SaTC: CORE: Small:

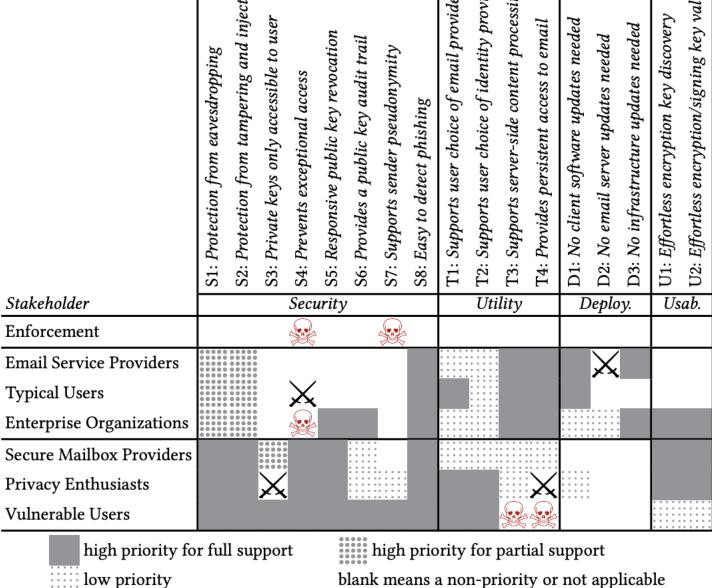
Usable Key Management and Forward Secrecy for Secure Email

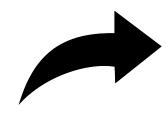
Kent Seamons and Daniel Zappala, Brigham Young University https://www.nsf.gov/awardsearch/showAward?AWD_ID=1816929

Why don't more people use secure email?

Stakeholder approach shows conflcting goals, resulting in fragmented solutions

	S1: Protection from eavesdropping	S2: Protection from tampering and injection	S3: Private keys only accessible to user	S4: Prevents exceptional access	S5: Responsive public key revocation	S6: Provides a public key audit trail	S7: Supports sender pseudonymity	S8: Easy to detect phishing	T1: Supports user choice of email providers	T2: Supports user choice of identity provider	T3: Supports server-side content processing	T4: Provides persistent access to email	D1: No client software updates needed	D2: No email server updates needed	D3: No infrastructure updates needed	U1: Effortless encryption key discovery	U2: Effortless encryption/signing key validation
	51: Pr	52: Pr	53: Pri	S4: Pro	55: Re	56: Pr	S7: Su	58: Ea	Γ1: <i>Su</i>	Γ2: Su	I3: Su	$\Gamma 4: Pr$	D1: N	D2: N	D3: N	01: Ef	J2: Ef
akeholder	Security						Utility			Deploy.			Usab.				
nforcement								6									
mail Service Providers ypical Users nterprise Organizations				X										X	6 6 6 6		
ecure Mailbox Providers rivacy Enthusiasts ulnerable Users			\times									X		0 0 0		· · · · · ·	





FIDO2

6-

hardware token

3

5

6

34 undergraduates

16 as authors on papers

11 from marginalized communities

1 as lead author (NDSS 2020)

Authenticator

Challenge: Can we make secure user authentication easy to use and easy to deploy?

Tackle a wider range of applications to increase impact

Scientific Impact

Authenticating users is applicable to a wide range of problems in security. Our work demonstrates how a focus on usability leads to automating key management and simplifying user interactions.

Web Authentication



 \mathbf{X} there is disagreement within the stakeholder group about the priority of this property kigh priority for no support

"SoK: Securing Email—A Stakeholder-Based Analysis." International Conference on Financial Cryptography and Data Security, 2021

Secure Messaging

Challenge: A malicious key server could provide fake public keys for users, leading to a man-in-the-middle attack

Alex

Signal Call +12345678906

Privacy Check

Have Alex read their identifier to you,

Your device identifier:

479 006 370 650 174

634 156 047 837 096

Alex's device identifier:

874 090 032 854 687

654 820 408 966 544

NO MATCH

and check if it matches your copy.

Do the same for Alex with yours

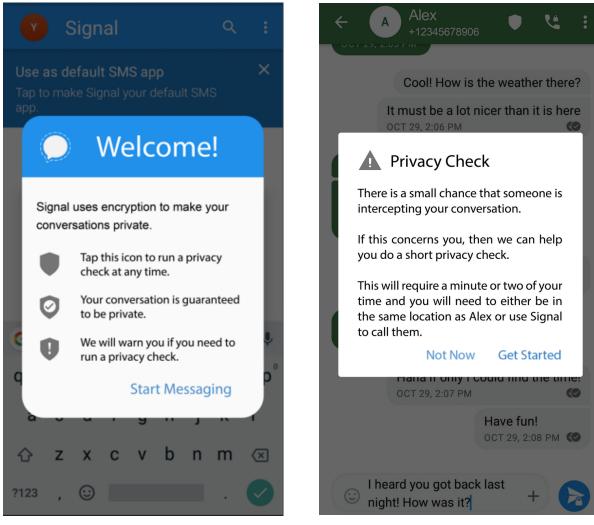
These are the device identifiers for

📣 🗞 🔤

you and Alex.

MATCH

Approach #1: Improve the usability of the authentication ceremony



"Something isn't secure, but I'm not sure how that translates into a problem": Promoting autonomy by designing for understanding in Signal, SOUPS, August 2019.

Approach #2: Detect fake key attacks using key transparency

Challenge: Replace passwords with a system that provides greater security while maintaining high usability

Approach: Automated and centralized management of keys and certificates with Let's Authenticate

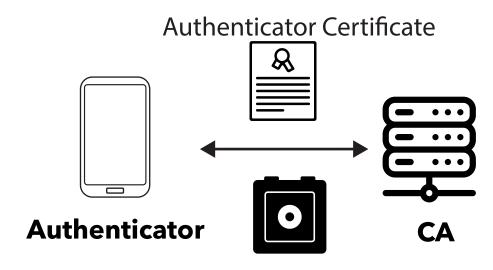
2

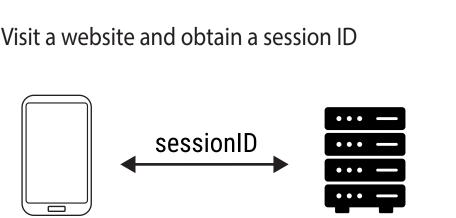
Use a FIDO2 hardware token to authorize or revoke authenticator access to your account with the CA.

Authenticator Certificate

R

Only authorized devices can download the vault, which contains cryptographic keys needed to login to websites.





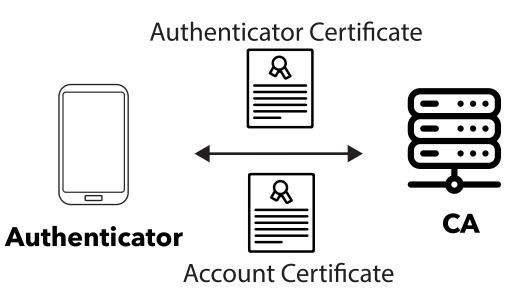
Relying Party

- •••

CA

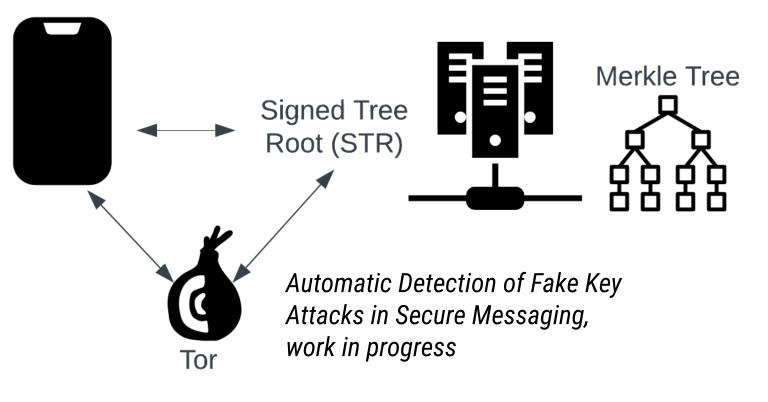
- Create a session key and sign a Session Certificate authorizing the sessionID to login using ID@letsauth.org
- Send the Account Certificate and the Session Certificate to the website to

Obtain an Account Certificate to prove ownership of a random ID@letsauth.org



no trusted third party and no need to carry

and anonymous client auditing



Broader Impacts

- Billions of users of secure messaging applications can use automated detection of attacks.
- Vulnerable users have clear methods to manually check fingerprints of public keys to guarantee their safety.

register or login

Client Device

Authenticator	Relying Party

hardware tokens

- simple account recovery when users lose a device
- portability among multiple authenticators

Let's Authenticate: Automated Certificates for User Authentication, NDSS 2022

Other Authentication Research 2FA Usability Studies (SOUPS 2019, EuroUSEC 2019) Scalable Certificate Revocation (NDSS 2020, ACSAC 2019)

Broader Impacts

- Users will have an easy-to-use method of authenticating to websites and applications that is more secure than passwords.
- Eliminates password breaches and phishing

The 5th NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting (2022 SaTC PI Meeting) June 1-2, 2022 | Arlington, Virginia