BYU
BRIGHAM YOUNG
UNIVERSITY

Usable Key Management and Forward Secrecy for Secure Email

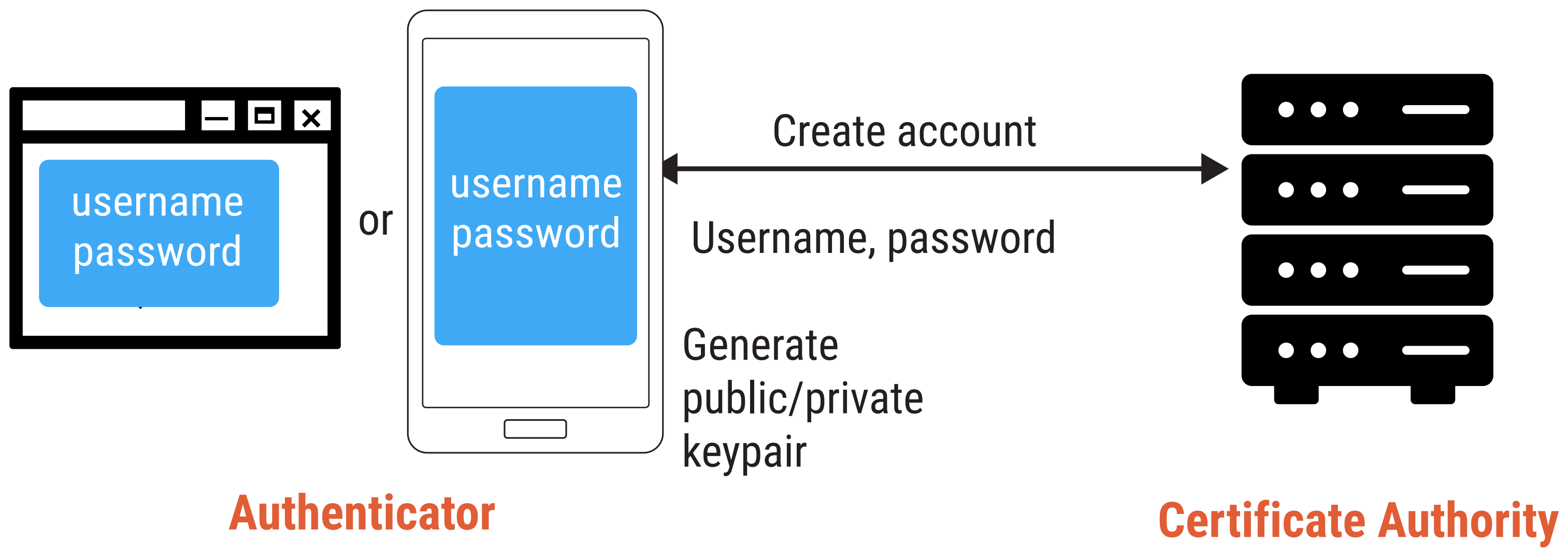
Kent Seamons and Daniel Zappala, Brigham Young University

Can we issue certificates to users as easily as Let's Encrypt?

Let's Authenticate

Replace passwords with certificates for website logins

Create an account with the CA



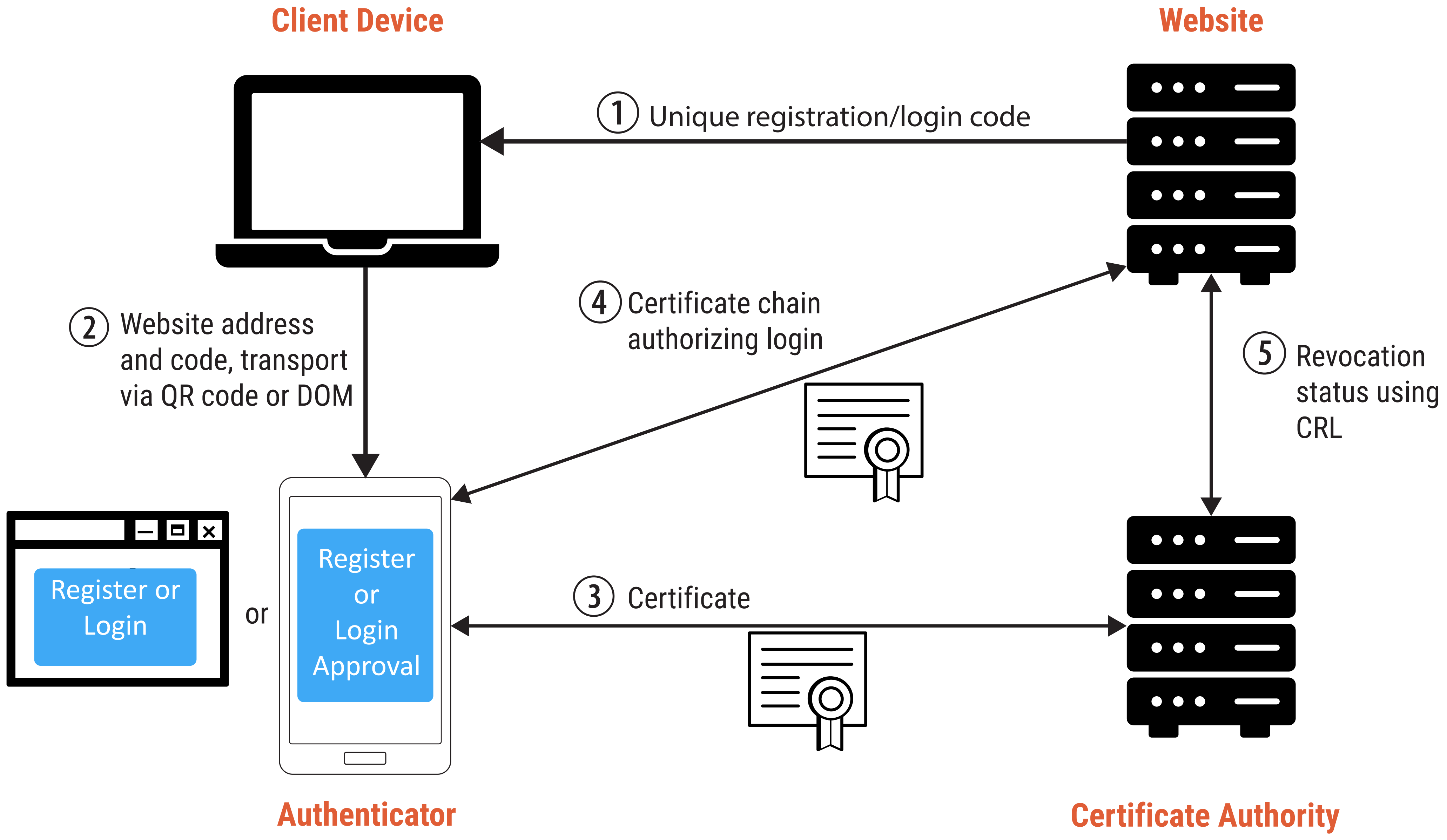
Automated issuance of certificates for registration and login

User only needs to know one username and (master) password, for their CA account, approve registration and login

Easy account recovery in case of lost authenticators

User enters username and master password in new authenticator, deauthorizes old authenticator

Register or login to a website using a certificate


Client Device
Website
1 Unique registration/login code
2 Website address and code, transport via QR code or DOM
4 Certificate chain authorizing login
5 Revocation status using CRL
Register or Login
or
Register or Login Approval
3 Certificate
Authenticator
Certificate Authority

Privacy preserving logins

Certificates are issued for id@ca.org, where id is a cryptographic hash of domain, username, password, salt

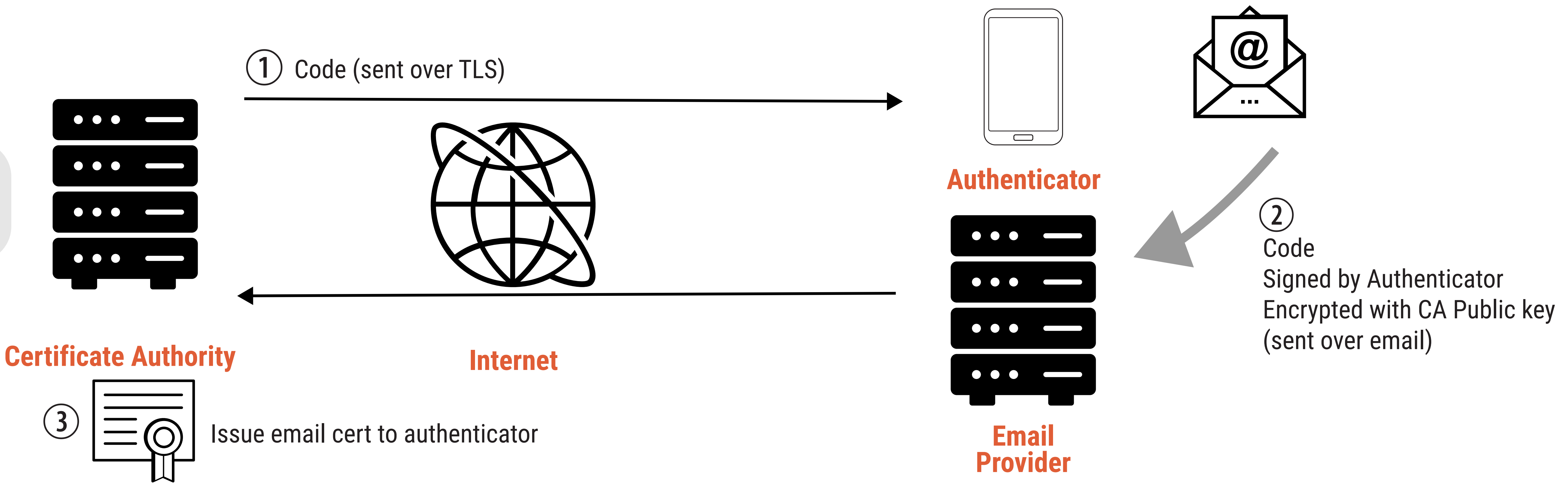
Each certificate is backed by a unique keypair generated by the authenticator

How can we issue certificates proving email ownership?

Let's Authenticate for Email

Email certificates with strong account validation

Get a certificate for email



The 4th NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
October 28-29, 2019 I Alexandria, Virginia