PUBLIC KEY INFRASTRUCTURE DEPLOYMENT FOR MOBILE DEVICES

Pekka Suomalainen

- Supervisor: Professor Jorma Jormakka
- Instructor: M.Sc. Jukka Pitkänen, Nokia
- Written in Nokia Ventures Organization

Contents of the Presentation

- Introduction
- Public Key Infrastructure
- VPN deployment in current networks
- Authentication in 3G
- Solution proposal
- Use cases
- Conclusions

Introduction

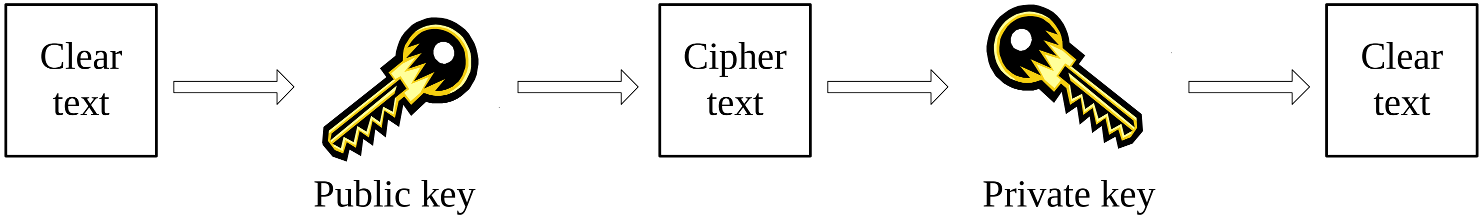
- 3G enables many new services
- 3G services and solutions need a secure and scalable authentication technology
- Public Key Infrastructure (PKI) meets these requirements
- PKI has to be deployed to 3G devices
- The standardization work is ongoing in 3GPP

PKI – Public Key Infrastructure

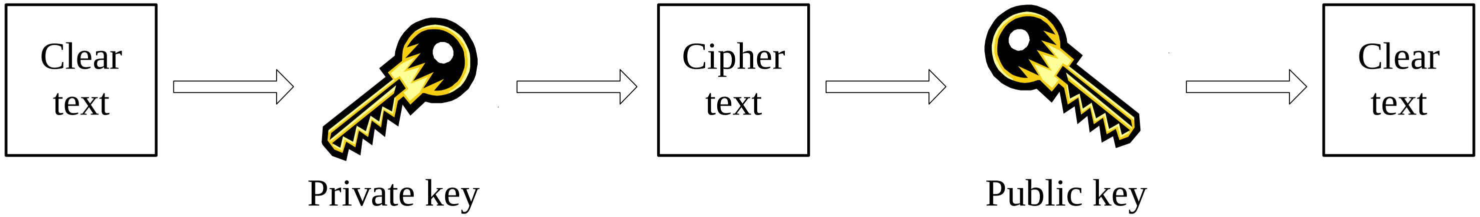
- Strong and scalable authentication technology offering many security services
- Based on public-key cryptography
  - public/private key pair
- Comprehensive infrastructure
  - Designed to scale even globally
  - Should be available everywhere like the Internet
- Existed for years but still not widely adopted
  - Problems are more political than technological
  - Trust issues are difficult to understand and solve
  - Pronounced dead by many “experts”
- Deployment of infrastructure is a slow process
- No feasible choice available

Public key cryptography

- Offers two keys, which can be used for different services
  - Confidentiality: encryption with the public key:

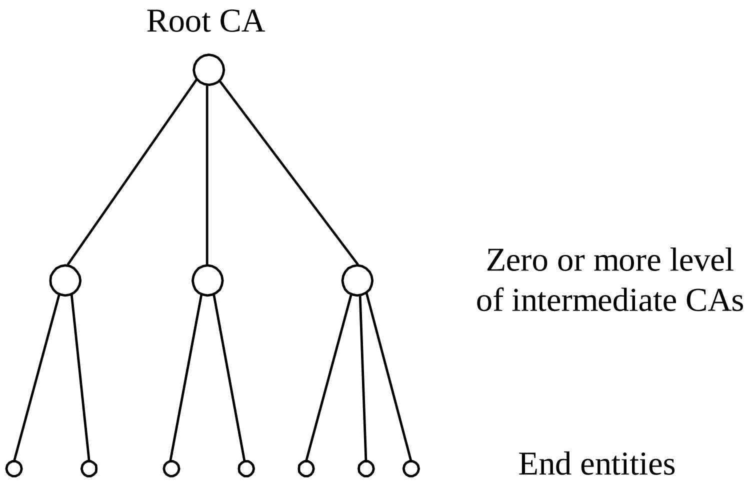


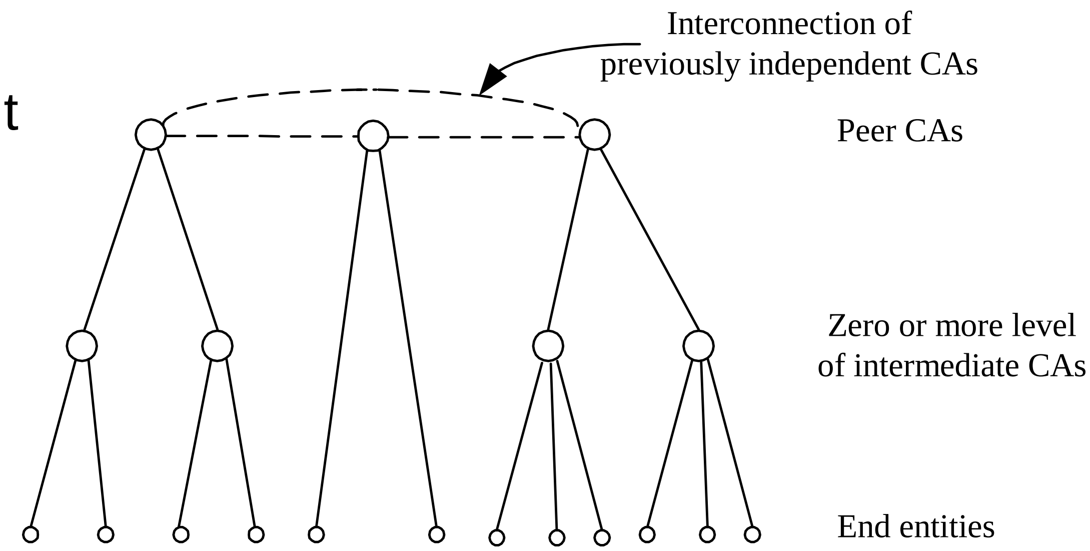
  - Integrity: signature with private key



PKI Technology

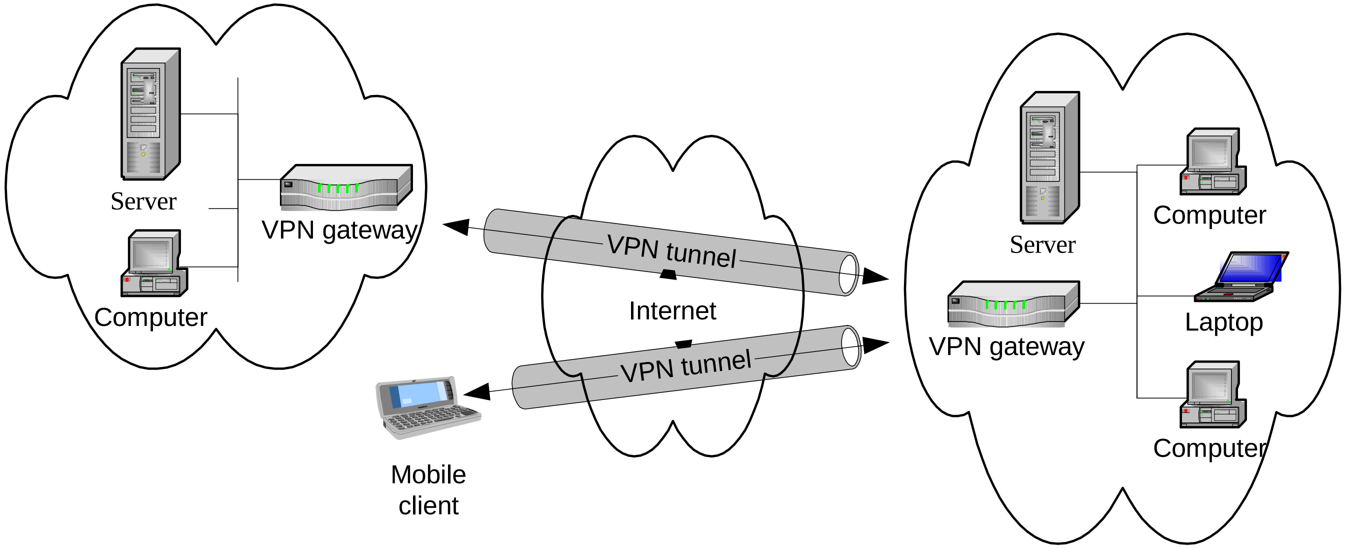
- Certificates are a central part of PKI
  - Bind identity and public key
  - Public documents
- Certification Authority (CA) issues and signs the certificates
- CA is a trusted third party, which everyone should trust
  - Anyone can verify the certificate using a proper CA
  - CAs can form a hierarchy
- Trust models define a set of trust relationships
  - Strict hierarchy of CAs
  - Distributed trust model




Interconnection of previously independent CAs
Peer CAs
Zero or more level of intermediate CAs
End entities

Virtual Private Networks

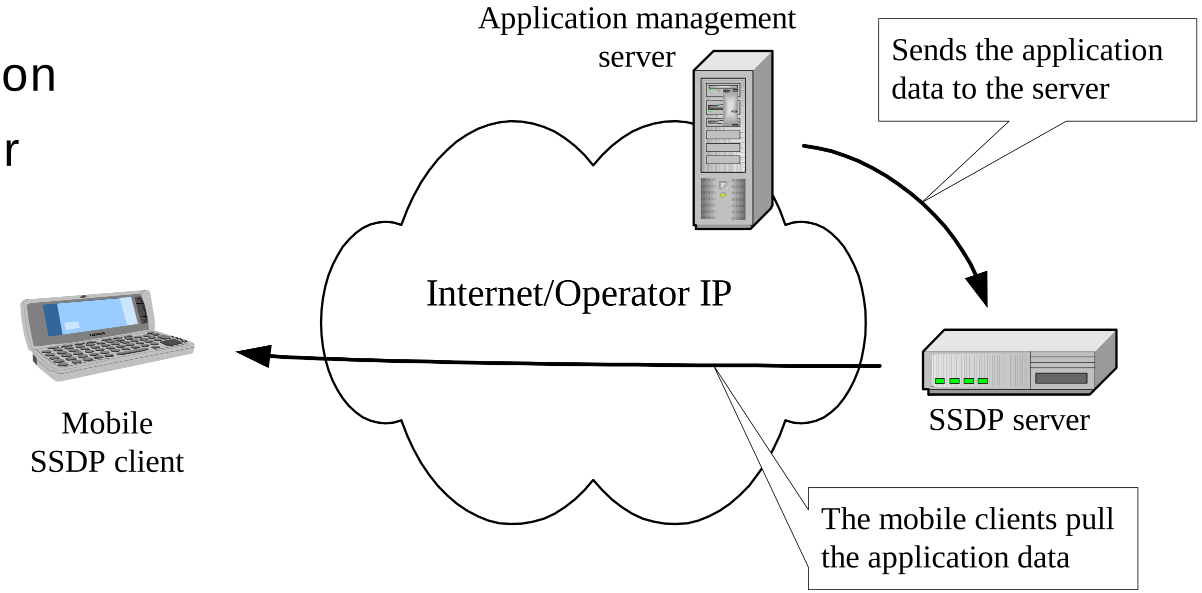
- VPN is used to establish a secure connection in public networks
  - between different sites
  - between a user and remote site
- VPN can be implemented with several technologies
  - Here the focus on IPSec
- VPN end entities must authenticate themselves before the connection can be established
- PKI is only solution, which can offer feasible choice for authentication



NOKIA

VPN and PKI Deployment

- Secure Service Deployment Platform (SSDP) is an existing concept for offering scalable VPN management
- SSDP acts as a proxy for clients delivering VPN policies and certificate for them
  - Management point for mobile terminals
  - Connection point between fixed and mobile world
  - Service point for authentication services (PKI CA/RA)
- Offers initial deployment of VPN
- Offers a two-way authentication
- Supports PKI-based authentication
- Enables certificate enrollment for clients
- May act as an internal CA or an enrollment gateway for any external CA

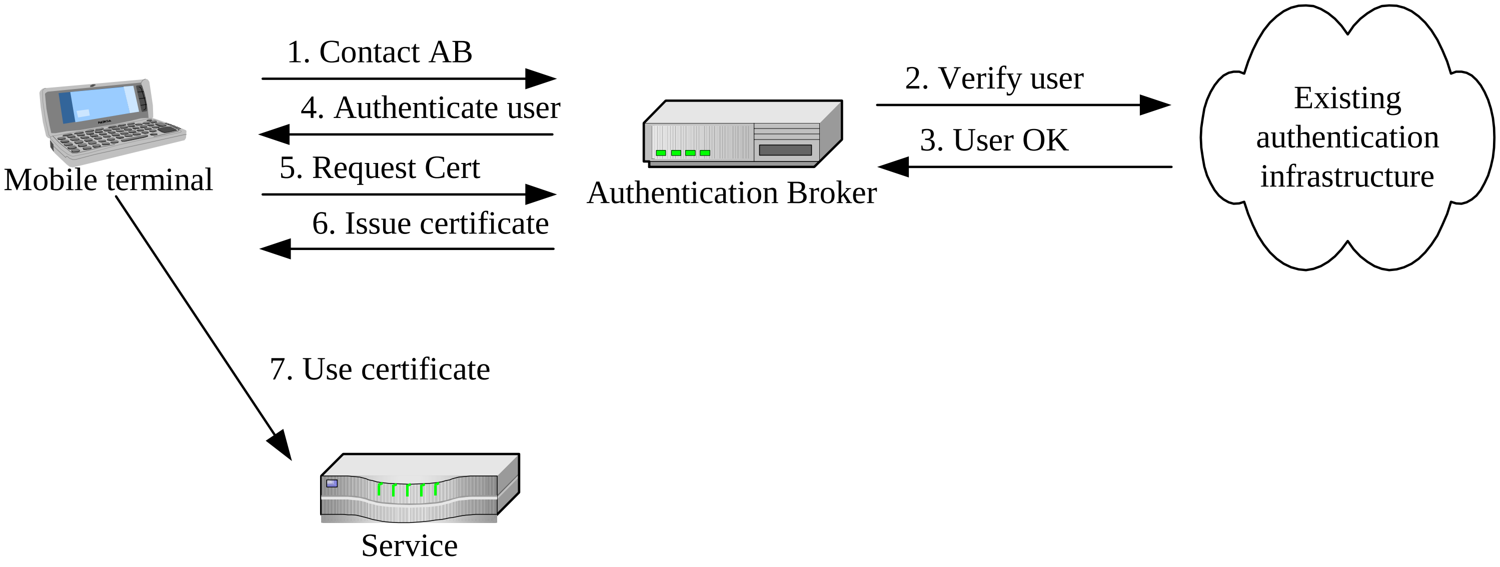

Application management server
Sends the application data to the server
Internet/Operator IP
SSDP server
Mobile SSDP client
The mobile clients pull the application data

3GPP Subscriber Certificates

- Will be defined in Release 6 of 3GPP standards
  - Available Q1/04?
  - The standard is subject to change
- Basic idea: mobile operators issue the certificates for end users
- Operators use their existing authentication infrastructure
- Provides migration path for global PKI
- Operators can adopt PKI
  - Possibility for many new services

Authentication Broker

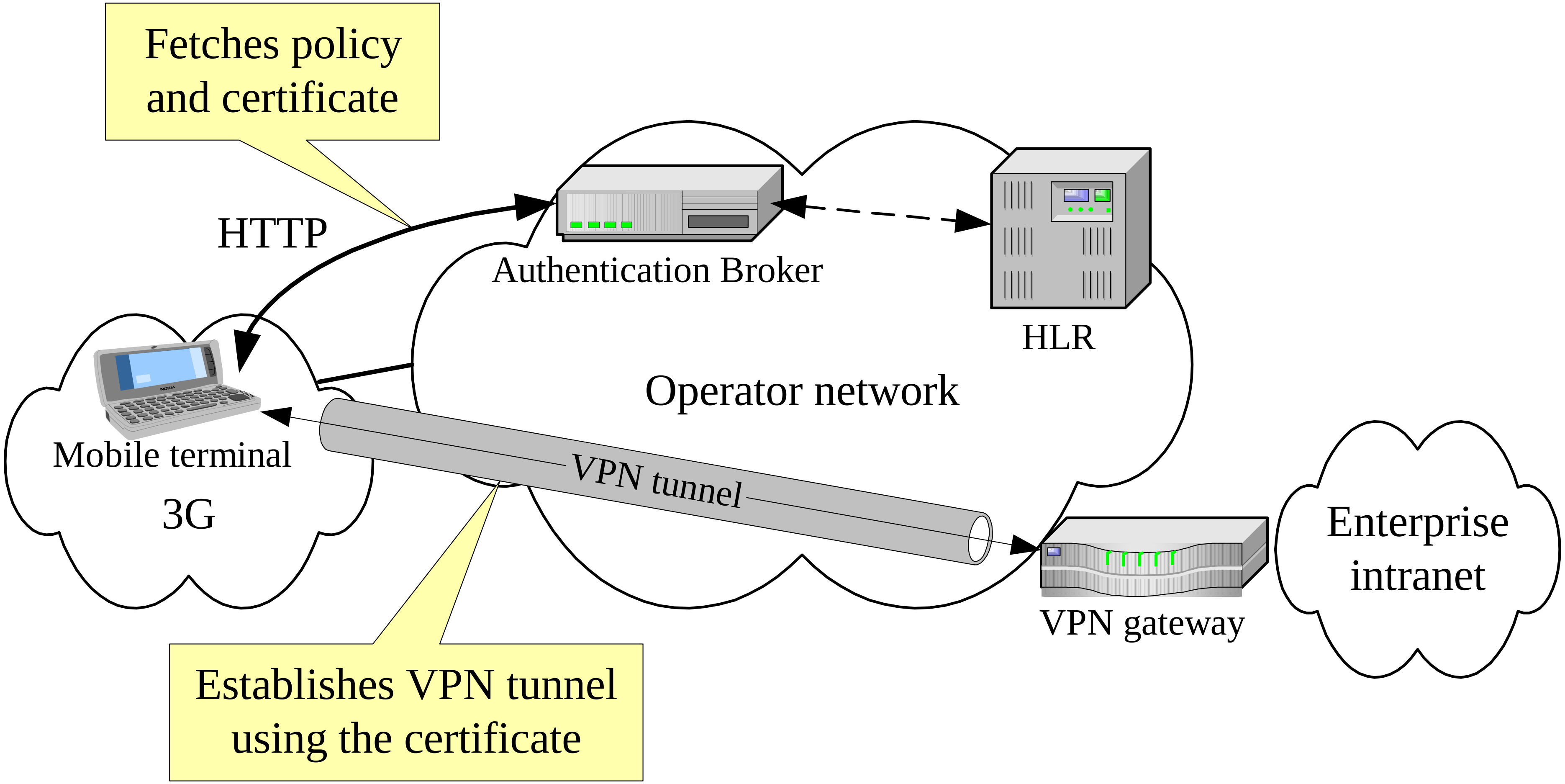
- One possible implementation of the subscriber certificate standard based on
  - “new gateway” element proposal (from SA2)
  - Generic SSDP model
- Offers automatically certificates for clients subscribing to the network
- Initial authentication based on USIM card
- May act as a internal CA or Registration Authority (RA) for external CA



Analysis of AB

- Meets the 3GPP generic security requirements and is standards compliant
- Significant role for mobile operators
- Benefits:
    - Supports multiple identities
    - Dynamic certificates: eases revocation process
    - Offers strong authentication through PKI for all parties
    - Possible source of revenues for operators and service providers
    - Access independence: works over GPRS, WLAN, UMTS, xDSL..
- Problems:
    - Initial solution works only in the domain of one operator
        - Roaming might be phased out from the Release 6
    - Does service provider or customer trust the USIM authentication?

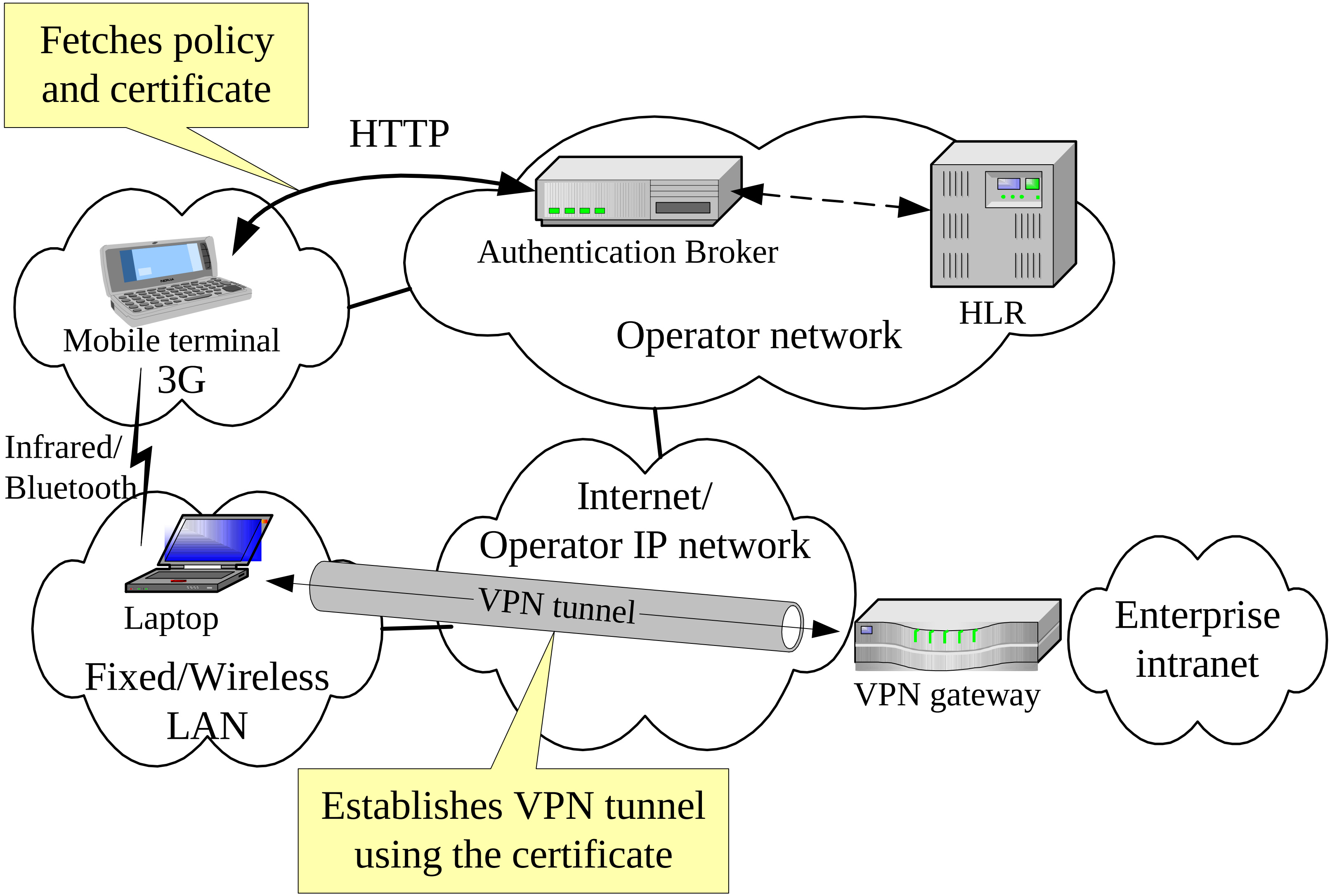
Use case 1: Cellular VPN authentication



Fetches policy and certificate

Establishes VPN tunnel using the certificate

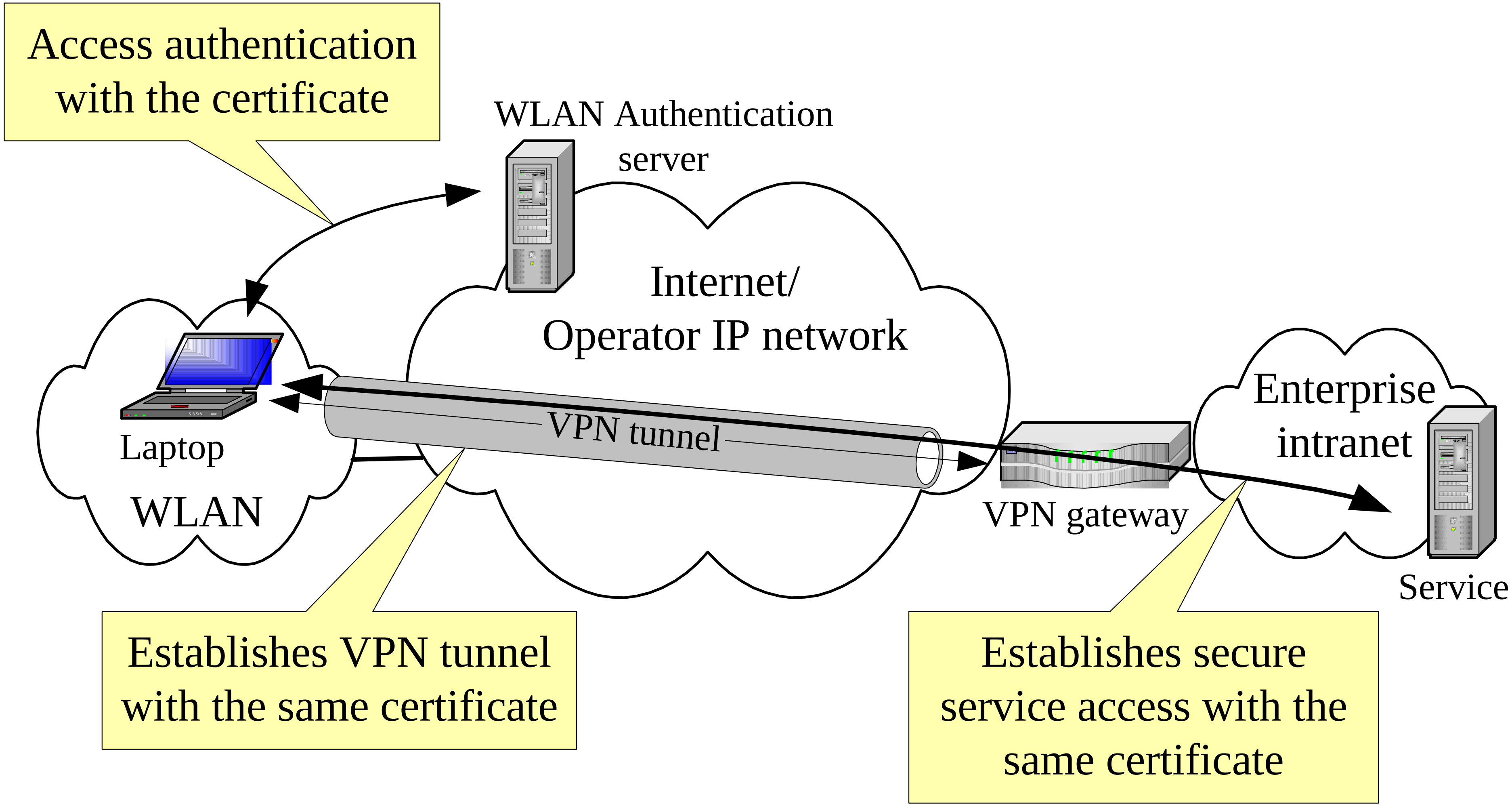
Use case 2: Non-cellular VPN authentication



Fetches policy and certificate

Establishes VPN tunnel using the certificate

Use case 3: Single sign-on



Access authentication with the certificate

WLAN Authentication server

Internet/ Operator IP network

Laptop

WLAN

VPN tunnel

VPN gateway

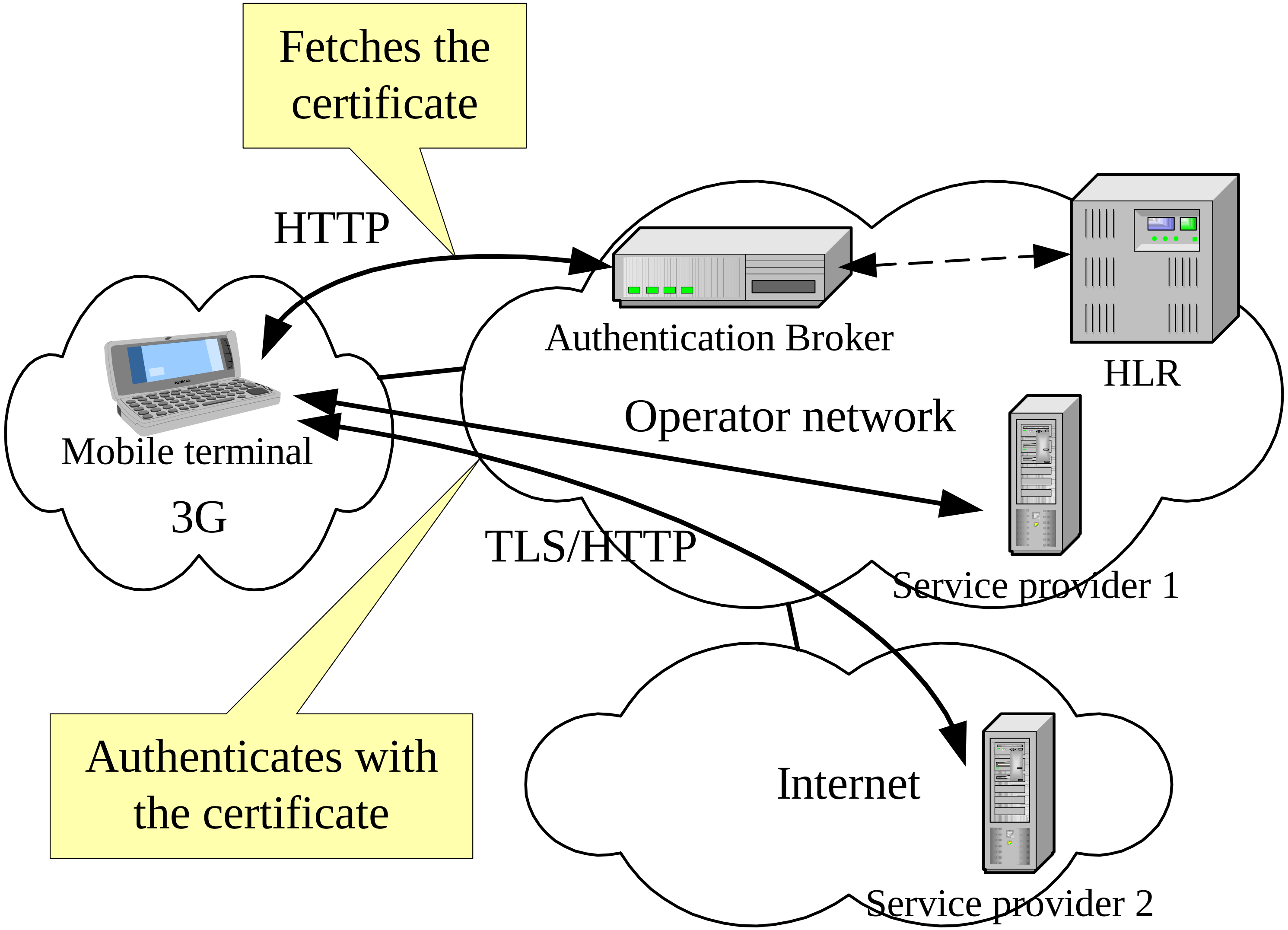
Enterprise intranet

Service

Establishes VPN tunnel with the same certificate

Establishes secure service access with the same certificate

Use case 4: Mobile payment



Conclusions

- PKI is the only truly scalable authentication method
- 3GPP Subscriber certificate provides a migration path to global PKI
- Authentication Broker is one possible implementation
  - Standard compliant
  - Based on Secure Service Deployment Platform concept
- Release 6 might not contain inter-operator functionality
  - The standard is subject to change
- USIM authentication might be restrictive issue

Thank you!

Questions?