Public Key Infrastructure (PKI)
Tutorial for CANS'20
Day 1: Introduction, X.509 and Constraints

Amir Herzberg
University of Connecticut

See ch. 8 of 'Applied Intro to Cryptography',
available at my site: .

Public Key Infrastructure (PKI)
Tutorial for CANS'20
Day 2: Revocation and Merkle Digest Schemes

Amir Herzberg
University of Connecticut

See ch. 8 of 'Applied Intro to Cryptography',
available at my site: .

Public Key Infrastructure (PKI)
Tutorial for CANS'20
Day 3: CA Failures and Certificate Transparency

Amir Herzberg
University of Connecticut

See ch. 8 of 'Applied Intro to Cryptography',
available at my site: .

PKI Tutorial – CANS'20: Agenda

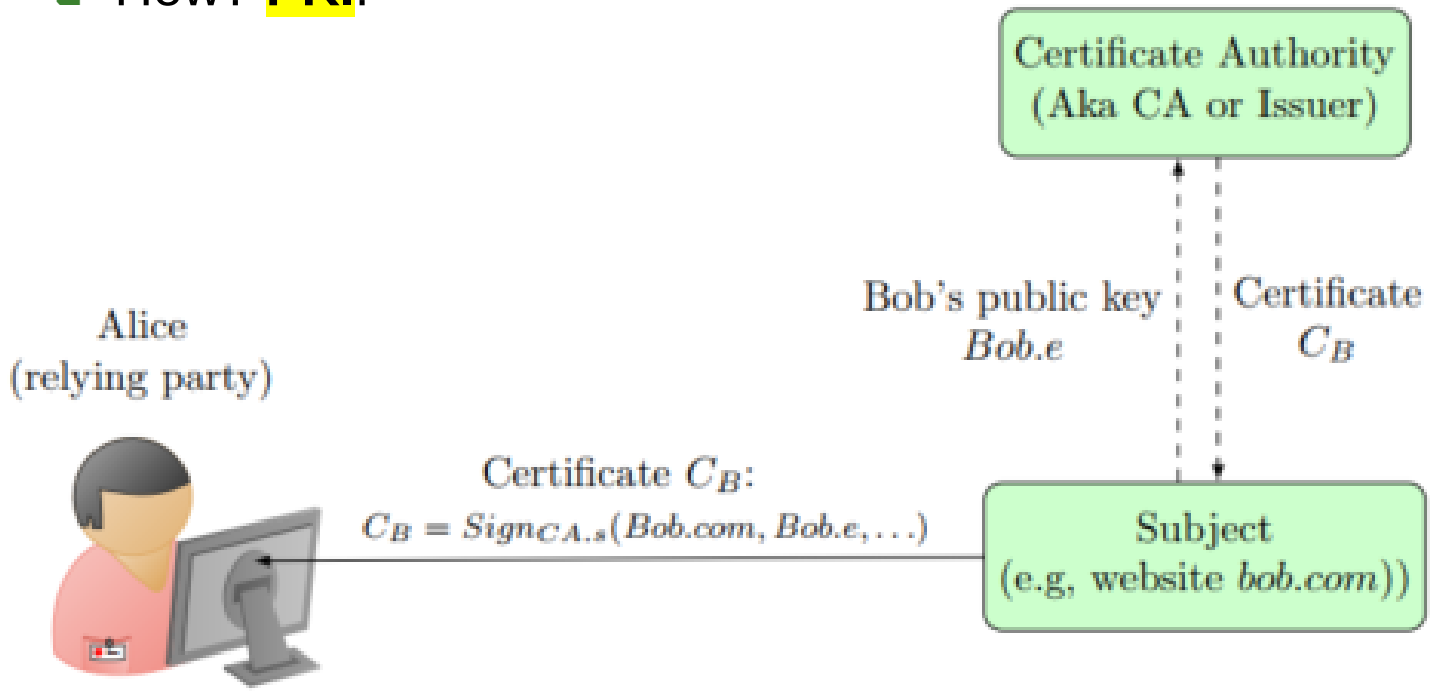
- **Day 1: Introduction, X.509 and constraints**
  - **Introduction**: certificate, PKI, failures, goals
  - **X.509**: Certificates, names and extensions
  - Indirect Certification in X.509: **Constraints**
- Day 2: Revocations and Merkle Digests
- Day 3: CA failures + Certificate Transparency
- Conclusions, directions and challenges

Public keys are very useful…

- Secure web connections
- Software signing (against malware)
- Secure messaging, email
- Crypto-currency, blockchains, financial crypto…
  - So far, not much use of personal public keys
    - Secure email: not widely deployed
    - Secure messaging: auth by provider (& user ??)
- How do we know the PK of an entity?
  - Mainly: signed by a **trusted Certificate Authority**
    - E.g., in TLS, browsers maintain list of ‘root CAs’

Public Key Certificates & Authorities

- *Certificate:* signature by Issuer / Certificate Authority (CA) over subject's public key and attributes
- Attributes: identity (ID) and others…
  - Validated by CA (liability?)
  - Used by **relying party** for decisions (e.g., use this website?)
  - How? **PKI**!



Public Key Infrastructure (PKI)

- 'PKI is the infrastructure established to support the issuing, revocation and validation of public-key certificates' [ITU-T recommendation X.509]
  - Other fuzzy definitions, e.g., two from NIST
- A **PKI scheme is a set of PPT algorithms:**

$$\mathcal{P} = (\mathsf{Init}, \mathsf{Issue}, \mathsf{Revoke}, \mathsf{Attest}, \mathsf{Audit}, \mathsf{WasValid}, \mathsf{Wakeup}, \mathsf{Receive}, \mathsf{PoM}, \mathsf{Monitor})$$

  - Algorithms CAs, relying parties and others should use
  - New, game-based definitions; beyond our scope ☹
    - See eprint or ask me
- **Two main applications:**
  - Web-PKI (mainly, TLS)
  - Code (software) signing

Main application: Web-PKI

PKI deployed by **TLS/SSL, browsers, web-servers**

Browsers contain keys of **Root CAs** (trust anchors)

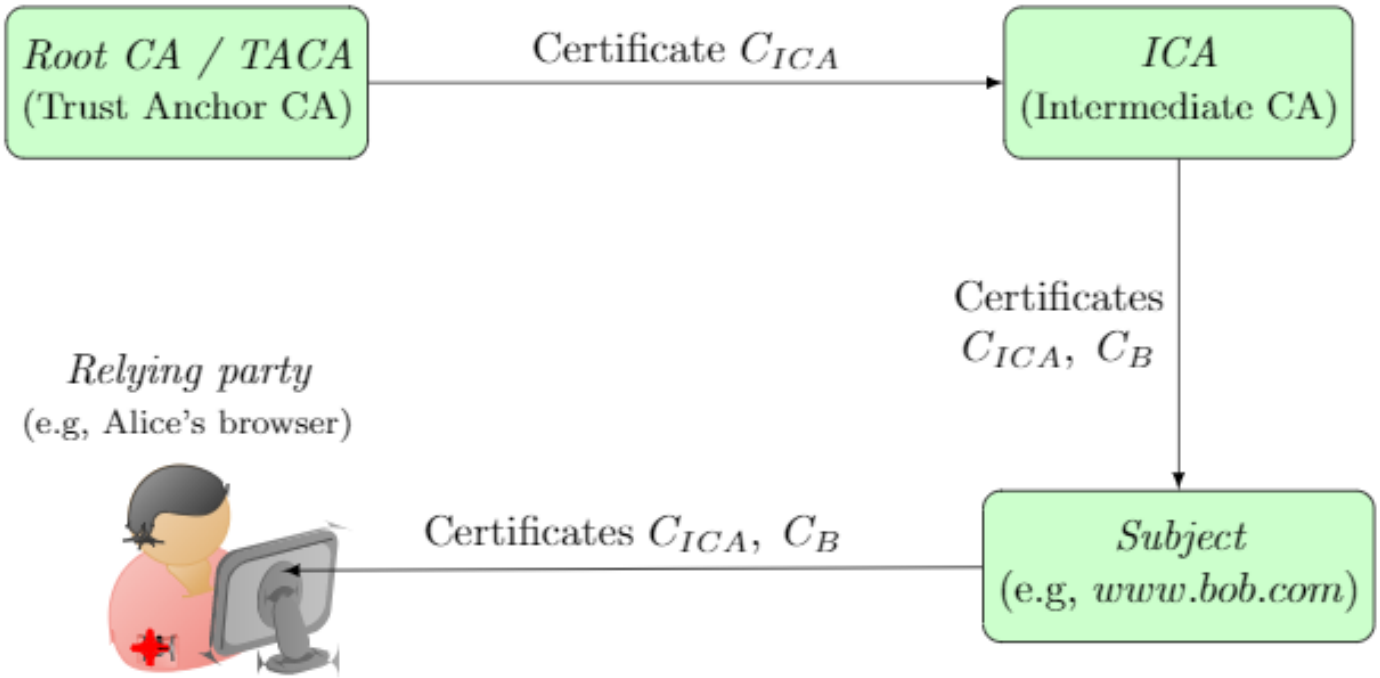
Root CAs defined by (four) **root programs**
(of Google, MS, Mozilla, Apple)

Root CA certifies **Intermediate CAs (ICA)**

Subject (website) certs issued by **intermediate CA**

Web-PKI

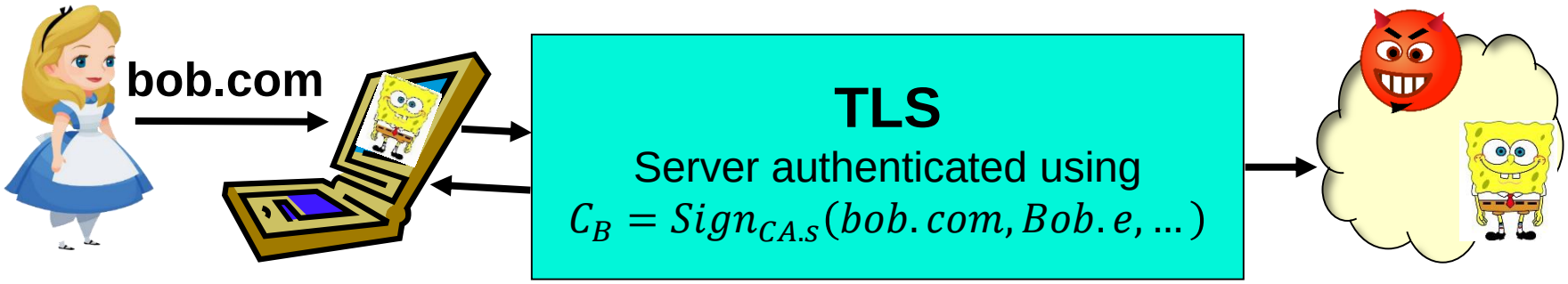
- Browsers contain keys of **Root CAs** (trust anchors)
- Root CAs defined by **root program**
  - Of Google, MS, Mozilla, Apple
- Subject (website) certs issued by root or intermediate CAs



Rogue Certificates

- Rogue cert: equivocating or misleading (domain) name
- Misleading certificates ('cybersquatting'):
  - Combo: bank.com vs. accts-bank.com, bank.accts.com, …
  - Domain-name hacking: accts.bank.com vs. accts-bank.com, … or accts-bank.co
  - Homographic: paypal.com [l is L] vs. paypaI.com [i is I]
  - Typo-squatting: bank.com vs. banc.com, baank.com, banl.com,…
  - Social-engineering attacks: exploit human vulnerabilities
    - Important, but not focus of PKI [except monitoring in Certificate Transparency]
- Threats/Exploits:
  - Impersonate: web-site, phishing email, signed malware…
  - Circumvent name-based security mechanisms: *blacklists, whitelists*, *Same-Origin-Policy (SOP)*: require equivocating cert
- PKI focuses on equivocating (same name) certificates

PKI Failures and Attack Vectors



- Is this webpage really from bob.com ?
- TLS: yes – if <u>private</u> key $Bob.d$ is not known to attacker
- Attack vectors:
  - Attacker exposes Bob's key $Bob.d$ (cryptanalysis, break-in)…
    - Mitigated by revoking certificate when suspecting exposure
  - Attacker tricks CA, gets $C_{ATK} = Sign_{CA.s}(bob.com, ATK.e, \dots)$
  - Rogue CA issues $C_{ATK} = Sign_{CA.s}(bob.com, ATK.e, \dots)$
  - Attacker exposes $CA.s$, then signs C_{ATK}
  - Root programs should not include rogue/negligent CAs

Some infamous PKI failures

2001	VeriSign: attacker gets code-signing certs
2008	Thawte: email-validation (attackers' mailbox)
2008,11	Comodo not performing domain validation
2011	DigiNotar compromised, over 500 rogue certs discovered
2011	TurkTrust issued intermediate-CA certs to users
2012	Trustwave issued intermediate-CA certificate for eavesdropping
2013	ANSSI, the French Network and Information Security Agency, issued intermediate-CA certificate to MitM traffic management device
2014	India CCA / NIC compromised (and issued rogue certs)
2015	CNNIC (China) issued CA-cert to MCS (Egypt), who issued rogue certs. Google and Mozilla removed CNNIC from their root programs.
2013-17	Audio driver of Savitech install root CA in Windows
2015,17	Symantec issued unauthorized certs for over 176 domains
2019	Mozilla, Google *software* blocks *customer-installed* Kazathhstan root CA (Qaznet)
2019	Mozilla, Google revoke intermediate-CA of DarkMatter, and refuse to add them to root program

2019: Blocking Qaznet

- Kazakhstan gov't requires installation of new root CA: Qaznet
- Detected use for MitM on users
- Mozilla, Google browsers reject Qaznet CA
  - Even when installed by user !
- Kazakhstan's response ?
  - Any Kazakhstanies here?
  - Hint: response was in 2020 ?
  - No spoilers!!
  - … Anybody from UAE here?

2017-19: DarkMatter

- DarkMatter: a UAE cybersecurity company
  - Employing Ex-NSA and Ex-NSO employees
    - NSO: Israeli surveillance company
- 2017: Intermediate-CA (from QuaVadis)
  - And: asks to be added to **root programs**

2017-19: DarkMatter

- DarkMatter: a UAE cybersecurity company
  - Employing Ex-NSA and Ex-NSO employees
    - NSO: Israeli surveillance company
- 2017: Intermediate-CA (from QuaVadis)
  - And: asks to be added to **root programs**
- 2019: refused **and** revoked by Mozilla, Google
- Why ??

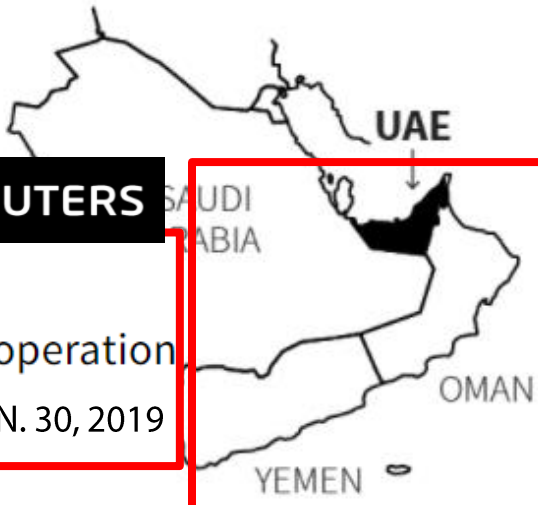
2017-19: DarkMatter

- DarkMatter: a UAE cybersecurity company
  - Employing Ex-NSA and Ex-NSO employees
    - NSO: Israeli surveillance com
- 2017: Intermediate-CA (fr
  - And: asks to be added to **root programs**
- 2019: refusec y Mozilla, Google
- Why ??

The Secret Cyberweapon

A spying squad based in Abu Dhabi used a hacking tool called Karma to spy on iPhones of opponents JAN. 30, 2019

REUTERS



REUTERS

Inside Project Raven

Reuters reveals a UAE spying operation by former NSA operatives JAN. 30, 2019

The New York Times Updated Aug. 14, 2020

a Popular Chat App. It's
Tool.

ging app that has been downloaded to
latest escalation of a digital arms race.

PKI Goals

Trustworthy issuers: Trust anchor/root CAs and Intermediary CAs; Limitations on Intermediary CAs (e.g., restricted domain names)

Transparency: public log of all certificate; no ‘hidden’ certs!

Accountability: identify issuer of given certificate

Timely, accountable, transparent revocation

Non-Equivocation: one entity – one certificate

Client privacy: why should CA know which site I use?

PKI Tutorial – CANS'20: Agenda

- **Day 1: Introduction, X.509 and constraints**
  - Introduction: certificate, PKI, failures, goals
  - **X.509**: **Certificates, names and extensions**
  - Indirect Certification in X.509: **Constraints**
- Day 2: Revocations and Merkle Digests
- Day 3: CA failures + Certificate Transparency
- Conclusions, directions and challenges

The X.500 Global Directory Standard

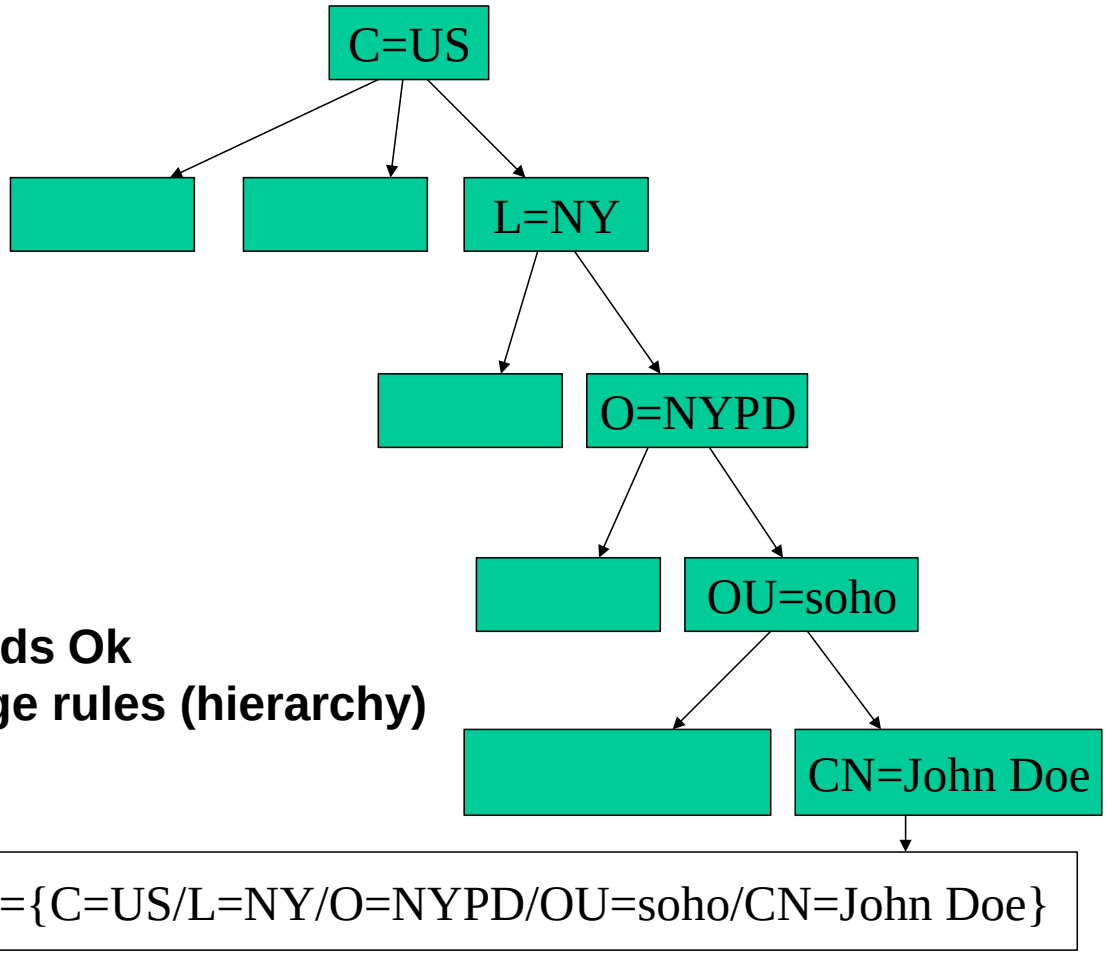
- X.500: an ITU standard, first issued 1988
  - ITU: International Telcos Union
- Idea: trusted global directory
  - Operated by hierarchy of trustworthy telcos
- Directory binds identifiers to attributes
  - Standard attributes (incl. public key)
  - Standard identifiers: Distinguished Names
- Never happened
  - Too complex, too revealing, too trusting of telcos
  - But we did get X.509 certificates – and DNs…

X.500 Distinguished Names (DN)

- Goals: meaningful, unique and decentralized identifiers
- Sequence of keywords, a string value for each of them
- Distributed directory, responsibility →*hierarchical DN*

Keyword	Meaning
C	Country
L	Locality name
O	Organization name
OU	Organization Unit name
CN	Common Name

Distinguished Name (DN) Hierarchy

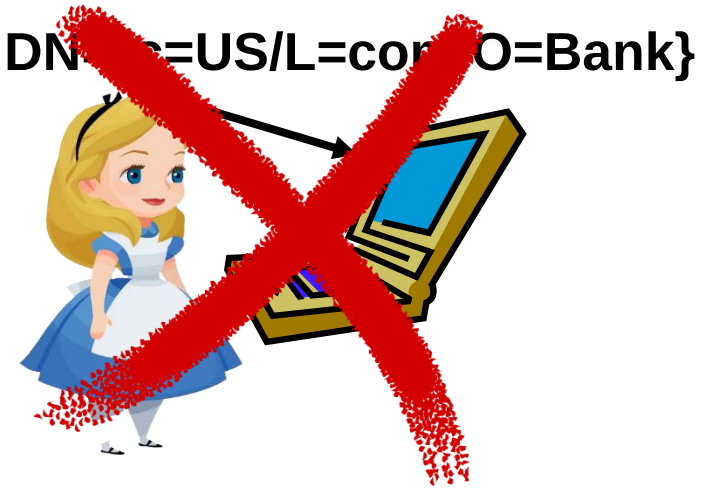


Comments:

1. **Other keywords Ok**
2. **No strict usage rules (hierarchy)**

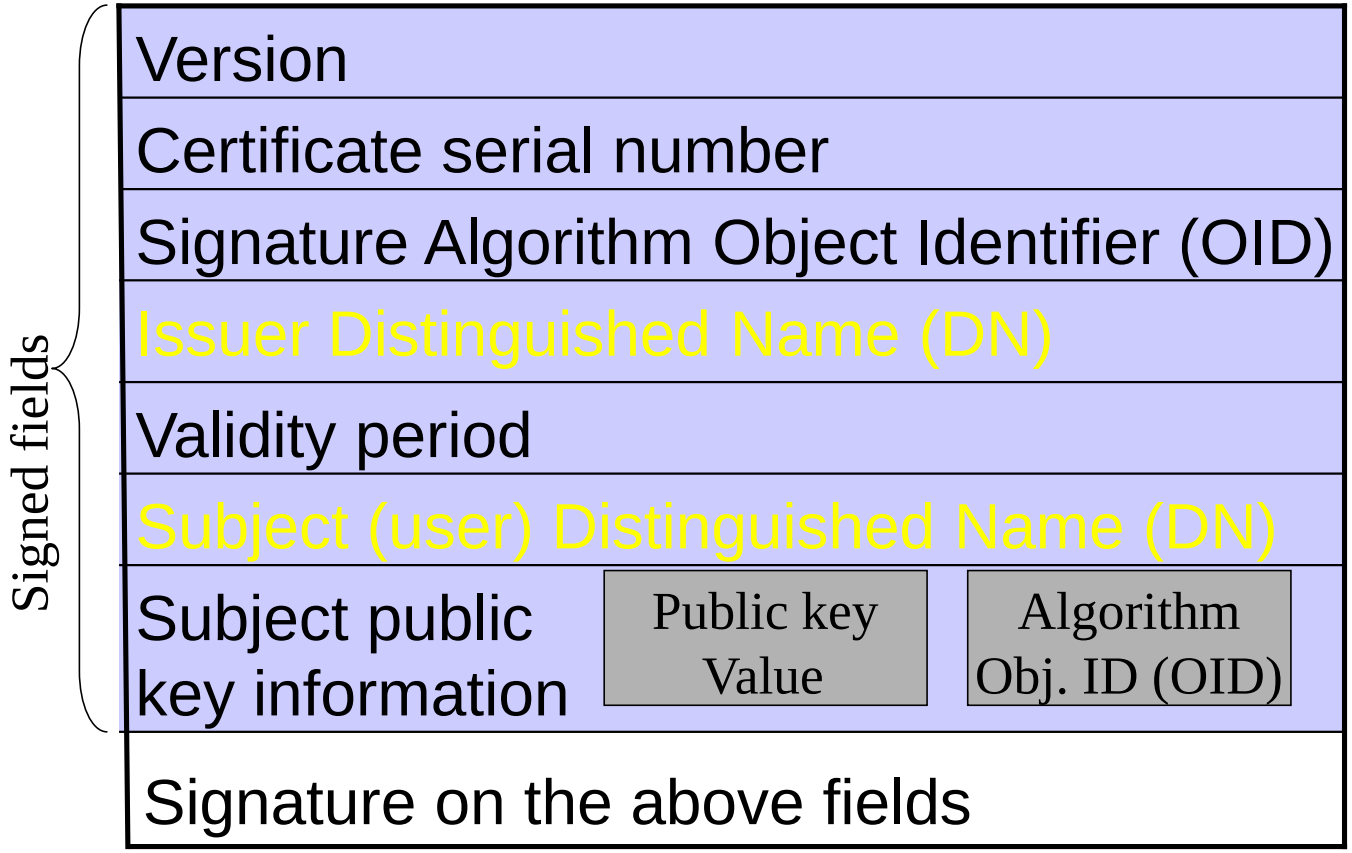
DNs aren't usable identifiers

- Relying parties (users) don't know the DN



- Internet applications use domain names, URLs
  - Even some users understand domains (in URLs) ☺
- From X.509**v3**, certs support **alternative names**
  - DNS name: `cert.SubjectAltName.dNSname`
    - Wildcard domain names: *.bank.com
  - And others, e.g., emails

X.509**v1** Public Key Certificates



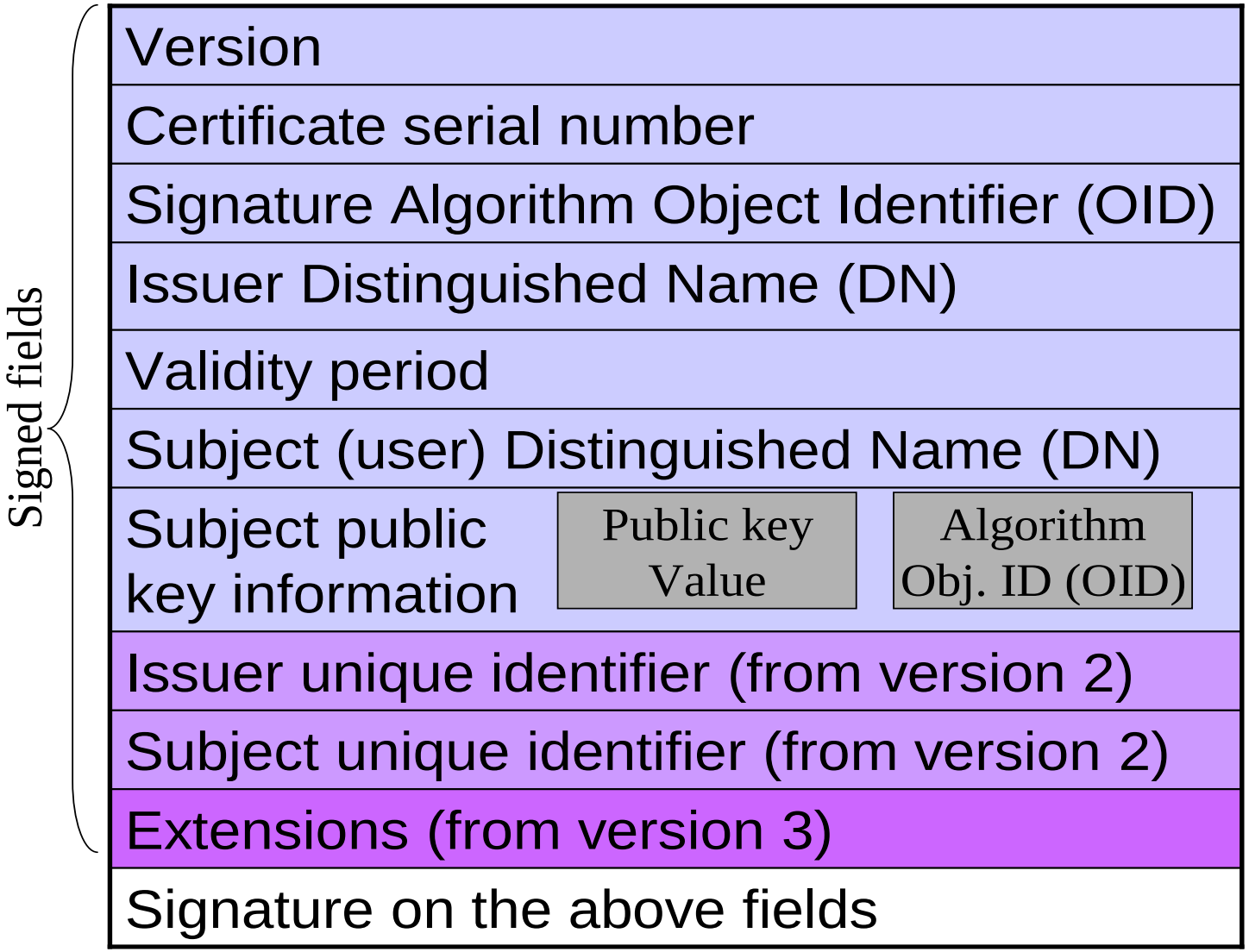
Object Identifiers (OID):

- Global, unique identifiers
- Sequence of numbers, e.g.: 1.16.840.1.45.33
  - Hierarchical

X.509 Certs & Subject Identifiers

- V1: Distinguished Name (for subject & issuer)
- V2: unique identifiers (for subject & issuer)
- **V3: extensions**
  - Some defined in X.509, others elsewhere
  - PKIX: IETF standard extensions profile
    - Widely adopted, including in SSL/TLS (& https)
  - Including SubjectAltName, IssuerAltName extensions
    - Including DNSname: identify website by domain name
- [V4: not covered, not widely deployed afaik]

X.509**v3** Public Key Certificates



X.509 V3 Extensions Mechanism

- Each extension contains…
- Extension identifier
  - As an OID (Object Identifier)
  - And as a name, e.g., SubjectAltName
- Extension value
  - E.g., `dNSName=IBM.COM`
- **Criticality indicator**
  - **If critical**, relying parties MUST NOT use a certificate with any unknown critical extension
  - **If non-critical:** use certificate w/o unknown critical extensions; **ignore** unknown (non-critical) extensions
  - X.509/PKIX: extension MUST/MAY/CAN'T be critical

SubjectAltName (SAN) Extension

- Bound identities to the subject
  - In addition/instead of Subject Distinguished Name
  - Same extension may contain multiple SANs
- Goal: unique and meaningful names
  - Common: DNS name (dNSName), e.g., a.com
    - TLS/SSL allows wildcard domains (*.a.com)
  - Or: email address, IP address, URI, other
- IssuerAltName (IAN) extensions
  - Similar – for issuer

Key Usage and Key Identifier Extensions

- Key-usage extension.
  - X.509: may be critical, PKIX: must be critical
  - Use of the public key being certified
    - Encrypt, verify-signature, verify-certificate, …
- Extended key usage extension
  - Additional optional use of the key: **Non-critical**
  - Details/restrictions related to `key usage' : **Critical**
- Subject/authority key identifier
  - Used when subject/CA has many keys; non-critical

Certificate Policy Extension

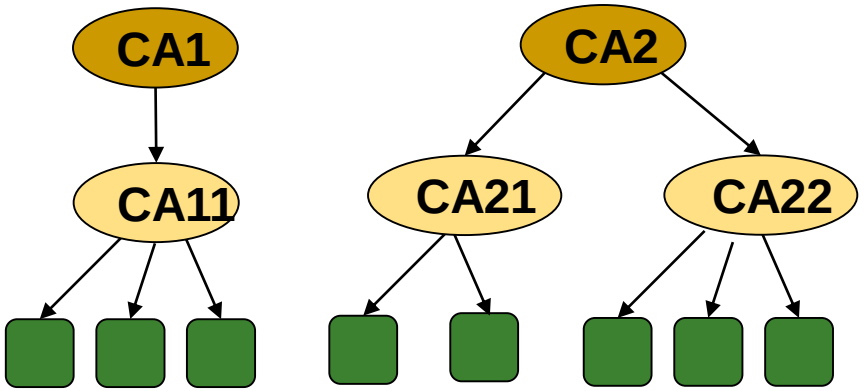
- Policies used/set by issuer
- Always critical
- Most important: method of subject validation
  - **Organization-Validated**
    - ‘Classical’ certificate; a person from CA checks subject
  - **Domain-Validated**
    - Automated check, e.g., send email to certified domain
  - **Extended validation**
    - Through checks, only for known organizations, companies
- Policy identified by Object Identifier (OID)
- **Do users know which was used? How ?**

PKI Tutorial – CANS'20: Agenda

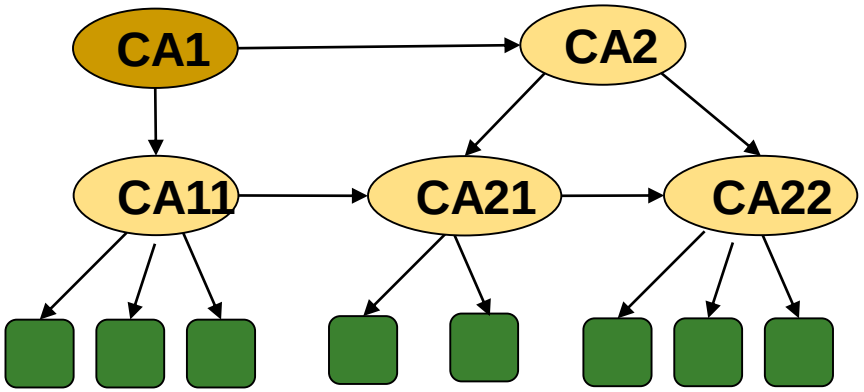
- **Day 1: Introduction, X.509 and constraints**
  - Introduction: certificate, PKI, failures, goals
  - X.509: Certificates, names and extensions
  - **Indirect Certification in X.509: Constraints**
- Day 2: Revocations and Merkle Digests
- Day 3: CA failures + Certificate Transparency
- Conclusions, directions and challenges

Certificate paths in different PKIs

- **Web/TLS PKI:** ‘root CAs’+‘intermediate CAs’:
  - Root CA issues cert for intermediate Cas

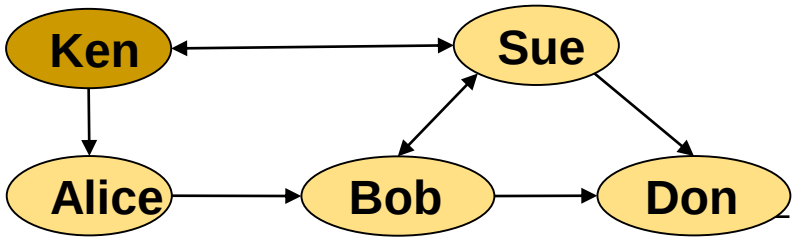


- **Web-of-Trust PKIs:**
  - Directed graph, not tree
  - Different variants/policies



Web of Trust PKI

- PGP's friends-based Web-of-Trust:
  - Everyone is subject, CA and relying party
  - As a CA, certify (pk, name) for `friends'
  - As a subject, ask friends to sign for you
  - As a relying party, trust certificates from friends
    - Or also from friends-of-friends? Your policy….
    - Should you trust all your friends (equally)?

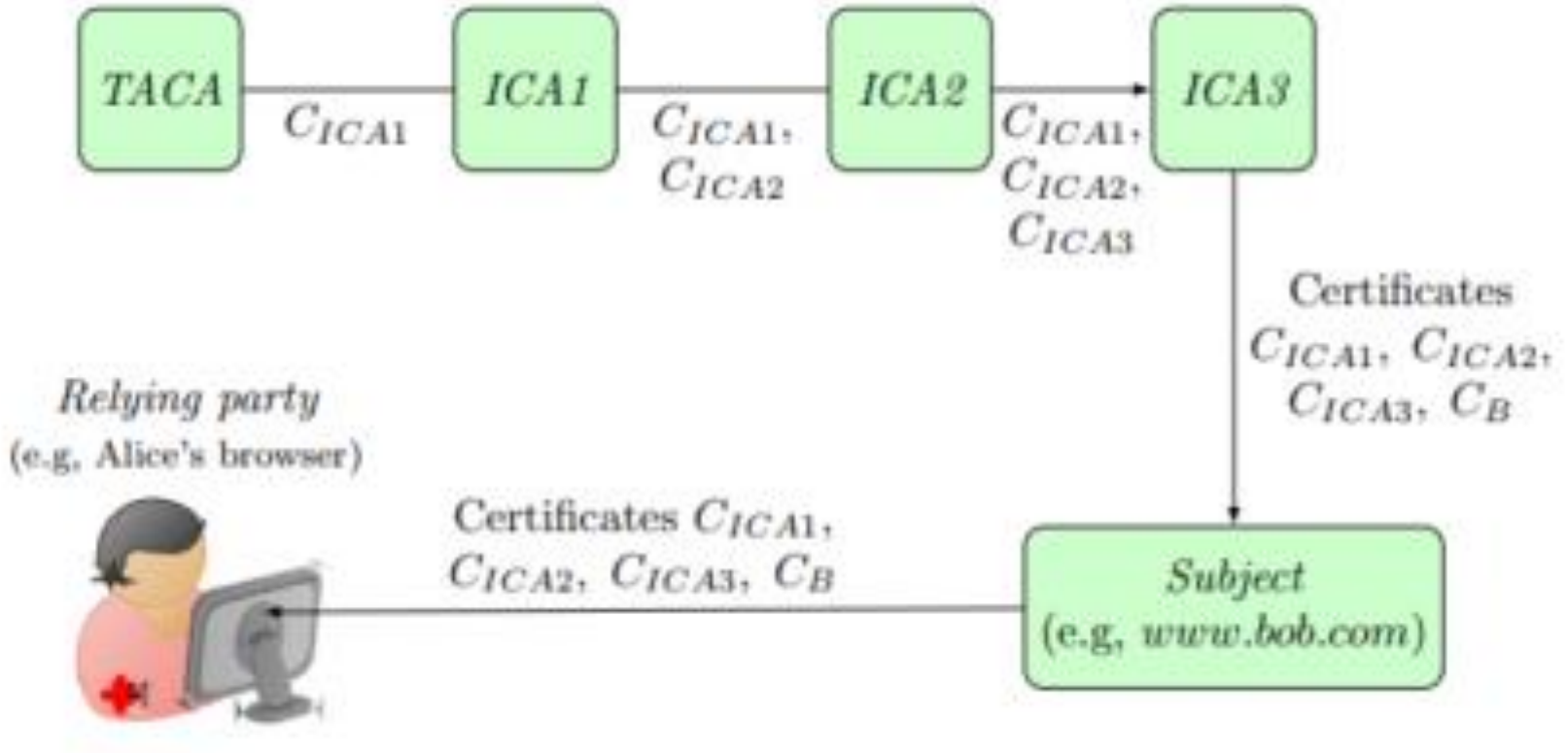


Web of Trust PKI

- PGP's friends-based Web-of-Trust:
  - Everyone is subject, CA and relying party
  - As a CA, certify (pk, name) for `friends'
  - As a subject, ask friends to sign for you
  - As a relying party, trust certificates from friends
    - Or also from friends-of-friends? Your policy….
    - Should you trust all your friends (equally)?

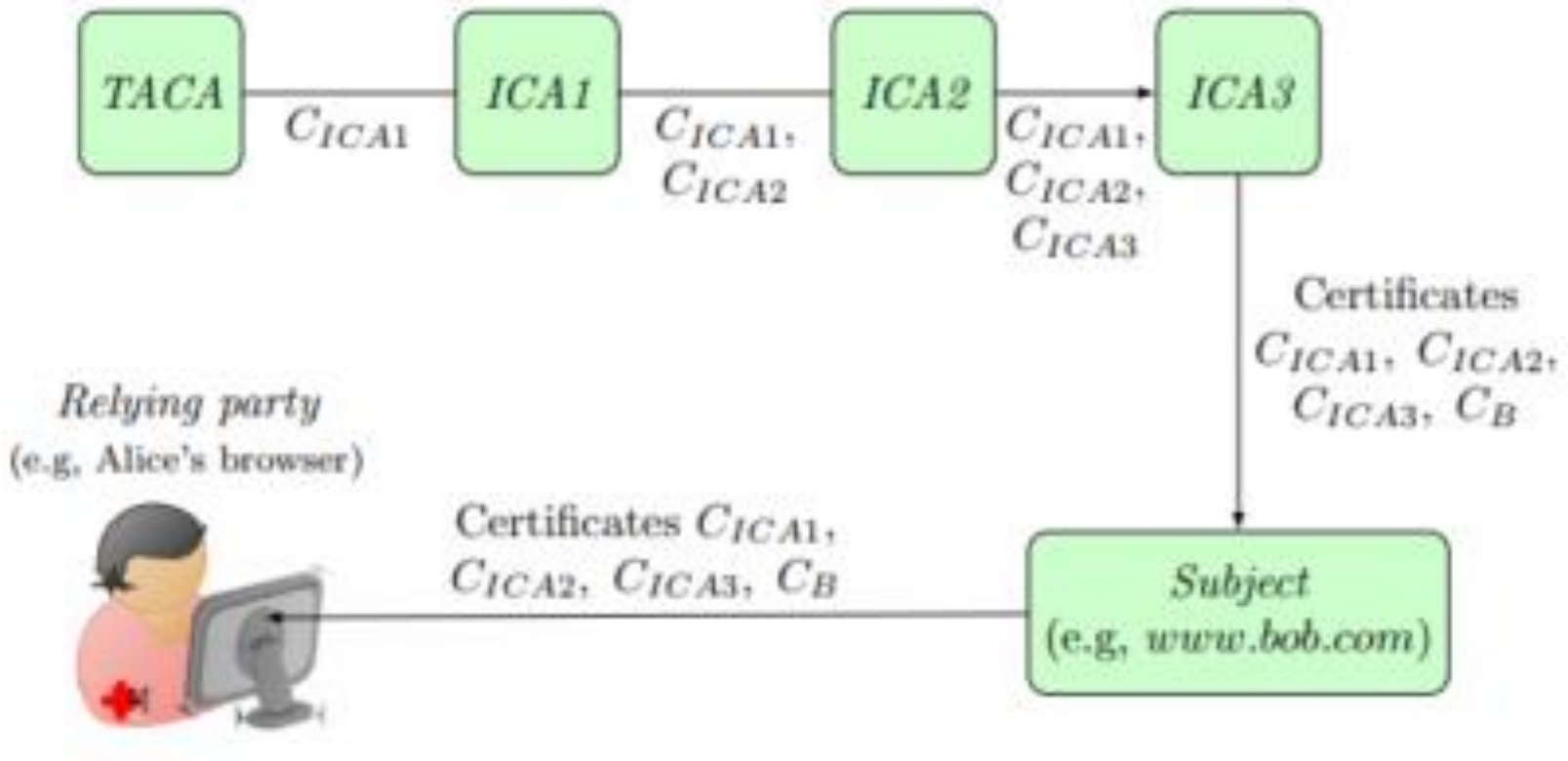
PKIX Certificate-Path: Basic Constraints

- IsCA (trust certs signed by subject)? (default: FALSE)
  - Has to be TRUE in $C_{ICA1}, C_{ICA2}, C_{ICA3}$ (False in C_B)
- pathLengthConstraint: maximal number of CAs in path
  - Has to be >2 in C_{ICA1}, >1 in C_{ICA2}

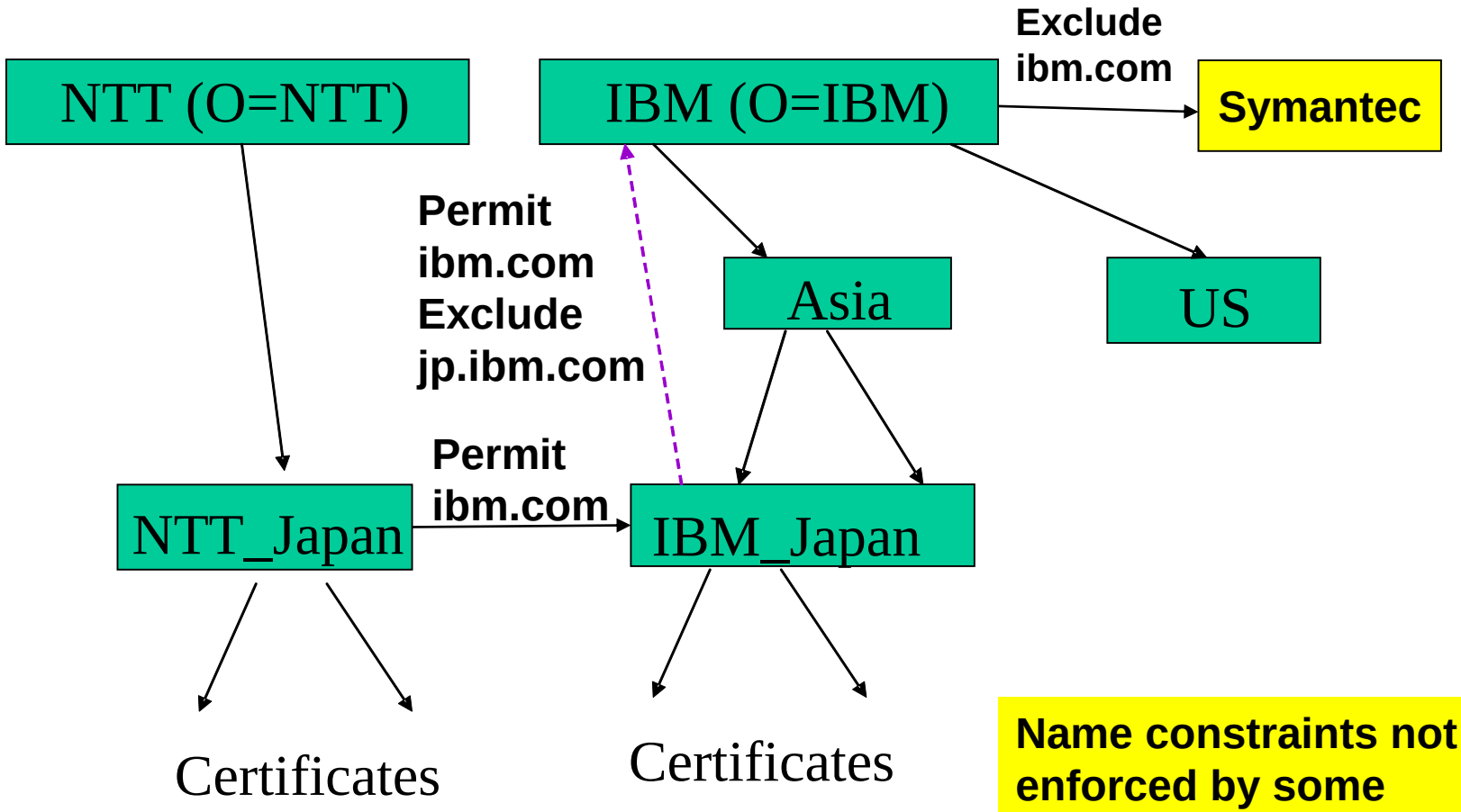


PKIX Certificate-Path: Name Constraints

- Constraints on DN and SubjectAltName
  - in certs issued by subject
- 'Permit': only allow (subdomains) of given domain
- 'Exclude': forbid (subdomains) of given domain



Name constraints on dNSName



PKI Tutorial – CANS'20: Agenda

- **Day 1: Introduction, X.509 and constraints**
- **Day 2: Revocations and Merkle Digests**
  - **The certificate revocation challenge**
  - Pre-fetching revocations: CRL, VRL, CRV
  - Just-in-Time fetching: OCSP and variants
- Day 3: CA failures + Certificate Transparency
- Conclusions, directions and challenges