Going Passwordless @ Stanford

IAM Online
Wednesday, November 13, 2019

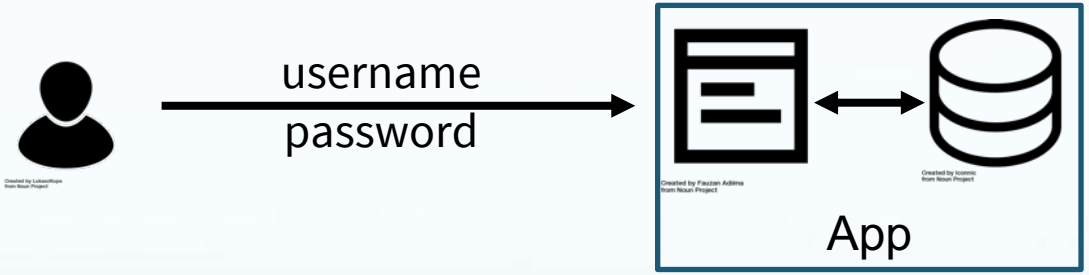
Michael Duff, CISO, Stanford University
Tom Barton (moderator), University of Chicago and Internet2

Make Authentication Strong

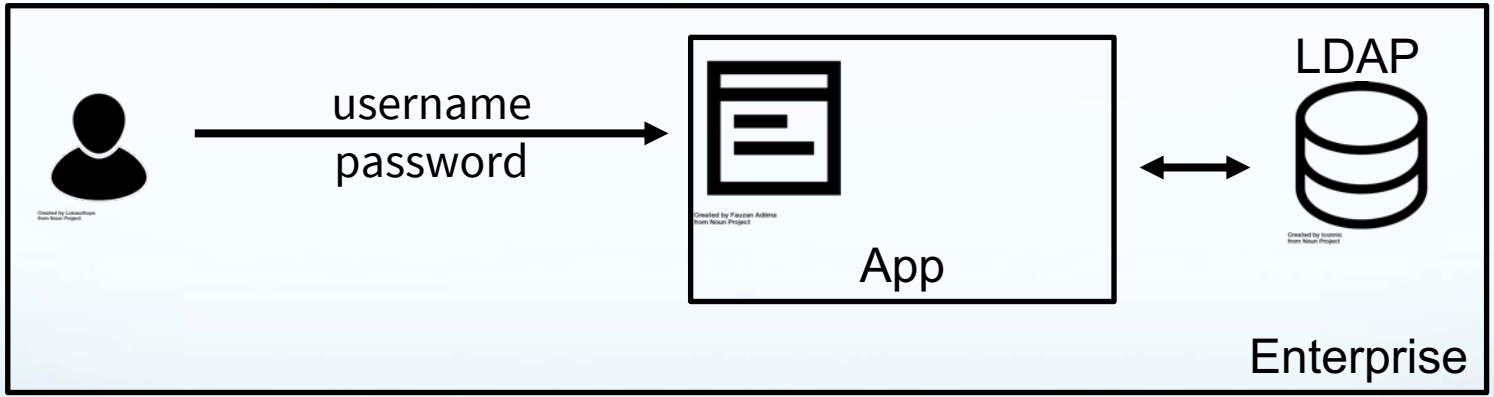
- Users are the weakest link in security
  - But they were put in that position by the IT profession, which built user access technologies around passwords
- Followed by application developers
  - But they were put in that position by those who pay them, and password credentials are easy to support (poorly)

So what's changed?

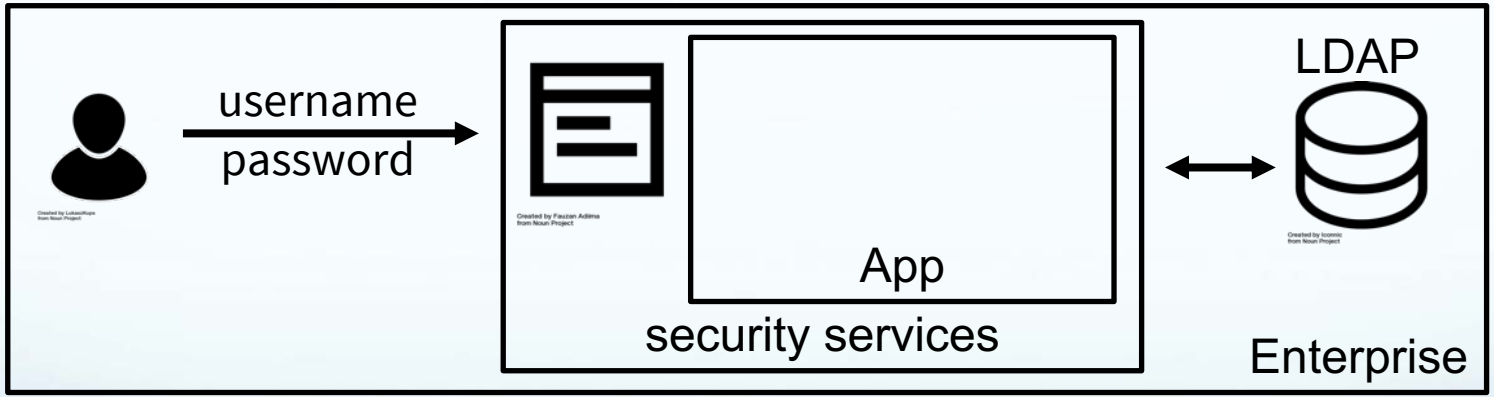
Changing Paradigm for Logins



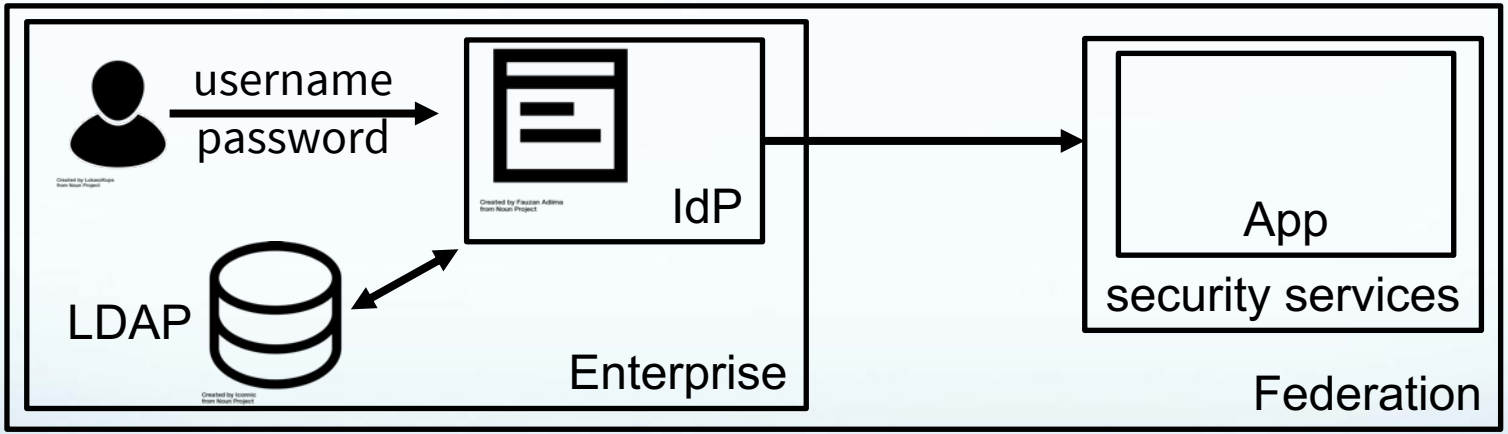
Changing Paradigm for Logins



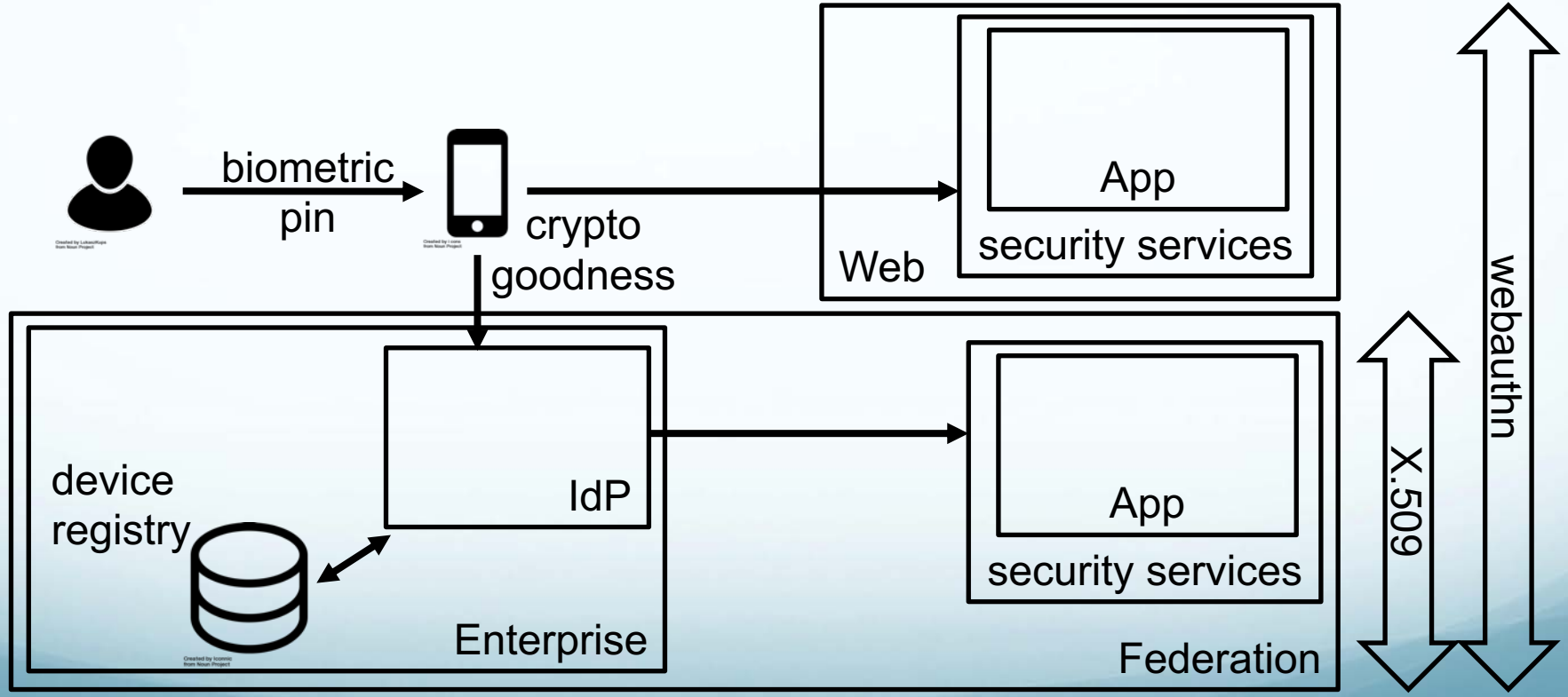
Changing Paradigm for Logins



Changing Paradigm for Logins



Changing Paradigm for Logins



Going Passwordless @ Stanford

Vision

Incidents as Catalysts

DISRUPT NY Shyp CEO Kevin Gibbon to speak at Disrupt NY Get Your Tickets Today

Stanford University stanford

Stanford University Is Investigating An Apparent Security Breach, Urges Community To Reset Passwords

Posted Jul 25, 2013 by Billy Gallagher (@gallagherbilly)

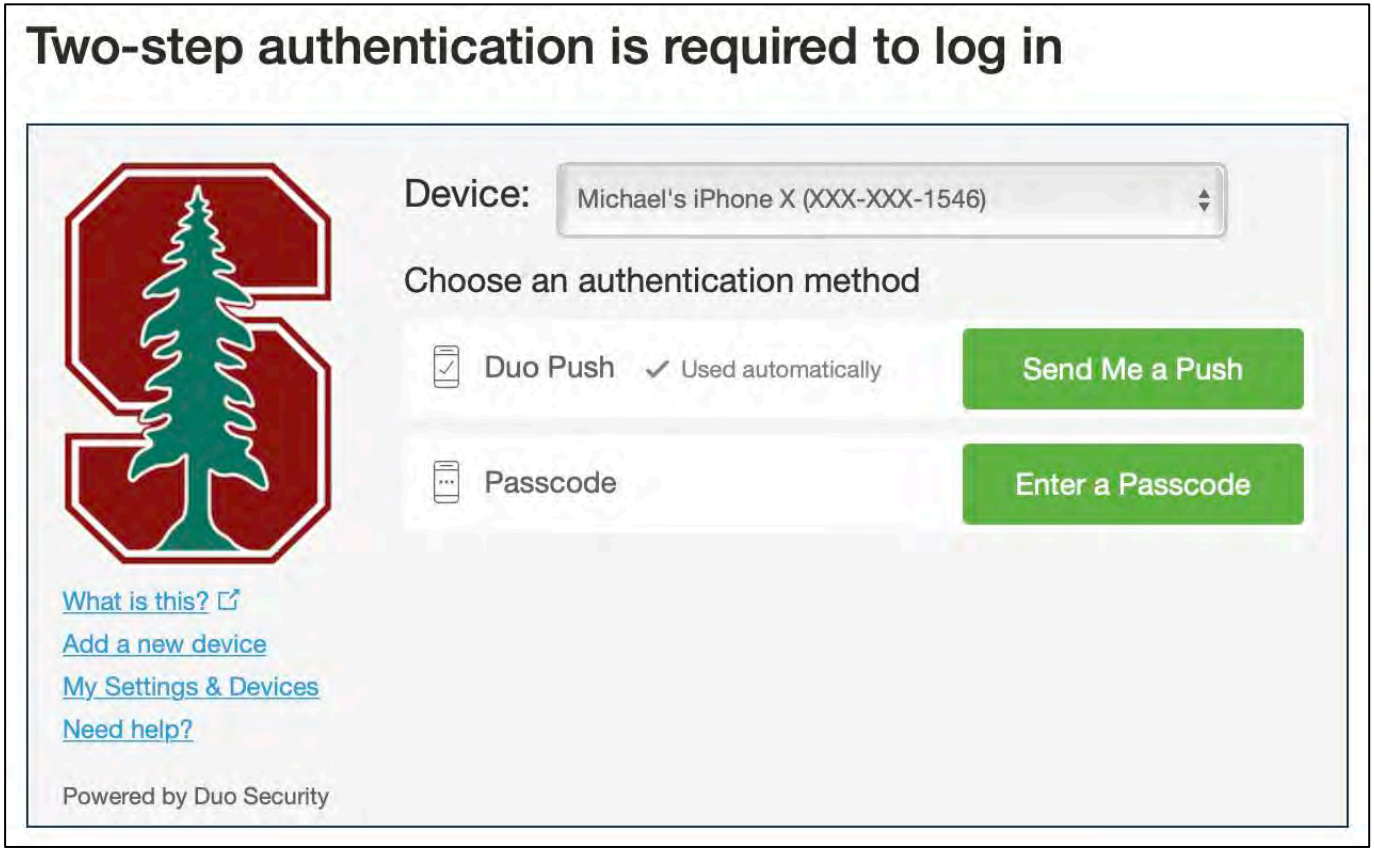
0 SHARES

Stanford University urged network users to change their passwords late Wednesday evening, explaining that it "is investigating an apparent breach of its information technology infrastructure."

Randall Livingston, Stanford's chief financial officer, emailed the entire Stanford community, noting that Stanford does "not yet know the scope of the intrusion."

Livingston's full email, which was sent via an IT Services announce email but signed by the school's CFO, reads:

Two Factor Authentication (Since Fall 2013)



Stanford reports fifth big HIPAA breach

Stolen laptop at children's hospital compromises PHI of 13,000

By Erin McCann | June 13, 2013 | 10:14 AM

SHARE 19

Officials at Stanford University's Lucile Packard Children's Hospital are notifying nearly 13,000 patients that their protected health information has been compromised following the theft of a hospital laptop.

An employee notified the hospital May 8 that an unencrypted laptop containing medical information on pediatric patients had been stolen from a badge-access controlled area of the hospital. Officials say the laptop contained patient names, ages, medical record numbers, surgical procedures, names of physicians involved in the procedures and telephone numbers.

This is the fifth big HIPPA breach for Stanford University.

Following Stanford's most recent HIPAA breach in January, hospital officials said they were "redoubling efforts to ensure that all computers and devices containing medical information are encrypted."

Create **effective** patient engagement to **strengthen** relationships and **improve** outcomes

encrypt.stanford.edu

Information Security

Overview | I want to... | Guides | Policies | News | About

Encryption at Stanford

The University has established a requirement to verifiably encrypt all Windows and Mac computers, as well as Apple and Android mobile devices that are used by employees on the campus network.

Encrypt your devices | View frequently asked questions

Stanford Information Security Goals

No incidents attributable to a lack of best practices

Automated standards enforcement wherever possible

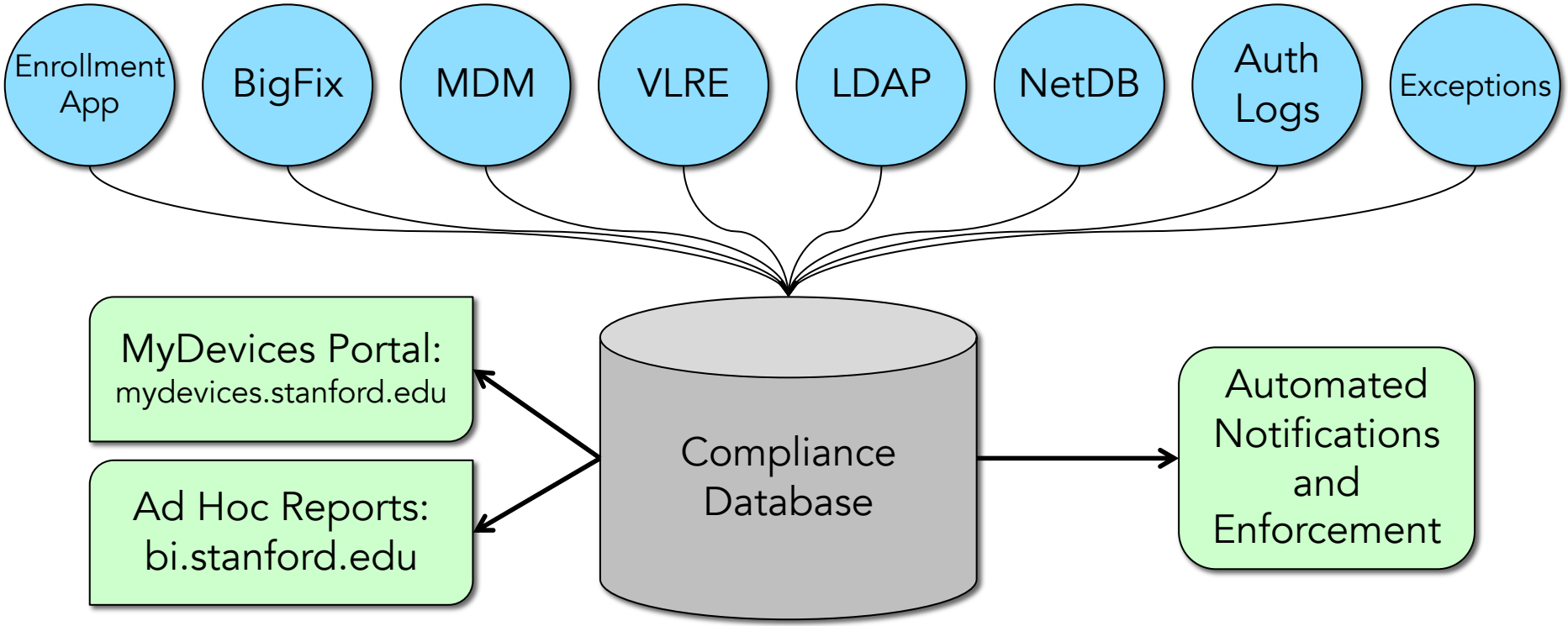
Uniform solutions across the University, Hospitals and SLAC

Balance security with usability and personal privacy

Stanford as a recognized leader in information security

MyDevices

High ROI



mydevices.stanford.edu

Stanford | MyDevices

Registered Devices

This page contains information about devices you use, according to University records. Changes to source systems may take up to 24 hours to display. If you have questions or concerns about the data, please contact your local IT support or submit a help ticket.

Show My Affiliations

Model	Name	Type	Operating System	Ownership	Compliance Status	Remove
Apple - MacBookPro15,2	ISO-C02XH4H6JHD2	Laptop	Mac OS X 10.14.6	Stanford	Compliant	Remove
iPad Pro with Wi-Fi (128 GB Space Gray)	mjduff iPad iOS 13.1.2 DQTQR3HKGMLL	Mobile	iOS 13.1.2	Stanford	Compliant	Remove
iPhone X (256 GB Space Gray)	mjduff iPhone iOS 13.1.2 F17VN78NJCL8	Mobile	iOS 13.1.2	Personal	Compliant	Remove

Learn about Stanford's Encryption Requirements

Imagine not needing to enter your username and password anymore, all while being dramatically more secure…

cardinalkey.stanford.edu

Stronger authentication

Phishing protection

Why are we doing this?

User experience

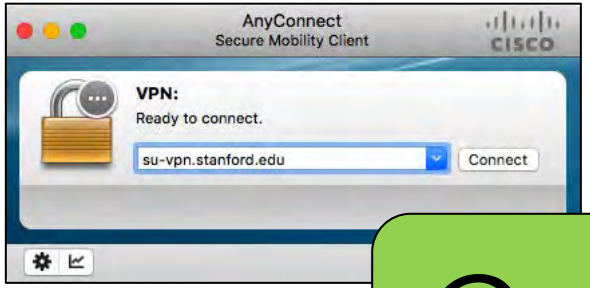
Device identification

Integration Points

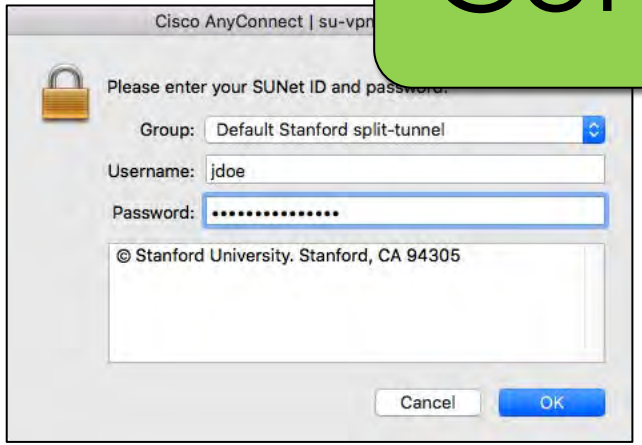
- ✓ VPN
- ✓ Web SSO
- Secure Wireless

VPN Connections with Username + Password + Two-Step

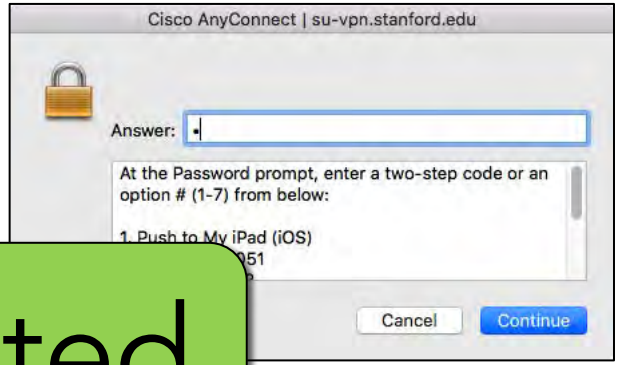
1



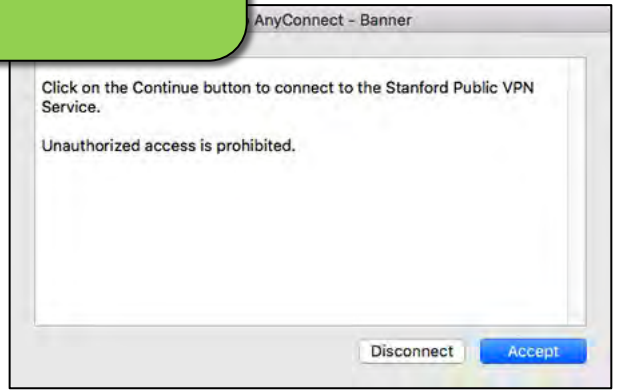
2



3



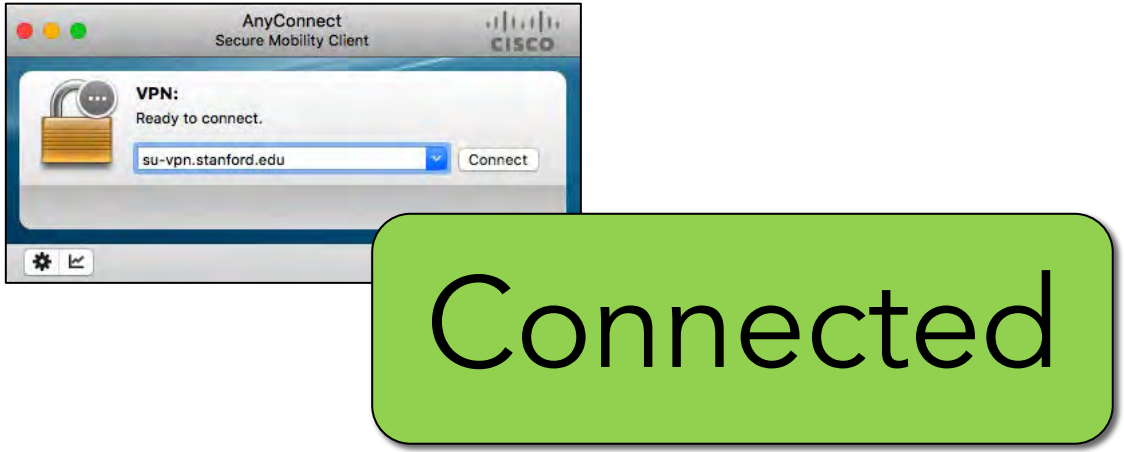
4



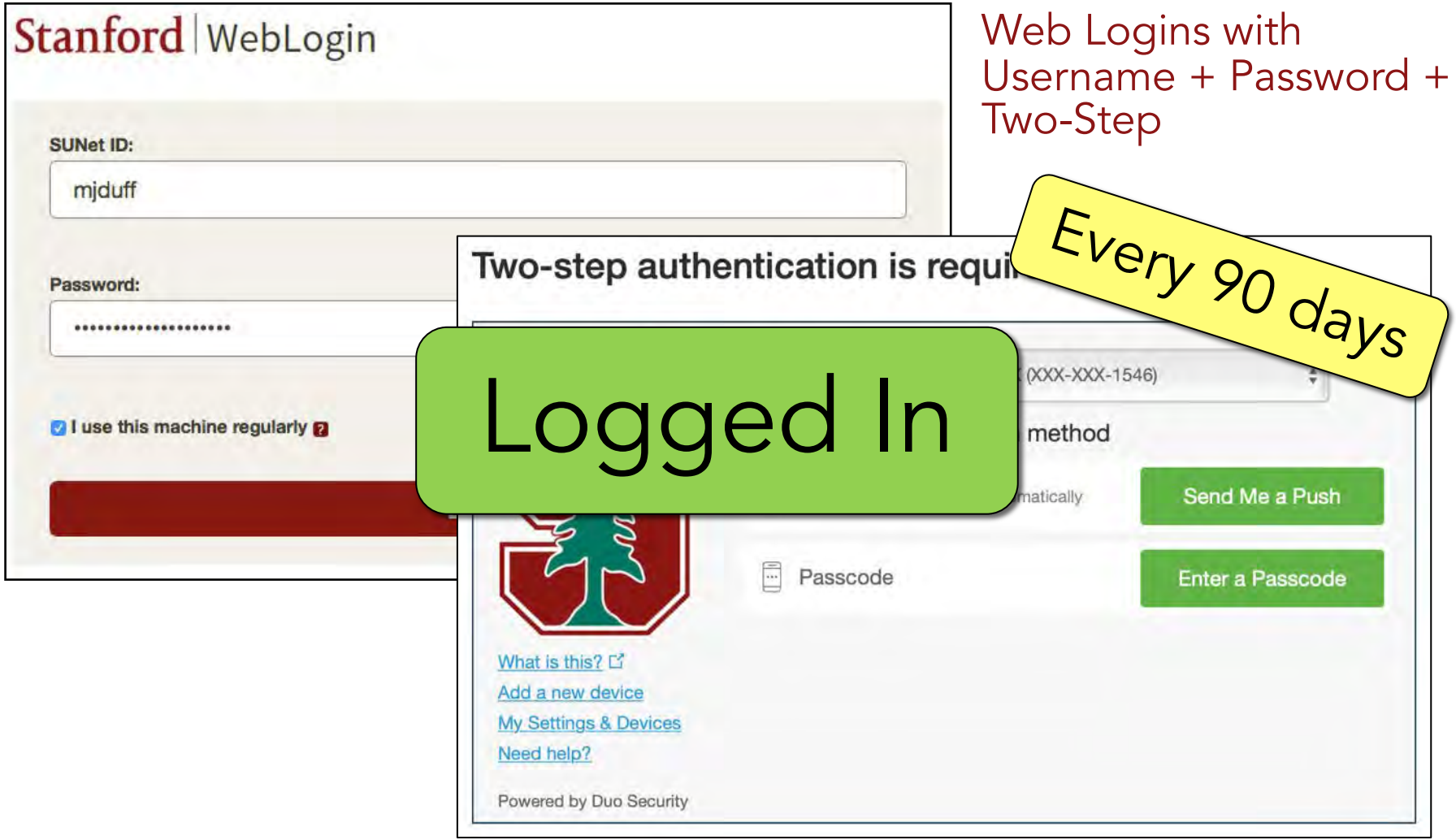
Connected

VPN Connections with a Cardinal Key

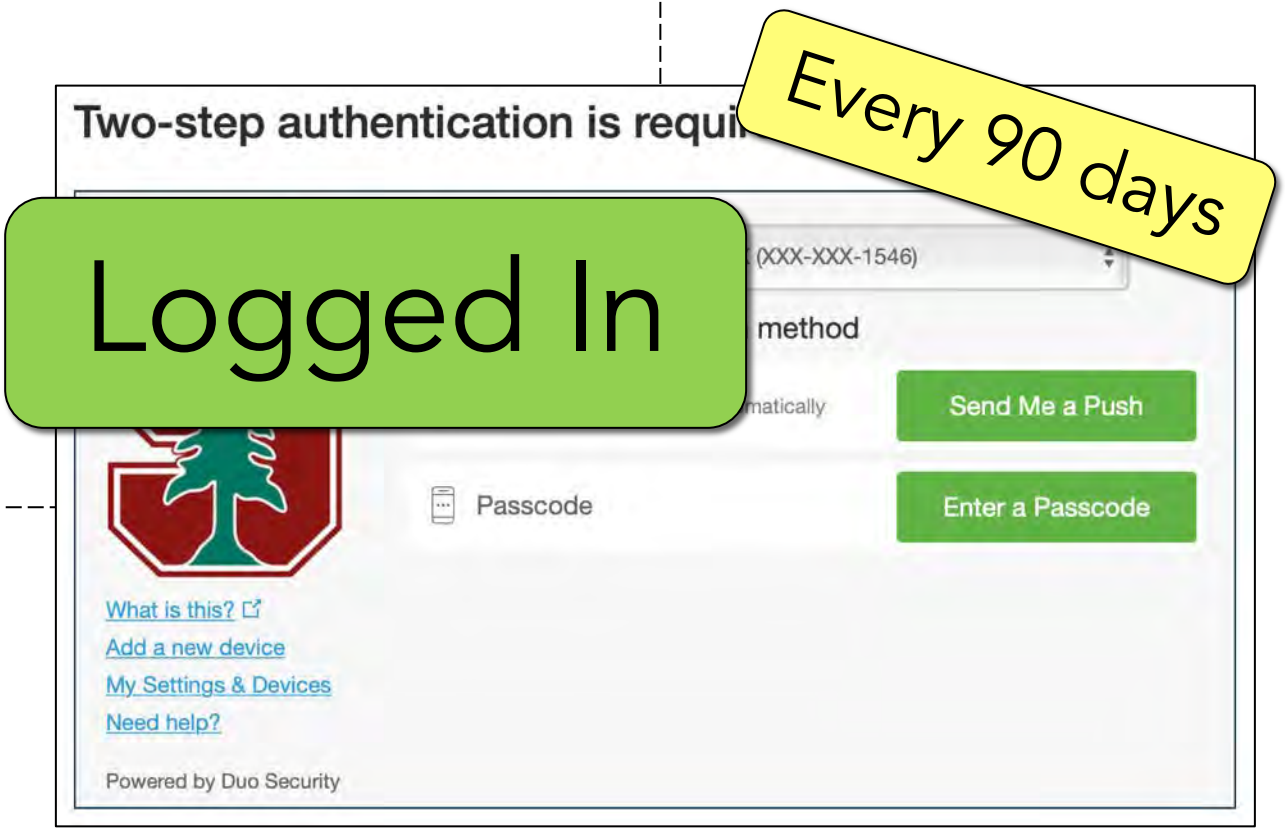
1



Web Logins with Username + Password + Two-Step



Web Logins with a Cardinal Key



Rollout

3 Years, 3 Phases

- Year 1: Infrastructure to support opt-in participation
- **Year 2: UX improvements and broad adoption**
- Year 3: Require for central services

Supported Platforms

PLATFORM	BROWSERS					VPN CLIENTS	
	CHROME	SAFARI	INTERNET EXPLORER	MICROSOFT EDGE	FIREFOX	CISCO ANYCONNECT	NATIVE VPN
Windows	✓	N/A	✓	✓	✗	✓	✗
Mac	✓	✓	N/A	N/A	✗	✓	✗
iOS	✗	✓	N/A	✗	✗	✗	✓
Android	Cardinal Key is not supported on Android and Linux platforms at this time.						
Linux							

Stanford is Going Passwordless (beta)

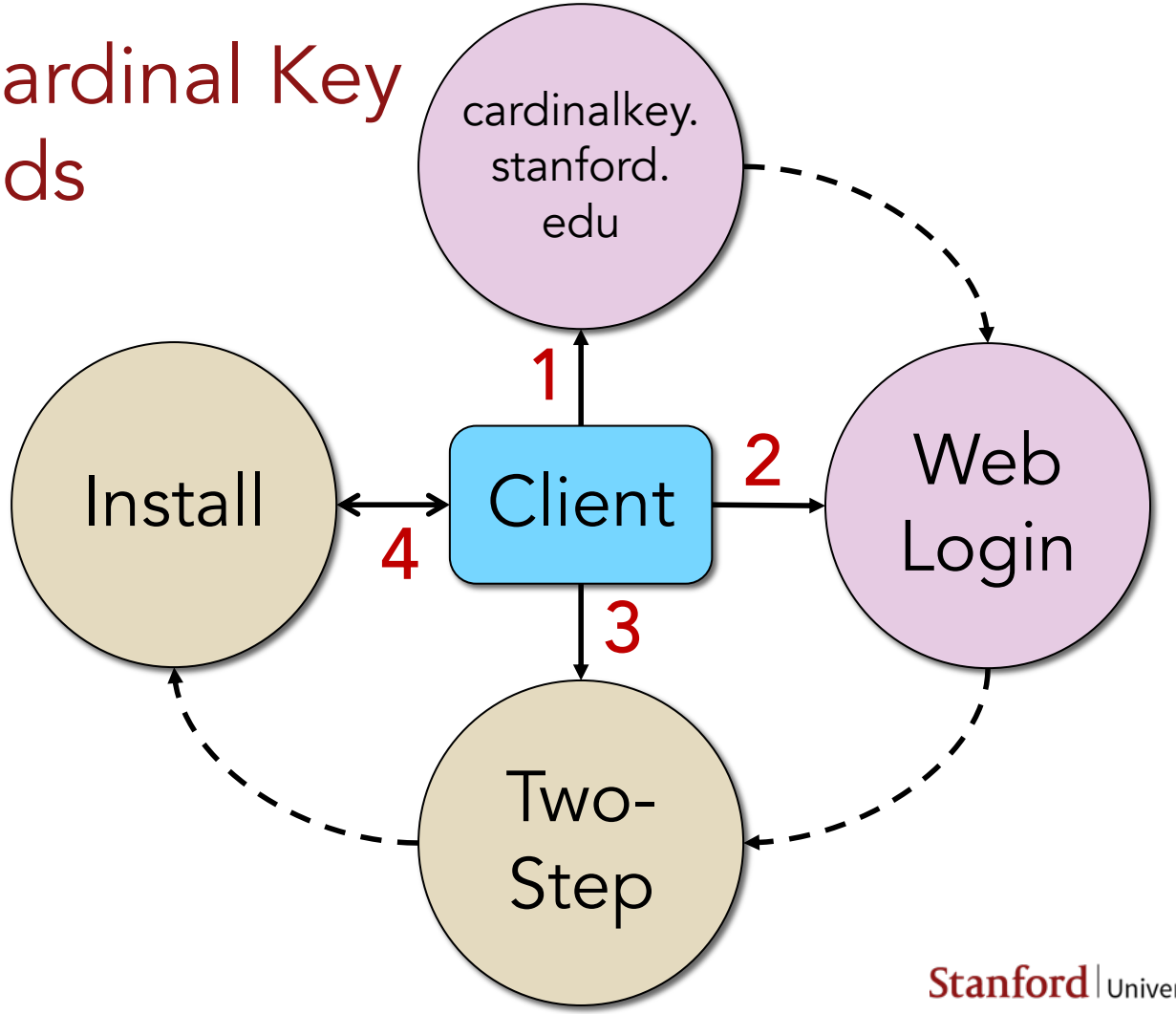
TUESDAY, FEBRUARY 19, 2019

Simplicity and security: the future of logins has arrived. Wouldn't it be nice to skip typing in your SUNet ID and password every day, while protecting your credentials from phishing? With Cardinal Key, you can do just that. University IT has made this new service available to all, with the understanding that it is a preliminary rollout and not yet fully refined.

> "Cardinal Key is a triumph of usability and security," said Michael Duff, chief information security officer. "This is the culmination of six years of concerted effort, and the Stanford community will reap the benefits for decades to come. While Cardinal Key is still in beta, the advantages are too compelling to wait any longer."

More than 1,000 staff and faculty are already using Cardinal Key as early adopters. Students are welcome to use Cardinal Key, but their devices must adhere to the same cybersecurity standards that apply to university employees.

Getting a Cardinal Key in 60 Seconds



Which Device Are You Using?

Please provide a name for the device that you are activating:

Device Name: Michael's MacBook

< Back

Continue >

To access the secure network, follow the instructions below based on your computer's operating system.

Mac OS X

Download for Mac 10.7 & Newer

Installs Stanford Client Configuration Profile

Quid Pro Quo

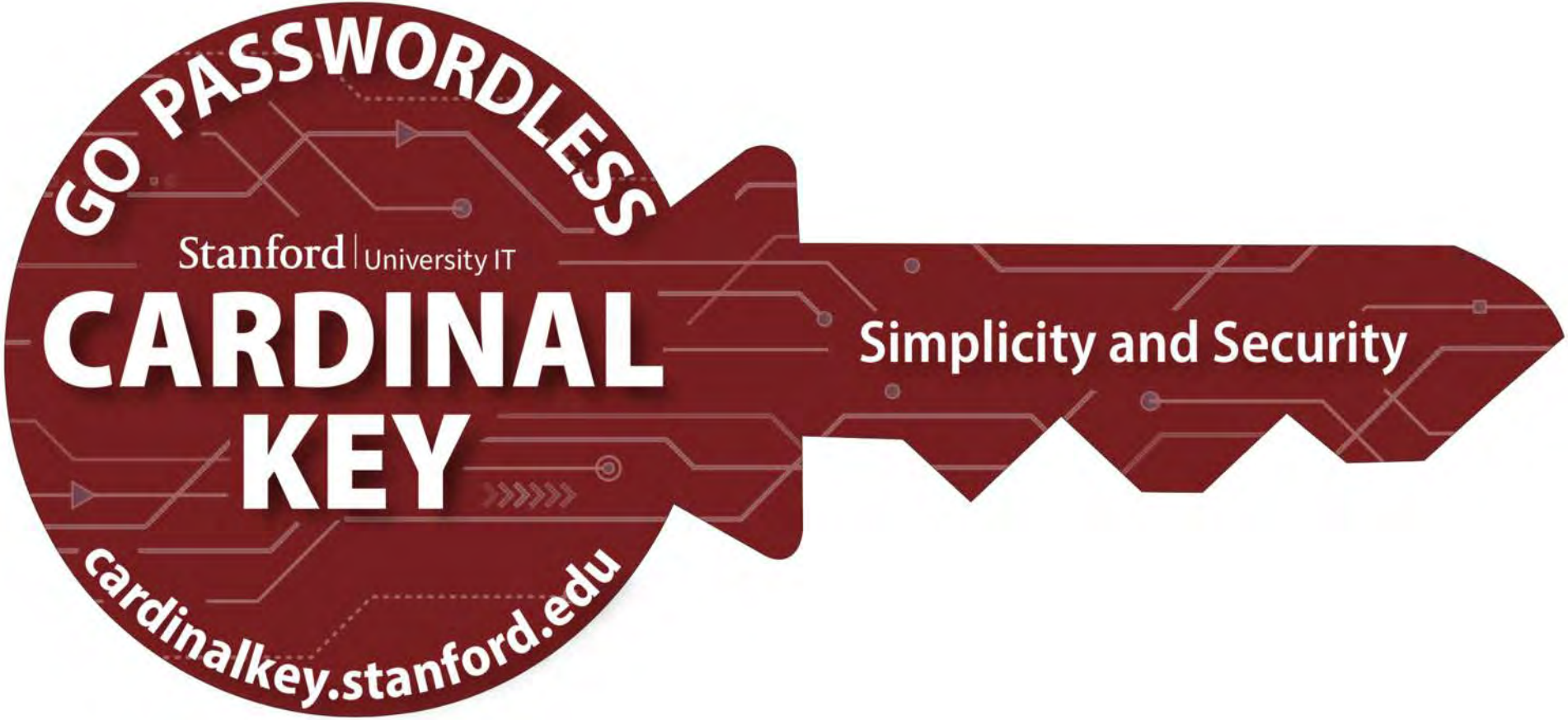
Incentives

- Simplified logins
- Protection against credential phishing

Requirements

- Must have endpoint agent
- Must meet our cybersecurity standards

Adoption


GO PASSWORDLESS
Stanford | University IT
CARDINAL KEY
Simplicity and Security
cardinalkey.stanford.edu

Stanford | Login

SUNet ID:

Password:

Login

Go passwordless and skip this login page with Cardinal Key.
Learn more »

Important Security Information: Logging in lets you access other protected Stanford websites with this browser, not just the website you requested.

LOGIN HELP

FORGOT YOUR PASSWORD?

Use of this system is subject to Stanford University's rules and regulations. See the Stanford Administrative Guide for more information.

Cardinal Key Stats: Past 30 Days

VPN: Total Cardinal Key Authorizations (Success & Rejects)

source: Radius VPN

31,925

VPN: Unique Cardinal Key Users

source: Radius VPN

1,905VPN

Web SSO: Enrollment ID Count

source: auth idp

6,368

Web SSO: User Count

source: auth idp

2,816Web SSO

Opt-in Security Doesn't Work

(even when the benefits are overwhelmingly compelling)

Enforcement Mechanisms

- Require by user in Shibboleth
- Require by service in Shibboleth

How It Works

mjduff/Enrollment-EAE917EB-8EAF-4E9D-8793-97937B95592F

Issued by: Stanford University MyDevices Intermediate CA

Expires: Monday, April 10, 2023 at 5:18:21 PM Pacific Daylight Time

This certificate is valid

5 Year Lifetime

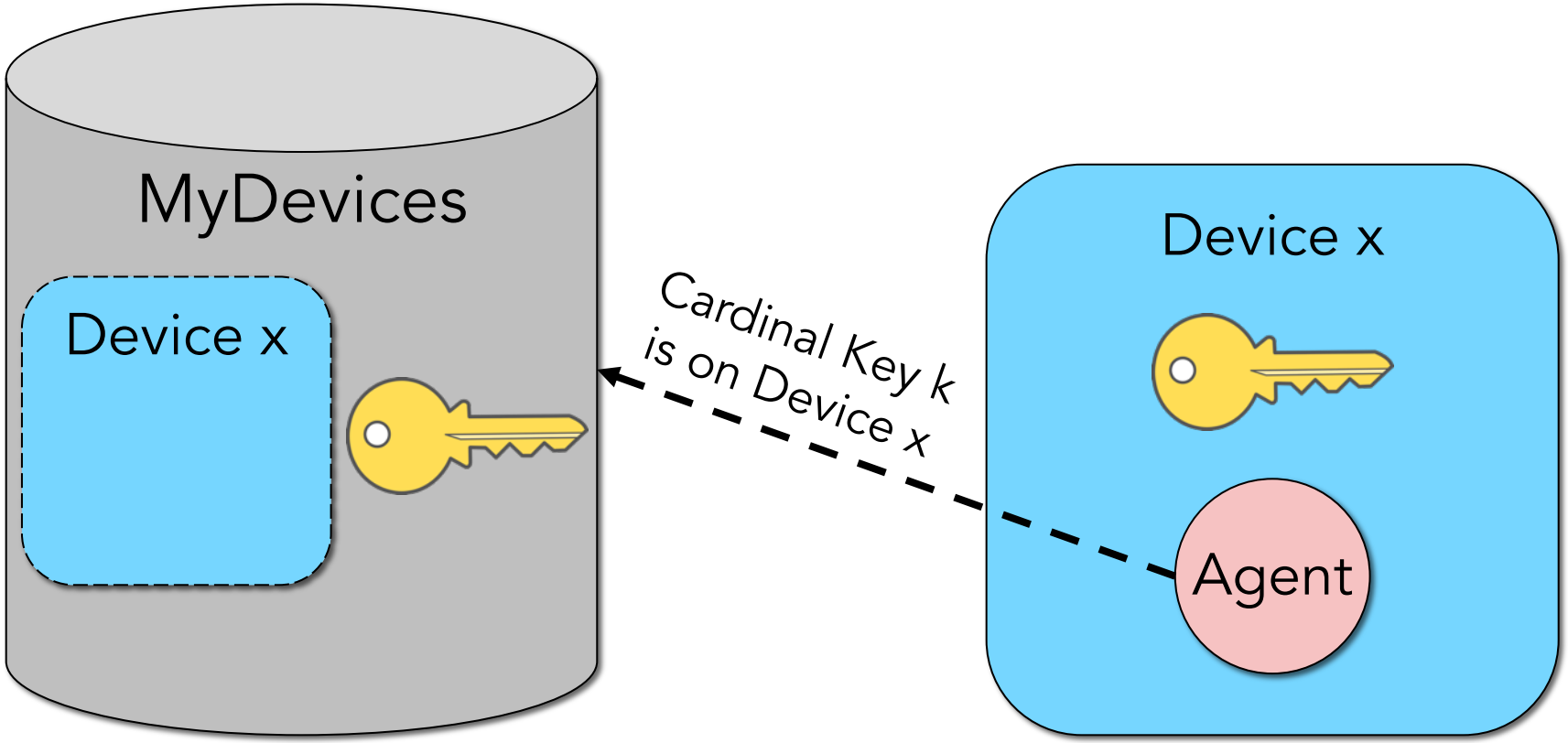
▶ **Trust**

▼ **Details**

Subject Name	
Common Name	mjduff/Enrollment-EAE917EB-8EAF-4E9D-8793-97937B95592F
Organization	Stanford University
Organizational Unit	MyDevices
Country	US
Title	Michael's MacBook
Issuer Name	
Country	US
Organization	Stanford University
Common Name	Stanford University MyDevices Intermediate CA

Identifies user and device

Mapping Cardinal Keys to Devices



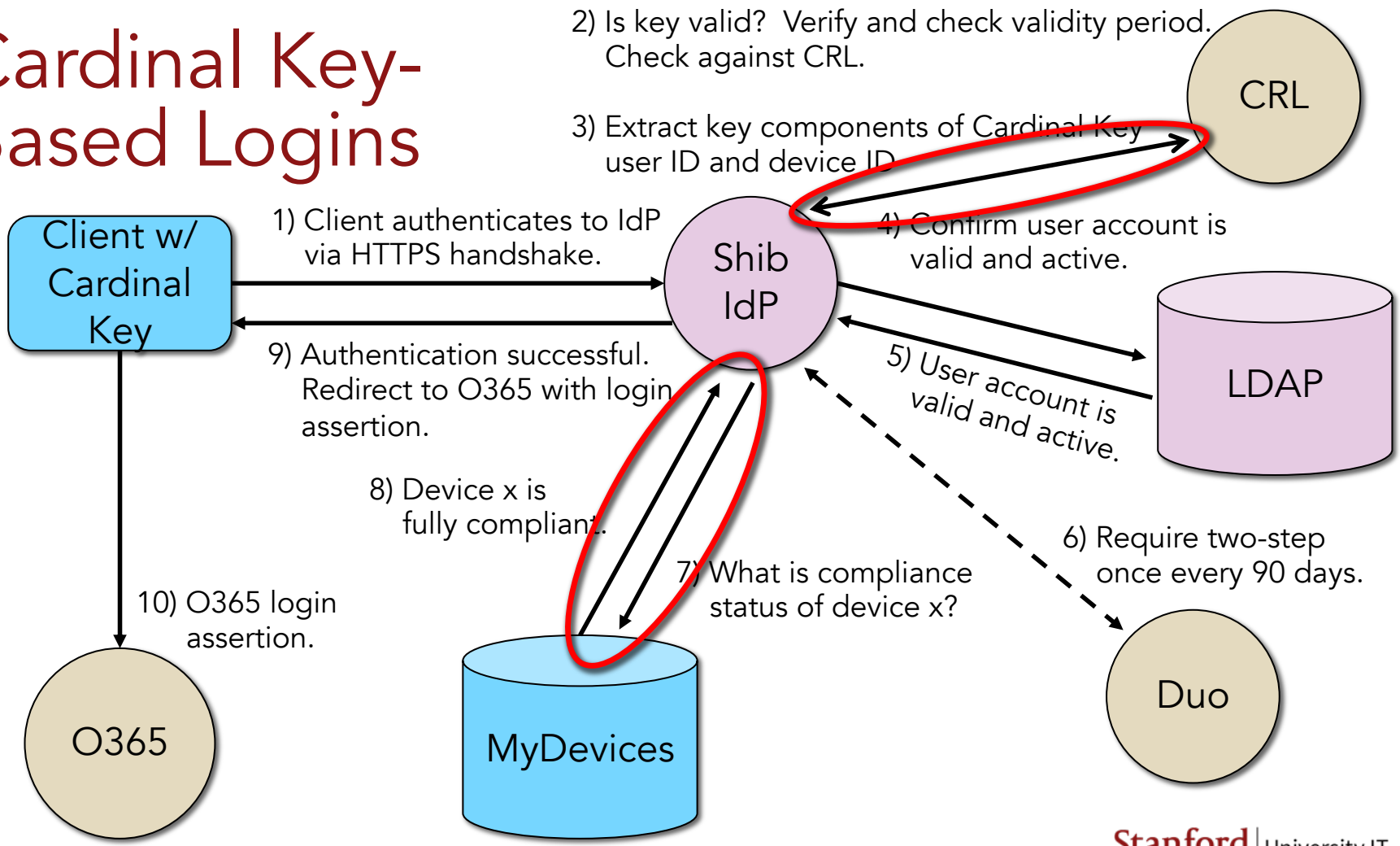
Device Information

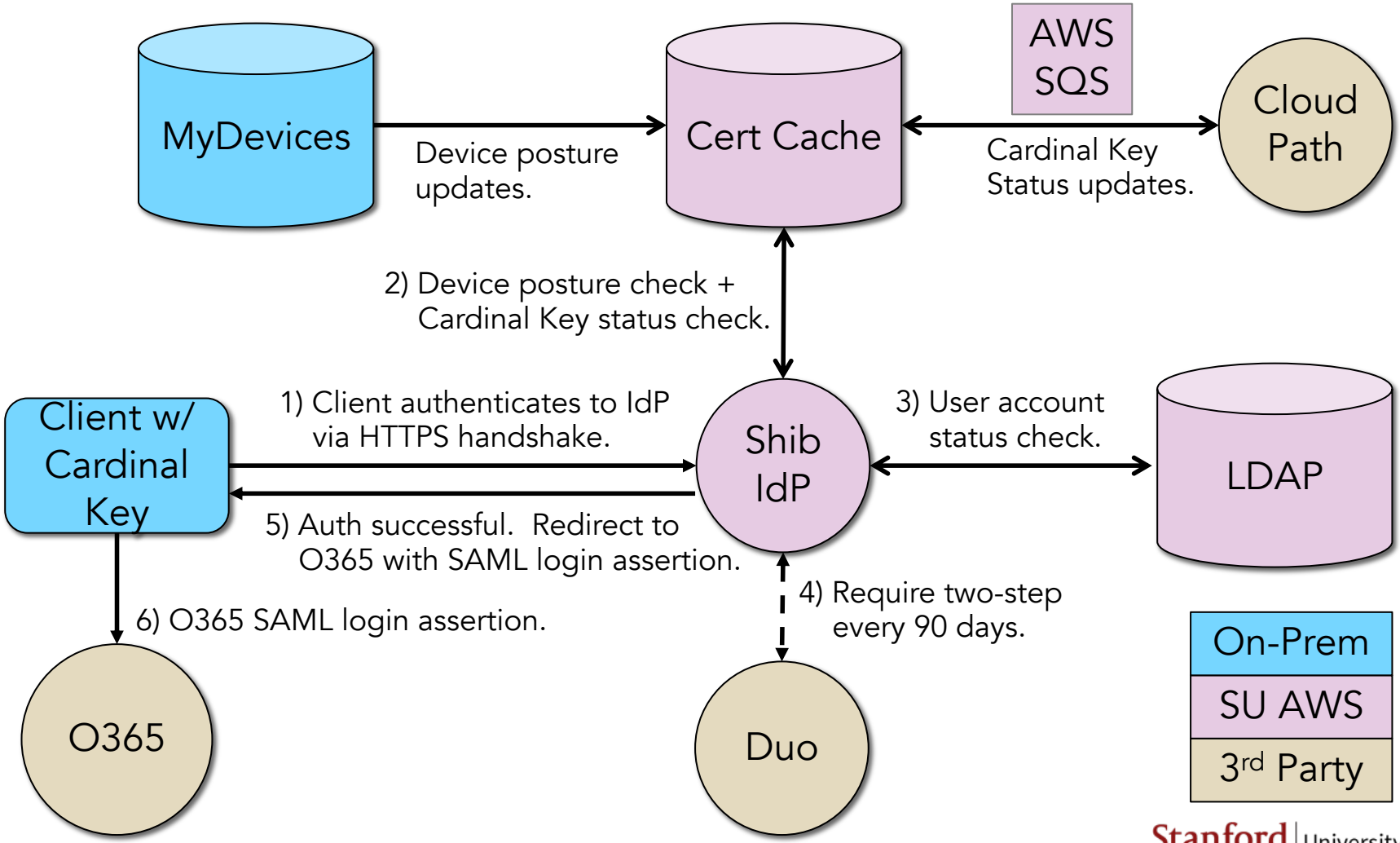
Model	Apple - MacBookPro15,2
Name	ISO-C02XH4H6JHD2
Type	Laptop
Serial Number	C02XH4H6JHD2
Operating System	Mac OS X 10.14.4
Encryption Status	Encrypted *Last checked at 2019-05-14 15:25:29* Recover your encryption key
Hardware Address(es)	3c:07:54:30:be:d5 f0:18:98:60:5b:aa
SUNet ID	mjduff

Cardinal Key Information

Cardinal Key	Work MacBook *Valid from 2018-10-21 to 2023-10-21*	View details

Cardinal Key-Based Logins



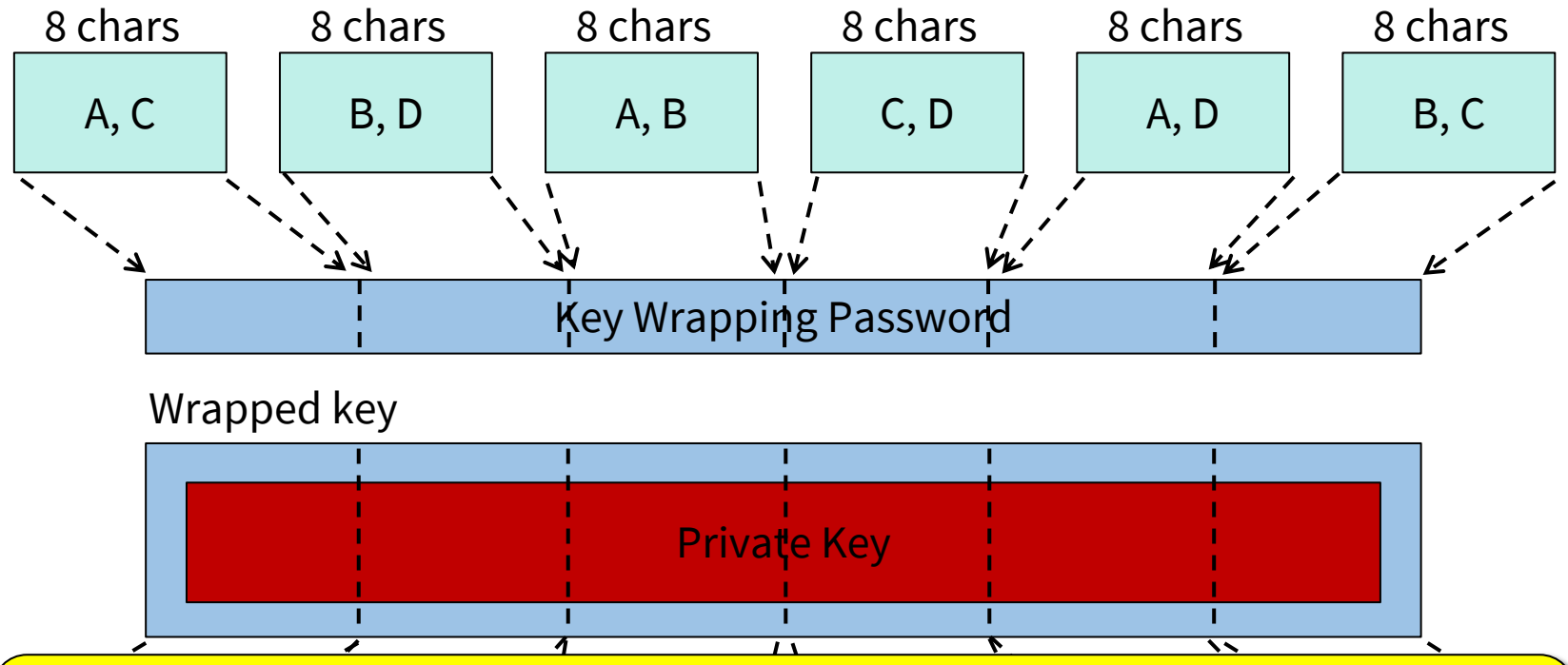

MyDevices
Device posture updates.
Cert Cache
AWS SQS
Cardinal Key Status updates.
Cloud Path
2) Device posture check + Cardinal Key status check.
Client w/ Cardinal Key
1) Client authenticates to IdP via HTTPS handshake.
Shib IdP
3) User account status check.
LDAP
5) Auth successful. Redirect to O365 with SAML login assertion.
4) Require two-step every 90 days.
6) O365 SAML login assertion.
O365
Duo
On-Prem
SU AWS
3rd Party

CA Key Ceremony

- Undisclosed location
- Recording (via Zoom)
- Raspberry Pi (instead of HSM) – no networking
- Standard keyboard & monitor
- Keys generated with OpenSSL → RAM disk
- No other computing devices permitted
- 10 pages of rehearsed step-by-step instructions
- 7 people x 10 hours

Key Ceremony

Key Masters: A, B, C, D



Use Shamir Secret Sharing instead

Cert Cache

- Transactional, HA MySQL database
  - Feature of Shibboleth IdP
  - Maps cert CN → device and cert status
- REST API written in node.js
  - Invoked by Shibboleth IdP, MyDevices, and CloudPath

Certificate Hierarchy

- Root CA (20 yrs): cn=Stanford University MyDevices Root CA, o=Stanford University, c=US
  - Intermediate CA (10 yrs): cn=Stanford University MyDevices Intermediate CA, o=Stanford University, c=US
    - User/device (5 yrs): cn=*userID/deviceID*, title=*Device Name*, ou=MyDevices, o=Stanford University, c=US
      - Subject Alternative Name: rfc822Name = *emailAddress*

Stanford University MyDevices Root CA

Root certificate authority

Expires: Saturday, January 9, 2038 at 8:20:44 AM Pacific Standard Time

Details

Subject Name

Country	US
Organization	Stanford University
Common Name	Stanford University MyDevices Root CA

Issuer Name

Country	US
Organization	Stanford University
Common Name	Stanford University MyDevices Root CA

Stanford University MyDevices Intermediate CA

Intermediate certificate authority

Expires: Sunday, January 9, 2028 at 9:20:45 AM Pacific Standard Time

▼ **Details**

Subject Name

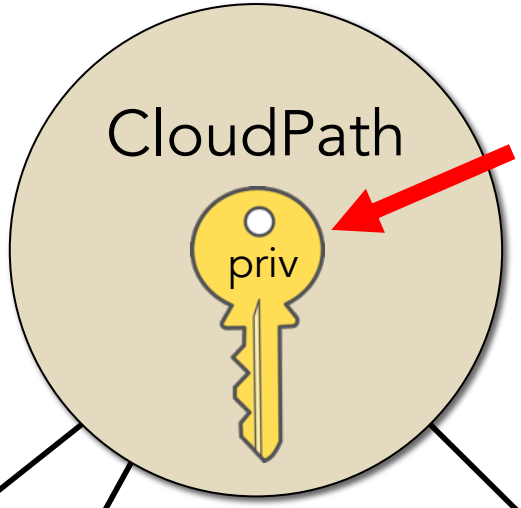
Country	US
Organization	Stanford University
Common Name	Stanford University MyDevices Intermediate CA

Issuer Name

Country	US
Organization	Stanford University
Common Name	Stanford University MyDevices Root CA

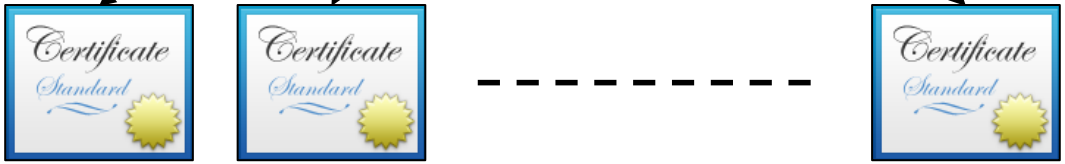
SaaS Certificate Issuing Service

Root CA private key:
Never online and requires
3 people to reassemble



Intermediate private key:
Stored in CloudPath and
used to generate certs

User/device
certs



Key Design Decision Summary

- Campus-wide 2FA
- Building MyDevices
- Device-specific user certs
- Certs do not convey device posture status → ID only
- 5-year user/device cert lifetimes
- Cert hierarchy, fields, and 4K key sizes
- CA key ceremony
- Requiring 2FA for cert fetch and web SSO (periodically)
- SaaS cert issuing service
- Cert cache infrastructure
- Mapping certs to devices in MyDevices

Lessons Learned

- Most calendar time consumed by design decisions
- MyDevices wildly successful, yet resource-intensive to build
  - Open source platforms now available: Netflix Stethoscope
  - Similar: Google's BeyondCorp, Duo Beyond
- UX improvements have a powerful impact
- Importance of branding

Resources

- cardinalkey.stanford.edu
- uit.stanford.edu/service/mydevices
- twostep.stanford.edu
- encrypt.stanford.edu
- riskclass.stanford.edu
- minsec.stanford.edu

michael.duff@stanford.edu

Please evaluate today's session

https://www.surveymonkey.com/r/IAMOnline-Nov2019

2019 Technology Exchange

https://meetings.internet2.edu/2019-technology-exchange/

December 9-13, 2019

New Orleans, Louisiana

2020 BaseCAMP

June 23-25, 2020

Milwaukee, Wisconsin