Lecture 11 – Digital signatures, UF-CMA, Schnorr, PKI

TEK4500

28.10.2026

Håkon Jacobsen

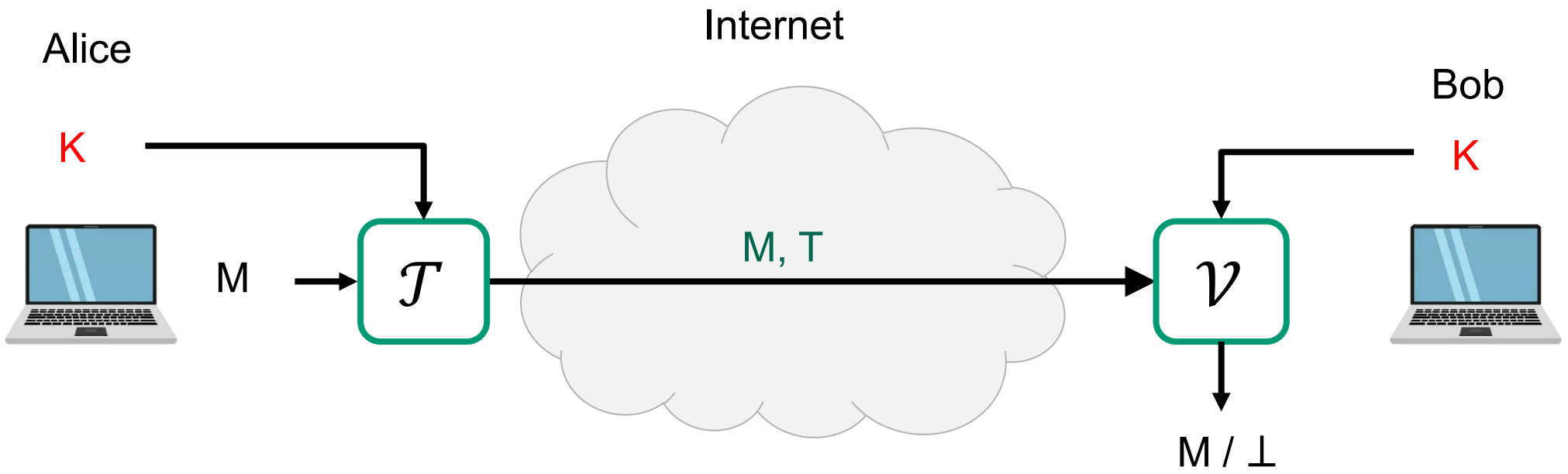
hakon.jacobsen@its.uio.no

Basic goals of cryptography

	Message privacy	**Message integrity / authentication**
Symmetric keys	Symmetric encryption	Message authentication codes (MAC)
Asymmetric keys	Public key encryption & Key enapsulation (KEM)	Digital signatures

Key exchange

MACs

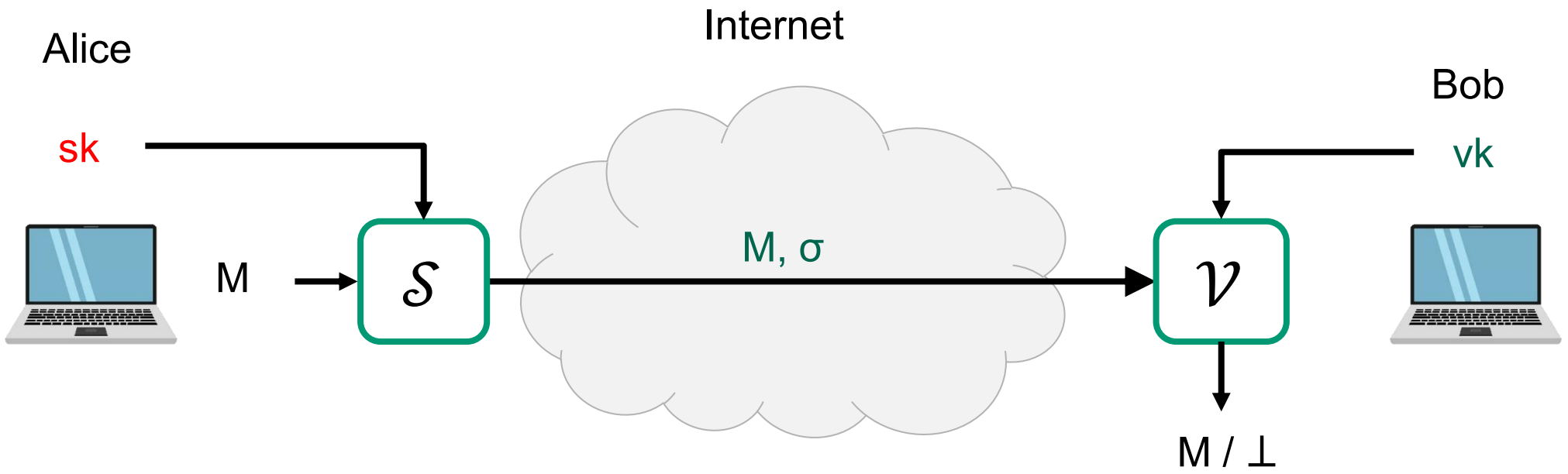


$\mathcal{T}$: tagging algorithm (public)

K : tagging / verification key (secret)

$\mathcal{V}$: verification algorithm (public)

Digital signatures



$\mathcal{S}$: signing algorithm (public)

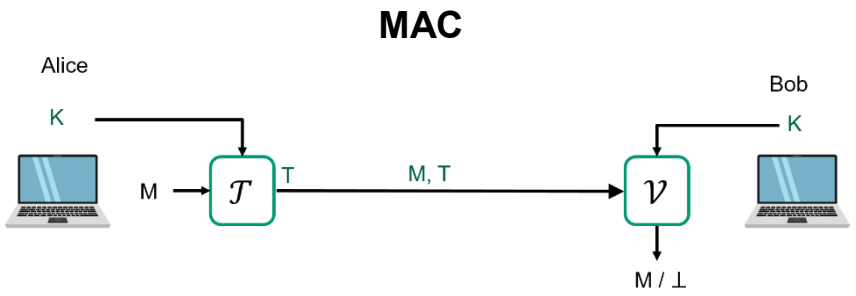
sk : signing key (secret)

$\mathcal{V}$: verification algorithm (public)

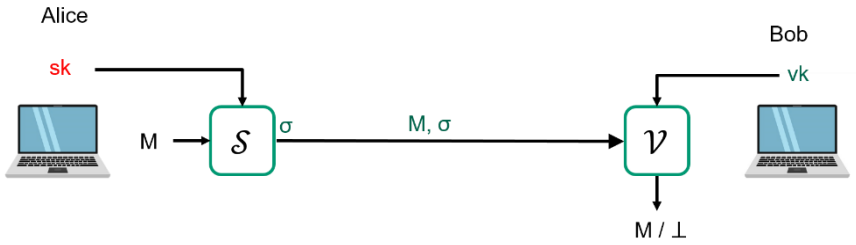
vk : verification key (public)

MACs vs. digital signatures

- MACs can only be verified by party sharing the same key



- Digital signatures can be verified by *anyone*

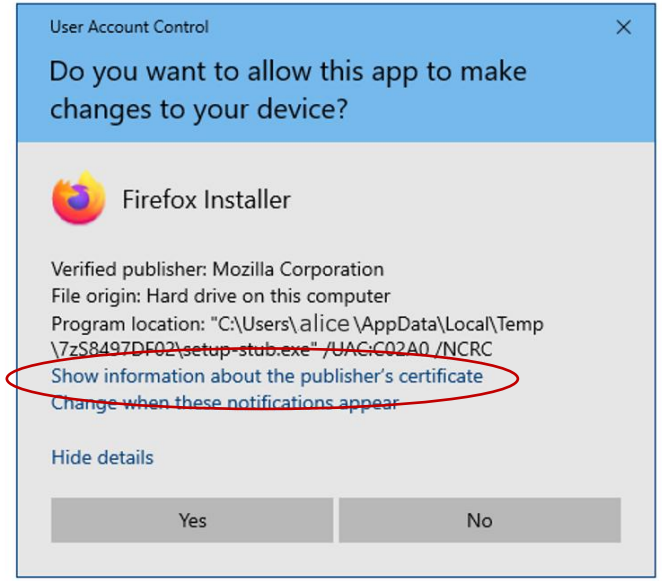


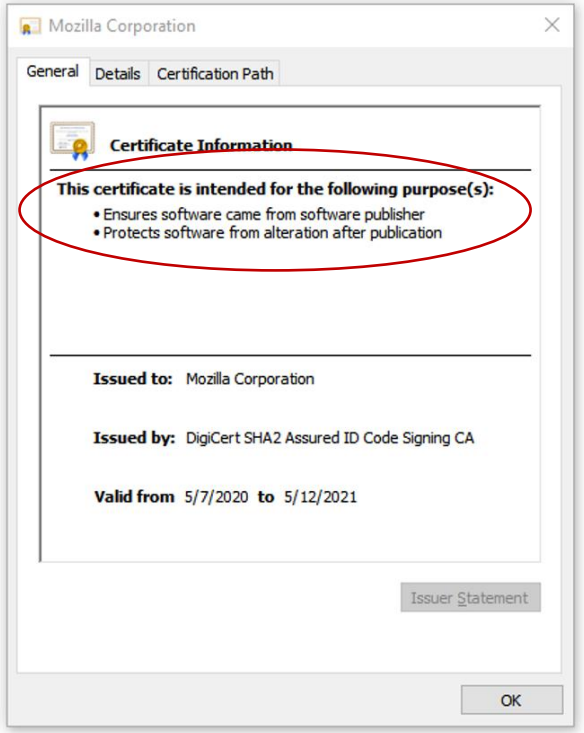
Digital signature

- **Non-repudiation:** Alice cannot deny having created σ
  - But she can deny having created T (since Bob could have done it)

Applications of digital signatures

- Electronic document signing
- HTTPS / TLS certificates
- Software installation
- Email sender authentication
- Bitcoin





Digital signatures – syntax

A **digital signature** scheme is a tuple of algorithms $\Sigma = (\text{KeyGen}, \text{Sign}, \text{Vrfy})$

$\text{KeyGen} : \mathcal{SK} \times \mathcal{VK}$

$(sk, vk) \leftarrow \text{KeyGen}$

$\text{Sign} : \mathcal{SK} \times \mathcal{M} \rightarrow \mathcal{S}$

$\text{Sign}(sk, M) = \text{Sign}_{sk}(M) = \sigma$

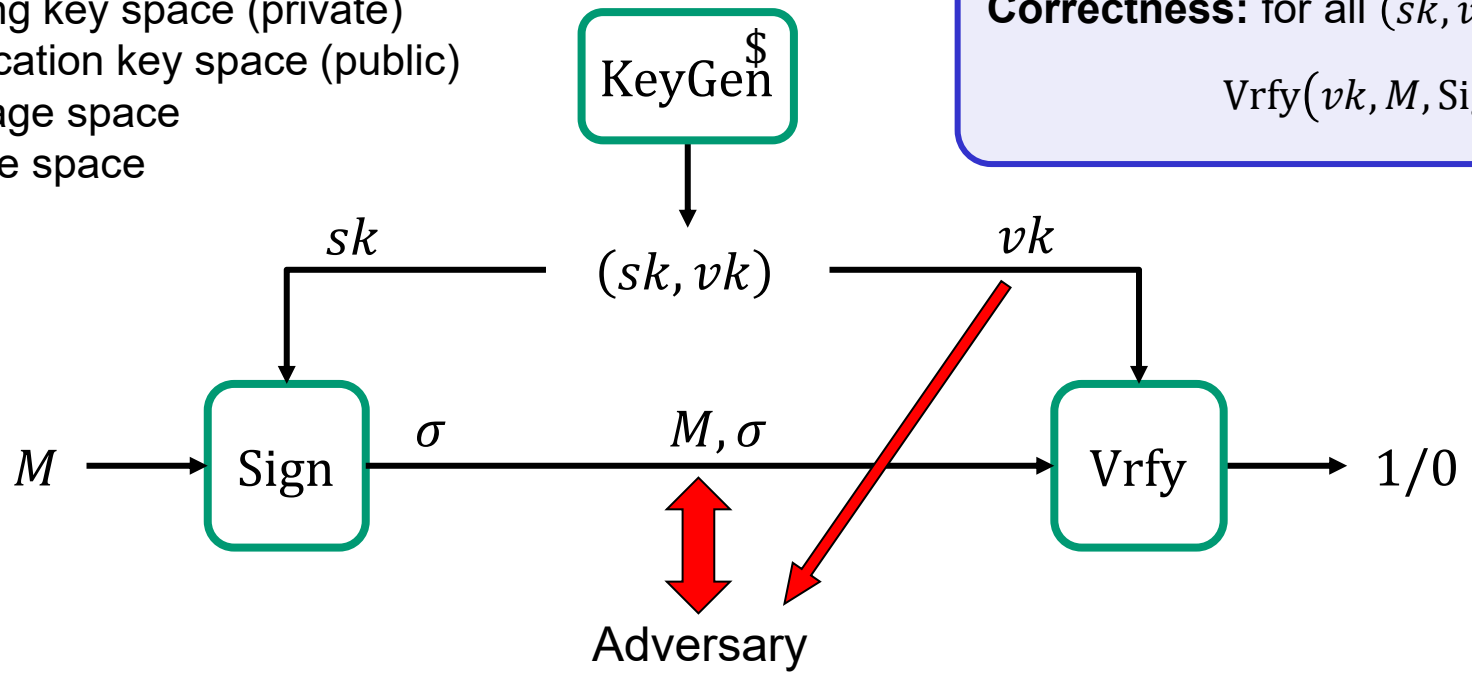
$\text{Vrfy} : \mathcal{VK} \times \mathcal{M} \times \mathcal{S} \rightarrow \{0,1\}$

$\text{Vrfy}(vk, M, \sigma) = \text{Vrfy}_{vk}(M, \sigma) = 1/0$

- $\mathcal{SK}$ – signing key space (private)
- $\mathcal{VK}$ – verification key space (public)
- $\mathcal{M}$ – message space
- $\mathcal{S}$ –signature space

Correctness: for all $(sk, vk) \leftarrow \text{KeyGen}$:

$$\text{Vrfy}\big(vk, M, \text{Sign}(sk, M)\big) = 1$$



7

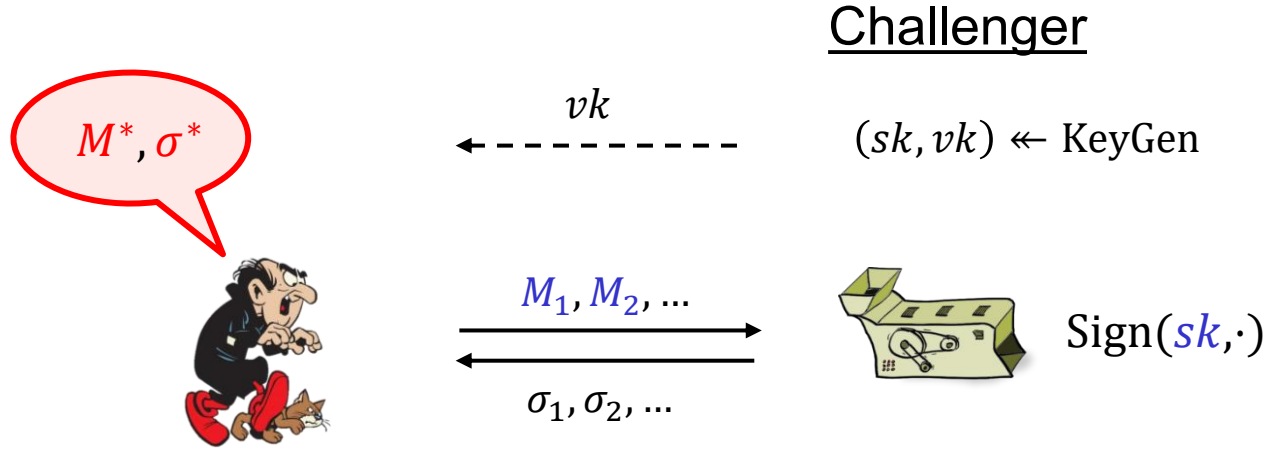
Digital signatures – security: UF-CMA

$\mathbf{Exp}_{\Sigma}^{\text{uf-cma}}(A)$

1. $(sk, vk) \leftarrow \Sigma.\text{KeyGen}$
2. $\text{Msgs} \leftarrow [\,]$ // bookkeeping
3. $(M^*, \sigma^*) \leftarrow A^{\mathcal{S}(\cdot)}(vk)$
4. $d \leftarrow \Sigma.\text{Vrfy}(vk, M^*, \sigma^*)$
5. **return** $d \stackrel{?}{=} 1$ **and** $M^* \notin \text{Msgs}$

$\mathcal{S}(M)$

1. $\sigma \leftarrow \Sigma.\text{Sign}(sk, M)$
2. $\text{Msgs.add}(M)$
3. **return** σ

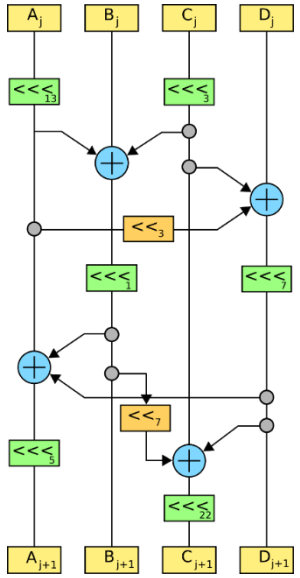


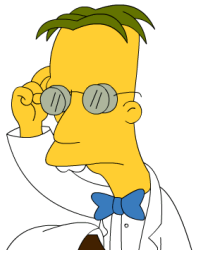
A has **forged** a signature if

- σ^* is a valid signature for M^*
- $M^* \notin \{M_1, M_2, \ldots\}$

Definition: The **UF-CMA-advantage** of an adversary A is

$$\mathbf{Adv}_{\Sigma}^{\text{uf-cma}}(A) = \Pr\left[\mathbf{Exp}_{\Sigma}^{\text{uf-cma}}(A) \Rightarrow 1\right]$$





Designing signature schemes

DLOG proof of knowledge

$A = g^a$ $(G,\star) = \langle g \rangle$



a



accept if $g^a = A$

Proof requirements

1. If Alice knows a she can get Bob to accept ✓
2. If Alice doesn't know a she can't get Bob to accept ✓
3. Bob learns nothing about a from the interaction ✗

DLOG proof of knowledge

$A = g^a$ $\quad (\boldsymbol{G}, \star) = \langle g \rangle$



$a + r \pmod{|\boldsymbol{G}|}$



$r \twoheadleftarrow \{1, \ldots, |\boldsymbol{G}|\}$

Proof requirements

1. If Alice knows a she can get Bob to accept **?**
2. If Alice doesn't know a she can't get Bob to accept **?**
3. Bob learns nothing about a from the interaction ✓

DLOG proof of knowledge

$A = g^a$ $\quad (\boldsymbol{G}, \star) = \langle g \rangle$





r

$r \leftarrow \{1, \ldots, |\boldsymbol{G}|\}$ $\quad a + r \pmod{|\boldsymbol{G}|}$ $\quad$ accept if $g^{z-r} = A$

z

Proof requirements

1. If Alice knows a she can get Bob to accept ✓
2. If Alice doesn't know a she can't get Bob to accept ✓
3. Bob learns nothing about a from the interaction ✗

DLOG proof of knowledge

$A = g^a$ $\qquad$ $(\boldsymbol{G}, \star) = \langle g \rangle$





$R = g^r$

$r \leftarrow \{1, \ldots, |\boldsymbol{G}|\}$ $\qquad$ $a + r \pmod{|\boldsymbol{G}|}$ $\qquad$ accept if $A \star R = g^z$

z

Proof requirements

1. If Alice knows a she can get Bob to accept ✓
2. If Alice doesn't know a she can't get Bob to accept ✗
3. Bob learns nothing about a from the interaction ✓

$A \star R = g^a g^r = g^{a+r} = g^z$

$R \leftarrow A^{-1} \star g^z \implies A \star R = A \star A^{-1} \star g^z = g^z$

(one-time pad + DLOG)

DLOG proof of knowledge

$A = g^a$ $\quad (\boldsymbol{G}, \star) = \langle g \rangle$





$R = g^r$ →

$r \leftarrow \{1, \ldots, |\boldsymbol{G}|\}$ $\quad$ ← b $\quad$ $b \leftarrow \{1, \ldots, |\boldsymbol{G}|\}$

$ab + r \pmod{|\boldsymbol{G}|}$ →

accept if $A^b \star R = g^z$

z

Proof requirements

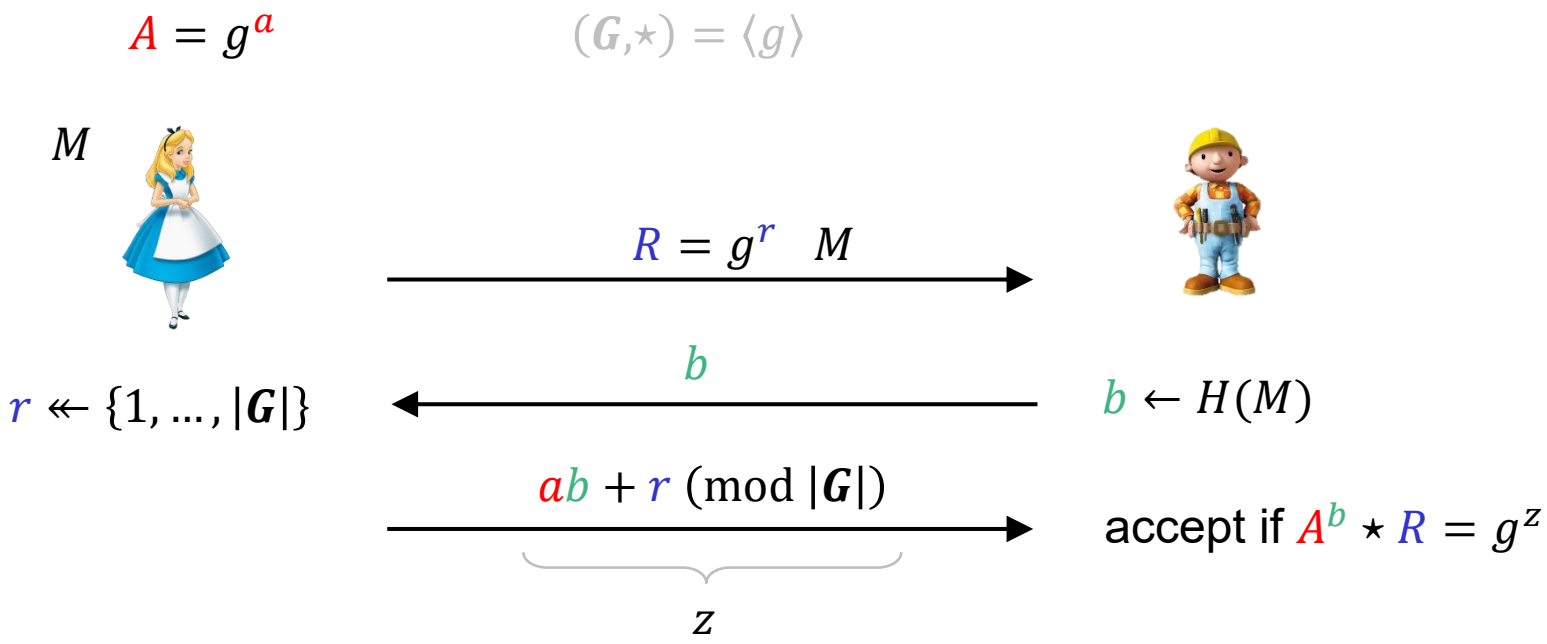
1. If Alice knows a she can get Bob to accept ✓
2. If Alice doesn't know a she can't get Bob to accept ✓
3. Bob learns nothing about a from the interaction ✓

$A^b \star R = g^{ab} g^r = g^{ab+r} = g^z$

$R \leftarrow A^{-1} \star g^z \implies A^b \star R = A^b \star A^{-1} \star g^z \neq g^z$

(one-time pad + DLOG)

Interactive signature scheme



Proof requirements

1. If Alice knows a she can get Bob to accept ✓
2. If Alice doesn't know a she can't get Bob to accept ✓
3. Bob learns nothing about a from the interaction ✓

Non-interactive signature scheme

$A = g^a$ $\quad (\boldsymbol{G}, \star) = \langle g \rangle$

M 

$R = g^r$ 

b

$r \leftarrow \{1, \dots, |\boldsymbol{G}|\}$

$b \leftarrow H(M)$

$ab + r \pmod{|\boldsymbol{G}|}$

z

accept if $A^b \star R = g^z$ and $H(M) = b$

Proof requirements

1. If Alice knows a she can get Bob to accept ✓
2. If Alice doesn't know a she can't get Bob to accept ✓
3. Bob learns nothing about a from the interaction ✓

Non-interactive signature scheme

$A = g^a$ $\quad (G,\star) = \langle g \rangle$

M





3 $\quad R = A^{-b} \star g^z$

2 $\quad b$

$r \leftarrow \{1, \ldots, |G|\}$

1 $\quad z$

$b \leftarrow H(M)$

accept if $A^b \star R = g^z$ and $H(M) = b$

z

Proof requirements

1. If Alice knows a she can get Bob to accept ✓
2. If Alice doesn't know a she can't get Bob to accept ✘
3. Bob learns nothing about a from the interaction ✓

$A^b \star R = A^b A^{-b} \star g^z = g^z$

Non-interactive signature scheme

$A = g^a$ $\quad (\boldsymbol{G}, \star) = \langle g \rangle$

M





$R = g^r$

b

$r \leftarrow \{1, \ldots, |\boldsymbol{G}|\}$

$\sigma = (R, b, z)$

$b \leftarrow H(A, R, M)$

$ab + r \pmod{|\boldsymbol{G}|}$

accept if $A^b \star R = g^z$ and $H(A, R, M) = b$

z

Proof requirements

1. If Alice knows a she can get Bob to accept ✓
2. If Alice doesn't know a she can't get Bob to accept ✓
3. Bob learns nothing about a from the interaction ✓

Schnorr signature scheme

KeyGen

1. $a \twoheadleftarrow \{1 \dots |\boldsymbol{G}|\}$
2. $A \leftarrow g^a$
3. **return** $(sk = a, vk = A)$

$(\boldsymbol{G}, \star) = \langle g \rangle$

Sign$(sk = a, M)$

1. $r \twoheadleftarrow \{1 \dots |\boldsymbol{G}|\}$
2. $R \leftarrow g^r$
3. $b \leftarrow H(A, R, M)$
4. $z \leftarrow ab + r \pmod{|\boldsymbol{G}|}$
5. $\sigma \leftarrow (R, b, z)$
6. **return** σ

$R = g^r$

b

$ab + r \pmod{|\boldsymbol{G}|}$

z



$\sigma = (R, b, z)$

Verify$(vk = A, M, \sigma = (R, b, z))$

1. **return** $A^b \star R \stackrel{?}{=} g^z$ and $H(A, R, M) \stackrel{?}{=} b$

Correctness:

$$A^b \star R = g^{ab} \star g^r = g^{ab+r} = g^z$$

r must be picked new *every time*!

Security: The Schnorr signature is UF-CMA secure if:

- The DLOG problem is hard in $(\boldsymbol{G}, \star)$
- The hash function H is modelled as a *random oracle*

$$\left.\begin{array}{l}\sigma = (R, b, z) \\ \sigma' = (R, b', z')\end{array}\right\} \Rightarrow z - z' = (ab + r) - (ab' + r) = a \cdot (b - b')$$

$$\Rightarrow a = (z - z') \cdot (b - b')^{-1} \bmod |\boldsymbol{G}|$$

Learned private signing key!

Discrete-log-based signatures

- Schnorr
  - Elegant design
  - Has formal security proof (based on DLOG problem and H assumed perfect)
  - Was patented

- (EC)DSA
  - Non-patented alternative
  - More complicated design than Schnorr
  - No security proof
  - Standardized by NIST (designed by the NSA)
  - Very widely used
  - Same sharp edge as Schnorr
    - Reuse of r leaks long-term signing key
    - Broke all PlayStation 3's produced by Sony





Public-key infrastructure (PKI)

What are identities?



"Alice", g^a

"Bob", g^b



$K \leftarrow g^{ab}$

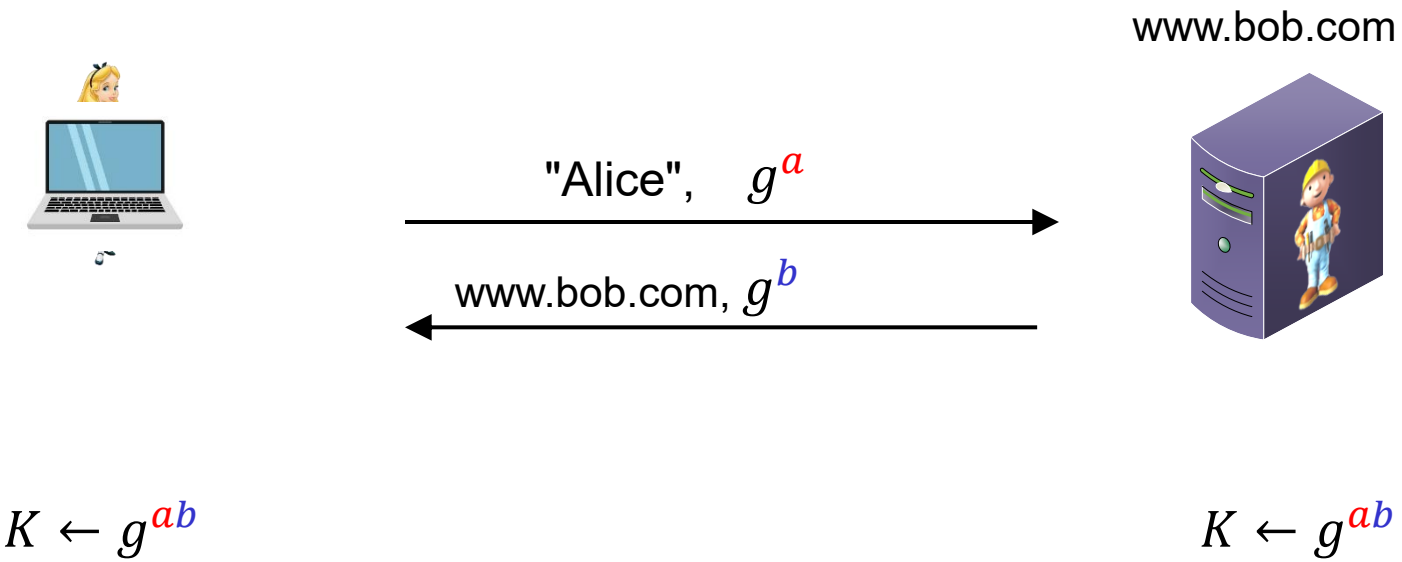
$K \leftarrow g^{ab}$

There are many Alice's and many Bob's

How do we know that g^a belongs to *this* particular Alice, and g^b to this particular Bob?

Need to **bind** public keys to entities

Identities on the internet

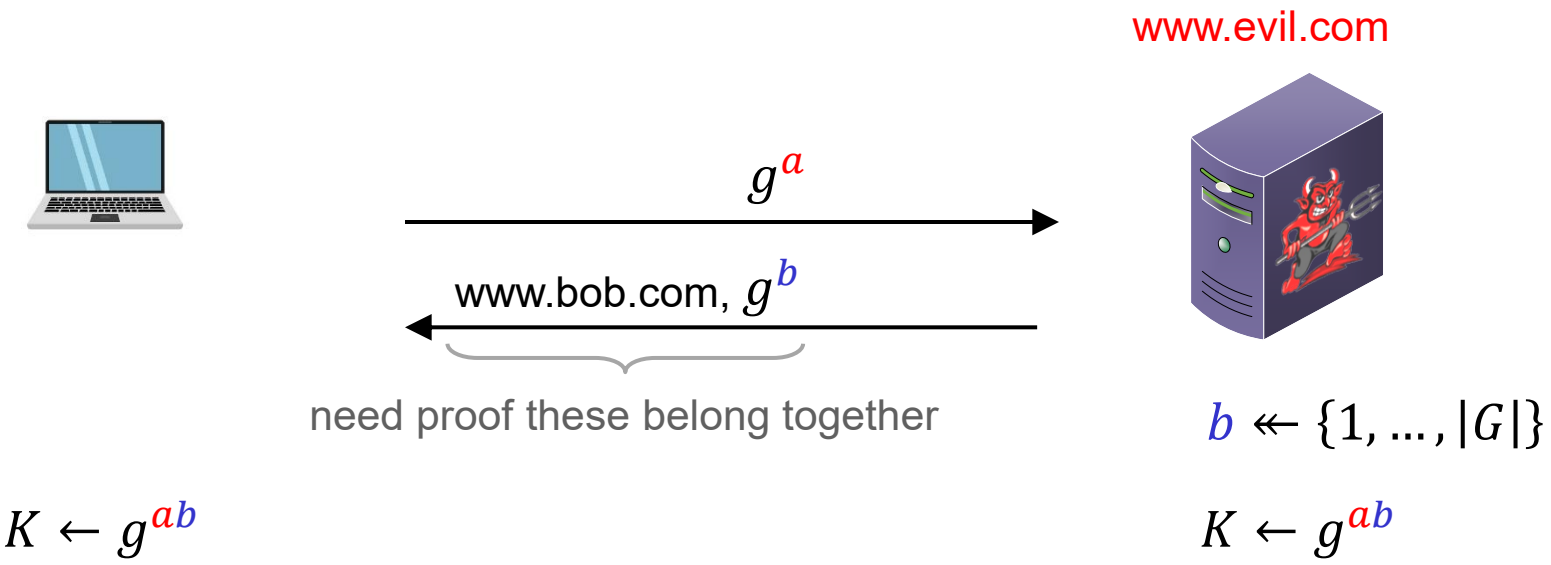


There are many Alice's and many Bob's

How do we know that g^a belongs to *this* particular Alice, and g^b to this particular Bob?

Need to **bind** public keys to entities – internet: bind public keys to **domain names**

Identities on the internet

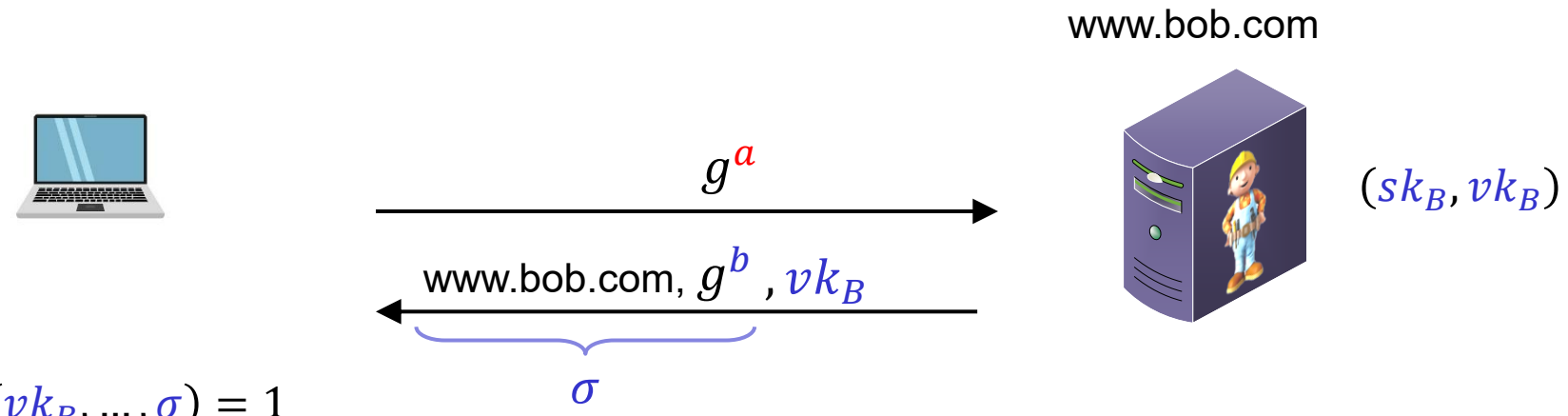


There are many Alice's and many Bob's

How do we know that g^a belongs to *this* particular Alice, and g^b to this particular Bob?

Need to **bind** public keys to entities – internet: bind public keys to **domain names**

Authenticated key exchange



if $\text{Vrfy}(vk_B, \ldots, \sigma) = 1$

$K \leftarrow g^{ab}$

else

abort

$K \leftarrow g^{ab}$

But why should we trust this vk_B? Could have been created by the adversary itself

Digital certificates

- **Digital certificate:** a way of binding a public key to an entity



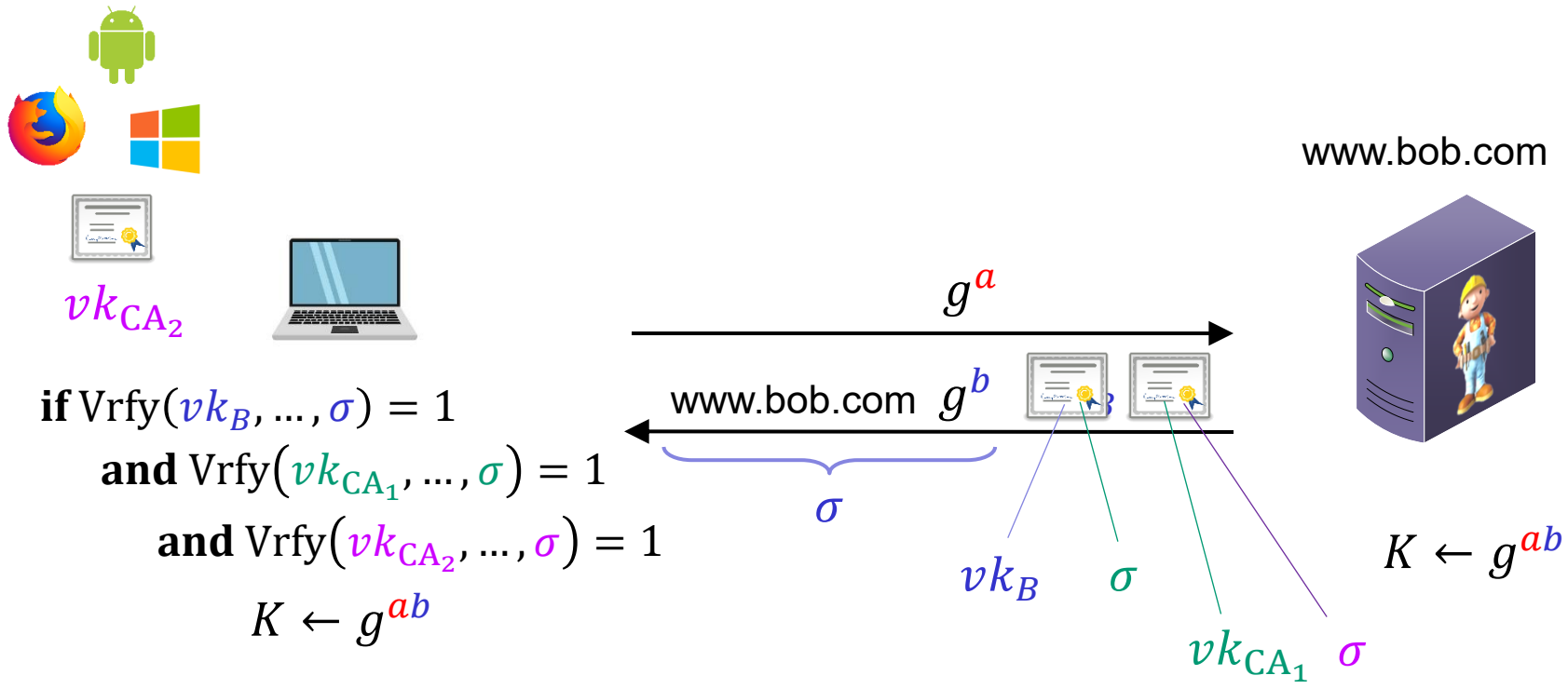
- A certificate consists of:
  - The public key of the entity
  - A bunch of information identifying the entity
    - Name
    - Address
    - Occupation
    - URL
    - Email-address
    - Phone number
    - …
  - A *digital signature* on all the above by a **certificate authority (CA)**

Certificate authorities (CA)

- **CA:** an issuer of digital certificates
- Acts as a trusted third-party, certifying (i.e., signing) the public keys of other entities
  - Verifies the identity of a claimed public-key owner
- The basis of a **public-key infrastructure (PKI)**



Authenticated key exchange + PKI



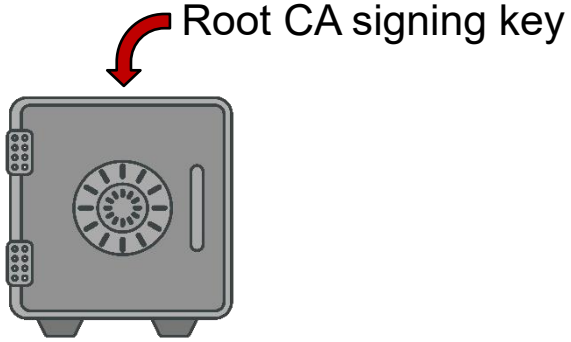
if $\mathrm{Vrfy}(vk_B, \ldots, \sigma) = 1$
  and $\mathrm{Vrfy}(vk_{\mathrm{CA}_1}, \ldots, \sigma) = 1$
    and $\mathrm{Vrfy}(vk_{\mathrm{CA}_2}, \ldots, \sigma) = 1$
      $K \leftarrow g^{ab}$

else
  abort

Root CAs

- **Root CAs:** CAs that sign other CAs' public keys
  - \+ only a few root CAs need to be trusted by end-users
  - \+ root CAs can distribute the signing + verification load to smaller CAs
  - \- single point of failure; private key must be *very heavily* guarded

  - Root CAs for the internet: a few large multinational corporations



COMODO

IdenTrust part of HID Global

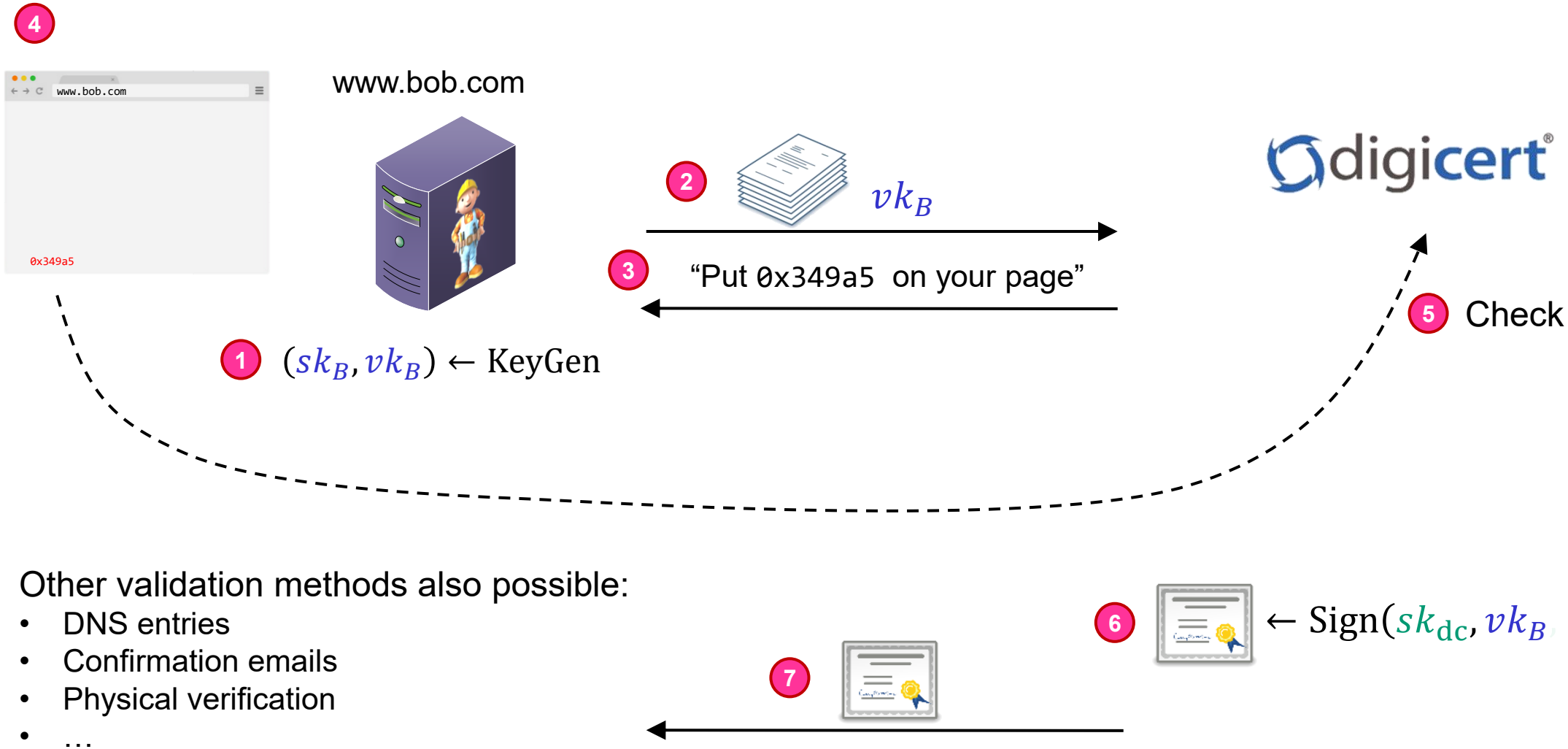
digicert

GoDaddy



Let's Encrypt

How to get a signed certificate?



Other validation methods also possible:

- DNS entries
- Confirmation emails
- Physical verification
- …

How to become an internet root CA?

- Need to prove yourself (trust)worthy to browser and OS vendors
  - Microsoft Root Certificate Program
  - Mozilla CA Certificate Program
  - Apple Root Certificate Program
  - Chrome Root CA Program



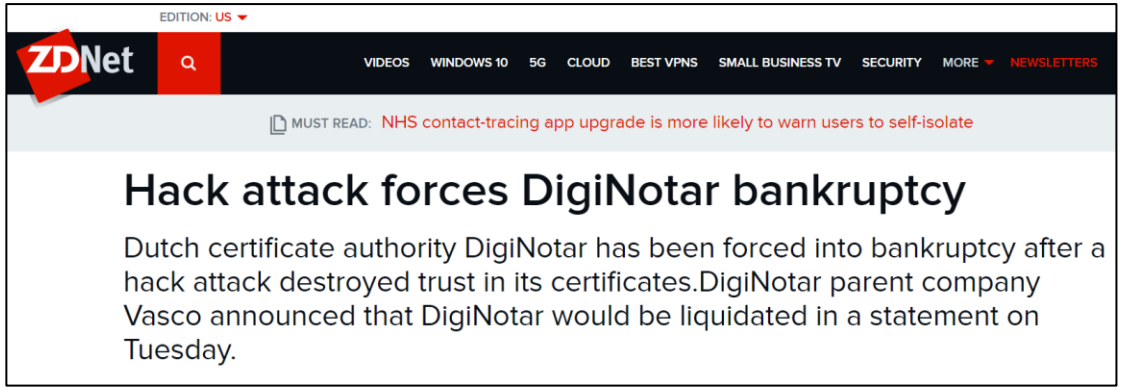
- Lot's of auditing and paperwork

- Many formal technical and non-technical security requirements
  - CA/Browser forum
  - Baseline Requirements v1.7.3

DigiNotar

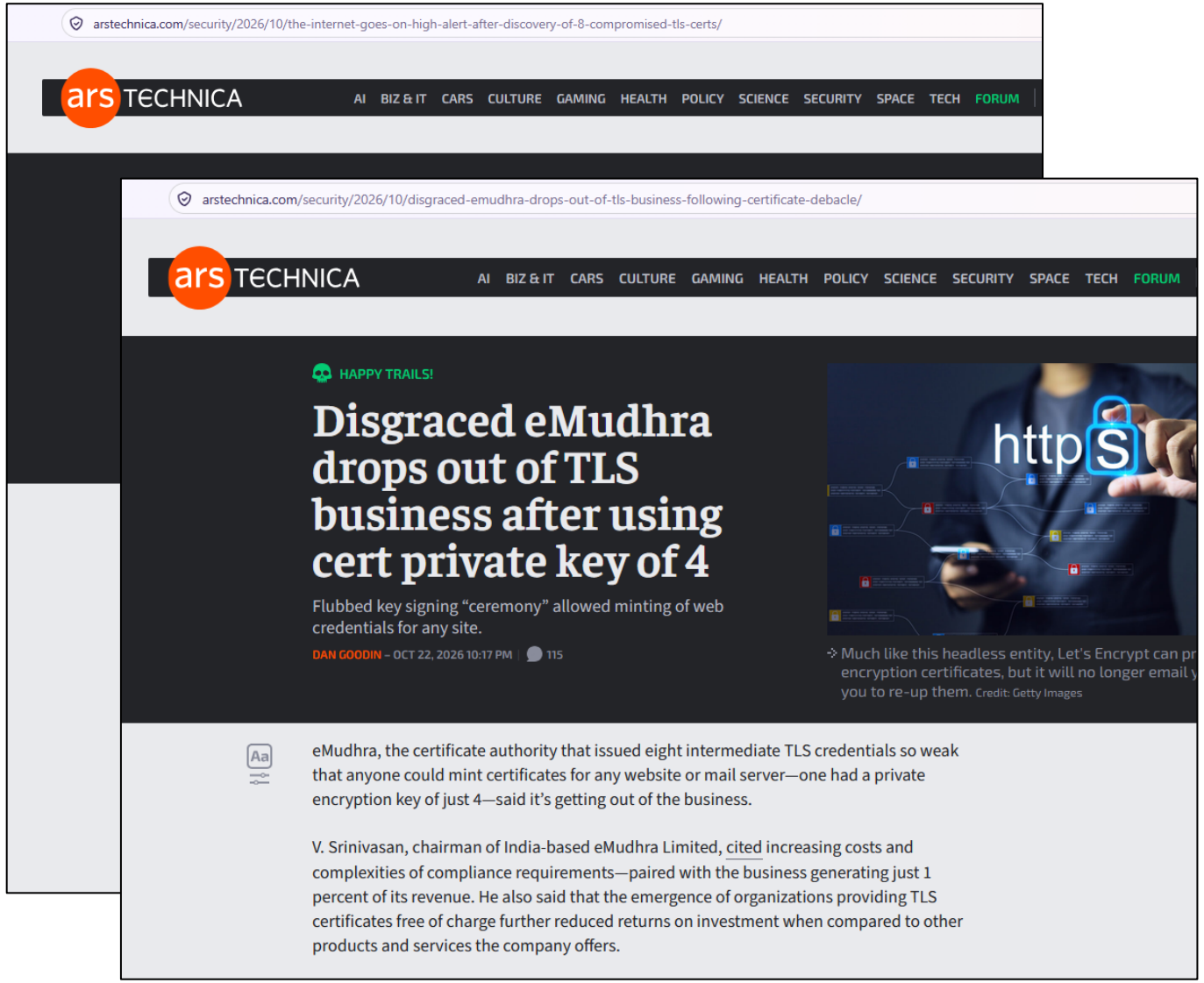
- Dutch root CA
- Lost control of their private signing key in 2011
- Fraudulent certificates issued for Gmail, Yahoo!, Mozilla, WordPress, …
- 30 000 Iranian Gmail users targeted





eMudhra

- Indian intermediate CA
- Created 8 CA certs where the private signing keys were (literally) numbers between 0 and 255!
- Apparently due to confusing test certs with production certs
- …no longer in the CA business



The problem with CAs

- Trusted third-parties on the Internet
  - One compromised CA enough to imitate *any* website on the Internet

- Lots of CAs compromised throughout the years

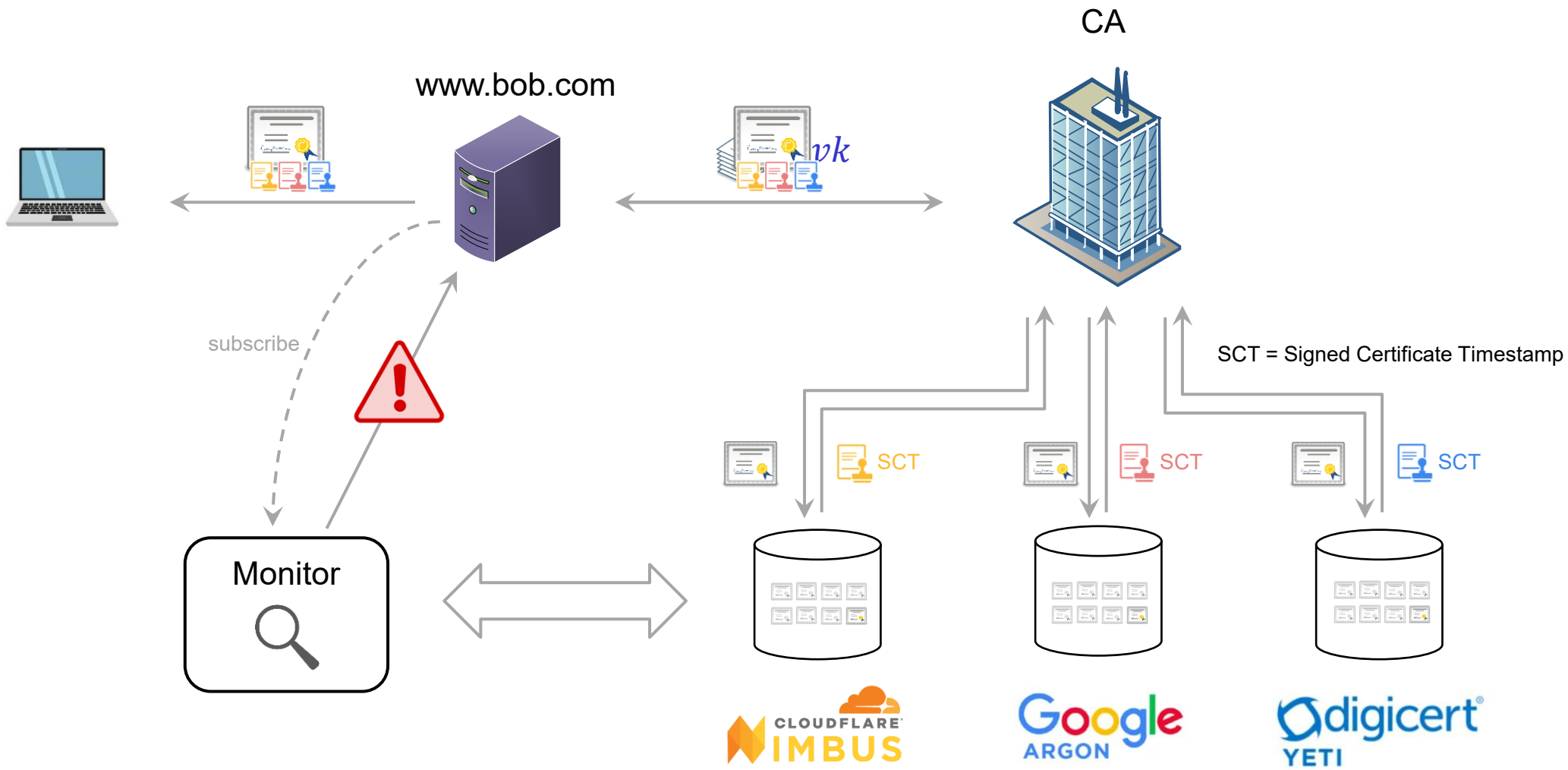
- Even more insidious:

  How do we know that CAs don't issue unauthorized certificates at the behest of government agencies?



- Above problems led to **Certificate Transparency**
  - Effort to keep CAs honest

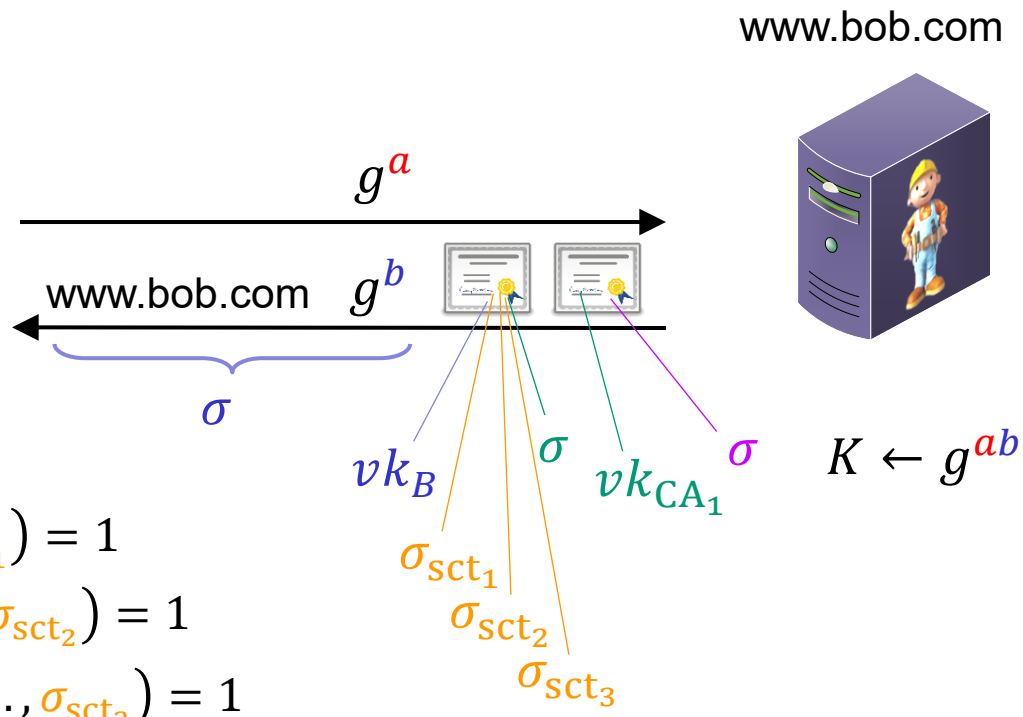
Certificate Transparency



Certificate Transparency Logs

Authenticated key exchange + PKI + CT



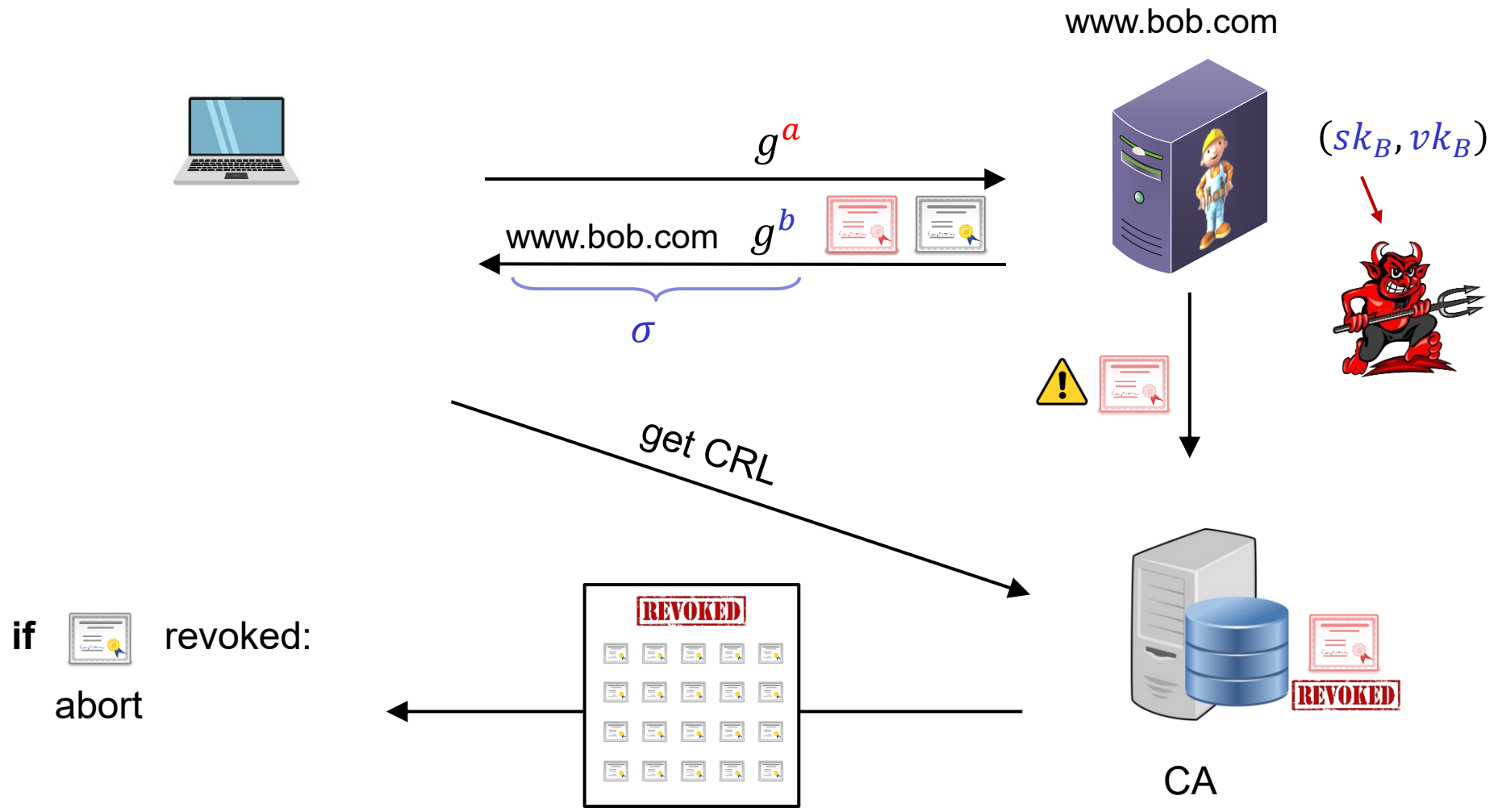


if $\mathrm{Vrfy}(vk_B, \ldots, \sigma) = 1$
  and $\mathrm{Vrfy}(vk_{CA_1}, \ldots, \sigma) = 1$
    and $\mathrm{Vrfy}(vk_{CA_2}, \ldots, \sigma) = 1$
      and $\mathrm{Vrfy}(vk_{CT_1}, \ldots, \sigma_{sct_1}) = 1$
        and $\mathrm{Vrfy}(vk_{CT_2}, \ldots, \sigma_{sct_2}) = 1$
          and $\mathrm{Vrfy}(vk_{CT_3}, \ldots, \sigma_{sct_3}) = 1$

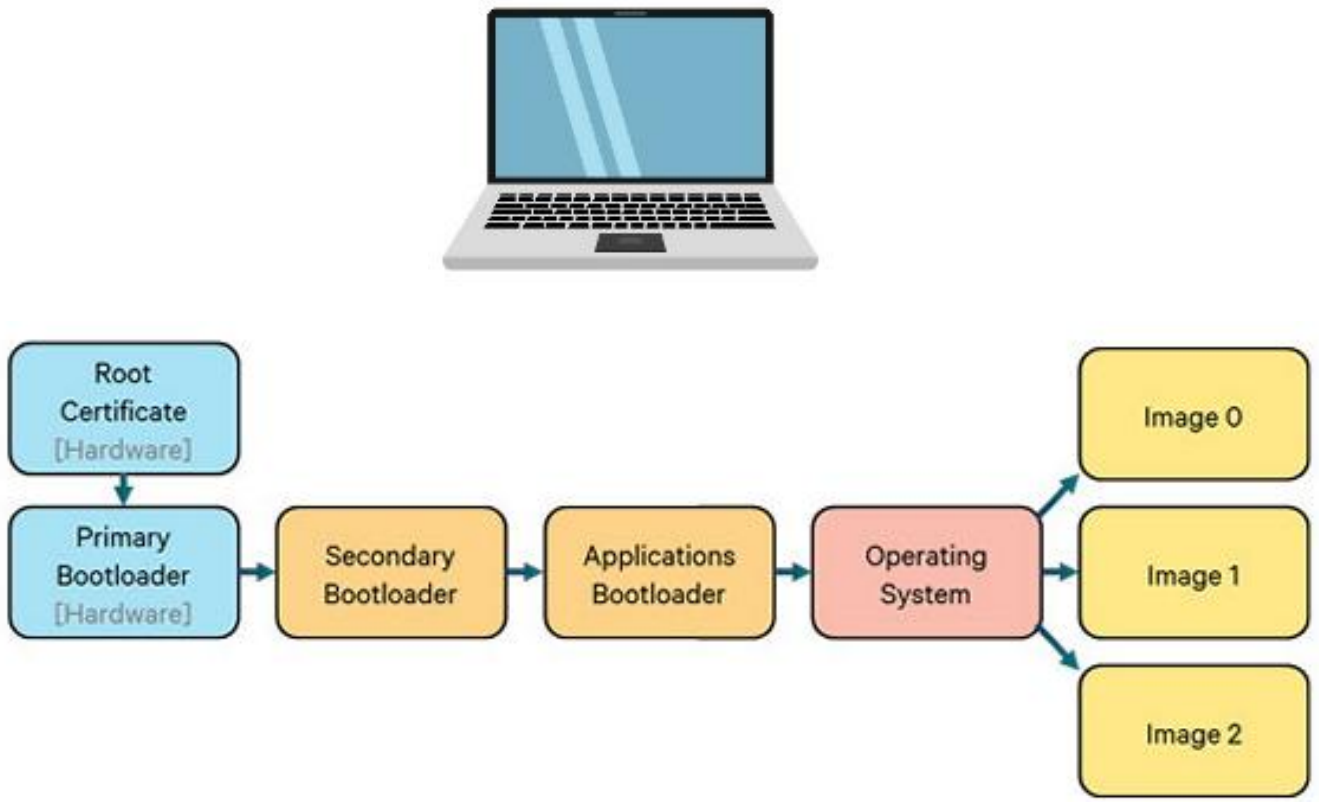
$K \leftarrow g^{ab}$

else
  abort

Certificate revocation

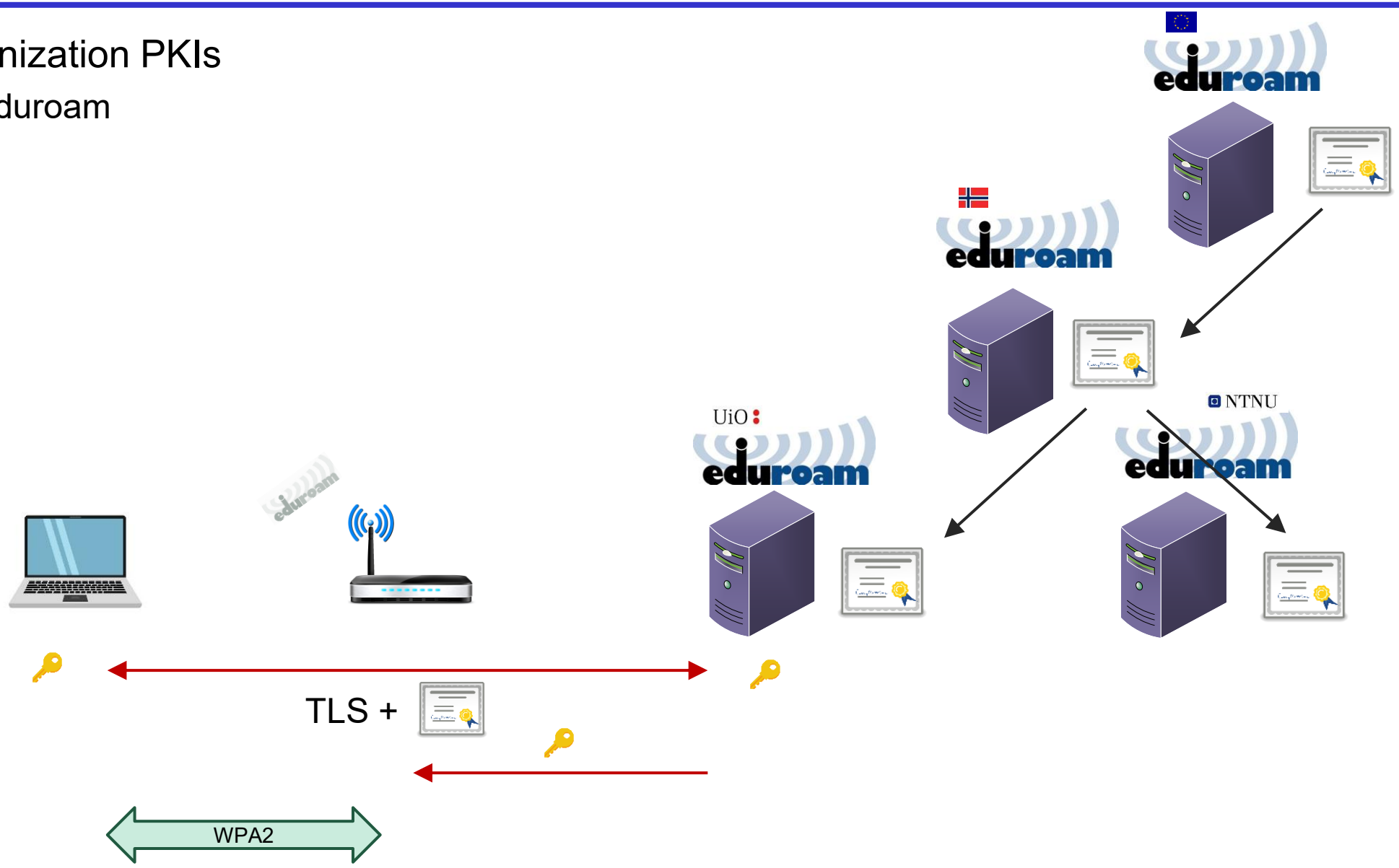


Hardware Root of Trust



Other PKIs exist

- Organization PKIs
  - eduroam



Next week

- Quantum computers

