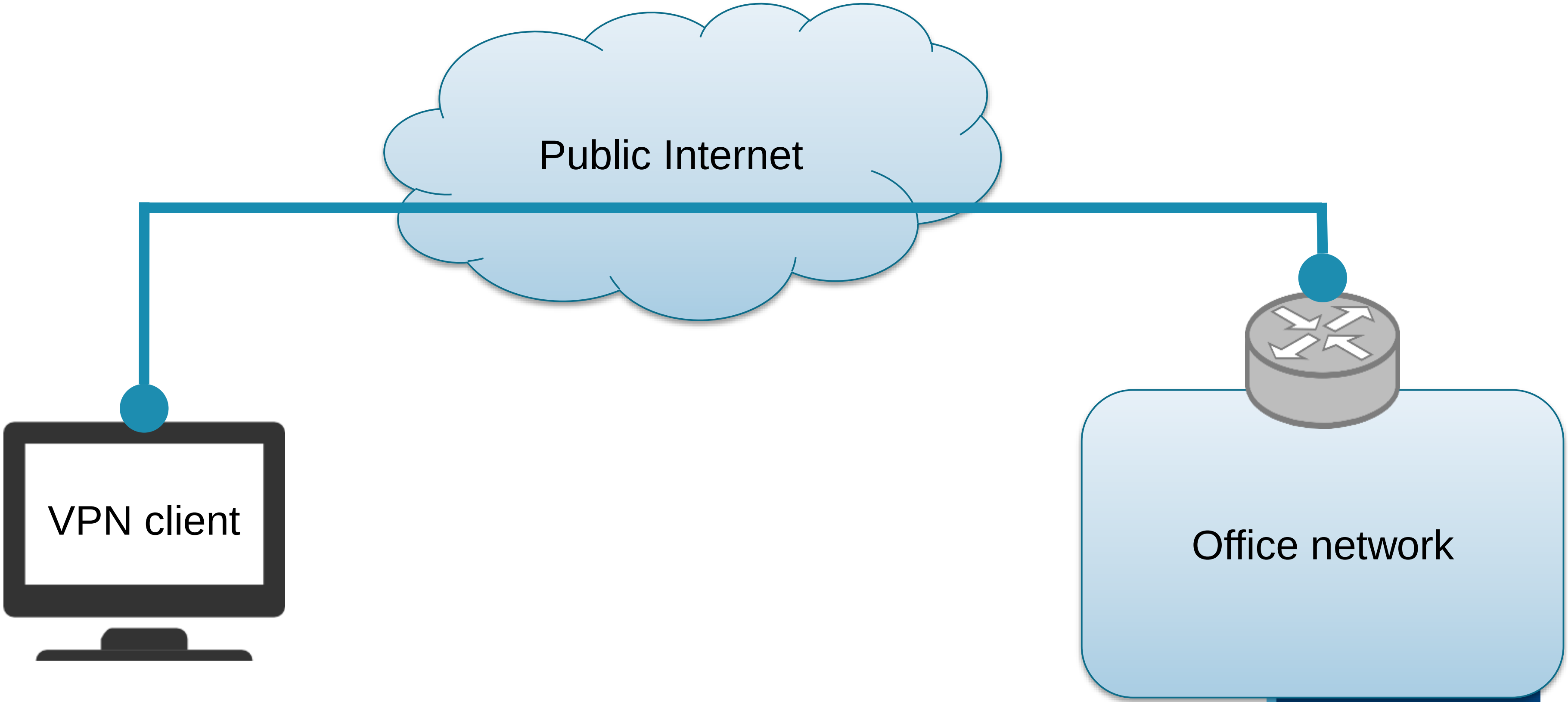
CISCO™

eWON

MACHINES CAN TALK

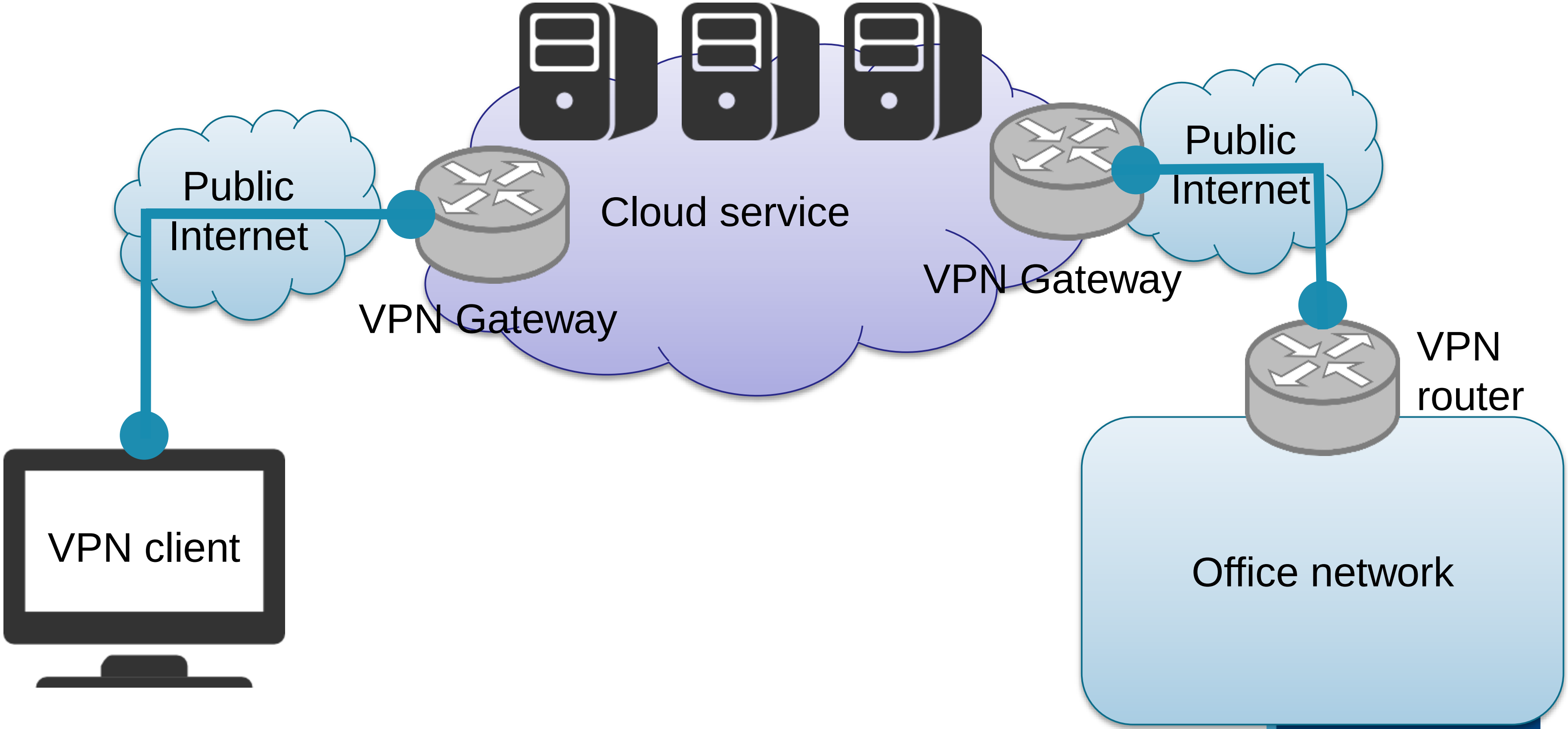
Devices

- End-to-End



Devices

- Cloud Service



Devices

End-to-End

SIEMENS

PHŒNIX CONTACT

CISCO™

Cloud Service

eWON

MACHINES CAN TALK

Devices

End-to-End

+ Highly configurable
+ Interoperability
+ End-to-end security

- Difficult to configure
- IPsec clients conflict

Cloud Service

+ High accessibility
+ Simple configuration

- Dependent on cloud
- No interoperability
- Need to trust cloud service

Questions?