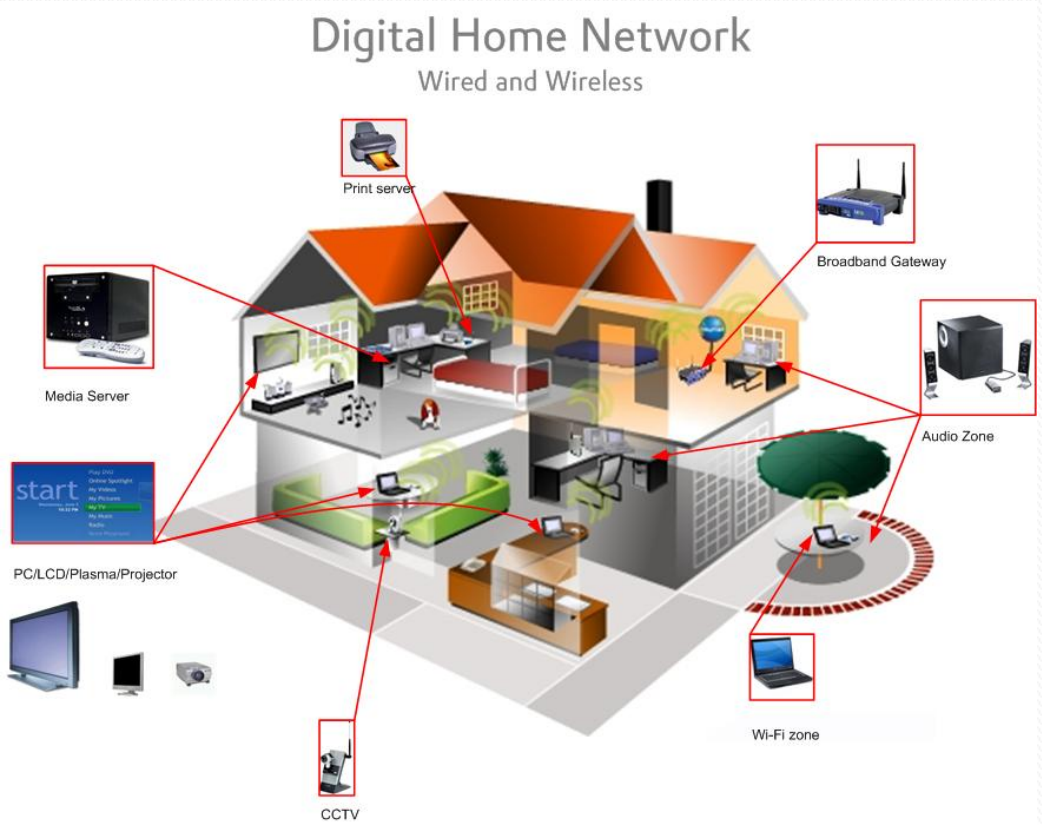
# NPCERT.ORG and ICTFRAME.COM Hosted First Cyber Security Meetup in Nepal


Event Name : Cyber Secuirty Meetup Nepal #1

# PKI based Home Network Device Authentication

Roja Kiran Basukala
*Deputy Director*, **NTA**
*Member*, CSRI

# Home Network




- Also known as Smart Home or Residential Network
- Collection of intelligent appliances like, computers, digitalized audio/visual appliances, control, sensors and devices and connection of them in home.
- The number of home network devices is growing day by day
- security of these intelligent devices has been an important factor to secure a home network.
  - A broadband connection to internet of home network is subjected to attacks not only from outside but also from inside
  - integration of wired and wireless technology has also made the possibility of unauthorized access by device included in neighbor home network.
- user authentication and authorization
  - permit only authorized persons to use home network services.
  - not fully secure due to some problems like leakage of user authentication information

# Device Authentication


- A second layer of authentication, ensuring that only a specific authorized device operated by specific authorized users can access the network.
- Even if a password or token has been compromised, the network is still protected as long as the authorized machine is not used.
- Confidential data is never exposed because unauthorized devices are not allowed onto a network, even when operated by an authorized user
- Mandatory technology that enables emerging context-aware services providing service automatically through device cooperation without user intervention

# Why PKI

## Symmetric Cryptography

- a single shared secret key is used using encryption standards
- can be used for home network with few devices.
- unique secret key is shared among several devices resulting vulnerability to key discovery.

## Asymmetric Cryptography

- two mathematically related public and private keys for encryption and decryption
  - Encryption by sending device's public key which can be seen by all devices in network
  - decryption by receiving device's private key which is kept secret
- using different encryption key algorithms
- supports non repudiation
  - only the sender knows their private key, only the sender could have sent the message,
- unable to provide data integrity.

## Digital Certificates

- addition of one-way secure hash functions with public key cryptography.
- In Hash algorithm like HAS-1, the Hash function generates fixed length value.
- Hence data integrity is ensured with hash value along with non-repudiation.
  - No two documents produce the same hash value.
- But no device is sure about the owner of the public key.

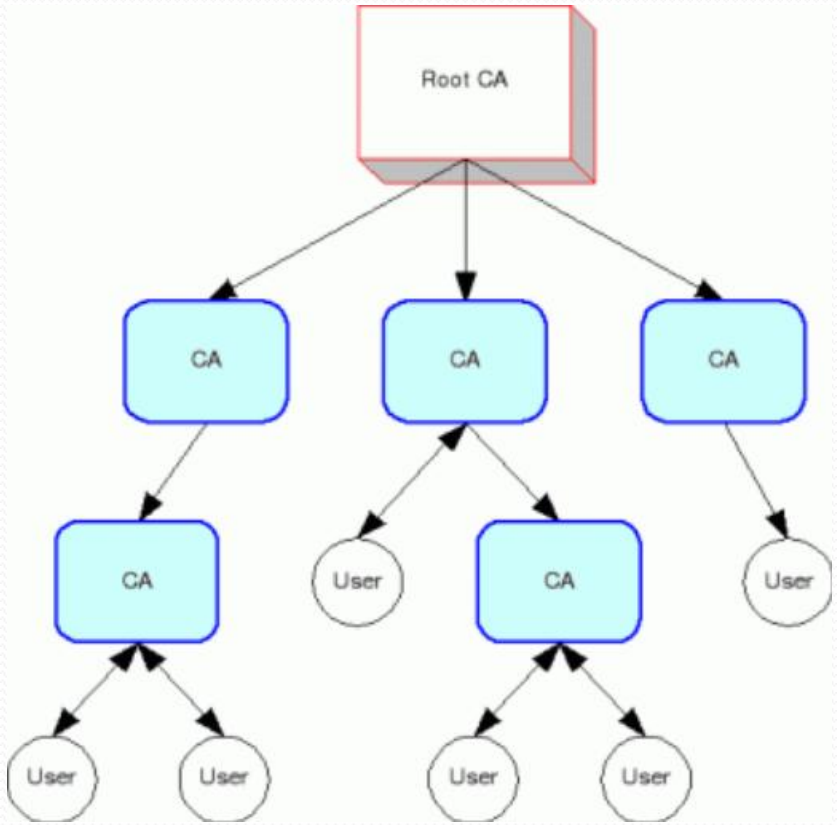
## PKI

- bind public keys to their owners
- helps in the distribution of reliable public keys in large heterogeneous networks.
- set of hardware, software, people, policies and procedures needed to create, manage, store, distribute, and revoke Public Key Certificates based on public-key cryptography.
- integrate digital certificates, public key cryptography, and certification authorities (CAs) into a complete ubiquitous home network security architecture

# PKI Architectures

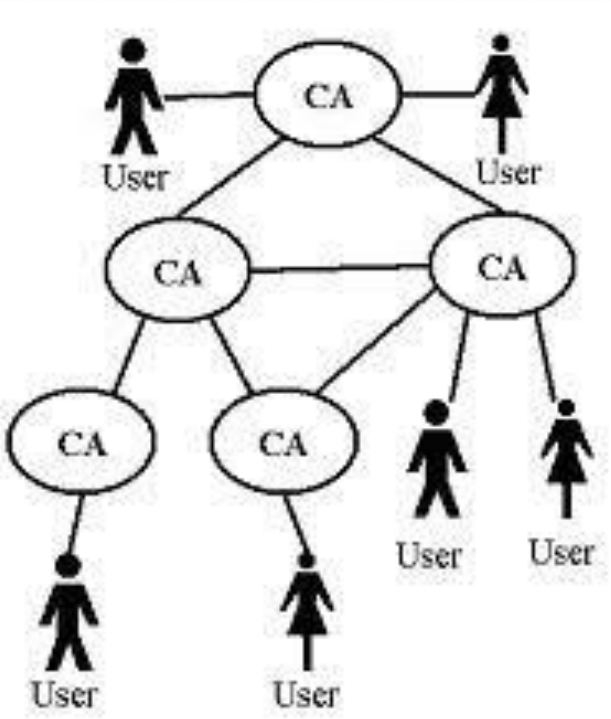
- PKI
  - composed of many CAs linked by trust paths
  - A trust path links a relying party with one or more trusted third parties, such that the relying party can have confidence in the validity of the certificate in use.
  - Recipients of a signed message who have no relationship with the CA that issued the certificate for the sender of the message can still validate the sender's certificate by finding a path between their CA and the one that issued the sender's certificate.
- two traditional PKI architectures
  - **hierarchical**
  - **mesh**
- More recently, third architecture has been developed
  - **Bridge**

# Hierarchical PKI



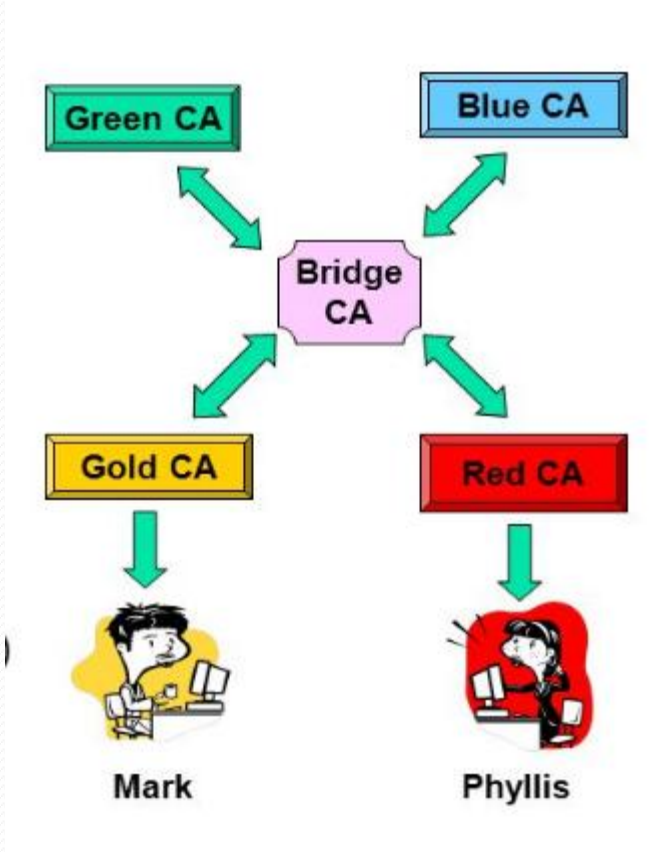

- Authorities are arranged hierarchically under a “root” CA that issues certificates to subordinate CAs.
- CAs may issue certificates to CAs below them in the hierarchy.
- Only one superior CA certifies each CA.
- Certificates are issued in only one direction, and a CA never certifies another CA "superior" to itself.
- Every relying party knows the public key of the root CA.
- Any entity certificate may be verified by verifying the certification path of certificates from the root CA.
- The path construction procedure is very simple
  - a single path exists from any end entity up to the root CA
  - retrieving issuer certificates successively until a certificate is located that was issued by the trusted root.
- Deploying a unique root CA for global ubiquitous environment is inappropriate for home networks.
  - this architecture is only directly applicable within one domain of home network.

# Mesh PKI



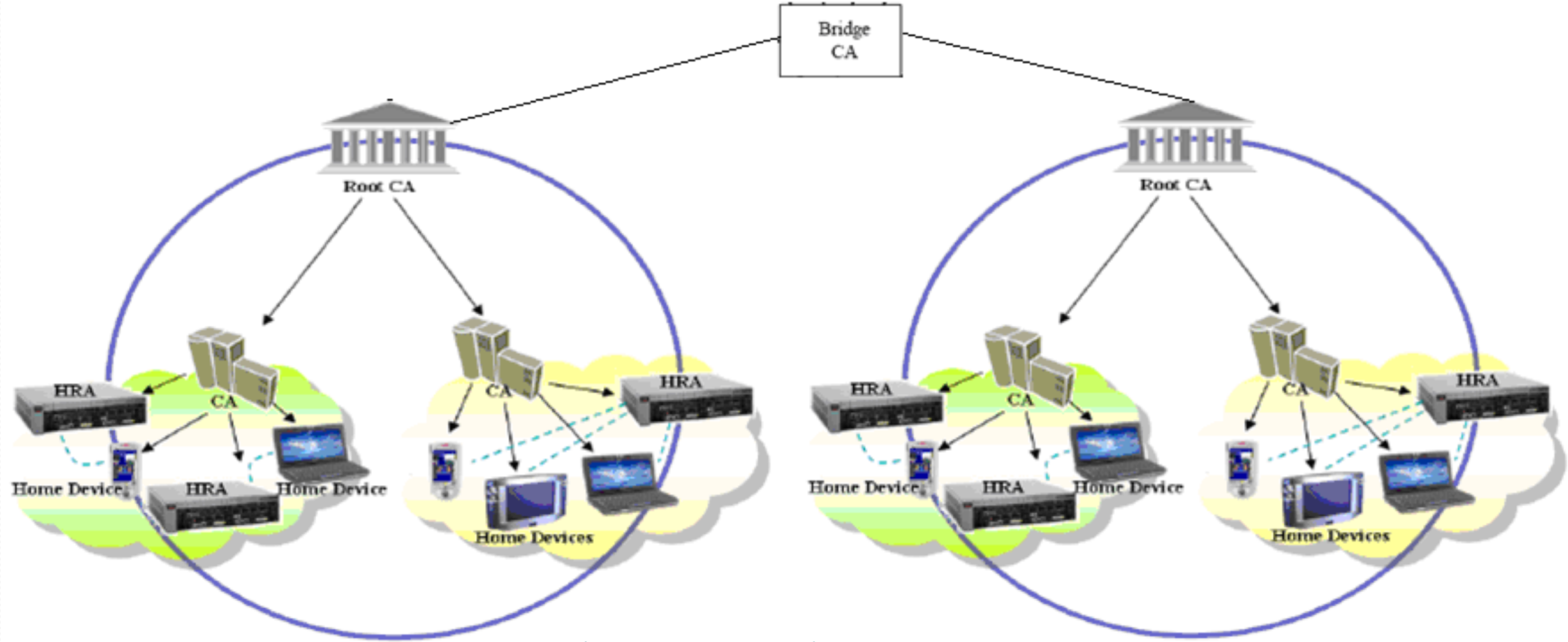

- bring trust development to inter-domain levels
- two CAs cross-certify each other once they agree to trust and rely on each other's issued public key certificates as if they had generated them themselves.
- Pairs of CAs exchange cross-certificates and enable devices from one administrative domain to interact electronically and securely with devices from the other.
- when the number of cross-certificates tends to grow exponentially with the number of CAs,
  - certification path construction becomes more complex
    - likely existence of multiple paths between a relying party's trust anchor and the certificate to be verified, and the potential for loops and "dead ends" in non-hierarchical certificate graphs.

# Bridge PKI




- connect PKIs regardless of the architecture
  - Bridge CA
    - establishes peer-to-peer relationships with different PKIs.
    - does not issue certificates directly to users.
    - simply acts as a gateway between isolated CAs.
    - map certificate policies and guarantee PKI equivalences adequately.
      - devices must rely on it regarding these mappings.
  - relationships can be combined to form a bridge of trust connecting the CAs from the different PKIs
    - If the trust domain is implemented as a hierarchical PKI, the Bridge CA will establish a relationship with the root CA.
    - If the domain is implemented as a mesh PKI, the bridge will establish a relationship with only one of its CAs.
  - bridges a natural joining point for the sending and validation aspects of PKI.
    - Individual CAs become able to focus on issuing certificates according to their own policies, and bridges focus on providing validation interoperability within acceptable trust bounds.

# Architecture of Proposed PKI based Home Device Authentication



# Bridge Certification Authority (BCA)

- Bridge of trust that provide trust paths between the various trust domains of public PKI as well as private PKI trust domains.
- Only root CA of one domain is eligible to cross-certify with the BCA.
  - When the BCA cross certifies with CAs it may include nameConstraints, pathLengthConstraints or policyConstraints that limit the propagation of trust to other, cross-certified domains for security.
- Not a single bridge in the center of an all encompassing star.
  - There can be any number of bridges;
  - but the goal is to concentrate to a smaller group of large hubs.
- Among other advantages, this reduces average path length, which helps the path discovery scaling problem.
- Private Home Networks that their own CA may find a bridge to be a natural trust anchor and issue a very small number of cross certificates to their chosen bridge(s).
  - allows inter-domain communication of home devices of private or public home networks.

# Root Certification Authority

- Certification is the act of binding a subject name with a public key.
- acts as the root agent of trust in the PKI with its self-signed certificate;
  - each member of the chain must implicitly trust the certificates generated by the Root CA. A Root CA mainly performs these functions.
- Issues certificates (i.e., creates and signs them);
- Maintains certificate status information and issues CRLs;
- Publishes its current (e.g., unexpired) certificates and CRLs, so devices can obtain the information they need to implement security services;
- Maintains archives of status information about the expired certificates that it issued.

# Sub-ordinate Certification Authority

- receives a certificate from its superior CA.
- inherits some policies and constraints  from its superior CA.
- never issues its self-signed certificate.
- has subordinate CAs or end devices of its own to which it issues certificates.
- subordinate CA has clear trust  relationship with its superior CA,
  - trusted easily by all home devices who trust the superior CA.

# Home Registration Authority

- A home device which has enough computing power for public key operation, communication ability with other home devices and user interface equipment and has more authority and requirement.
- Offloads many of the administrative functions of  subordinate CA.
- Normally associated with the End Device registration process.
  - includes the verification of the identity of the home device attempting to register with the PKI.
- Validates the attributes of the subject who is requesting the certificate
- Verifies that the subject has possession of the private key being registered
- Generates shared secrets to support the initialization and certification process
- Public/private key pair-generation
- Conducts interactions with the CA (or several CAs) as an intermediary of the End Entity
  - key compromise notifications
  - key recovery requests
- Parameter  validation of public keys presented for registration

# Other entities

- **Manufacturing Company**
  - Manufactures home devices with networking ability.
  - Each device is given a unique information in any form like, bar code, serial number, MAC address etc. of the device.
  - Since the manufacturer servers possess  home devices identification  information, they are used for verification purpose in this architecture during device registration process with HRA and certificate issuing process with subordinate CA.

- **Home Devices**
  - Home devices are the control devices, home appliances, and devices with home networking ability used in home network
  - Communicate with each other and have basic computing ability.
    - Eg. internet-microwave, internet-refrigerator, digital TV such as IPTV, internet-washing machine, PDA, notebook, computer, wall-pad, PC, cellular phone, etc.

# Home Device Registration and Certificate Issuing

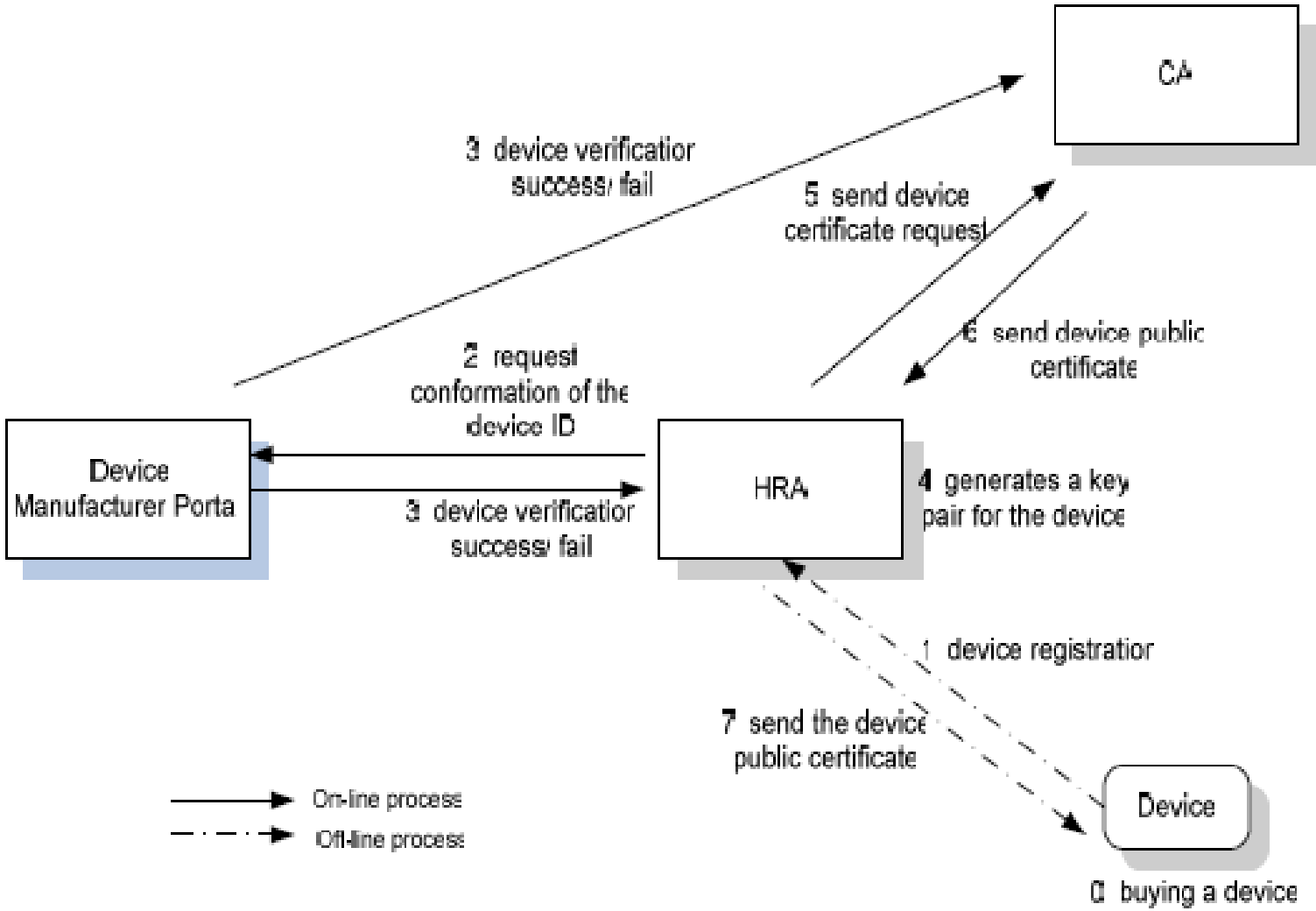



**Fig. 2.** Issuing process of home device public certificate

# References


1) Yun-kyung Lee, Deok Gyu Lee, Jong-wook Han : Home Device Authentication Method based on PKI

2) Yun-kyung Lee, Deok Gyu Lee, Jong-wook Han, and Kyo-il Chung : Home Network Device Authentication: Device Authentication Framework and Device Certificate Profile

3) SafeNet, Inc. August 2003 : Device Authentication: A Valuable Addition to Agency Cyber-Security Programs

4) W. E. Burr, Public Key Infrastructure (PKI) Technical Specifications: Part A - Technical Concept of Operations

5) Kenneth D. Stillson Public Key Infrastructure Interoperability: Tools and Concepts

6) Helena Rifa-Pous and Jordi Herrera-Joancomart, An Interdomain PKI Model Based on Trust Lists

7) D. Richard Kuhn, Vincent C. Hu, W. Timothy Polk, Shu-Jen Chang: Introduction to Public Key Technology and the Federal PKI Infrastructure

8) David P. Lemire, Peter M. Hesse : Managing Interoperability in Non-Hierarchical Public Key Infrastructures

9) Sashi Kiran, Patricia Lareau, Steve Lloyd : PKI Basics - A Technical Perspective