

#### 4 steps to Manage Authentication

**Relatore** Schwartz, Michael

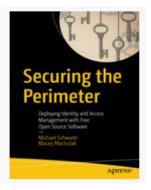




# Mike Schwartz







Podcast Interviews w/ 50+ successful open source software vendors

### **Gluu Founder / CEO**

20+ years in IAM

Author Apress book on IAM





### Step 1: Select Authenticators



#### **Authenticators**



Authenticators you don't have to license

- Password
- Email / SMS
- Social Login
- HOTP / TOTP
- Enterprise Federated Login FIDO USB / Bluetooth / Platform / NFC
- Smart Card

**Commercial Authenticators** 

- Duo
- Transmit
- Stytch
- BioID
- etc.





# Step 2: Offer Self-Service Authenticator Life Cycle



#### Self-Service Authenticator Life Cycle

- Study Google "2-step Verification"
- Let people register as many credentials as they want
- Note innovation in FIDO:
  - MacBook Air (Platform)
  - OnePlus 9 smartphone (Bluetooth)
  - FIDO devices can't be top-down provisioned--tied to biometric

	Øcasa	=	Michael Schwartz v
e	2FA credentials Security Keys and built-in	← Home page	
	Platform Authenticators Super Gluu Devices Biometric Credentials Mobile Phane Numbers DUO Credentials	Security Keys and built-in Platform Authenticators Protect your online accounts against unauthorized access by using 2 factor auth /NFC] and built-in Platform authenticators (Apple's Touch ID).	entication with Security keys ( USB
	OTP Tokens  Password Reset  Administration console	ATKey.Pro-C Adada or: Jan 20, 2021-04:06 PM	× =
	<ul> <li>Accounts linking</li> <li>Consent management</li> </ul>	Added on: Mar 30, 2021 - 11:24 AM	× =
		Yubi-C Added or: May 11, 2021-09:04 AM	
		Vubikey 4 Added on: Jul 16, 2021 - 12:35 PM	
		Yubi Blue Added on: Aug 11, 2021-09:49 AM	
		OnePlus 9 (LE2110) Added or: Oct 22, 2021 - 11:15 AM	× •
		Yubi-C FIPS Added or: Nov 10, 2021-05:11 PM	
		MacBook Air Added or: Nov 10, 2021 - 05:24 PM	
		HyperFIDO Mini Added or: Nev 10, 2021-05-26 PM	
Gluu Casa	! ──→	Yubi Bio Added or: Nev 10, 2021-05:31 PM	
		Register a security key Insert your security key and press the "Ready" button below Ready	



## Step 3: Define Application Interfaces



#### Application interfaces

**OpenID Connect** 

- Preferred interface for "person authentication"
- Required for all new internal custom applications
- Choose security profile based on transaction value and risk
  - Is Mutual TLS required?
  - Are shared secrets allowed for client authentication?

OAuth

- Required for "machine-to-machine" authentication (i.e. backchannel API)
- For risky transactions, asymmetric client authentication should be required at the token endpoint

#### SAML

• Ok for "person authentication" for SaaS / legacy web applications

Non-Web

• Consider operating system, VPN, and other edge cases.





## Step 4: Implement Continuous Adaptive Authentication



#### Continuous Adaptive Authentication

Behavior

- Typing
- Mobile phone swipe history
- Activity pattern
- Smell

Context

- Previously known browser
- IP Address / Geolocation
- Using VPN?
- Fraud score
- Time of Day
- Client software
- Transaction value
- Status of consent



# Excellence in Digital Identity is a competitive advantage for organizations.







#### Join the project



#### **#OSW2021**



