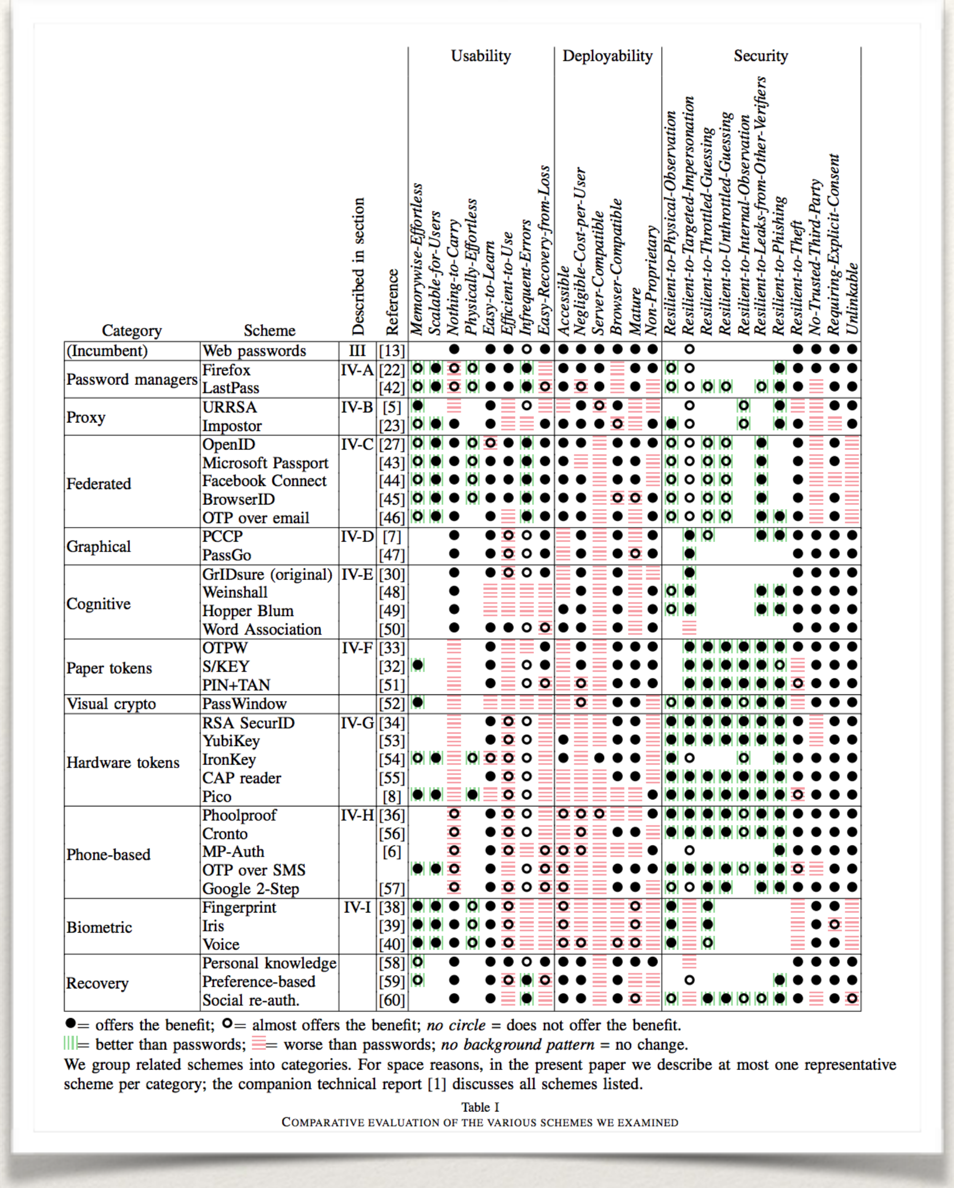
Killing Passwords Once And For All With

Usable TLS Client Authentication

Mark O’Neill
Daniel Zappala
Kent Seamons
and a great team of undergrads

Passwords are the worst kind of authentication…

The Quest to Replace Passswords, Joseph Bonneau, Cormac Herley, Paul C. Van Oorschot, Frank Stajano. 2012 IEEE Symposium on Security and Privacy



				Usability								Deployability						Security										
Category	Scheme	Described in section	Reference	*Memorywise-Effortless*	*Scalable-for-Users*	*Nothing-to-Carry*	*Physically-Effortless*	*Easy-to-Learn*	*Efficient-to-Use*	*Infrequent-Errors*	*Easy-Recovery-from-Loss*	*Accessible*	*Negligible-Cost-per-User*	*Server-Compatible*	*Browser-Compatible*	*Mature*	*Non-Proprietary*	*Resilient-to-Physical-Observation*	*Resilient-to-Targeted-Impersonation*	*Resilient-to-Throttled-Guessing*	*Resilient-to-Unthrottled-Guessing*	*Resilient-to-Internal-Observation*	*Resilient-to-Leaks-from-Other-Verifiers*	*Resilient-to-Phishing*	*Resilient-to-Theft*	*No-Trusted-Third-Party*	*Requiring-Explicit-Consent*	*Unlinkable*
(Incumbent)	Web passwords	III	[13]			●		●	●	○	●	●	●	●	●	●	●		○						●	●	●	●
Password managers	Firefox	IV-A	[22]	○	●	○	○	●	●	●		●	●	●		●	●	○	○					●	●	●	●	●
	LastPass		[42]	○	●	○	○	●	●	●	○	●	○	●		●		○	○	○	○		○	●	●		●	●
Proxy	URRSA	IV-B	[5]	●				●		○			●	○	●				○			○		●			●	●
	Impostor		[23]	○	●	●		●			●	●	●	●	○		●	●	○			○		●	●			●
Federated	OpenID	IV-C	[27]	○	●	●	○	○	●	●	●	●	●		●	●	●	○	○	○	○		●		●		●	
	Microsoft Passport		[43]	○	●	●	○	●	●	●	●	●			●	●		○	○	○	○		●		●		●	
	Facebook Connect		[44]	○	●	●	○	●	●	●	●	●	●		●	●		○	○	○	○		●		●			
	BrowserID		[45]	○	●	●	○	●	●	●	●	●	●		○	○	●	○	○	○	○		●		●		●	
	OTP over email		[46]	○	●	●		●		●	●	●	●		●		●	○	○	○	○		●	●	●		●	
Graphical	PCCP	IV-D	[7]			●		●	○	○	●		●		●		●		●	○			●	●	●	●	●	●
	PassGo		[47]			●		●	○	○	●		●		●	○	●		●						●	●	●	●
Cognitive	GrIDsure (original)	IV-E	[30]			●		●	○	○	●		●		●				●						●	●	●	●
	Weinshall		[48]			●							●		●		●	○	●				●	●	●	●	●	●
	Hopper Blum		[49]			●						●	●		●		●	○	●				●	●	●	●	●	●
	Word Association		[50]			●		●	●	○	○	●	●		●		●								●	●	●	●
Paper tokens	OTPW	IV-F	[33]					●			●		●		●	●	●		●	●	●	●	●	●	●	●	●	●
	S/KEY		[32]	●				●		○	●		●		●	●	●		●	●	●	●	●	○		●	●	●
	PIN+TAN		[51]					●		○	○		○		●	●	●		●	●	●	●	●	●	○	●	●	●
Visual crypto	PassWindow		[52]	●									○		●	●		○	●	●	●	○	●	●		●	●	●
Hardware tokens	RSA SecurID	IV-G	[34]					●	○	○					●	●		●	●	●	●	●	●	●	●		●	●
	YubiKey		[53]					●	○	○		●			●	●		●	●	●	●	●	●	●	●		●	●
	IronKey		[54]	○	●		○	○	○	○		●		●	●	●		●	○			○		●	●	●	●	●
	CAP reader		[55]					●	○	○					●	●		●	●	●	●	●	●	●	●	●	●	●
	Pico		[8]	●	●		●		○	○							●	●	●	●	●	●	●	●	○	●	●	●
Phone-based	Phoolproof	IV-H	[36]			○		●	○	○		○	○	○			●	●	●	●	●	○	●	●	●	●	●	●
	Cronto		[56]			○		●	○	○			○		●	●		●	●	●	●	○	●	●	●	●	●	●
	MP-Auth		[6]			○		●	○		○	○	○				●		○					●	●	●	●	●
	OTP over SMS			●	●	○		●		○	○	○			●	●	●	●	●	●	●	○	●	●	○		●	●
	Google 2-Step		[57]			○		●	○	○	○	○			●	●		○	○	●	●		●	●	●	●	●	●
Biometric	Fingerprint	IV-I	[38]	●	●	●	○	●	○			○				○		●		●						●	●	
	Iris		[39]	●	●	●	○	●	○			○				○		●		●						●	○	
	Voice		[40]	●	●	●	○	●	○			○	○		○	○		●		○						●	●	
Recovery	Personal knowledge		[58]	○		●		●	●	○	●	●	●		●	●	●								●	●	●	●
	Preference-based		[59]	○		●		●	○	●	○	●	●		●				○					●	●	●	●	●
	Social re-auth.		[60]			●		●		●		●	●		●	○		○		●	●	○	○	●	●		●	○

●= offers the benefit; ○= almost offers the benefit; *no circle* = does not offer the benefit.
▥= better than passwords; ▤= worse than passwords; *no background pattern* = no change.
We group related schemes into categories. For space reasons, in the present paper we describe at most one representative scheme per category; the companion technical report [1] discusses all schemes listed.

Table I
COMPARATIVE EVALUATION OF THE VARIOUS SCHEMES WE EXAMINED

…except for everything else.

TLS client authentication has been around since early versions of SSL in

1995

Sorry State of TLS Client Authentication

(1) Purchase a cert

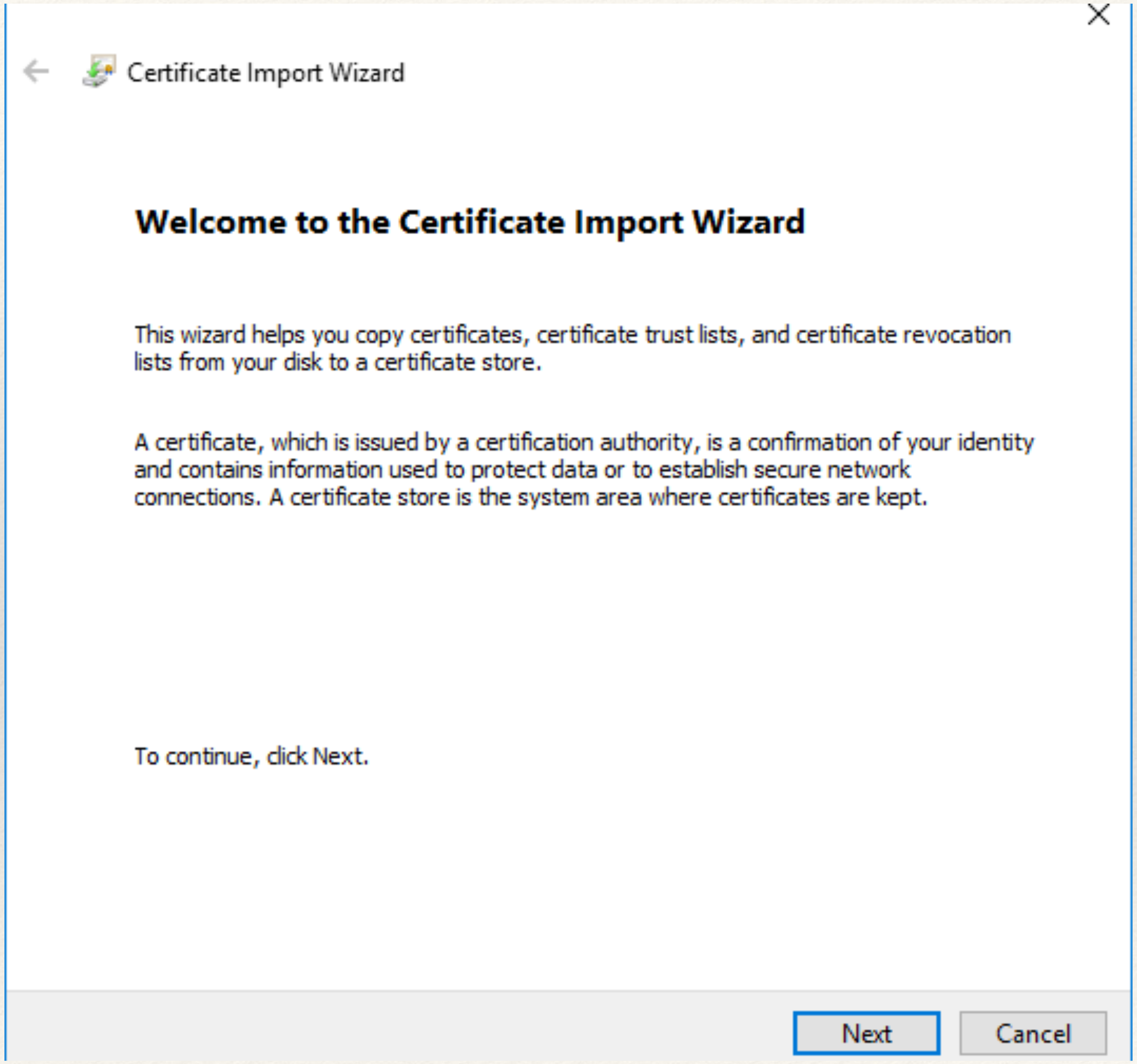
(2) Download the cert,

(3) Go to Settings,

(4) Advanced Settings,

(5) Use the wizard to import a cert,

(6) Select it



Welcome to the Certificate Import Wizard

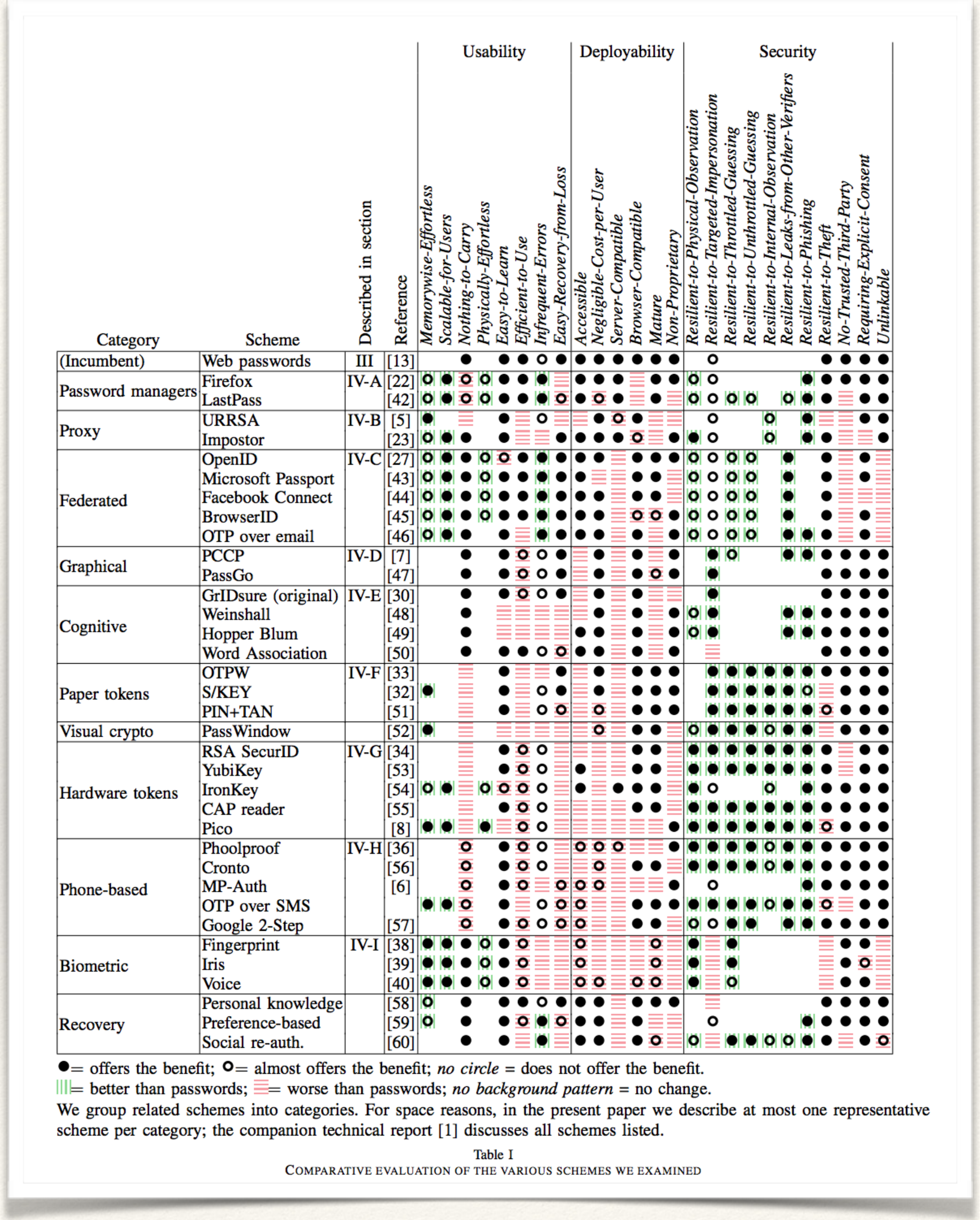
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Start the wizard

TLS Client Authentication was not even included in The Quest to Replace Passwords



				Usability								Deployability						Security										
Category	Scheme	Described in section	Reference	*Memorywise-Effortless*	*Scalable-for-Users*	*Nothing-to-Carry*	*Physically-Effortless*	*Easy-to-Learn*	*Efficient-to-Use*	*Infrequent-Errors*	*Easy-Recovery-from-Loss*	*Accessible*	*Negligible-Cost-per-User*	*Server-Compatible*	*Browser-Compatible*	*Mature*	*Non-Proprietary*	*Resilient-to-Physical-Observation*	*Resilient-to-Targeted-Impersonation*	*Resilient-to-Throttled-Guessing*	*Resilient-to-Unthrottled-Guessing*	*Resilient-to-Internal-Observation*	*Resilient-to-Leaks-from-Other-Verifiers*	*Resilient-to-Phishing*	*Resilient-to-Theft*	*No-Trusted-Third-Party*	*Requiring-Explicit-Consent*	*Unlinkable*
(Incumbent)	Web passwords	III	[13]			●		●	●	○	●	●	●	●	●	●	●		○						●	●	●	●
Password managers	Firefox	IV-A	[22]	○🟩	●🟩	○🟥	○🟩	●	●	●🟩	🟥	●	●	●	🟥	●	●	○🟩	○					●🟩	●	●	●	●
	LastPass		[42]	○🟩	●🟩	○🟥	○🟩	●	●	●🟩	○🟥	●	○🟥	●	🟥	●	🟥	○🟩	○	○🟩	○🟩		○🟩	●🟩	●	🟥	●	●
Proxy	URRSA	IV-B	[5]	●🟩		🟥		●	🟥	○	🟥	🟥	●	○🟥	●	🟥	🟥		○			○🟩		●🟩	🟥	🟥	●	●
	Impostor		[23]	○🟩	●🟩	●		●	🟥	🟥	●	●	●	●	○🟥	🟥	●	●🟩	○			○🟩		●🟩	●	🟥	🟥	●
Federated	OpenID	IV-C	[27]	○🟩	●🟩	●	○🟩	○🟥	●	●🟩	●	●	●	🟥	●	●	●	○🟩	○	○🟩	○🟩		●🟩		●	🟥	●	🟥
	Microsoft Passport		[43]	○🟩	●🟩	●	○🟩	●	●	●🟩	●	●	🟥	🟥	●	●	🟥	○🟩	○	○🟩	○🟩		●🟩		●	🟥	●	🟥
	Facebook Connect		[44]	○🟩	●🟩	●	○🟩	●	●	●🟩	●	●	●	🟥	●	●	🟥	○🟩	○	○🟩	○🟩		●🟩		●	🟥	🟥	🟥
	BrowserID		[45]	○🟩	●🟩	●	○🟩	●	●	●🟩	●	●	●	🟥	○🟥	○🟥	●	○🟩	○	○🟩	○🟩		●🟩		●	🟥	●	🟥
	OTP over email		[46]	○🟩	●🟩	●		●	🟥	●🟩	●	●	●	🟥	●	🟥	●	○🟩	○	○🟩	○🟩		●🟩	●🟩	●	🟥	●	🟥
Graphical	PCCP	IV-D	[7]			●		●	○🟥	○	●	🟥	●	🟥	●	🟥	●		●🟩	○🟩			●🟩	●🟩	●	●	●	●
	PassGo		[47]			●		●	○🟥	○	●	🟥	●	🟥	●	○🟥	●		●🟩						●	●	●	●
Cognitive	GrIDsure (original)	IV-E	[30]			●		●	○🟥	○	●	🟥	●	🟥	●	🟥	🟥		●🟩						●	●	●	●
	Weinshall		[48]			●		🟥	🟥	🟥	🟥	🟥	●	🟥	●	🟥	●	○🟩	●🟩				●🟩	●🟩	●	●	●	●
	Hopper Blum		[49]			●		🟥	🟥	🟥	🟥	●	●	🟥	●	🟥	●	○🟩	●🟩				●🟩	●🟩	●	●	●	●
	Word Association		[50]			●		●	●	○	○🟥	●	●	🟥	●	🟥	●		🟥						●	●	●	●
Paper tokens	OTPW	IV-F	[33]			🟥		●	🟥	🟥	●	🟥	●	🟥	●	●	●		●🟩	●🟩	●🟩	●🟩	●🟩	●🟩	●	●	●	●
	S/KEY		[32]	●🟩		🟥		●	🟥	○	●	🟥	●	🟥	●	●	●		●🟩	●🟩	●🟩	●🟩	●🟩	○🟩	🟥	●	●	●
	PIN+TAN		[51]			🟥		●	🟥	○	○🟥	🟥	○🟥	🟥	●	●	●		●🟩	●🟩	●🟩	●🟩	●🟩	●🟩	○🟥	●	●	●
Visual crypto	PassWindow		[52]	●🟩		🟥		🟥	🟥	🟥	🟥	🟥	○🟥	🟥	●	●	🟥	○🟩	●🟩	●🟩	●🟩	○🟩	●🟩	●🟩	🟥	●	●	●
Hardware tokens	RSA SecurID	IV-G	[34]			🟥		●	○🟥	○	🟥	🟥	🟥	🟥	●	●	🟥	●🟩	●🟩	●🟩	●🟩	●🟩	●🟩	●🟩	●	🟥	●	●
	YubiKey		[53]			🟥		●	○🟥	○	🟥	●	🟥	🟥	●	●	🟥	●🟩	●🟩	●🟩	●🟩	●🟩	●🟩	●🟩	●	🟥	●	●
	IronKey		[54]	○🟩	●🟩	🟥	○🟩	○🟥	○🟥	○	🟥	●	🟥	●	●	●	🟥	●🟩	○			○🟩		●🟩	●	●	●	●
	CAP reader		[55]			🟥		●	○🟥	○	🟥	🟥	🟥	🟥	●	●	🟥	●🟩	●🟩	●🟩	●🟩	●🟩	●🟩	●🟩	●	●	●	●
	Pico		[8]	●🟩	●🟩	🟥	●🟩	🟥	○🟥	○	🟥	🟥	🟥	🟥	🟥	🟥	●	●🟩	●🟩	●🟩	●🟩	●🟩	●🟩	●🟩	○🟥	●	●	●
Phone-based	Phoolproof	IV-H	[36]			○🟥		●	○🟥	○	🟥	○🟥	○🟥	○🟥	🟥	🟥	●	●🟩	●🟩	●🟩	●🟩	○🟩	●🟩	●🟩	●	●	●	●
	Cronto		[56]			○🟥		●	○🟥	○	🟥	🟥	○🟥	🟥	●	●	🟥	●🟩	●🟩	●🟩	●🟩	○🟩	●🟩	●🟩	●	●	●	●
	MP-Auth		[6]			○🟥		●	○🟥	🟥	○🟥	○🟥	○🟥	🟥	🟥	🟥	●		○					●🟩	●	●	●	●
	OTP over SMS			●🟩	●🟩	○🟥		●	🟥	○	○🟥	○🟥	🟥	🟥	●	●	●	●🟩	●🟩	●🟩	●🟩	○🟩	●🟩	●🟩	○🟥	🟥	●	●
	Google 2-Step		[57]			○🟥		●	○🟥	○	○🟥	○🟥	🟥	🟥	●	●	🟥	○🟩	○	●🟩	●🟩		●🟩	●🟩	●	●	●	●
Biometric	Fingerprint	IV-I	[38]	●🟩	●🟩	●	○🟩	●	○🟥	🟥	🟥	○🟥	🟥	🟥	🟥	○🟥	🟥	●🟩	🟥	●🟩					🟥	●	●	🟥
	Iris		[39]	●🟩	●🟩	●	○🟩	●	○🟥	🟥	🟥	○🟥	🟥	🟥	🟥	○🟥	🟥	●🟩	🟥	●🟩					🟥	●	○🟥	🟥
	Voice		[40]	●🟩	●🟩	●	○🟩	●	○🟥	🟥	🟥	○🟥	○🟥	🟥	○🟥	○🟥	🟥	●🟩	🟥	○🟩					🟥	●	●	🟥
Recovery	Personal knowledge		[58]	○🟩		●		●	●	○	●	●	●	🟥	●	●	●		🟥						●	●	●	●
	Preference-based		[59]	○🟩		●		●	○🟥	●🟩	○🟥	●	●	🟥	●	🟥	🟥		○					●🟩	●	●	●	●
	Social re-auth.		[60]			●		●	🟥	●🟩	🟥	●	●	🟥	●	○🟥	🟥	○🟩	🟥	●🟩	●🟩	○🟩	○🟩	●🟩	●	🟥	●	○🟥

●= offers the benefit; ○= almost offers the benefit; *no circle* = does not offer the benefit.
🟩= better than passwords; 🟥= worse than passwords; *no background pattern* = no change.
We group related schemes into categories. For space reasons, in the present paper we describe at most one representative scheme per category; the companion technical report [1] discusses all schemes listed.

Table I
COMPARATIVE EVALUATION OF THE VARIOUS SCHEMES WE EXAMINED

What Makes Us Think We Can Make TLS Client Authentication Viable?

(Or Even Usable)

TLS 1.3

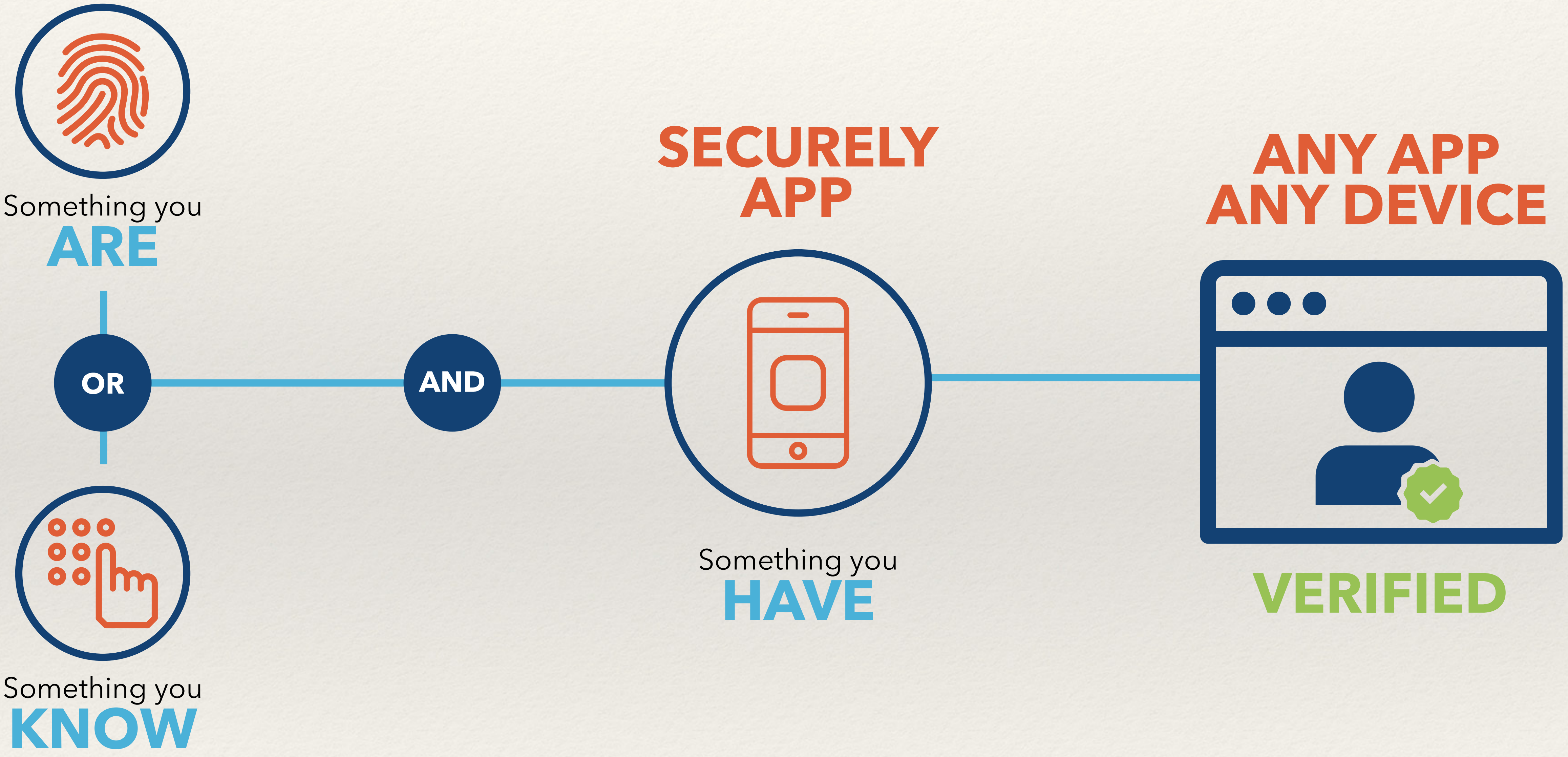
- Encrypts the client cert in the handshake (necessary for privacy)
- Post-handshake authentication
  - Can request authentication at any time or for any purpose
  - E.g. a separate cert for login vs purchase authority vs streaming adult content vs change billing info…

Secure Socket API

See our USENIX Security paper!

```
int fd = socket(PF_INET, SOCK_STREAM, IPPROTO_TLS);
```

User Experience



Something you **ARE**

OR

Something you **KNOW**

AND

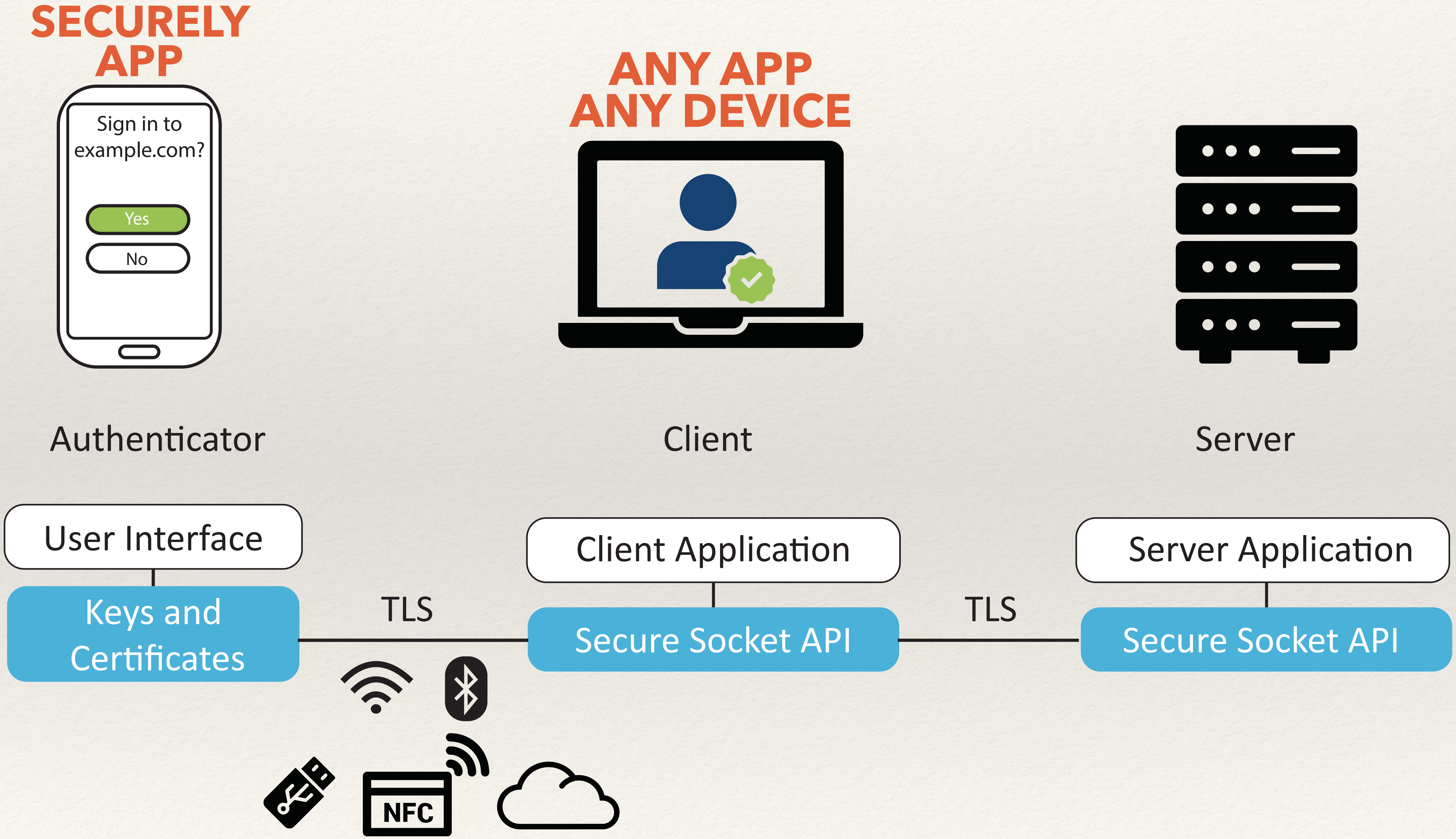
SECURELY APP

Something you **HAVE**

ANY APP ANY DEVICE

VERIFIED

Architecture



SECURELY APP

Sign in to example.com?

Yes

No

ANY APP ANY DEVICE

Authenticator

Client

Server

User Interface

Keys and Certificates

TLS

Client Application

Secure Socket API

TLS

Server Application

Secure Socket API

NFC

Client Auth using Secure Socket API

Client Code:

(none)

Server Code

```
setsockopt(fd, IPPROTO_TLS, SO_REQUEST_PEER_AUTH, data, data_len);

getsockopt(fd, IPPROTO_TLS, SO_PEER_IDENTITY, id, id_len);

setsockopt(client->fd, IPPROTO_TLS, SO_TRUSTED_PEER_CERTIFICATES,
           CA_FILE, sizeof(CA_FILE);
```

Privacy-Preserving Credentials

- Certs provided by an authority
- Certs signed by a web site at registration
- Certs that are self-signed (throw away accounts), one per web site
- Certs that are created and thrown away with each use

We have a demo

Questions/Discussion

- Is certificate-based authentication a viable path forward? A desirable path? If so, what is the best path forward for certificate-based authentication of users? How does this compare to FIDO 2? What about SRP? Other password alternatives?
- For global identity, how do we avoid all the pitfalls of the current Certificate Authority system?
- Are there alternative devices for storing credentials besides a cell phone that would work better?
- How can users backup credentials that are critical (e.g. for a bank account)? How can we handle revocation/renewal?
- How should servers negotiate certificate requirements with a user — e.g. requesting real name, email, or phone? Should a user be able to say "no" to some requests?

What about FIDO 2 (CTAP + WebAuth)?

- SSA lets us provide CTAP (authenticator to device secure channel) for every app instead of just those few that implement it
- WebAuth is only the web — lots of non-web credentials
  - SSH, DropBox, Steam, OneDrive, Discord, OS Login, OS Updates …
- Can trust OS and not an app (e.g. library computer) — browser doesn't even get the public key