# Digital Signatures and Certificates

## CS/ECE 407

# Today's objectives

Review man-in the middle attack

Review Digital Signatures

Discuss security of Schnorr Signatures

See how to use digital signatures to induce a chain of trust — Certificates and Public-key Infrastructure

$g^a$

$g^c$

$g^d$

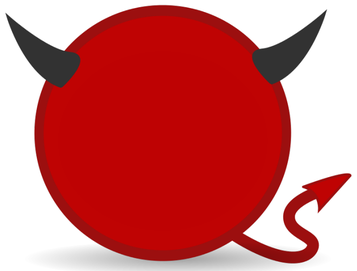
$g^b$

**Alice**

**Bob**

$a \xleftarrow{\$} \mathbb{Z}_q$

$b \xleftarrow{\$} \mathbb{Z}_q$



$g^{ad}$

$c \xleftarrow{\$} \mathbb{Z}_q$

$g^{bc}$

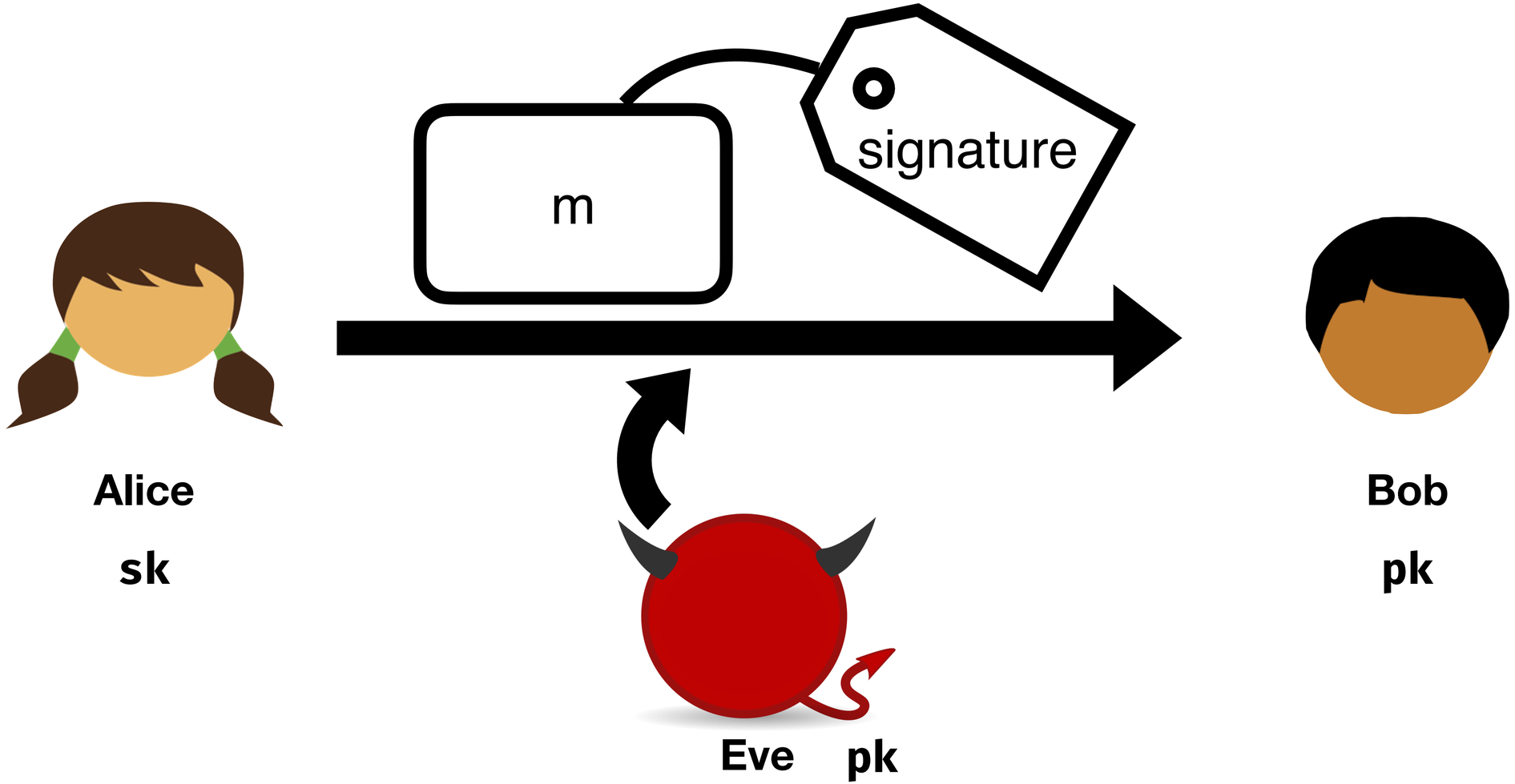
$d \xleftarrow{\$} \mathbb{Z}_q$

$g^{ad}, g^{bc}$

**Eve**

To prevent this attack, we will need some kind of public-key authentication

# Digital Signatures




*“Eve cannot change m without breaking the signature”*

# Digital Signatures

`Gen()` outputs a **key pair** `(pk, sk)`

`Sign(sk, m)` outputs a **signature** σ

`Verify(pk, m, σ)` outputs `{0,1}`

**Correctness:** `(pk, sk) ← Gen()`

`Verify(m, Sign(sk, m), pk) = 1`

*“Public key MACs”*

# Existential Unforgeability under Chosen Message Attack (EUF-CMA)

```
(pk, sk) ← KeyGen()

key(): return pk

get(m):
  return sign(sk, m)

check(m, σ):
  return verify(pk, m, σ)
```

≈

```
(pk, sk) ← KeyGen()
S ← empty-set

key(): return pk

get(m):
  σ ← sign(sk, m)
  S ← S ∪ {(m, σ)}
  return σ

check(m, σ):
  return (m, σ) ∈ S
```

# Identification Scheme

**Alice**

$sk \leftarrow Z_q$

$r \leftarrow Z_q$

$g^r$

$c \leftarrow Z_q$

$s = r + sk \cdot c$

**Bob**

$pk = g^{sk}$

$g^r \cdot pk^c \stackrel{?}{=} g^{r+sk \cdot c}$

# Identification Scheme + Fiat Shamir

**Alice**

$sk \leftarrow Z_q$

$r \leftarrow Z_q$

$g^r$

$c = H(g^r, m)$

$s = r + sk \cdot c$

# Identification Scheme + Fiat Shamir yields a signature scheme

**Alice**

$sk \leftarrow Z_q$

$r \leftarrow Z_q$

$g^r$

$c = H(g^r, m)$

$s = r + sk \cdot c$

$\sigma = (g^r, s)$

# Schnorr Signatures

```
KeyGen():
  sk ←$ Z_q
  return (sk, g^sk)
```

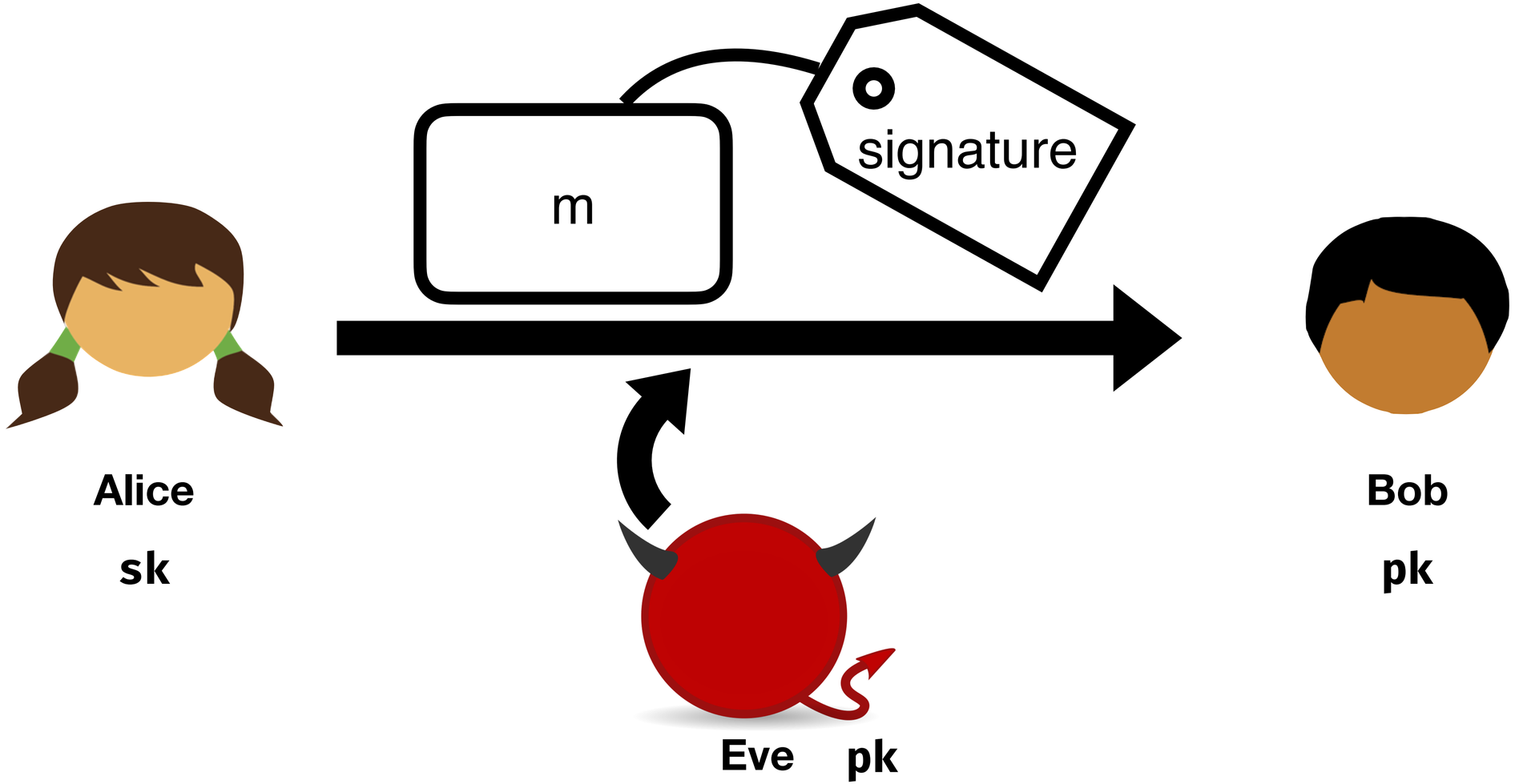
**G** group with order **q**, **g** generator

```
sign(sk, m):
  r ← Z_q
  c ← H(g^r || m)
  s ← r + sk·c
  return (g^r, s)
```

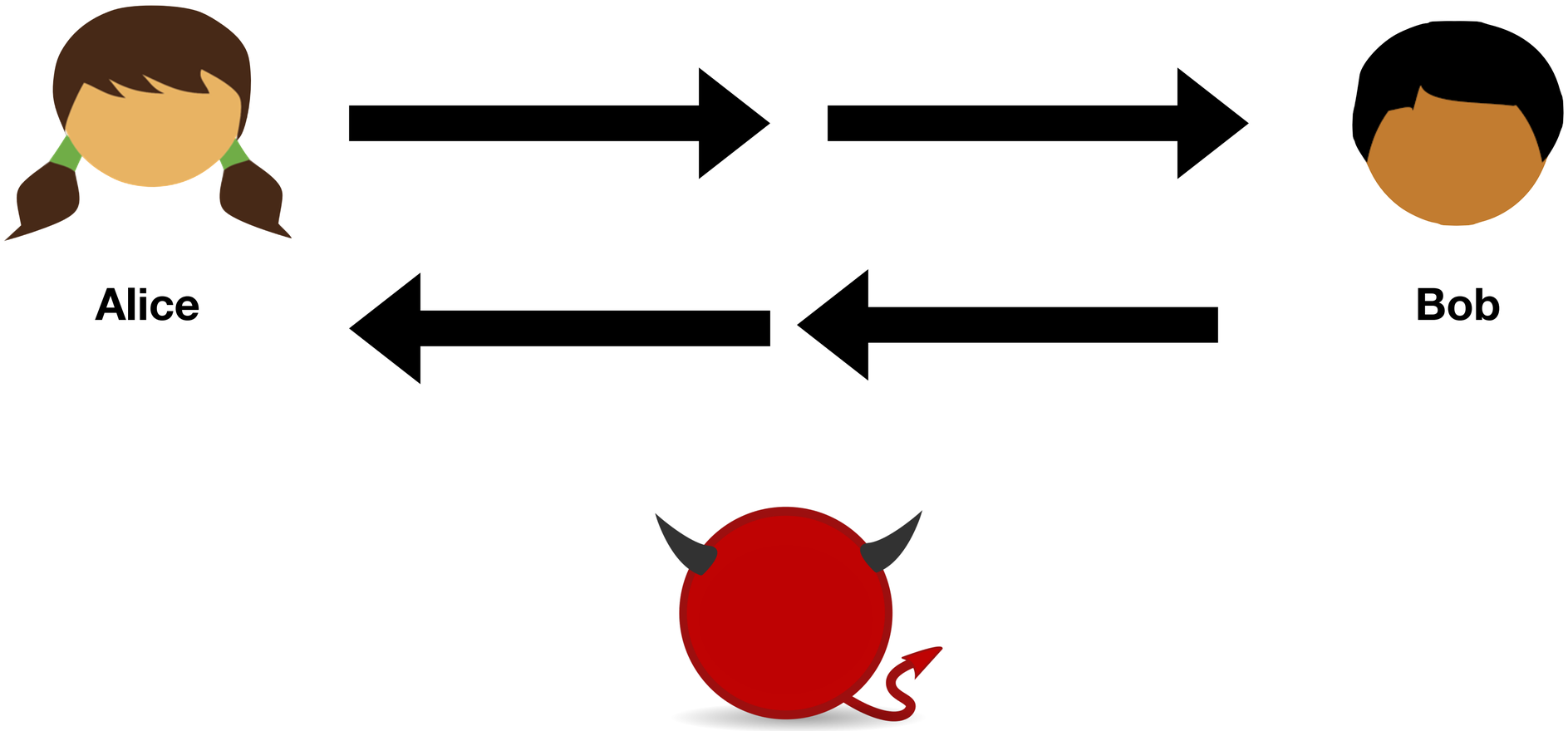
```
verify(g^sk, m, (g^r, s)):
  c ← H(g^r || m)
  return g^s = g^r·(g^sk)^c
```

If discrete log assumption holds for G, and if H is a random oracle, then Schnorr signatures are EUF-CMA secure

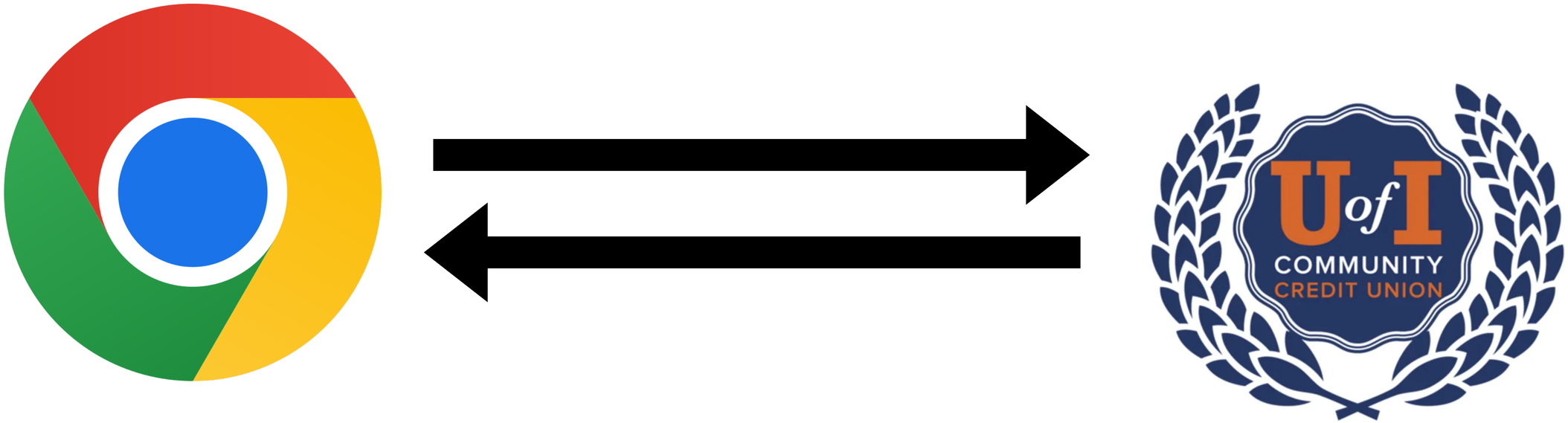
# Digital Signatures




*Requires that Bob already had Alice's secret key*




*Man-in-the-middle attack still possible*




**How do you know you’re really talking to your bank?**

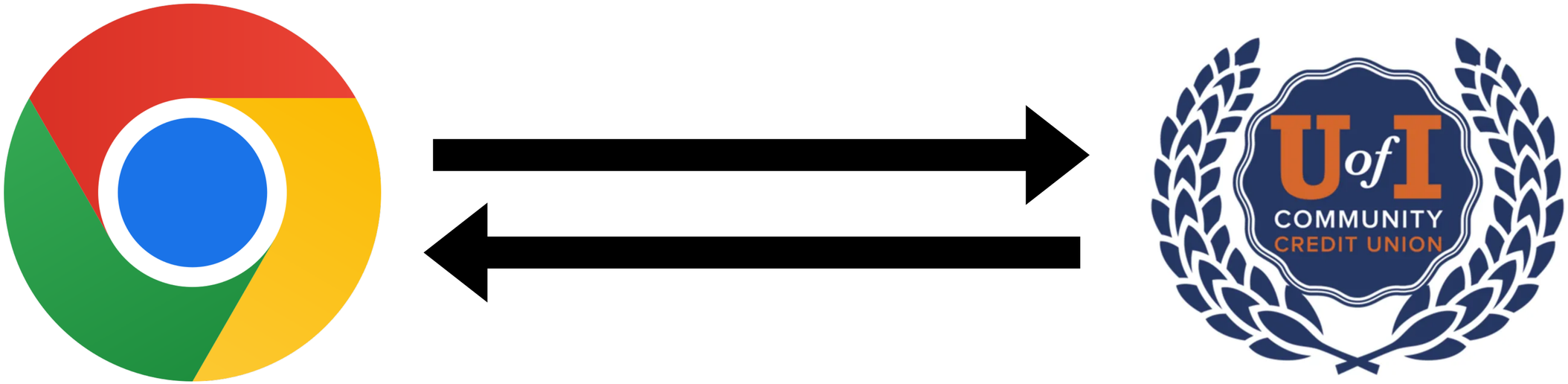
# Question to think about…

You just bought a brand new computer

It comes with a web browser built into the operating system

You for the first time navigate to your local bank's website and log in

**How can you have confidence you're really talking to your bank?**



# Certificates




Charlie

Certificate Authority

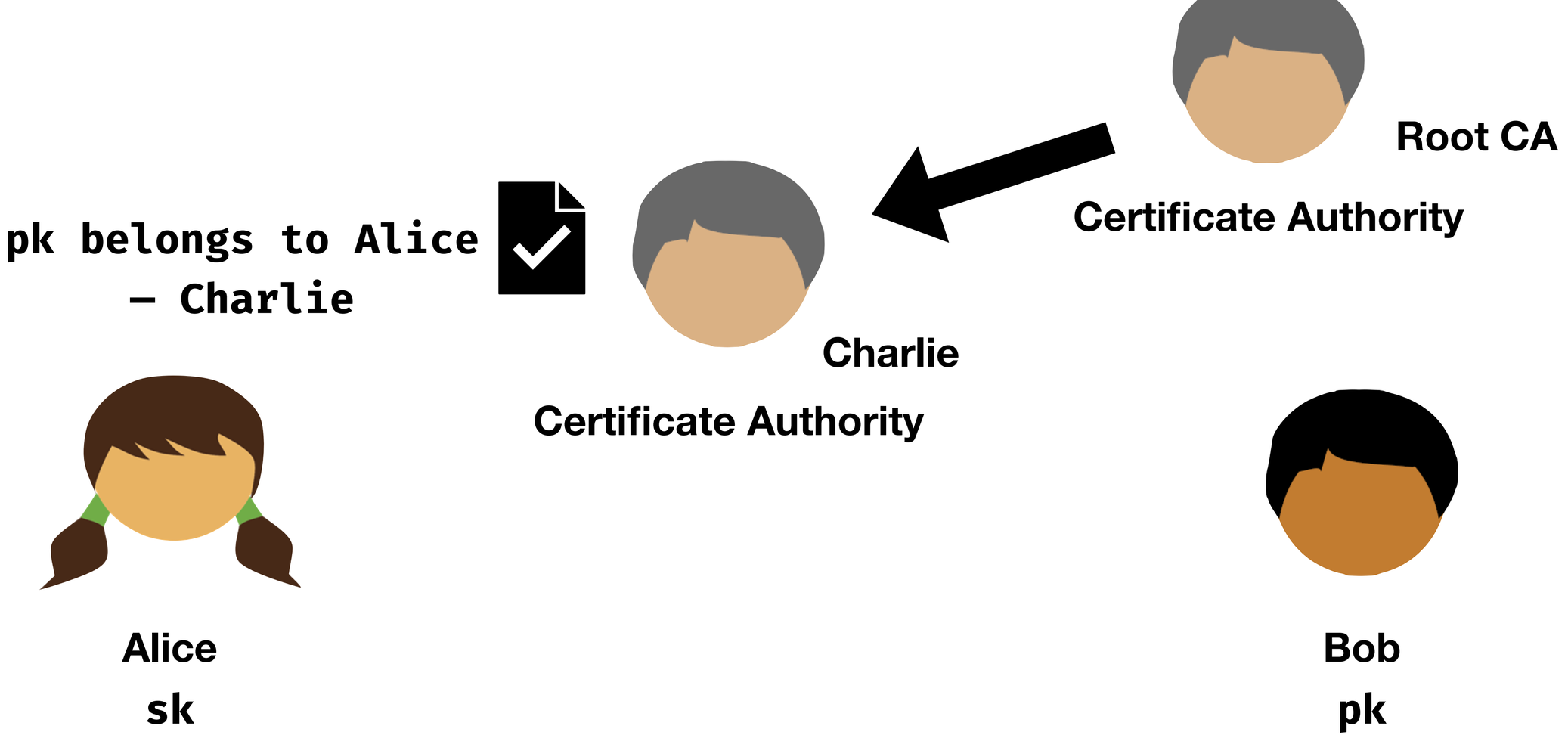
Alice

sk

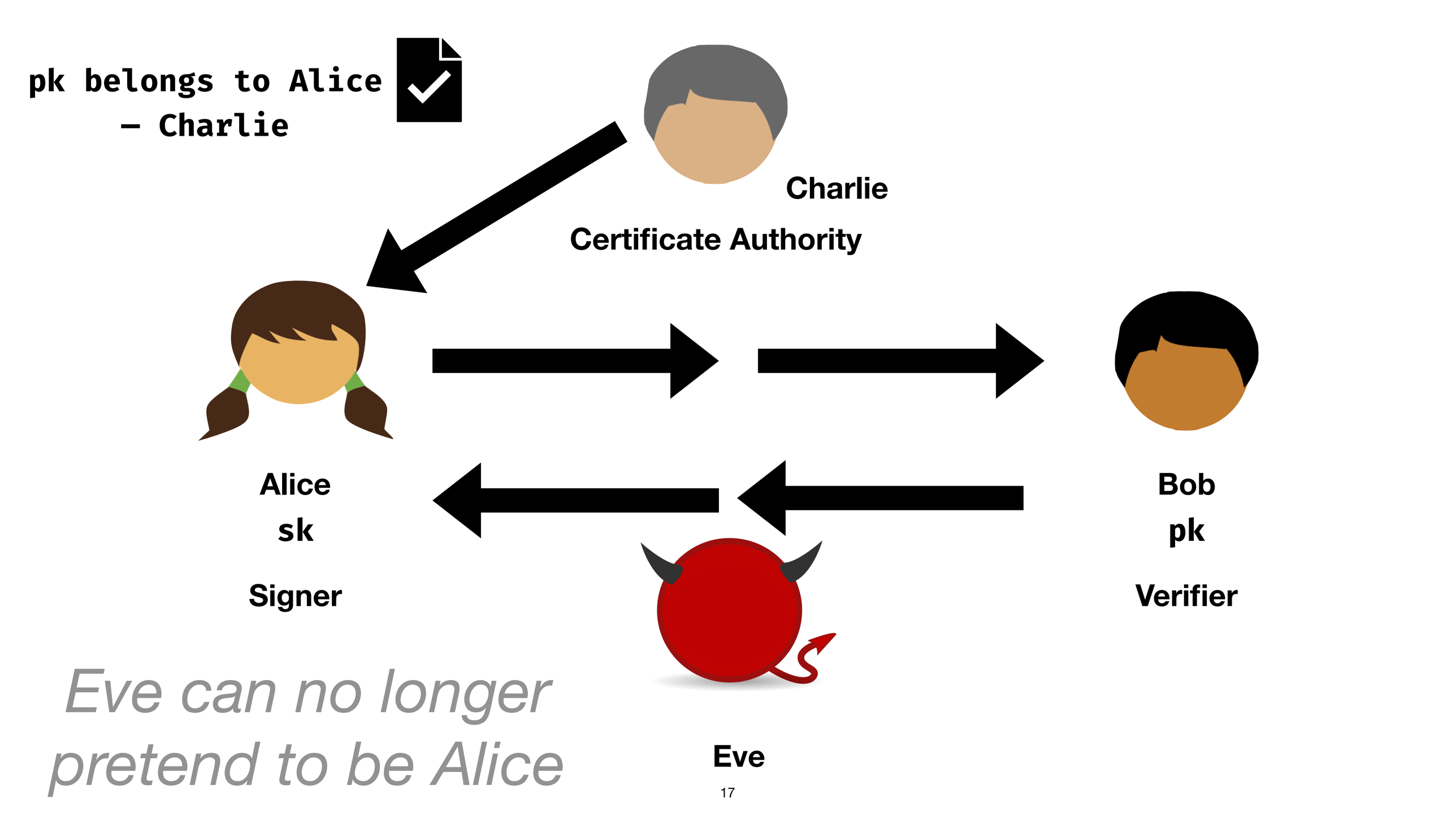
Bob

pk

A certificate **binds** an identity to a public key




A certificate **binds** an identity to a public key




*Eve can no longer pretend to be Alice*

# Today's objectives

Review man-in the middle attack

Review Digital Signatures

Discuss security of Schnorr Signatures

See how to use digital signatures to induce a chain of trust — Certificates and Public-key Infrastructure