

---

# *Federated Identity in OneHealthPort*

*Ravi Sandhu\**  
*Chief Scientist*  
*NSD Security*

[www.nsdsecurity.com](http://www.nsdsecurity.com)

[sandhu@nsdsecurity.com](mailto:sandhu@nsdsecurity.com)

*703.283.3484*

\*Also Professor of Information Security and Assurance  
at George Mason University, Fairfax, Virginia

# Outline

---

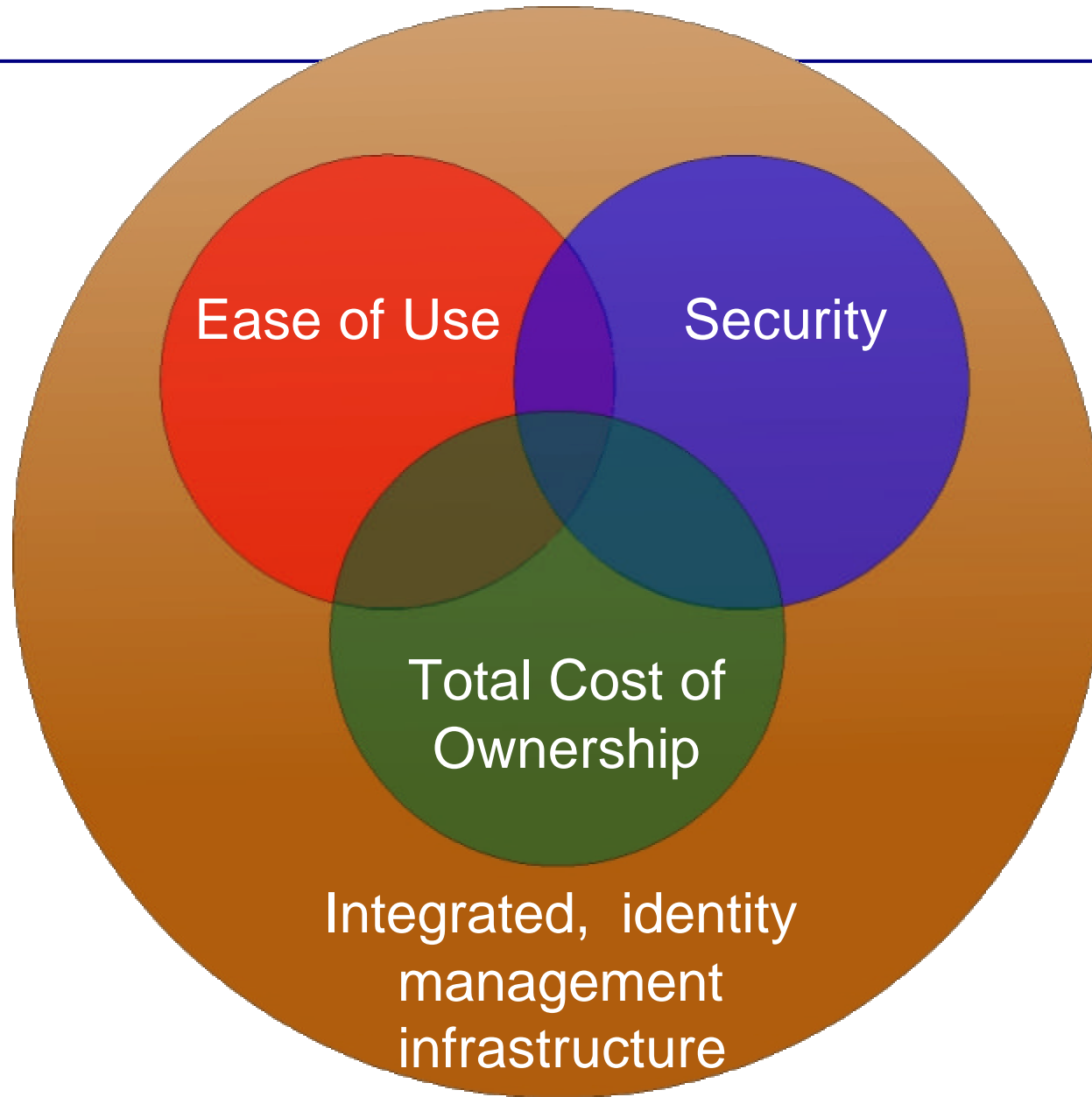
- What is security?
- What is OneHealthPort?
- What is OneHealthPort federated identity?
- What is the technology behind OneHealthPort federated identity?

# What is Security

---

- Catastrophic failure is a whole lot worse than occasional failure
- A single multi-functional infrastructure is better than multiple stovepipes
- Good enough security
  - Is all we can achieve
  - Tolerates occasional failure
  - Does not tolerate catastrophic failure

# Security is Only One Objective



# What is OneHealthPort?

---

- [What is OneHealthPort \(OHP\)?](#)

# The technology behind OneHealthPort

---

OneHealthPort



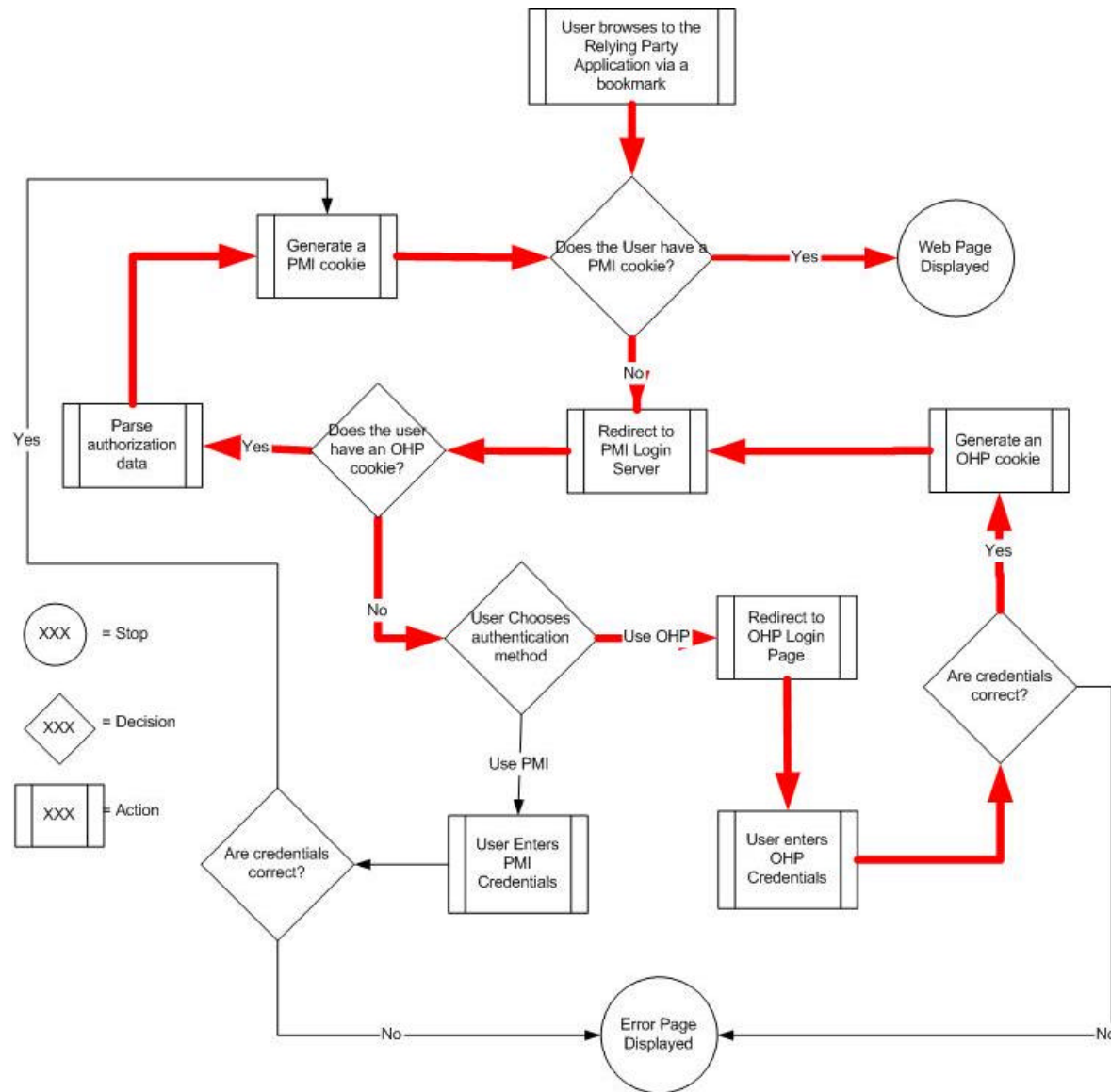
# What is OneHealthPort federated identity?

---

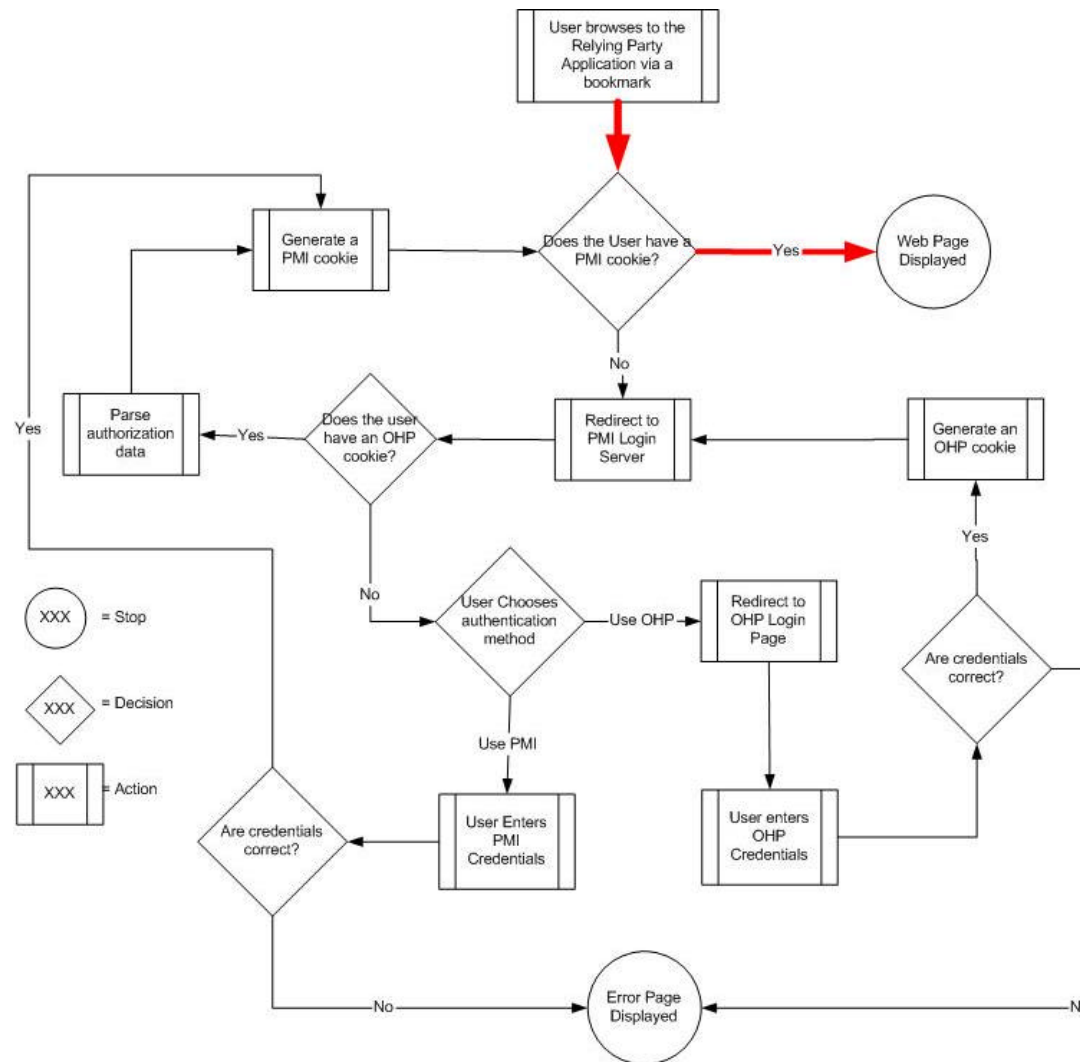
- [OHP Overview](#)
- [OHP Process Overview](#)
- [OHP Registration Flow](#)

# Use case 1: Subscriber has no Cookies

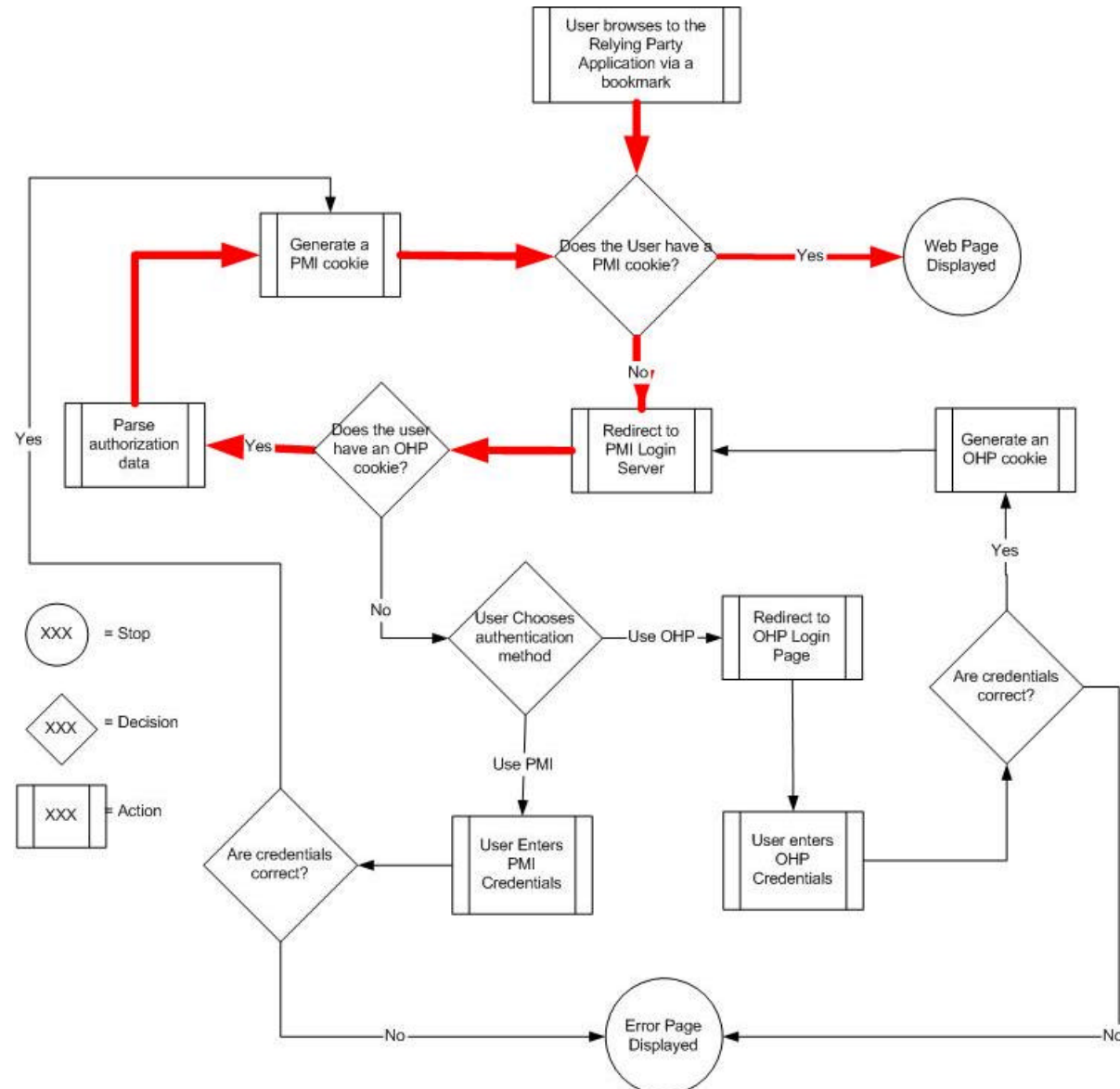
Gets OHP Cookie (planted by OHP at beTRUSTed) and PMI Cookie (planted by Relying Party)



## Use case 2: Subscriber has PMI Cookie (planted by Relying Party)



## Use case 3: Subscriber has OHP Cookie but no PMI Cookie



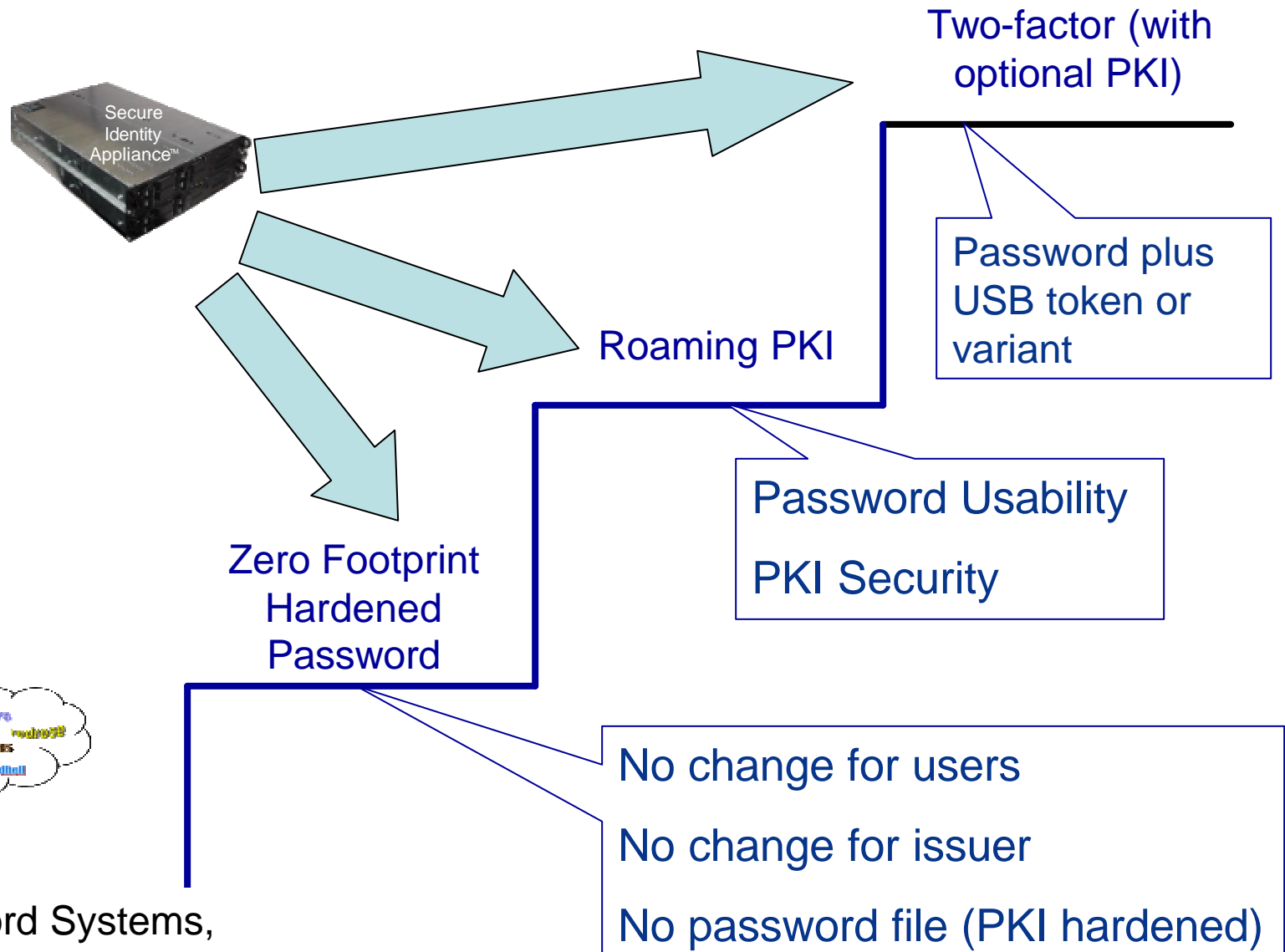
# Security Appliances

---

- Dedicated (but COTS) hardware
- Hardened OS
- Managed by restricted protocols (no root access)
- Highly available, scalable and secure



# Authentication Ladder



Weak Password Systems,  
Catastrophic Dictionary attacks

# 2-Key RSA vs PA

Old PKI

Practical PKI

Keys:

- a) Alice Public =  $e$
- b) Alice Private =  $d$
- c) Alice Cert =  $C$

- a) Alice Public =  $e$
- b) Alice *password* =  $d1$
- c) Alice Cert =  $C$

Signing:

- a)  $S = \text{Sign}(M, d)$

Signing:

- a) *Alice logs on to appliance using strong authentication and creates secure channel*
- b) *Spartial = Sign(M, d2)*
- c)  $S = \text{Sign}(\text{Spartial}, d1)$

Send [S, C] to Bob

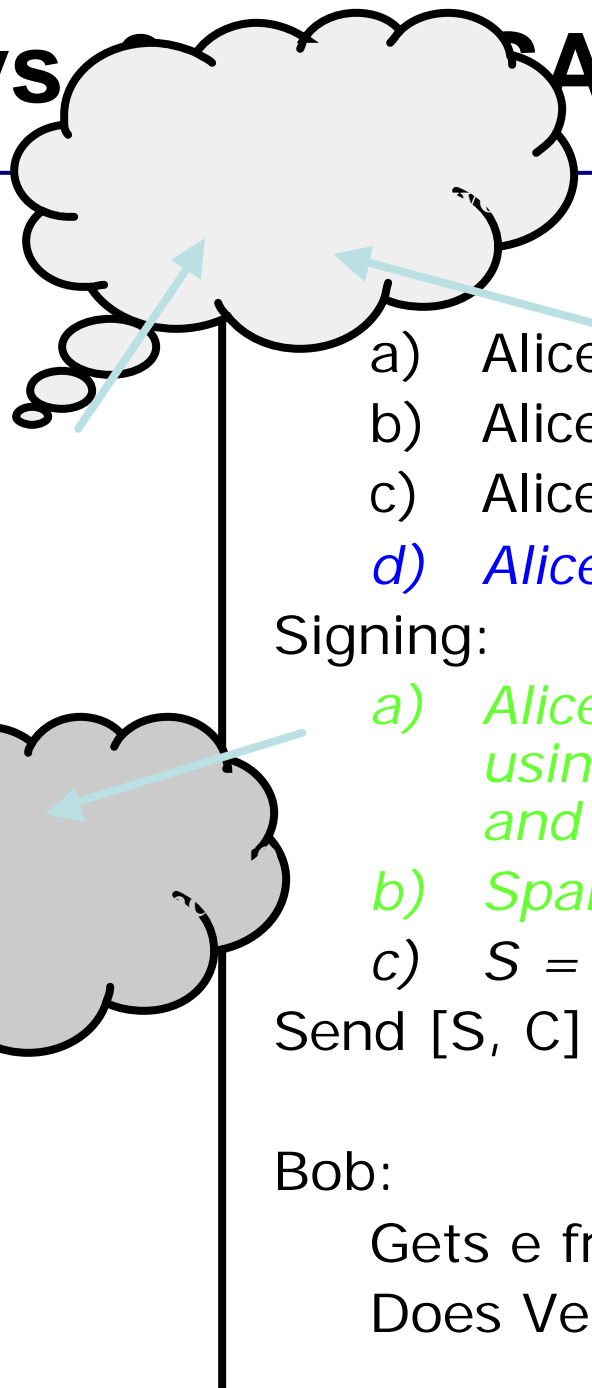
Send [S, C] to Bob

Bob:

Gets  $e$  from  $C$   
Does  $\text{Verify}(S, e) = M?$

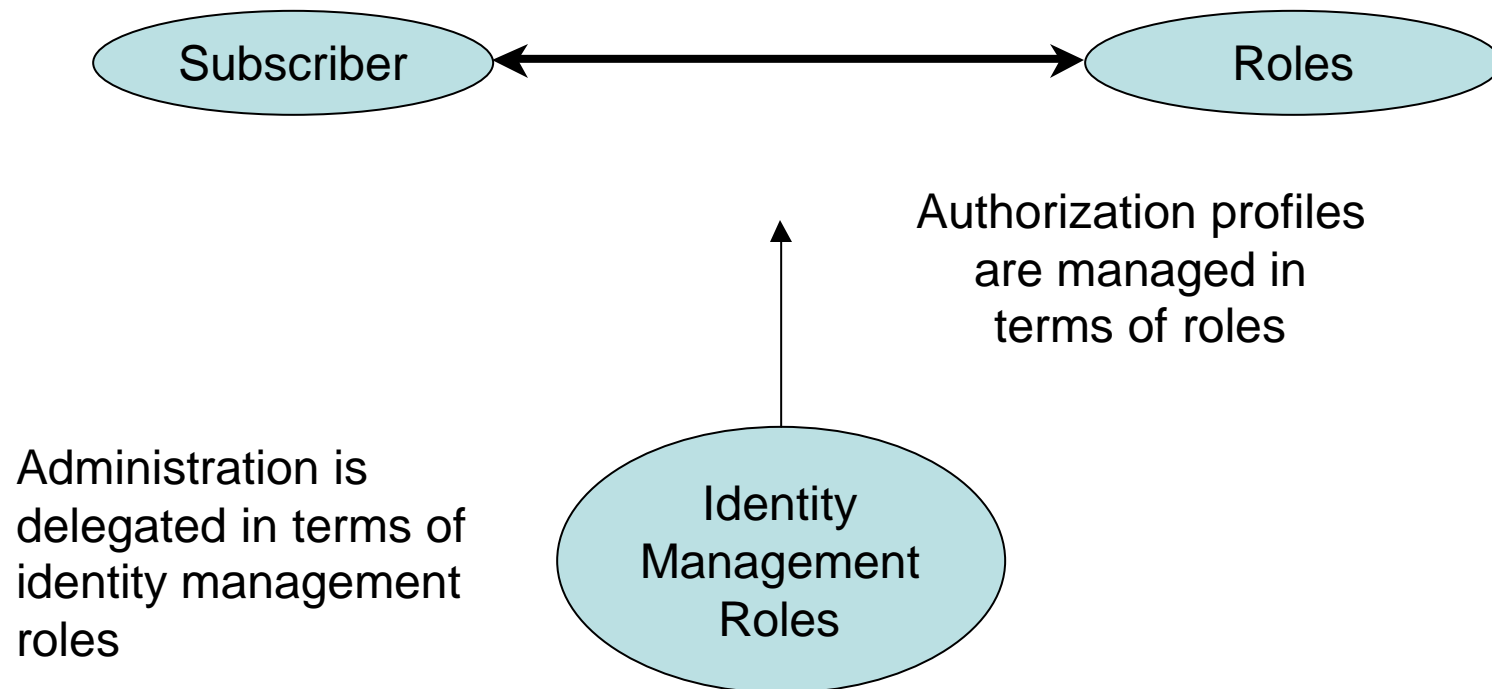
Bob:

Gets  $e$  from  $C$   
Does  $\text{Verify}(S, e) = M?$



# Role-Based Management

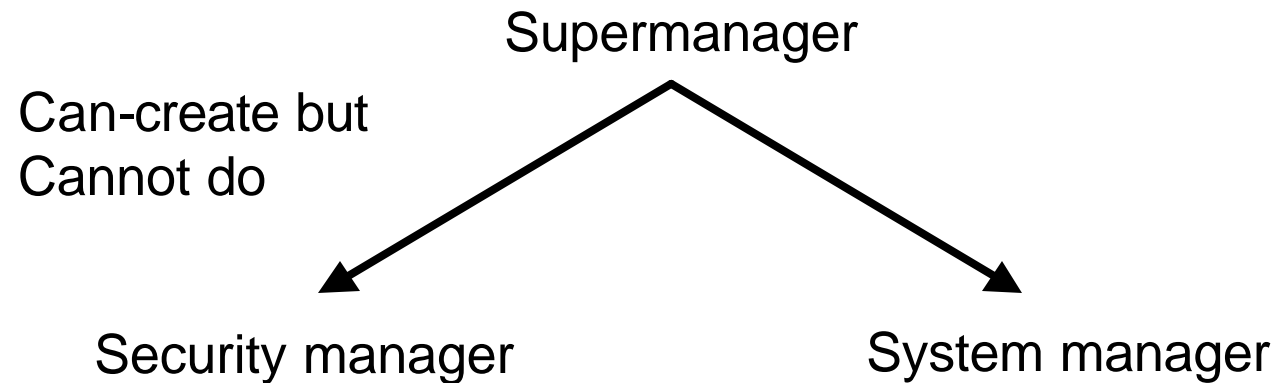
---



# Appliance Management Roles

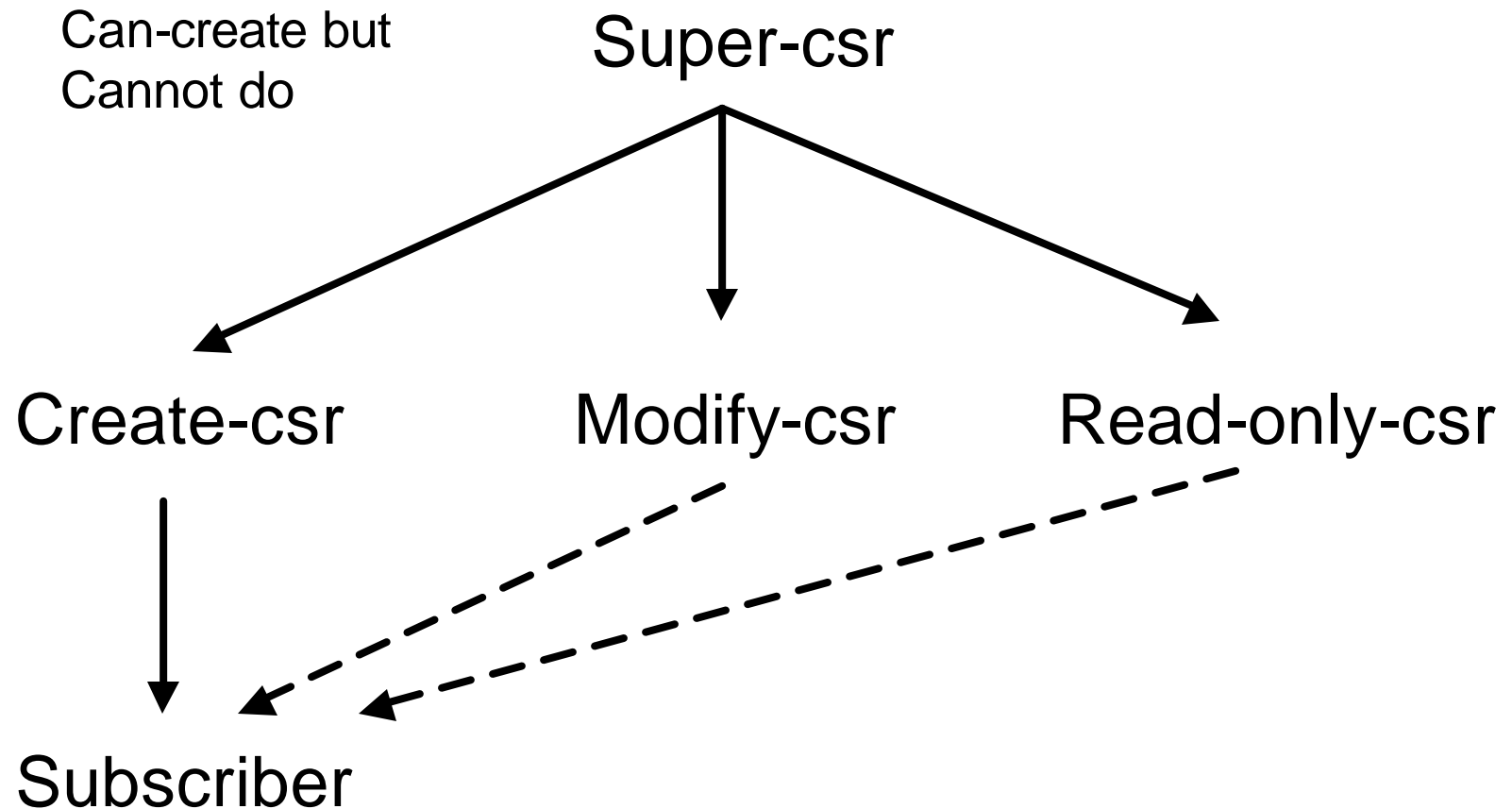
---

- Supermanager
  - Not your usual root user
- Security manager
- System manager



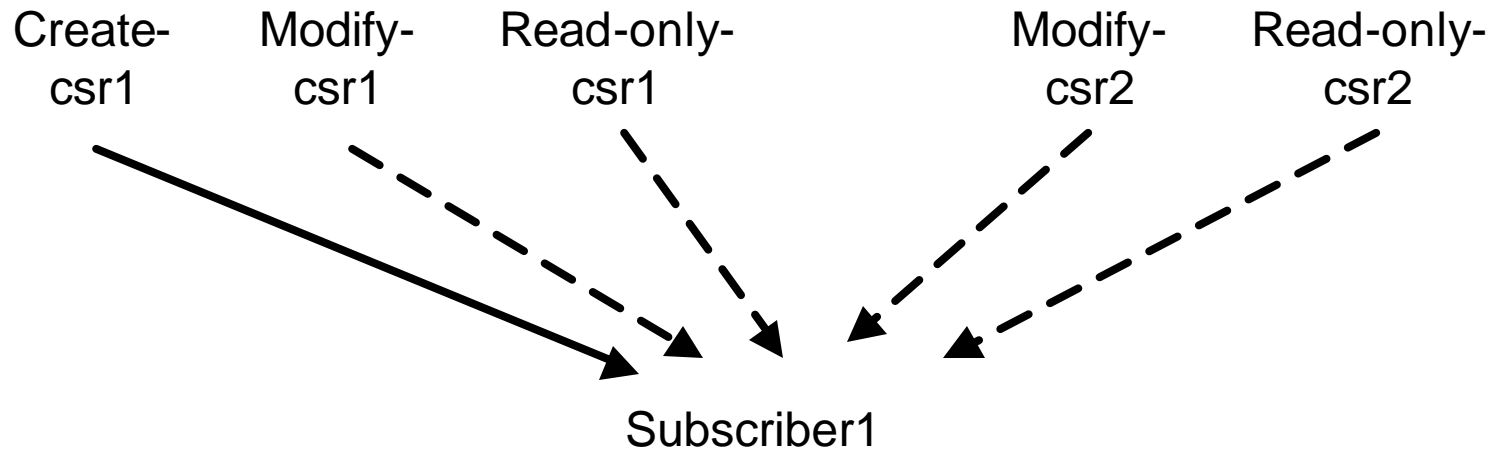
# Consumer Management Roles

---



# Subscriber Management Roles

---



userid	user personal profile	org1 roles	org2 roles	.....
--------	-----------------------	------------	------------	-------

# Conclusion

---

- Good enough security tolerates occasional failure but does not tolerate catastrophic failure
- Identity management is the most important security issue for organizations
- The authentication ladder is real
- Role-based federated identity management is a proven technology in production today
- NSDS's Secure Identity Appliance is a multifunctional product that supports these objectives

