



4 steps to Manage Authentication

Relatore
Schwartz, Michael



#OSW2021



RETE ITALIANA
OPEN SOURCE

Mike Schwartz



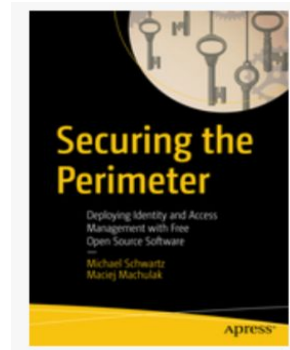
Podcast

Interviews w/ 50+ successful open source software vendors



Gluu Founder / CEO

20+ years in IAM



Author

Apress book on IAM





Step 1: Select Authenticators



RETE ITALIANA
OPEN SOURCE

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
- Stytn
- BiID
- etc.



Step 2: Offer Self-Service Authenticator Life Cycle

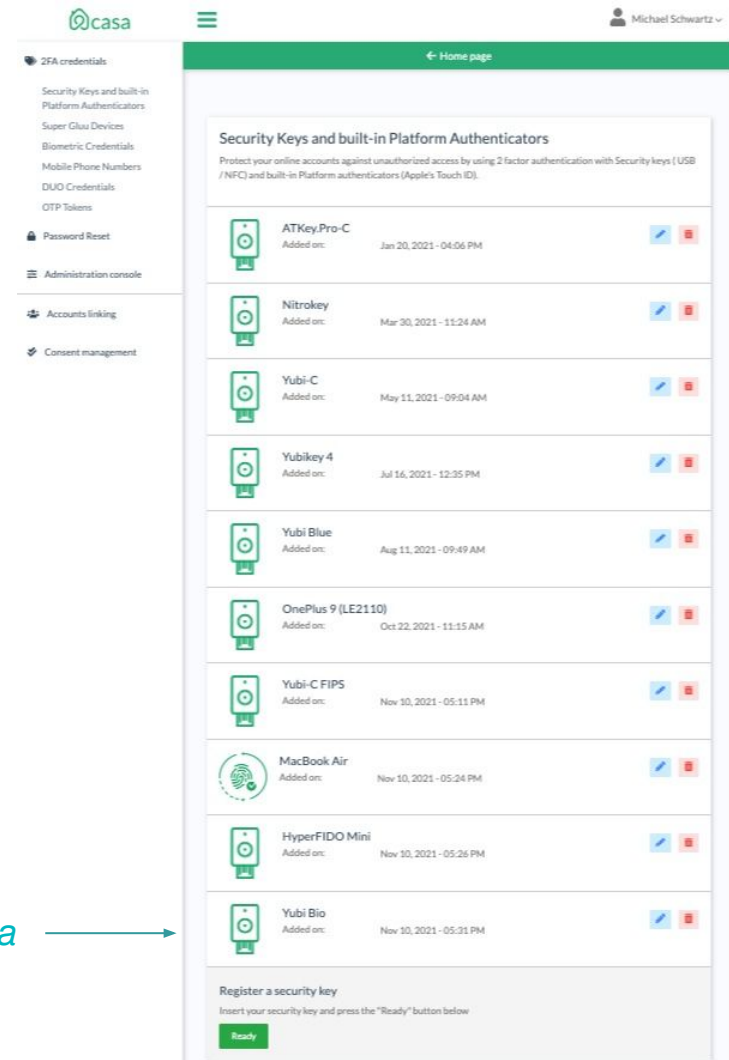


RETE ITALIANA
OPEN SOURCE

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*

Gluu Casa →





Step 3: Define Application Interfaces



RETE ITALIANA
OPEN SOURCE

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



RETE ITALIANA
OPEN SOURCE

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

The background is a solid teal color with faint, semi-transparent white line and bar charts overlaid. One line chart is in the upper left, another in the upper right, and a bar chart is in the lower right.

Excellence in Digital Identity is a competitive
advantage for organizations.



Join the project



#OSW2021



<http://www.reteitalianaopensource.net>



RETE ITALIANA
OPEN SOURCE