

# RSA®Conference2015

Singapore | 22-24 July | Marina Bay Sands

SESSION ID: CDS-R02

## The Secret Life of Data: Protecting Sensitive Information, Mobile to Cloud

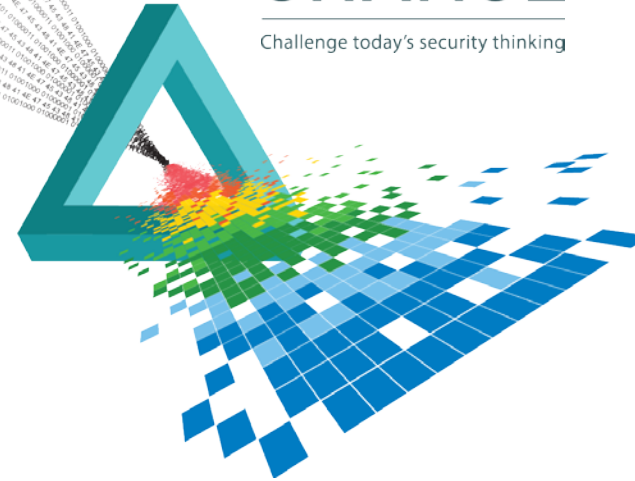
**Dan Griffin**

---

President  
JW Secure, Inc.  
@JWSdan

# CHANGE

Challenge today's security thinking



# WWNSAD?

- ◆ Intelligence agencies have been public about:
  - Inevitability of mobile computing
  - Support need for cloud-based services, even when using secret data in the field
- ◆ What works for them can work for you













# Building blocks of security

- ◆ What is a TPM?
- ◆ What is “measured boot”?
- ◆ What is “remote attestation”?



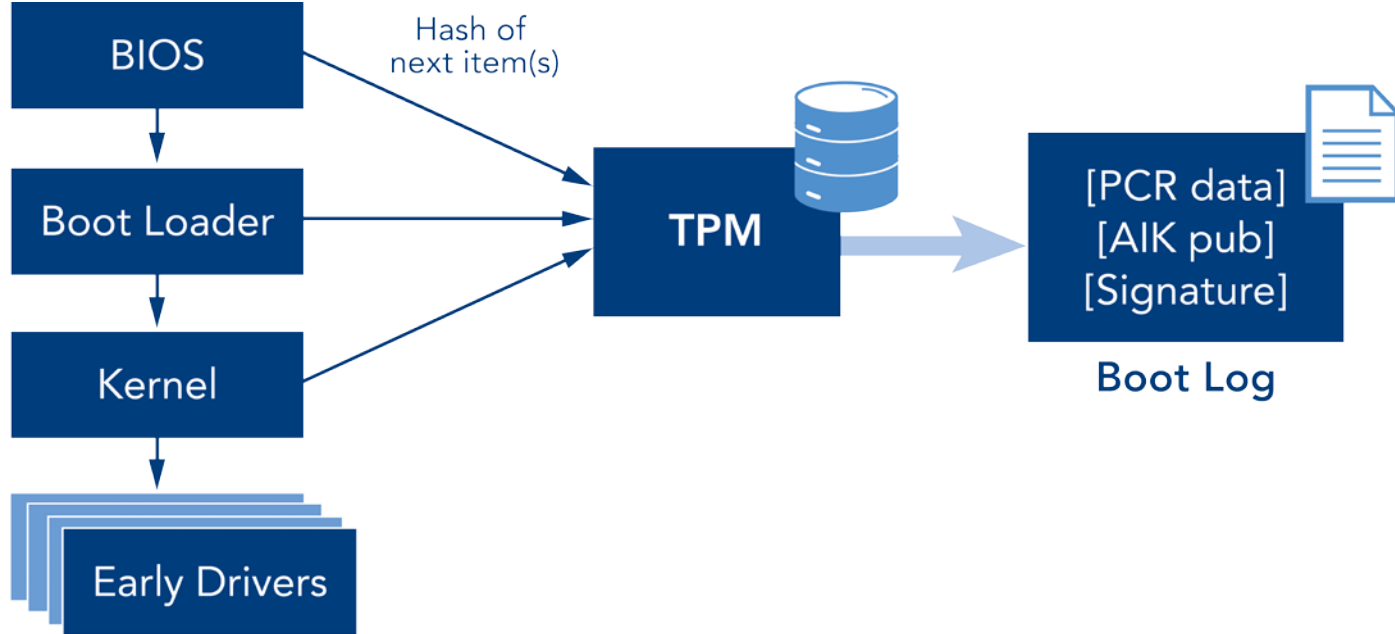
# RSA<sup>®</sup>Conference2015

Singapore | 22-24 July | Marina Bay Sands

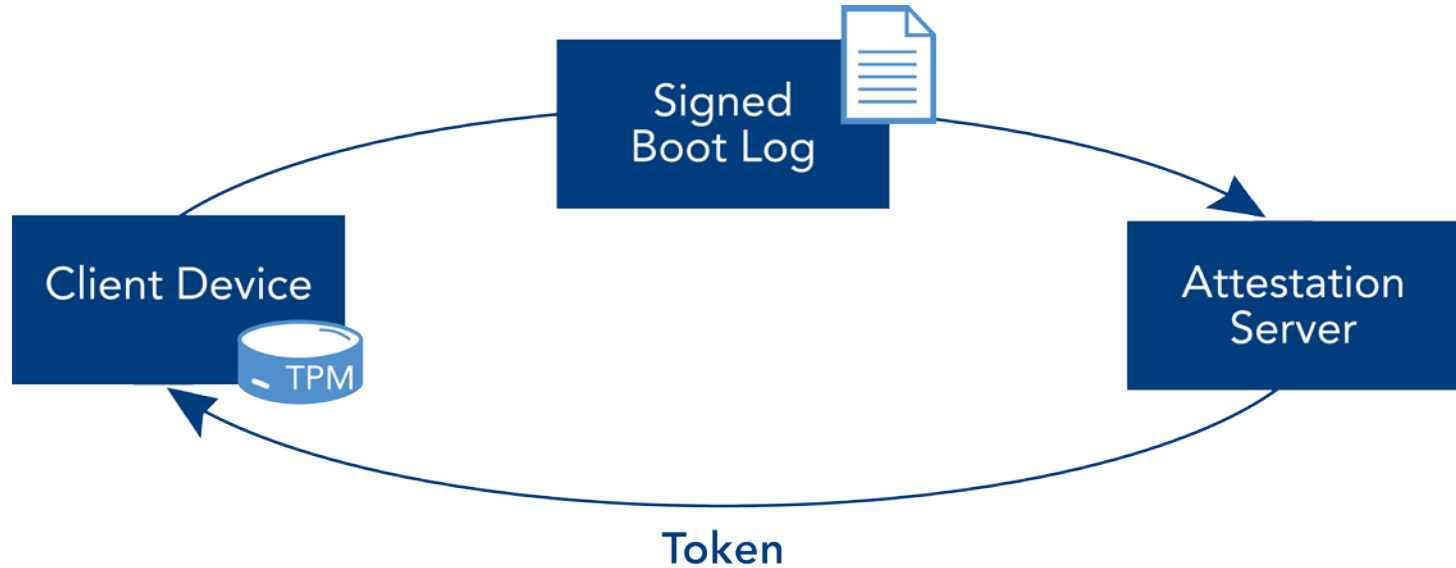
## Measured Boot + Remote Attestation



# What is measured boot?



# What is remote attestation?



# DEMO

- ◆ Sample application #1: reduce fraud in mobile/consumer scenarios

# Cloud services demand ID

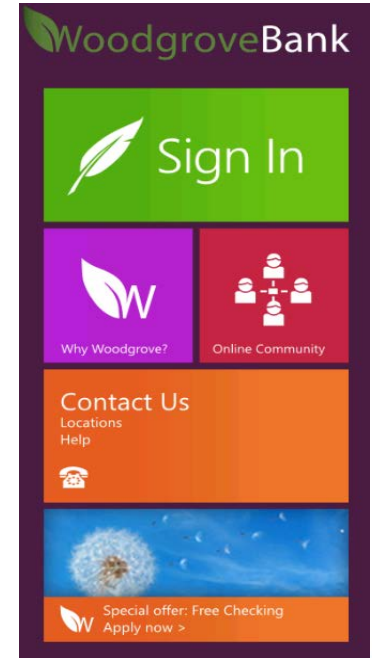
- ◆ Enterprise: BYOD
- ◆ Consumer
  - Targeted advertising
  - eCommerce, mobile banking, etc.
- ◆ Most user IDs are static & cached on a device
  - That only works for low-value purchases
  - How do you improve ID for high-value purchases?

# Low friction authentication

- ◆ Each additional screen requires user input
  - Slows down the process while user re-orientates
  - Causes more users to abandon the web site
- ◆ In contrast, progressive authentication
  - Lets users investigate a site using just cookies
  - Defers questions until information is needed
  - Reduces user drop out from frustration

# Splash screen

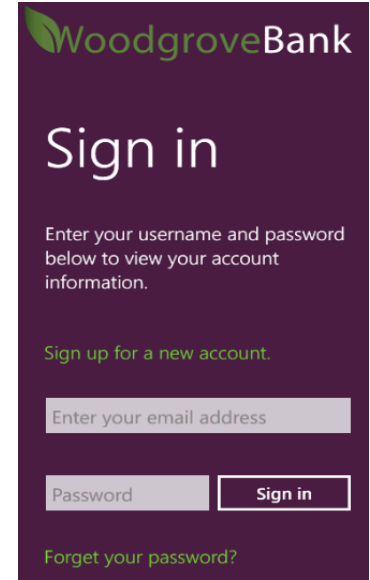
- ◆ The screen a user sees when app launched
- ◆ Similar data in the launch tile





# User sign in

- ◆ User name can be taken from cookie
- ◆ Account details are hidden until the user enters a password



WoodgroveBank

## Sign in

Enter your username and password below to view your account information.

[Sign up for a new account.](#)

Enter your email address

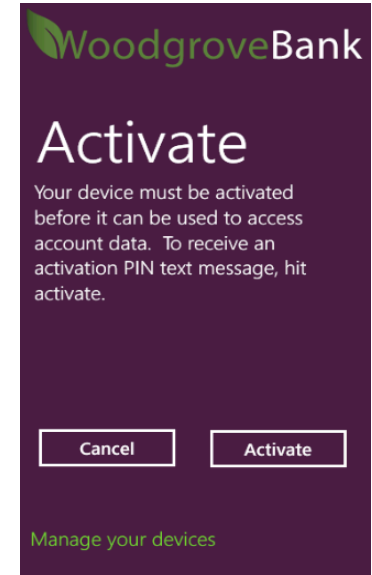
Password

[Sign in](#)

[Forget your password?](#)

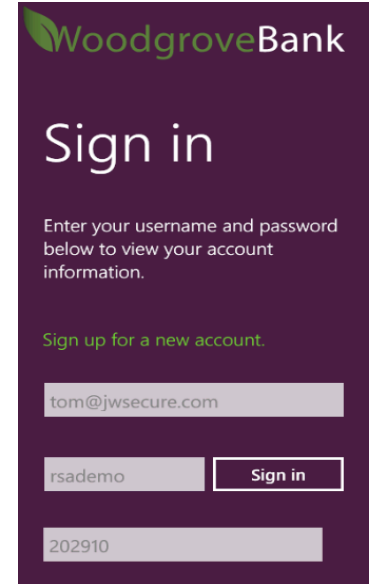
# Enrollment: 1

- ◆ The first time the app is used the user must activate the app
- ◆ When this button is pressed, an SMS message is sent to the phone # on file



## Enrollment: 2

- ◆ After the user gets the pin from the SMS message, it is entered
- ◆ After this, the user proceeds as with a normal sign-in procedure



WoodgroveBank

### Sign in

Enter your username and password below to view your account information.

[Sign up for a new account.](#)

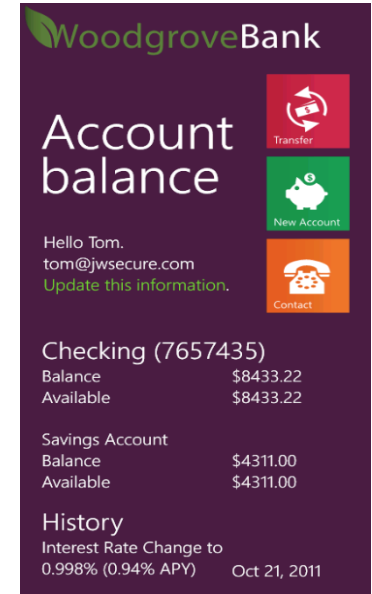
tom@jwsecure.com

rsademo

202910

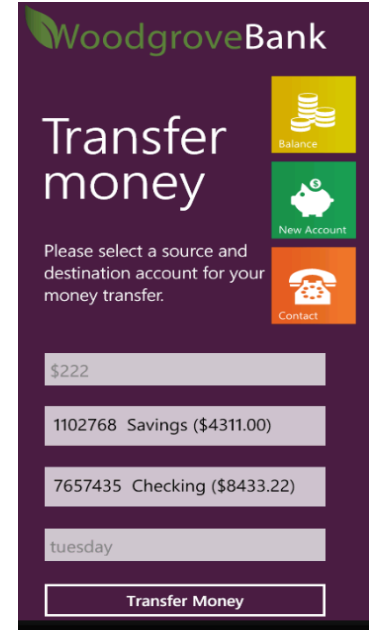
# After sign in

- ◆ The user sees all account information



# User tries to move money

- ◆ When user goes to move \$ out of account, the health of the device is checked



WoodgroveBank

## Transfer money

Please select a source and destination account for your money transfer.

- Balance
- New Account
- Contact

\$222

1102768 Savings (\$4311.00)

7657435 Checking (\$8433.22)

tuesday

Transfer Money

# Remediation needed

- ◆ If the device is not healthy enough to allow money transfer, the user is directed to a site to fix the problem

The device does not appear to be updated with the latest firmware.

Please visit our website at <http://www.woodgrovebank.com/mobile> to find out how to solve the problem.

ok

Contact

\$222

1102768 Savings (\$3534.00)

7657435 Checking (\$9210.22)

Memo (optional)

Transfer Money

# Protecting cloud data with attestation

- ◆ Data or access key is hardware encrypted
- ◆ Key is bound to specific authenticated TPM
- ◆ Device must be policy compliant for key to work
- ◆ Otherwise data cannot be viewed and network resources cannot be accessed



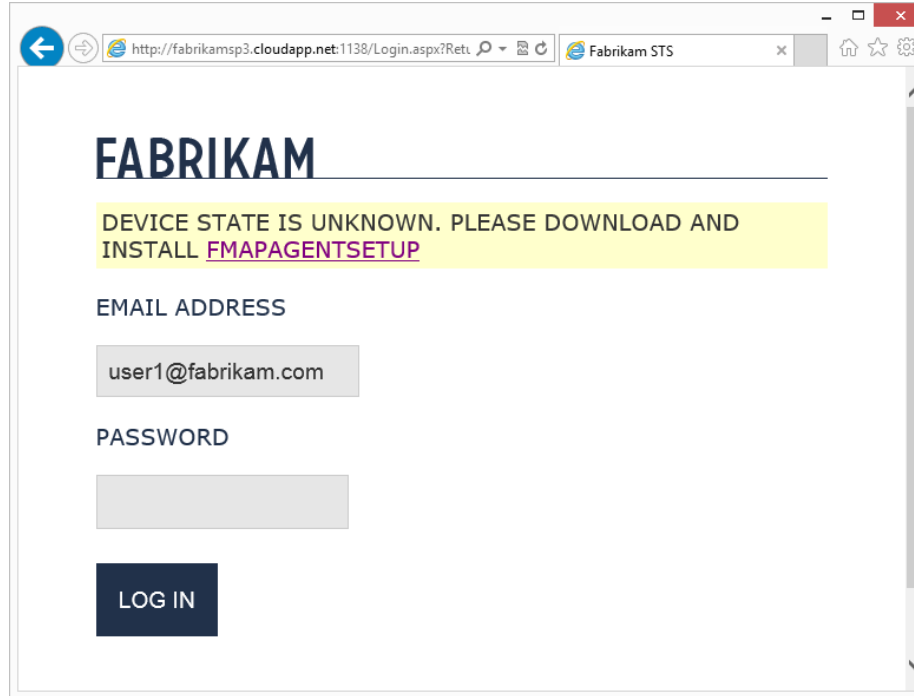
# DEMO

- ◆ Sample application #2: protect cloud data

# Policy-enforced file access

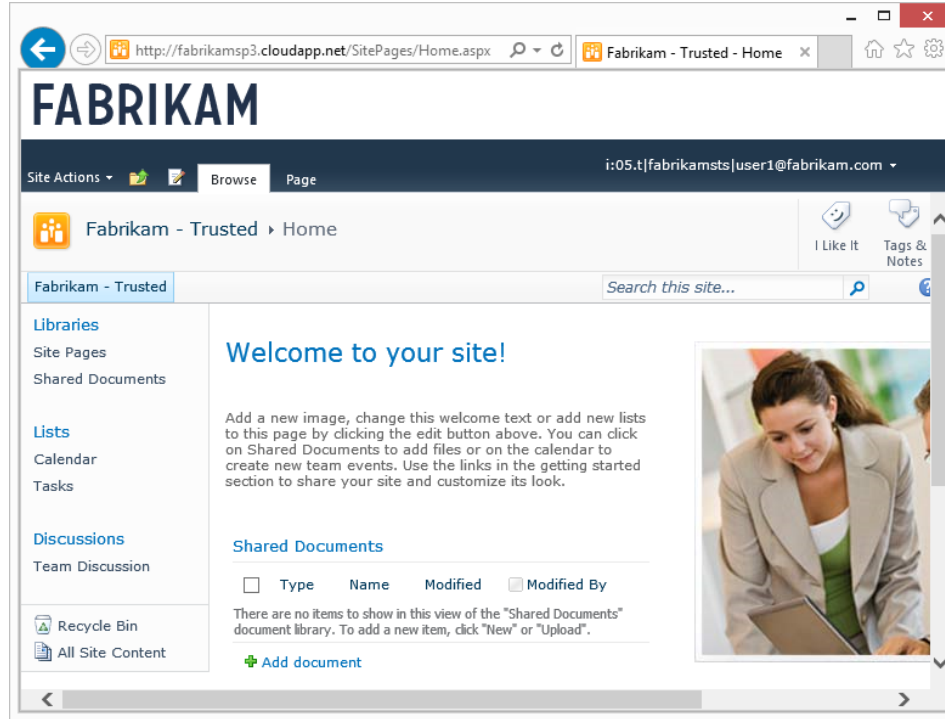
- ◆ BYOD
- ◆ Download sensitive files from document repository
- ◆ Leave laptop in back of taxi

# Device authorization for SharePoint

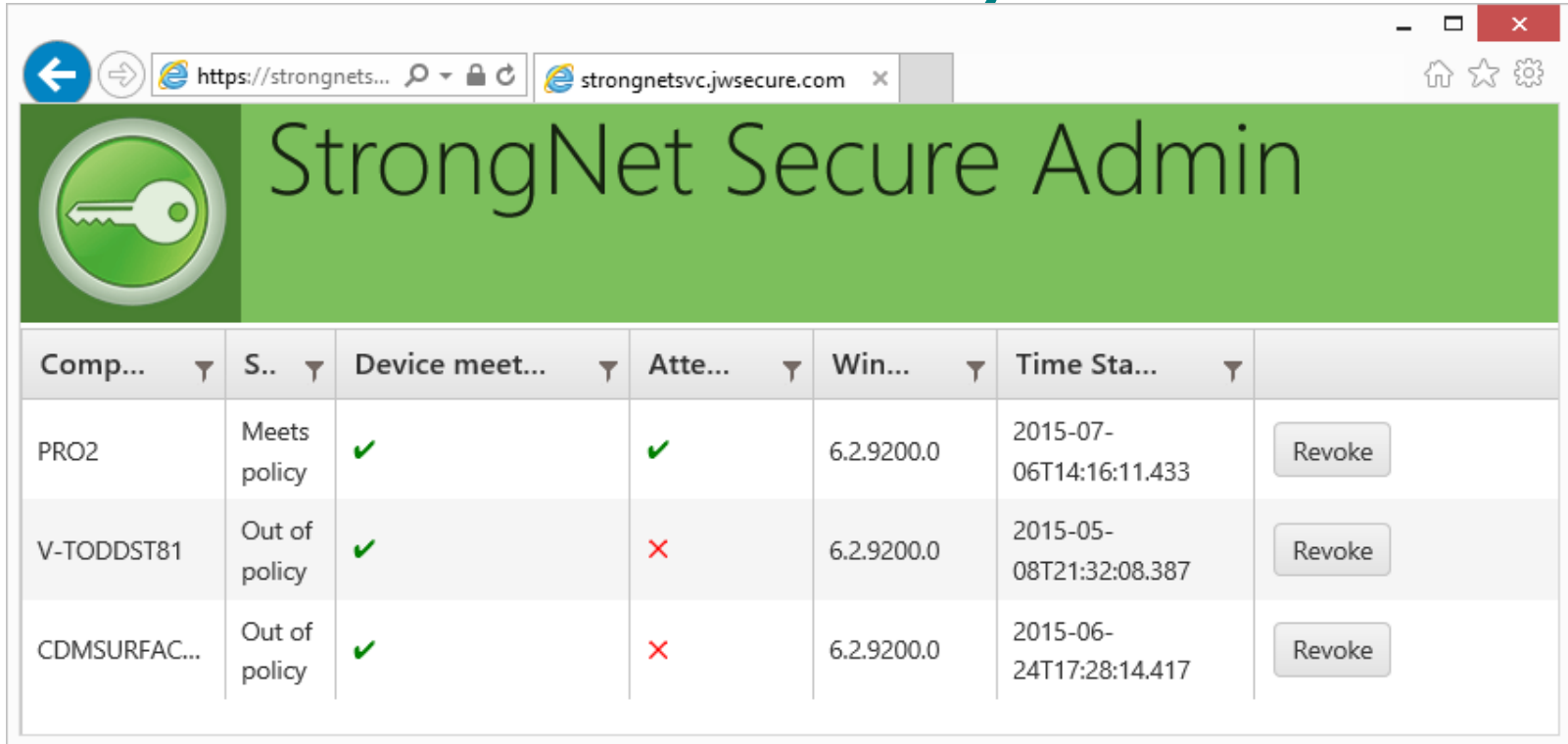


The screenshot shows a web browser window with the address bar displaying `http://fabrikamp3.cloudapp.net:1138/Login.aspx?Retu...` and the page title "Fabrikam STS". The main content area features the "FABRIKAM" logo at the top. Below the logo, a yellow highlighted box contains the message: "DEVICE STATE IS UNKNOWN. PLEASE DOWNLOAD AND INSTALL [FMAPAGENTSETUP](#)". Underneath this, there are input fields for "EMAIL ADDRESS" (containing "user1@fabrikam.com") and "PASSWORD" (empty). A dark blue "LOG IN" button is positioned at the bottom of the form.

# Device authorization for SharePoint



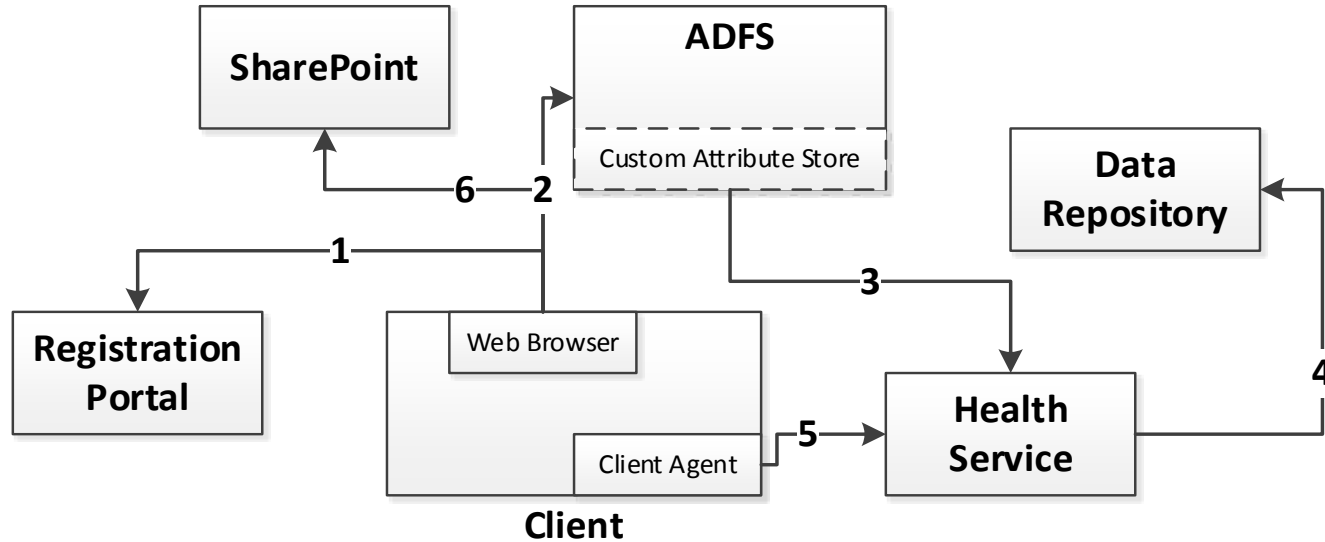
# Device authorization telemetry



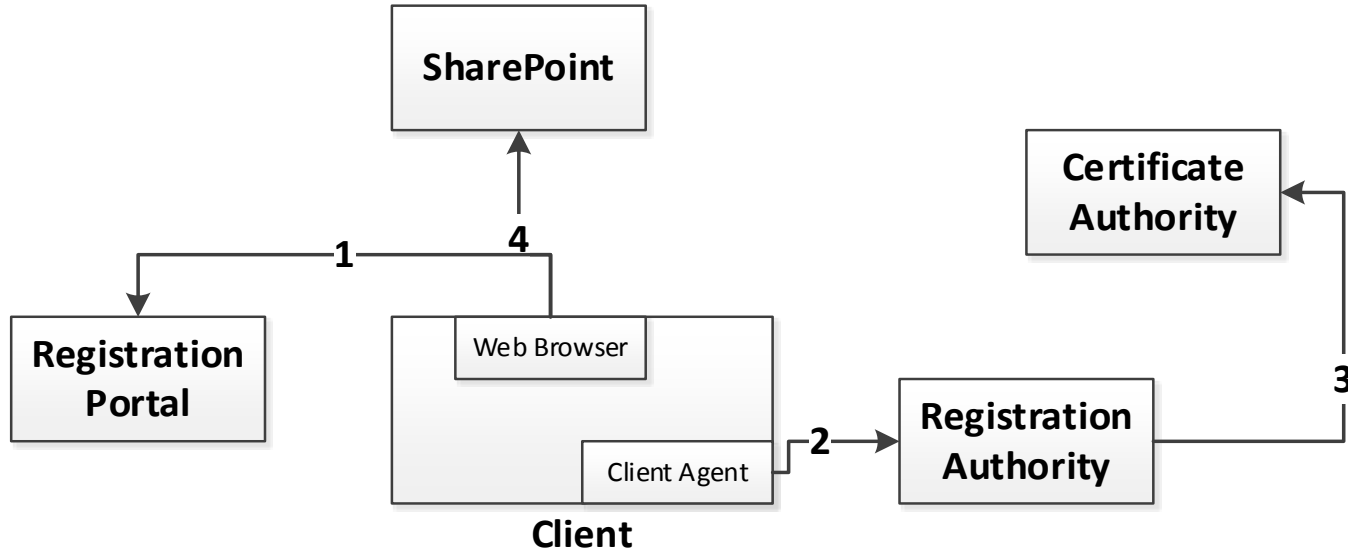
The screenshot shows a web browser window with the address bar displaying `https://strongnetsvc.jwsecure.com`. The page title is "StrongNet Secure Admin" with a key icon. Below the header is a table with columns: Comp..., S..., Device meet..., Atte..., Win..., Time Sta..., and an action column. The table contains three rows of data, each with a "Revoke" button.

Comp...	S...	Device meet...	Atte...	Win...	Time Sta...	
PRO2	Meets policy	✓	✓	6.2.9200.0	2015-07-06T14:16:11.433	Revoke
V-TODDST81	Out of policy	✓	✗	6.2.9200.0	2015-05-08T21:32:08.387	Revoke
CDMSURFAC...	Out of policy	✓	✗	6.2.9200.0	2015-06-24T17:28:14.417	Revoke

# Device authorization for SharePoint



# Device authorization for SharePoint





# Weaknesses of TPM remote platform attestation

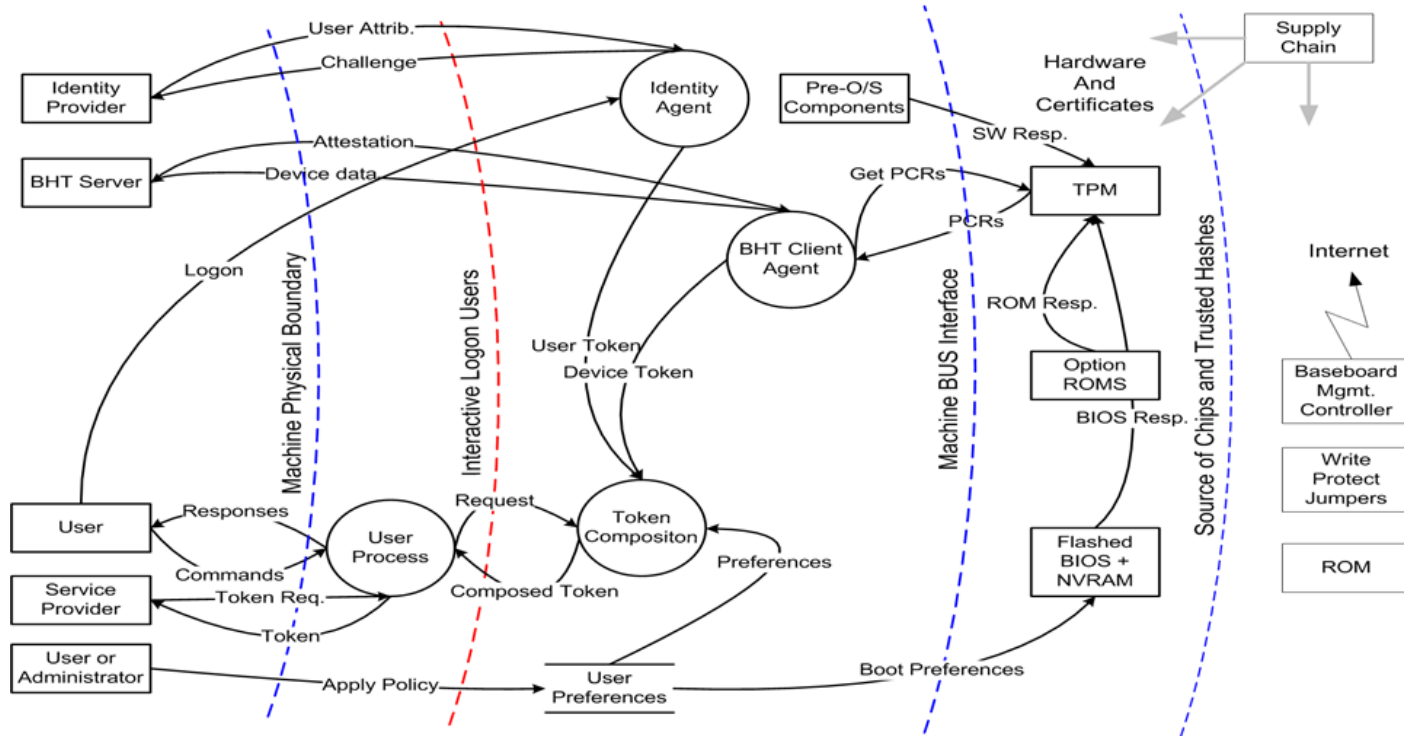
## ◆ Provisioning

- Secure supply chain?
- TPM EK database
- Patching delay and whitelist maintenance (firmware and drivers)

## ◆ Integrity of the TPM hardware

- Capping - electron microscopes
- Migration trend from hardware to firmware

# Attestation Data Flow Diagram



# Recent developments

- ◆ Measurement-bound keys
  - “Trusted Tamperproof Time on Mobile Devices”
  - See <http://www.jwsecure.com/dan>
- ◆ Commercial availability
  - JW Secure StrongNet
  - Google Chromebook
  - Intel Trust Attestation Solution
  - Microsoft TPM Key Attestation

# Next steps

- ◆ Audit current systems
  - How do you prevent stolen credentials?
  - Do you depend on encryption alone?
  - Who has admin access to critical systems?
  - Is your BYOD policy managed tightly, or is it increasing your risk?
  - Are you relying on static passwords and traditional antivirus programs?
  - Do you authenticate computers as well as users?

## In summary, you can:

- ◆ Continuously enforce security policy in hardware, firmware and software
- ◆ Ensure that sensitive data is always encrypted—everywhere
- ◆ Enable strong authentication of users and computers
- ◆ Mitigate credential theft



# Questions?

Call or email me with questions, or to request a demo of StrongNet:

[dan@jwsecure.com](mailto:dan@jwsecure.com)

+1 206 683 6551

@JWSdan

JW Secure provides custom security software development services.