FIPS 201 Update:
Federation, PIV, and Derived PIV

Justin Richer

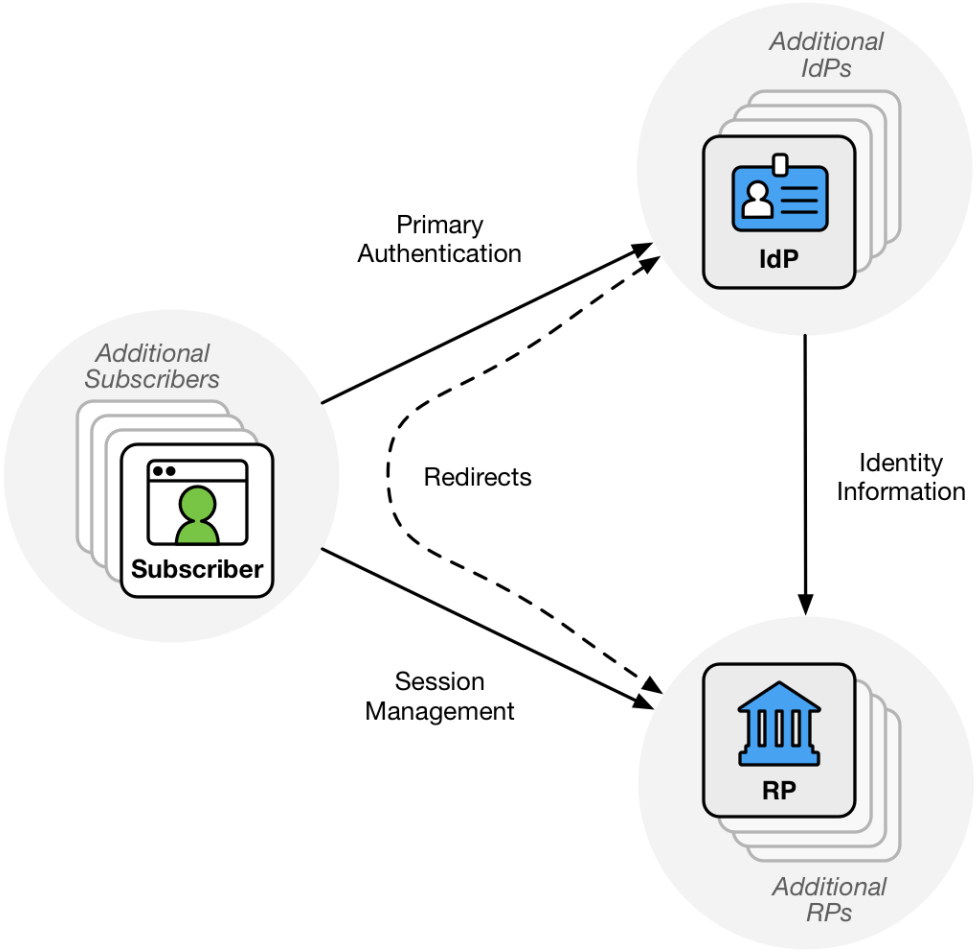
National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

What is federation?

A process that allows the conveyance of identity and authentication information across a set of networked systems.

- NIST SP 800-63-3 Appendix A

Federation protocols

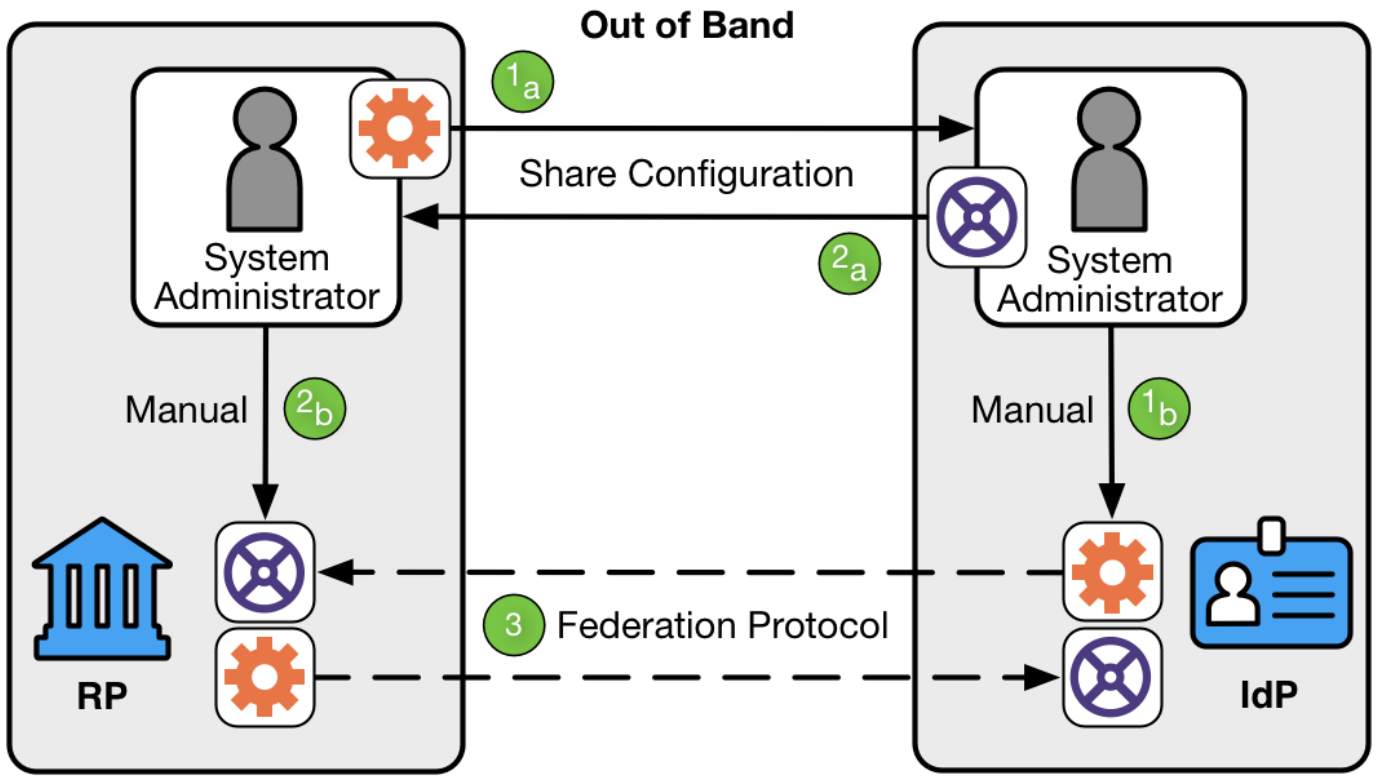


National Institute of Standards and Technology
U.S. Department of Commerce

Federation agreements

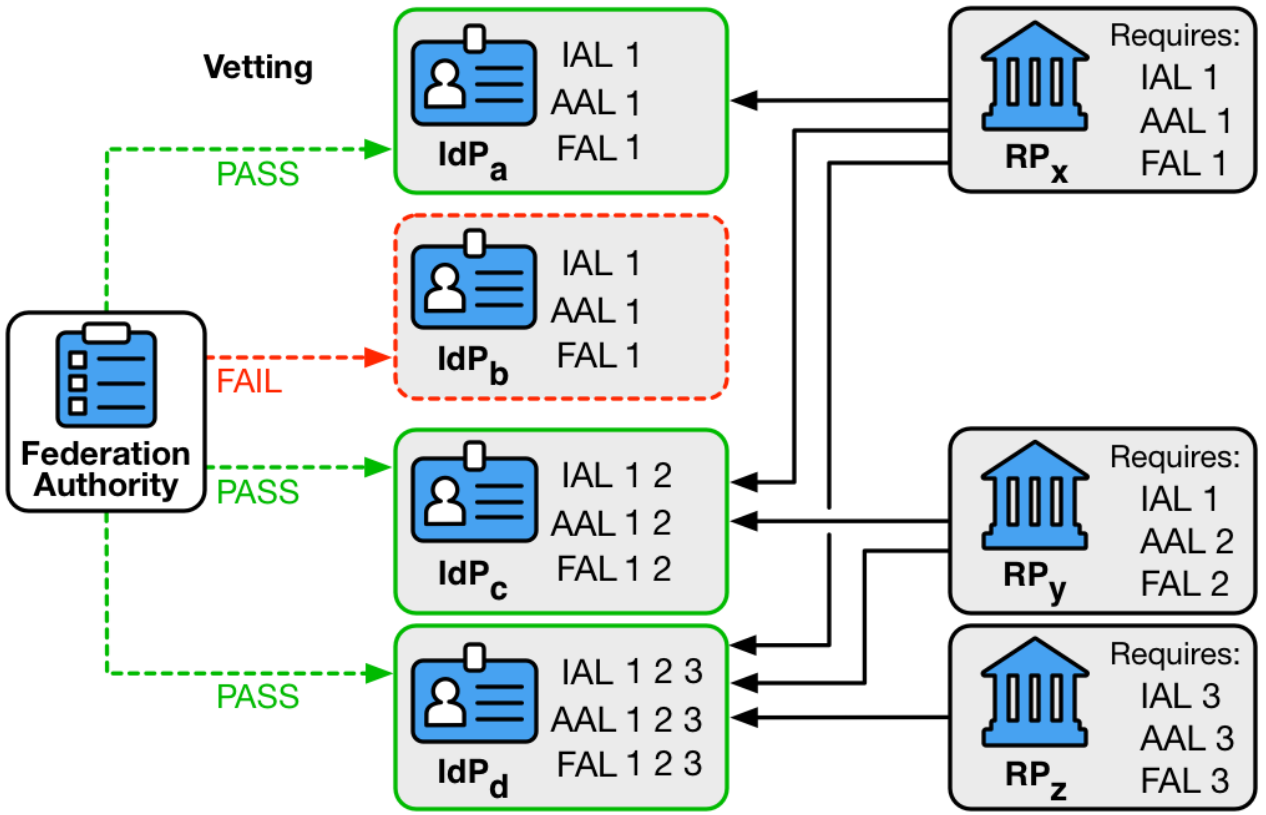
- How does the RP trust the IdP?
- How does the IdP trust the RP?
- How does the user trust any of this?
- Who gets in trouble when something goes wrong?

Point to point connection

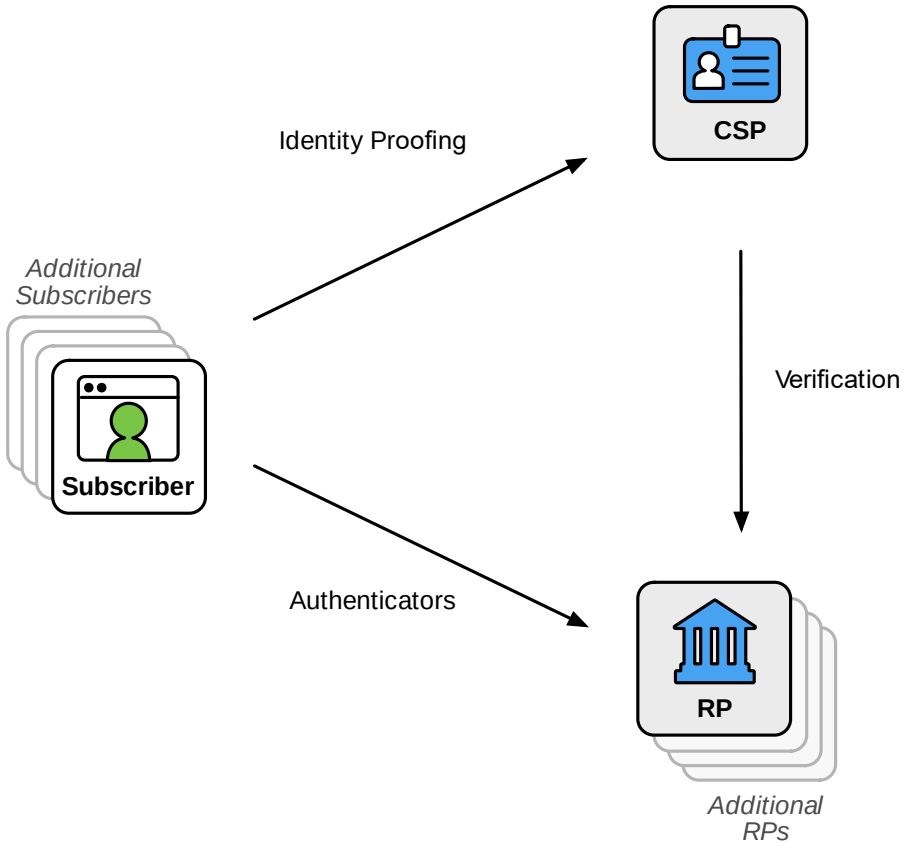


National Institute of Standards and Technology
U.S. Department of Commerce

Federation Authority



Is it just like authentication?

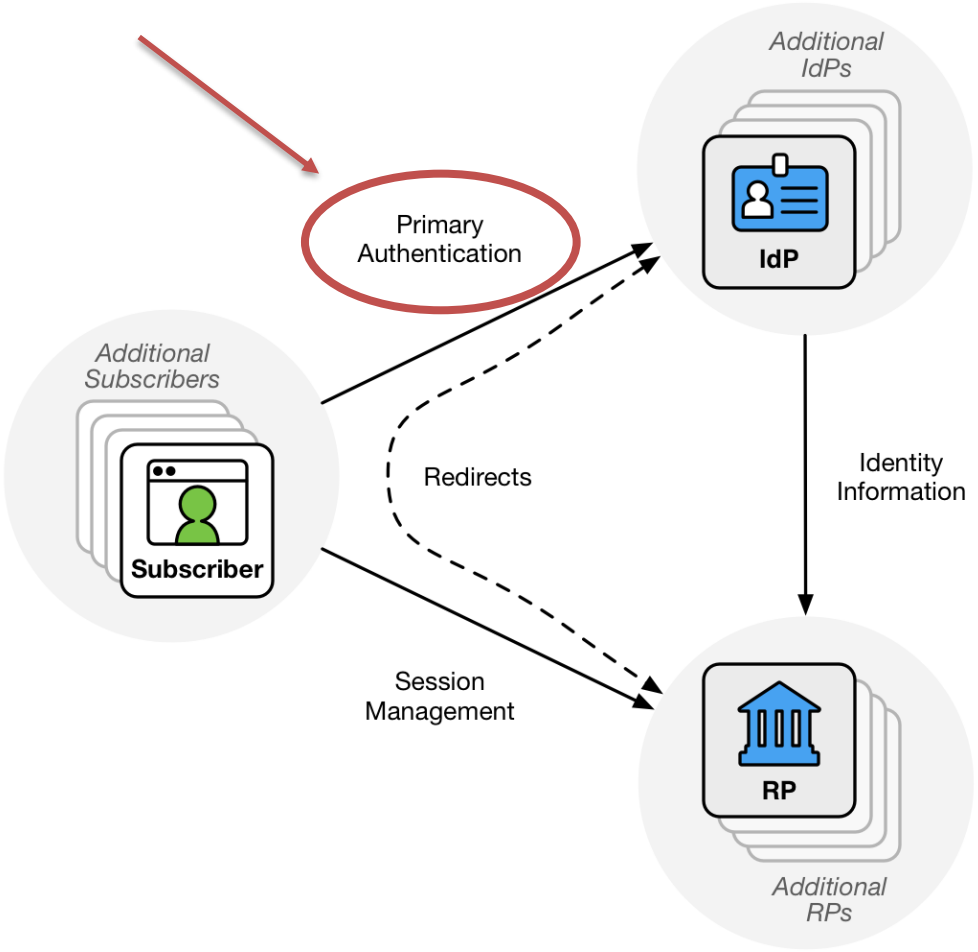


National Institute of Standards and Technology
U.S. Department of Commerce

Not the same process

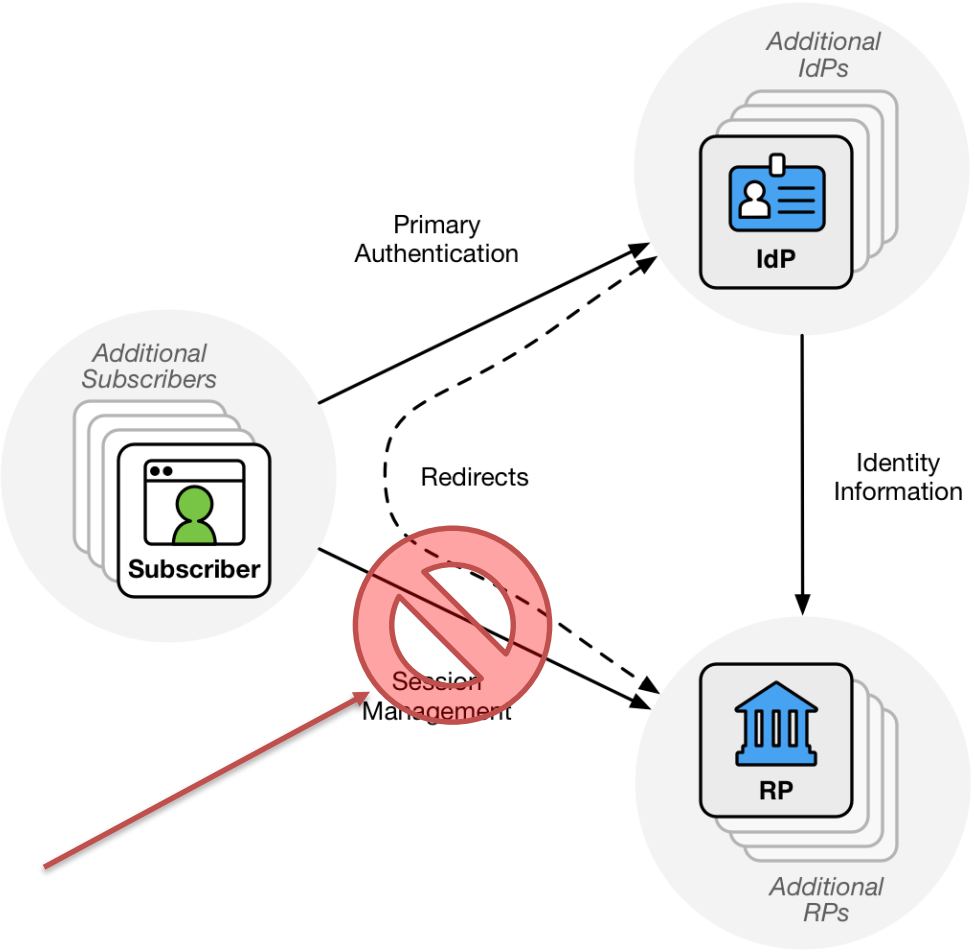
- In Authentication
  - Subscriber presents authenticators to the RP
- In Federation:
  - Subscriber presents authenticators to the IdP
  - IdP provides *identity assertion* to the RP

Authenticators are here



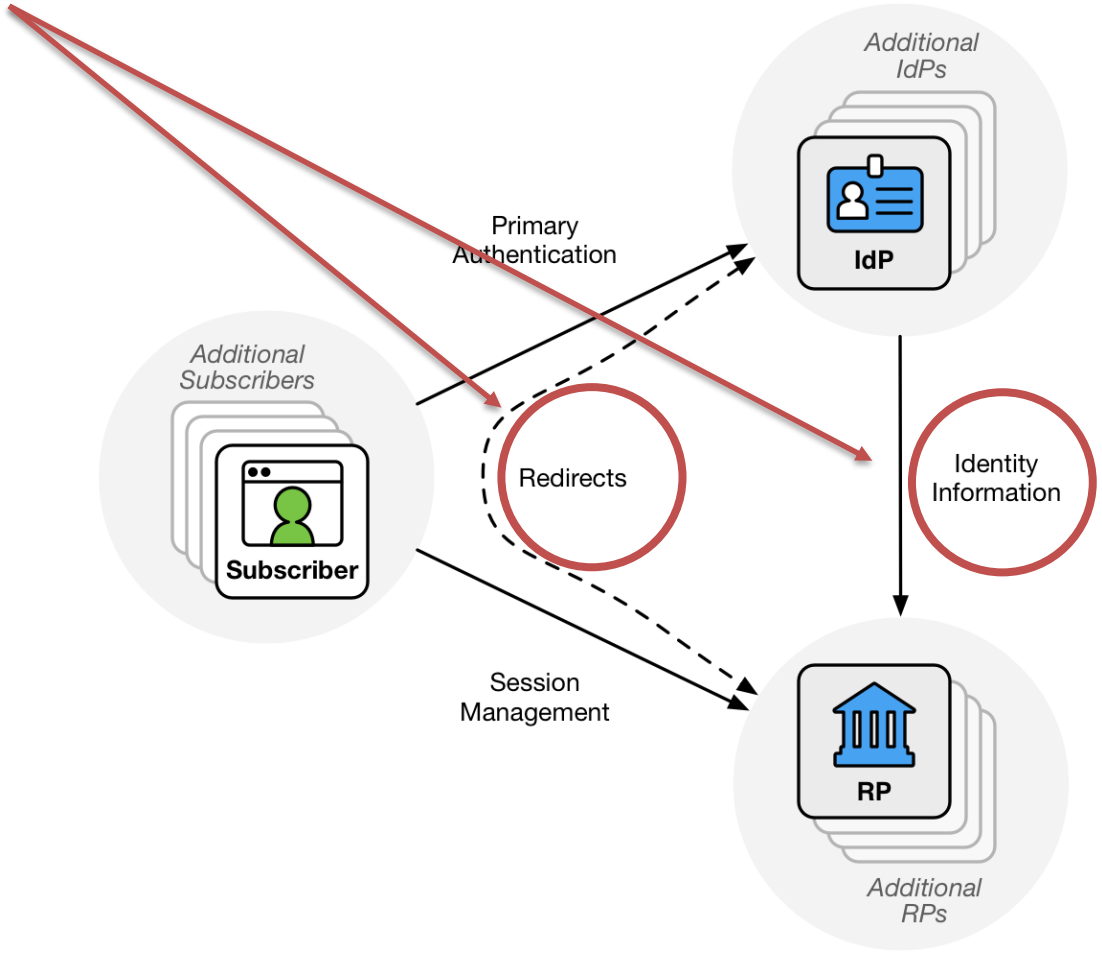
National Institute of Standards and Technology
U.S. Department of Commerce

Authenticators are NOT here



National Institute of Standards and Technology
U.S. Department of Commerce

Assertions are here

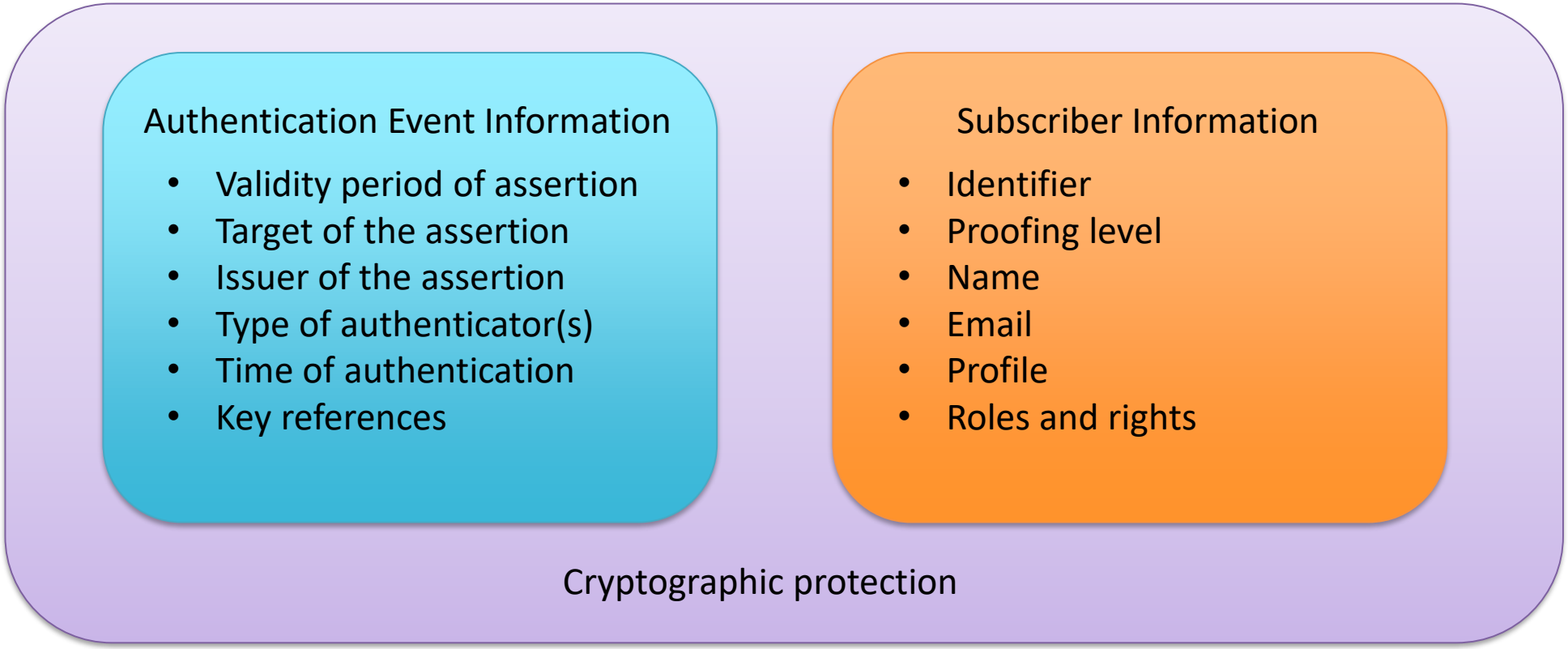


National Institute of Standards and Technology
U.S. Department of Commerce

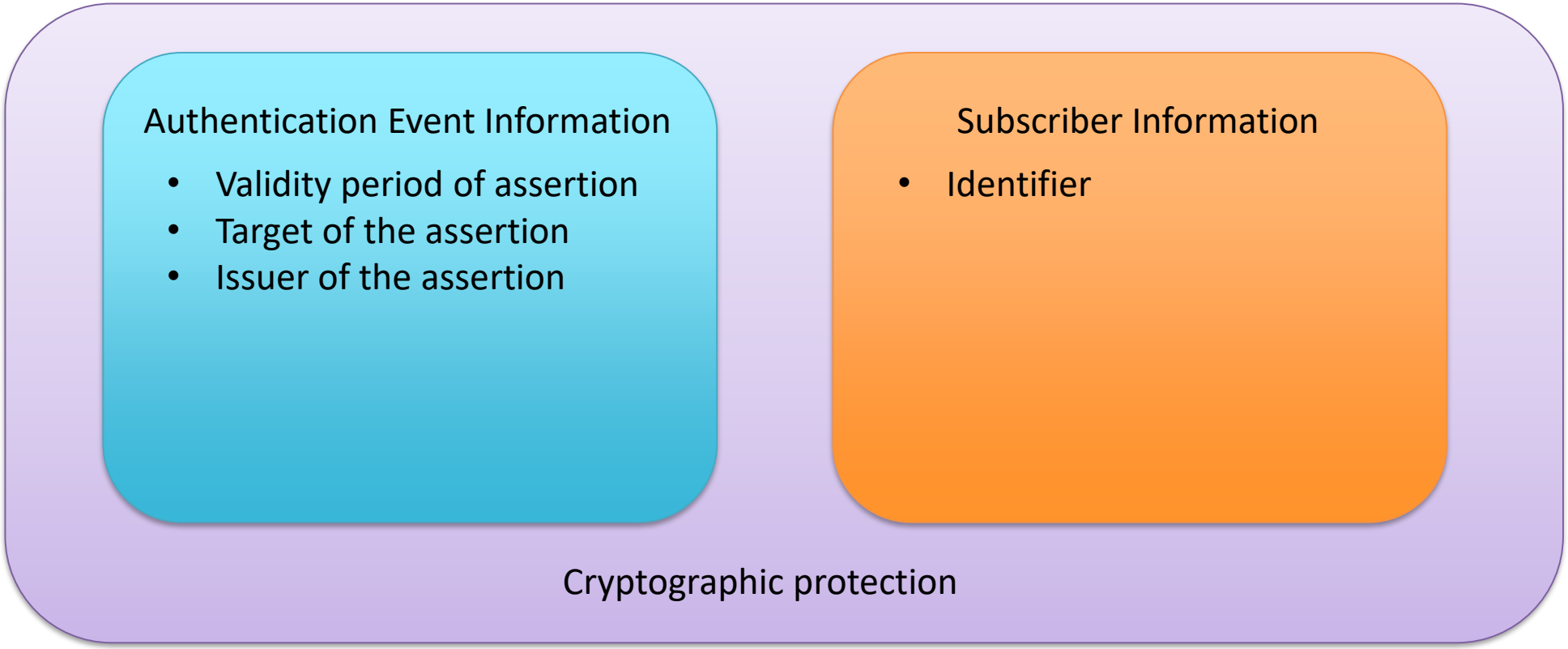
What is an assertion?

A statement from a IdP to an RP that contains information about a subscriber's authenticated state at the IdP. Assertions may also contain verified attributes about the subscriber.

What's in an assertion



What's in an assertion (minimal edition)



Why does this matter?

Technology	SP 800-63-2	SP-800-63-3
Browser cookies	Assertion	
X.509 certificate	Assertion?	
Kerberos ticket	Assertion	
SAML	Assertion	
OIDC ID Token	Assertion (Probably)	

Why does this matter?

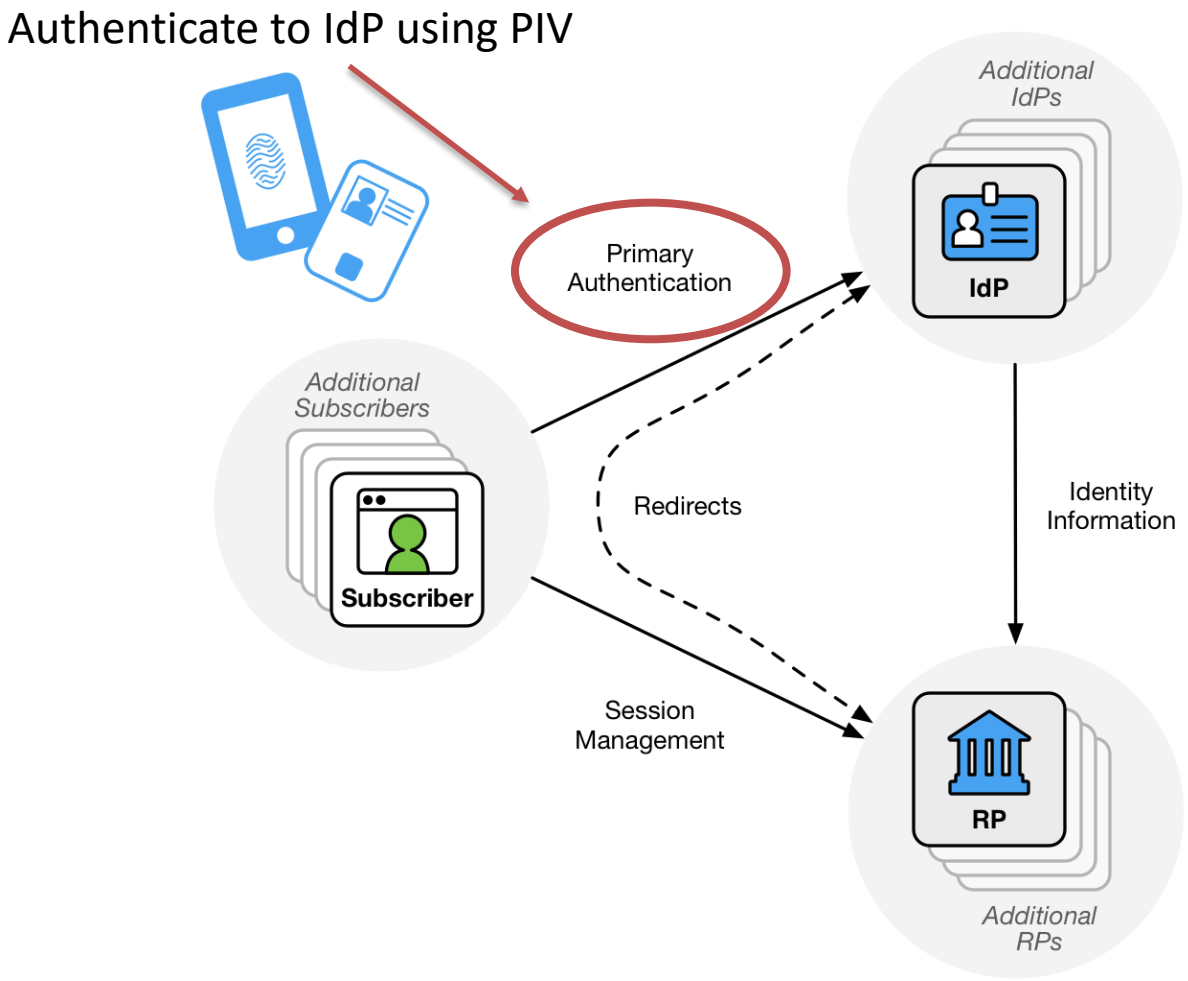
Technology	SP 800-63-2	SP-800-63-3
Browser cookies	Assertion	Session management
X.509 certificate	Assertion?	Authenticator
Kerberos ticket	Assertion	“Not truly federation”
SAML	Assertion	Assertion
OIDC ID Token	Assertion (Probably)	Assertion

In other words:

Derived PIV (and other PKI) used to be considered "federation" but it now falls under the "authenticator" umbrella.

But you can federate with PIV through a federation protocol.

Federation with PIV

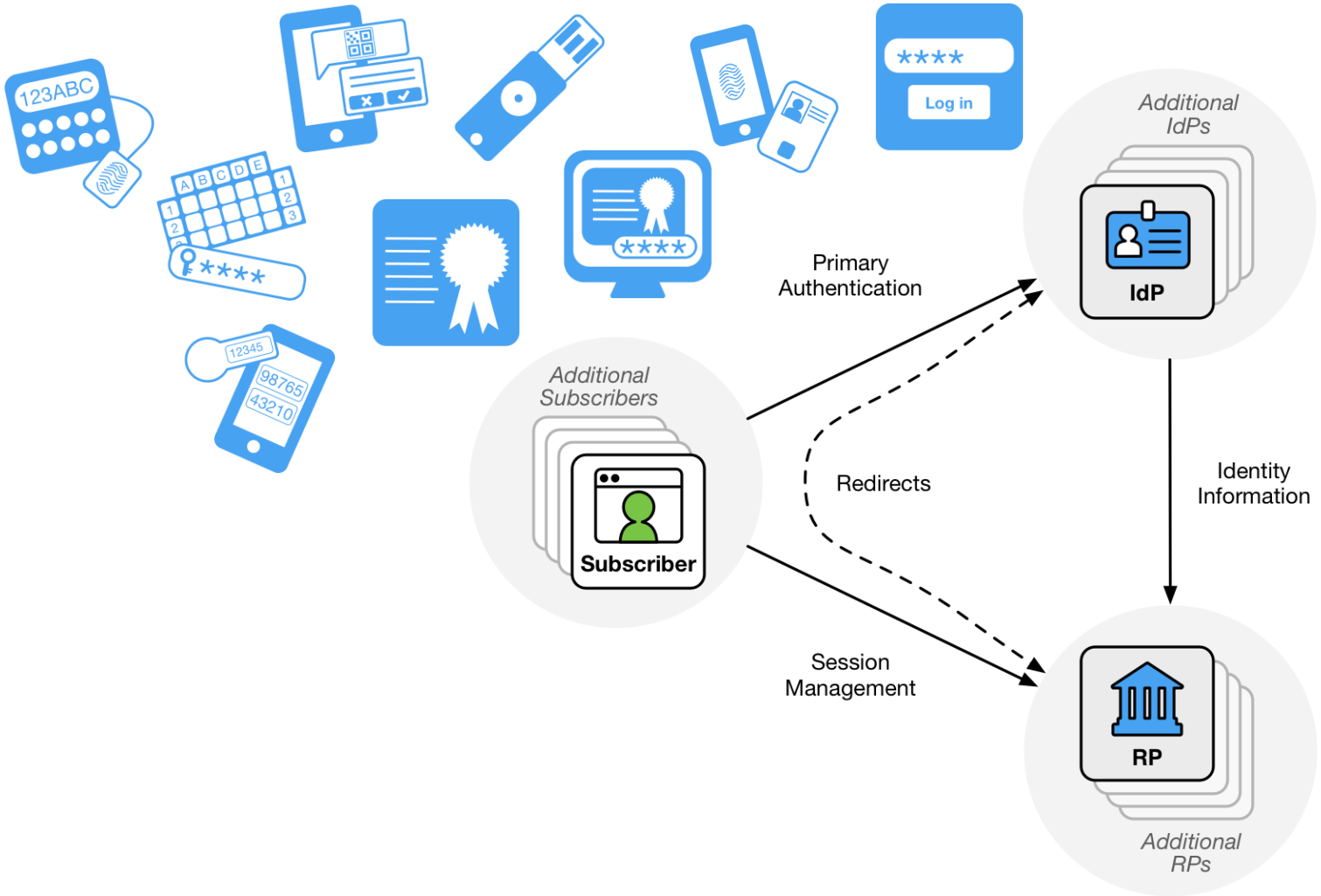


National Institute of Standards and Technology
U.S. Department of Commerce

Why federate?

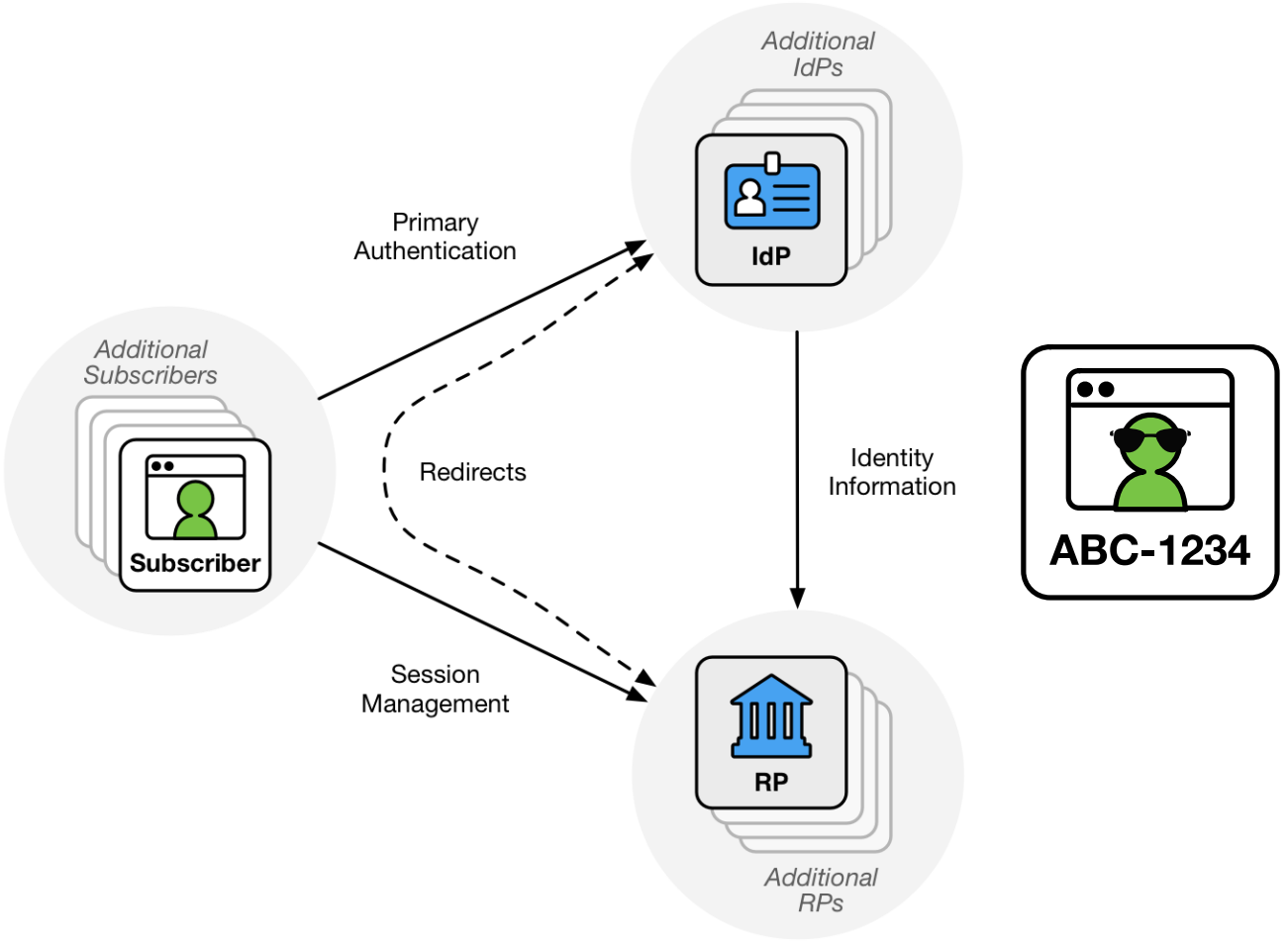
- Abstraction layer
- Attribute disclosure
- Timeliness
- Cross-boundary
- RP Control

Abstraction layer across authenticators



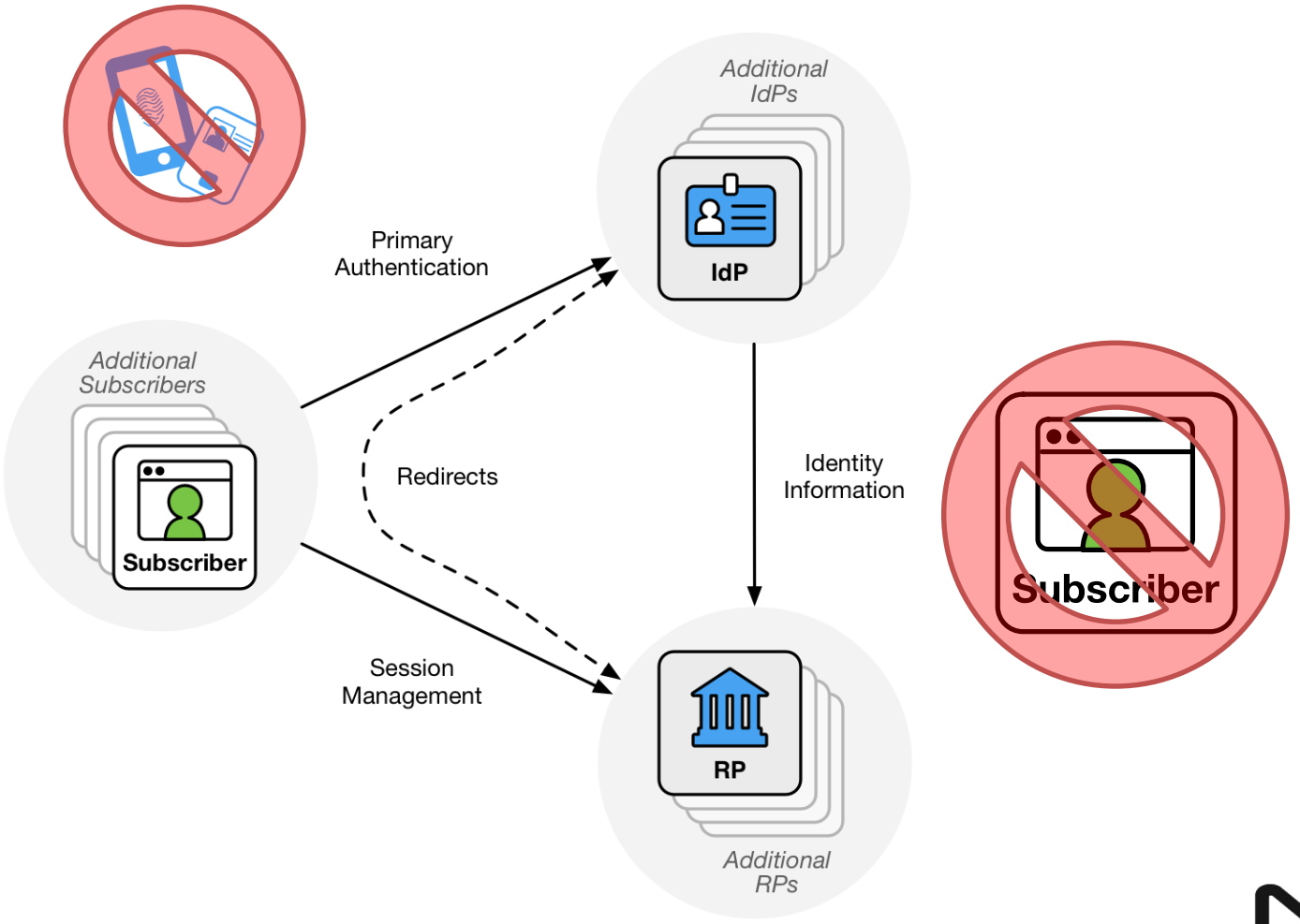
National Institute of Standards and Technology
U.S. Department of Commerce

Selective attribute disclosure



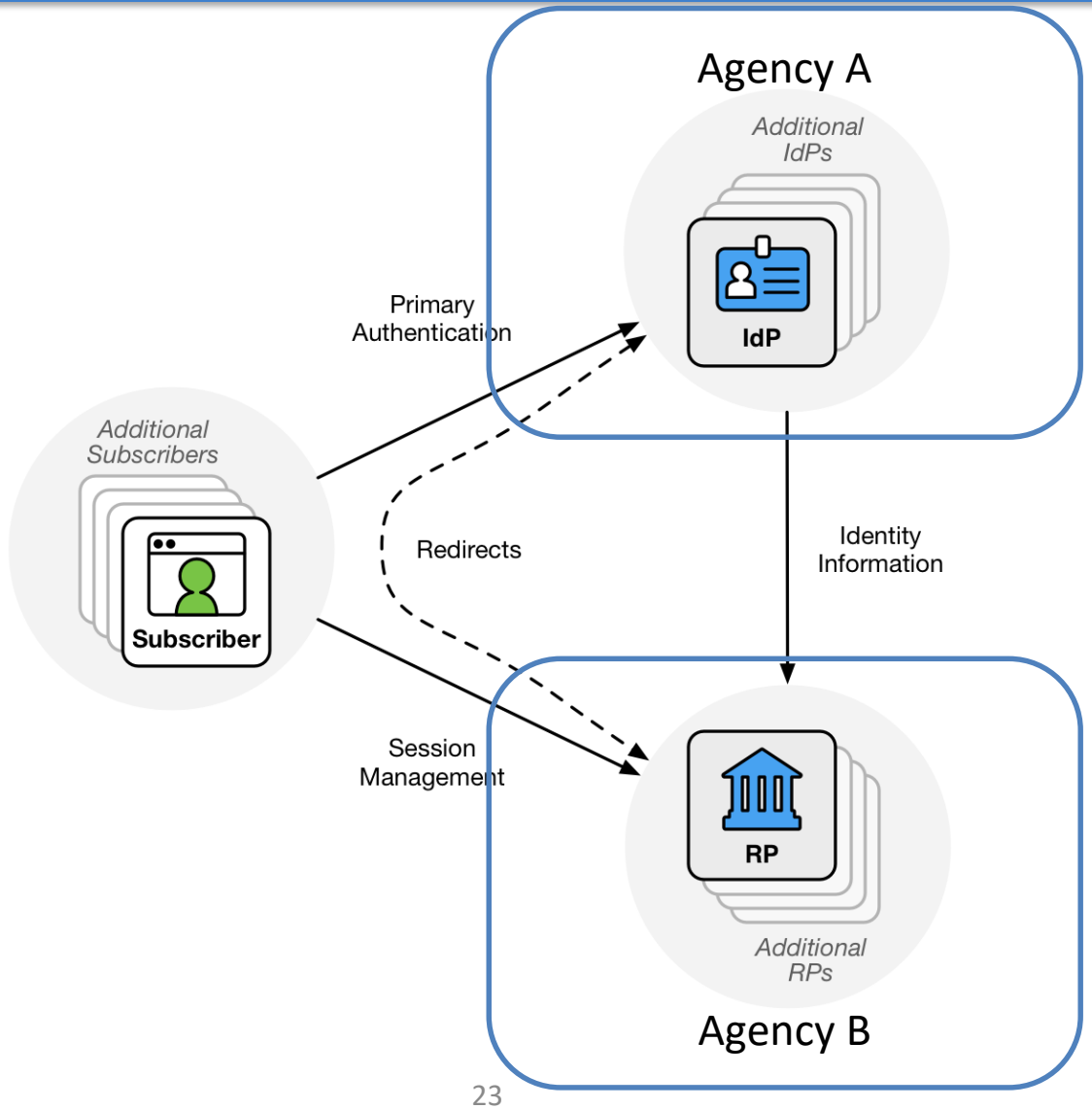
National Institute of Standards and Technology
U.S. Department of Commerce

Time-bound



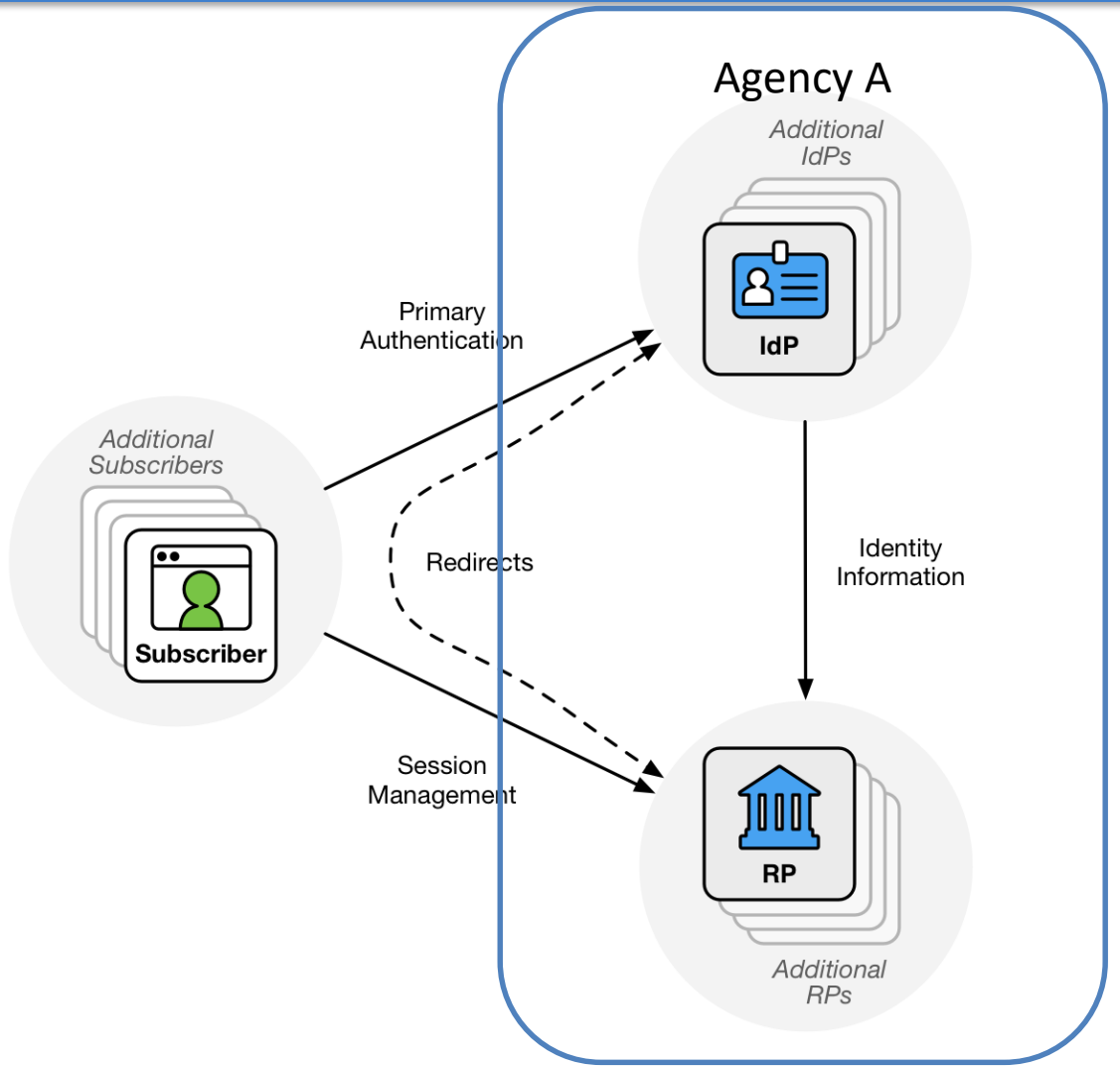
National Institute of Standards and Technology
U.S. Department of Commerce

Can cross boundaries



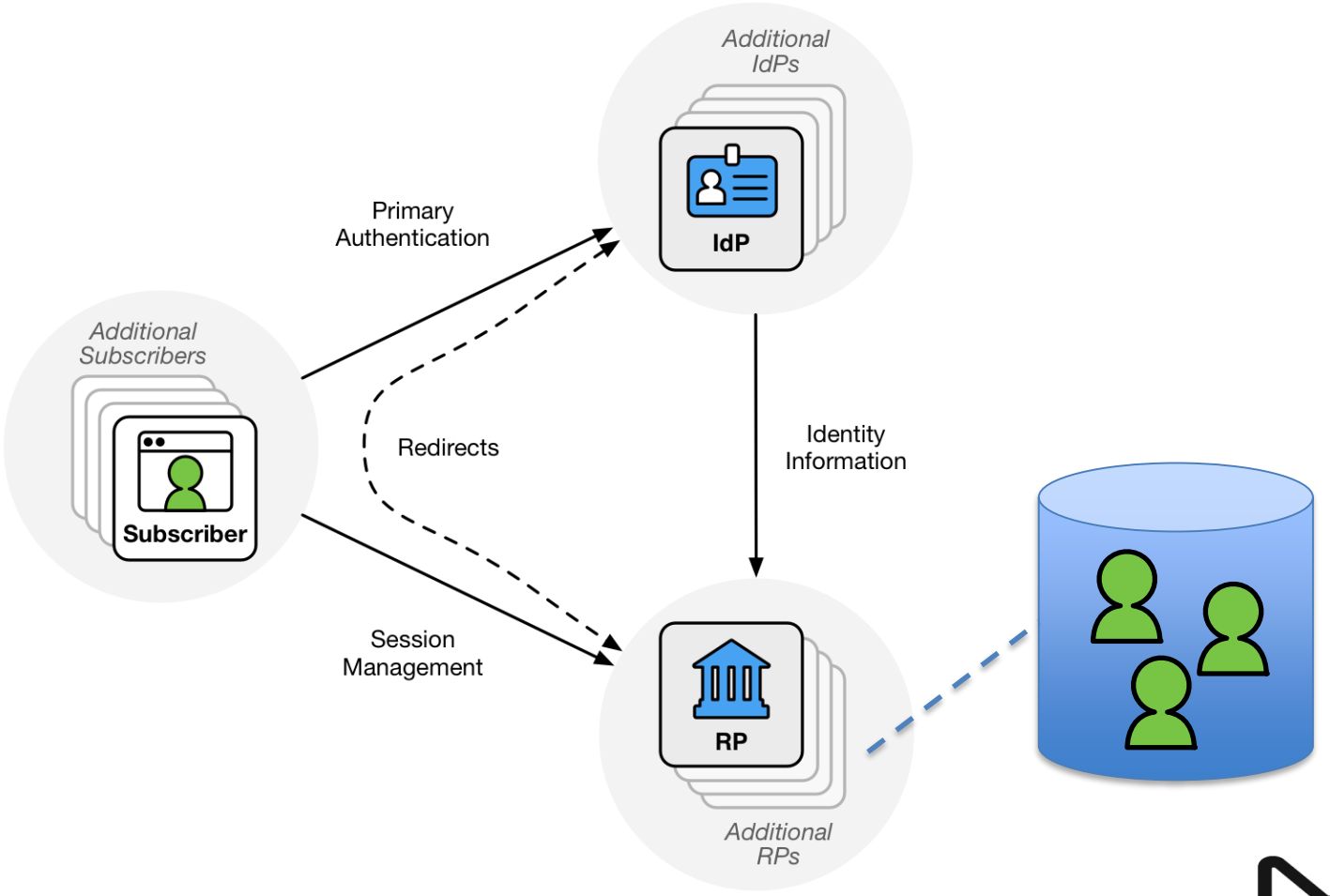
National Institute of Standards and Technology
U.S. Department of Commerce

Can work internally



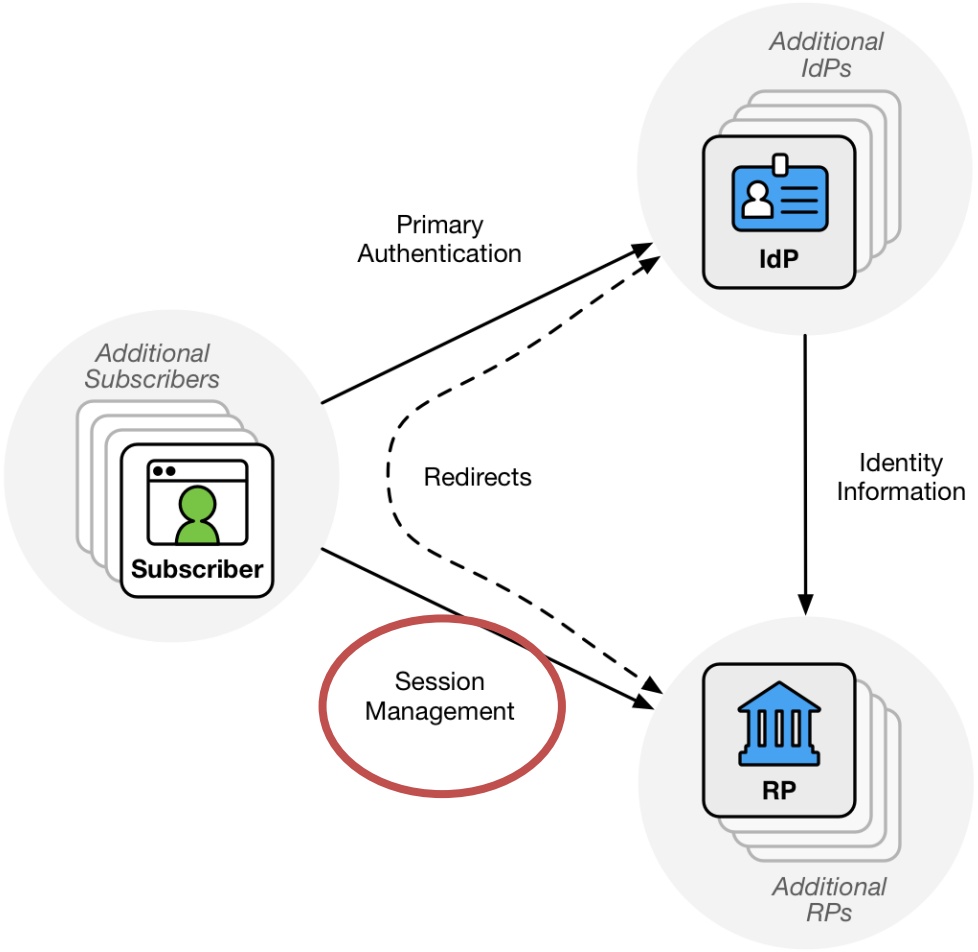
National Institute of Standards and Technology
U.S. Department of Commerce

RP maps subscriber to local user



National Institute of Standards and Technology
U.S. Department of Commerce

RP controls session and re-authentication



National Institute of Standards and Technology
U.S. Department of Commerce

Federation in parallel with authenticators

- Different classes of users
  - Eg., External vs. internal
- Combine authenticators for users
- Bind external accounts

MAX.gov Login

Don't Have a MAX ID Yet? Register Now

Home | Manage Password | Contact Us

Login with ...

PIV or CAC Card

Login with your PIV or CAC

Remember to plug in your PIV/CAC card

Register a Secure+ SMS 2-Factor Device

Login with PIV/CAC

MAX.gov User ID & Password

User ID

Password Forgot, Set, or Change Your Password?

Use MAX Secure+ SMS 2-Factor

Login With User ID

MAX Agency Federated Partner Automated Login

NASA	DOJ	HHS	MCC
USAID	NAVMED	Treasury	OGE
ED	VA	DHS OIG	GSA
Energy	US Courts	OMB	EOP PITC
MAX Int			

Use this agency login every time I log into MAX.

MAX.GOV LOGIN

Don't Have a MAX ID Yet? REGISTER NOW

HOME | MANAGE PASSWORD | CONTACT US

LOGIN WITH ...

PIV OR CAC CARD

LOGIN WITH YOUR PIV OR CAC

Remember to plug in your PIV/CAC card

Register a Secure+ SMS 2-Factor Device

LOGIN WITH PIV/CAC

MAX.GOV USER ID & PASSWORD

User ID

Password — Forgot, Set, or Change Your Password?

Use MAX Secure+ SMS 2-Factor

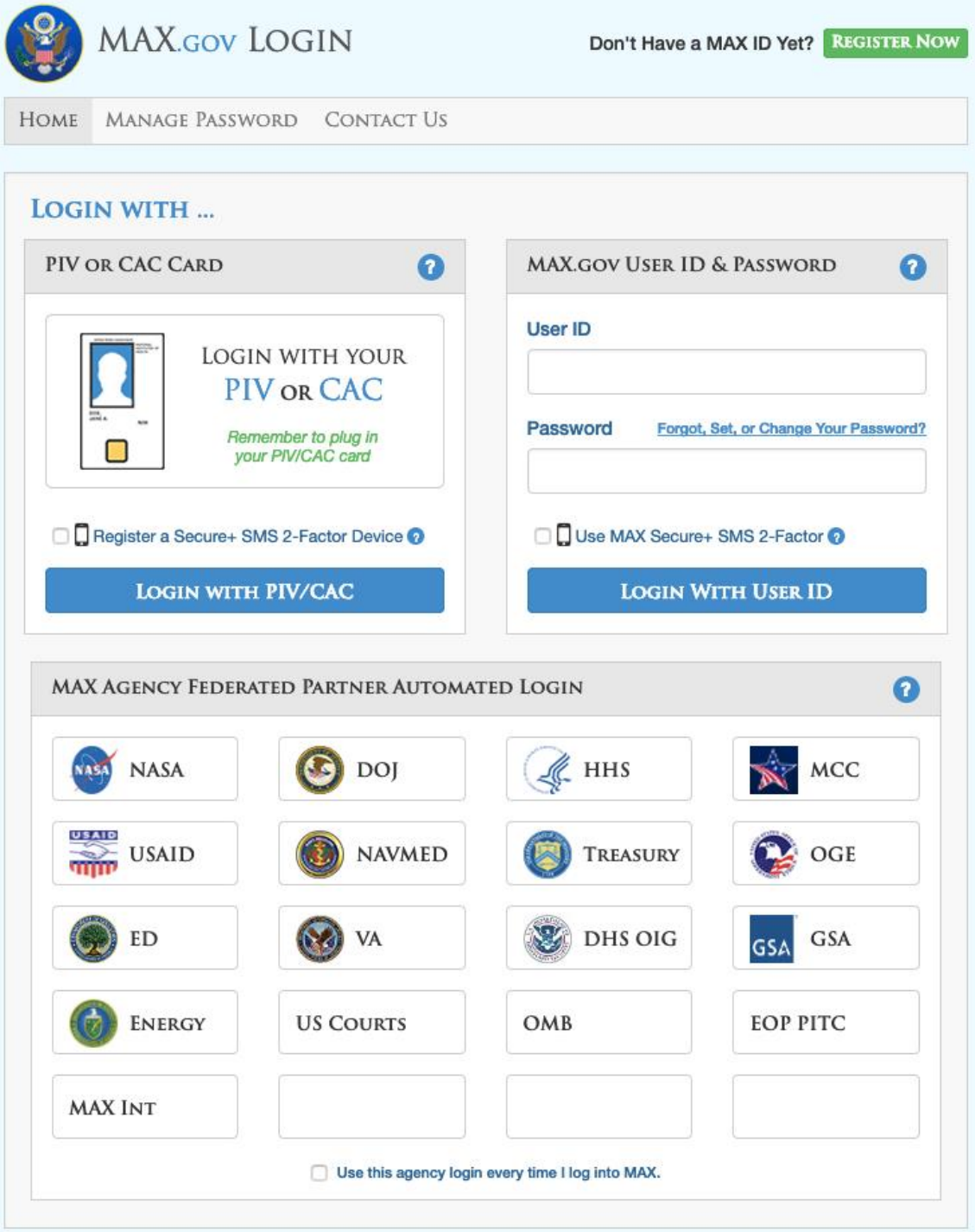
LOGIN WITH USER ID

MAX AGENCY FEDERATED PARTNER AUTOMATED LOGIN

NASA	DOJ	HHS	MCC
USAID	NAVMED	TREASURY	OGE
ED	VA	DHS OIG	GSA
ENERGY	US COURTS	OMB	EOP PITC
MAX INT			

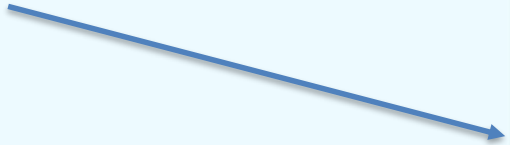
Use this agency login every time I log into MAX.

Shared secret authenticator



(Deprecated 2nd factor out of band authenticator over SMS sshhh….)

Hardware based cryptographic authenticator smartcard



MAX.GOV LOGIN

Don't Have a MAX ID Yet? REGISTER NOW

HOME | MANAGE PASSWORD | CONTACT US

LOGIN WITH ...

PIV OR CAC CARD

LOGIN WITH YOUR PIV OR CAC

Remember to plug in your PIV/CAC card

Register a Secure+ SMS 2-Factor Device

LOGIN WITH PIV/CAC

MAX.GOV USER ID & PASSWORD

User ID

Password Forgot, Set, or Change Your Password?

Use MAX Secure+ SMS 2-Factor

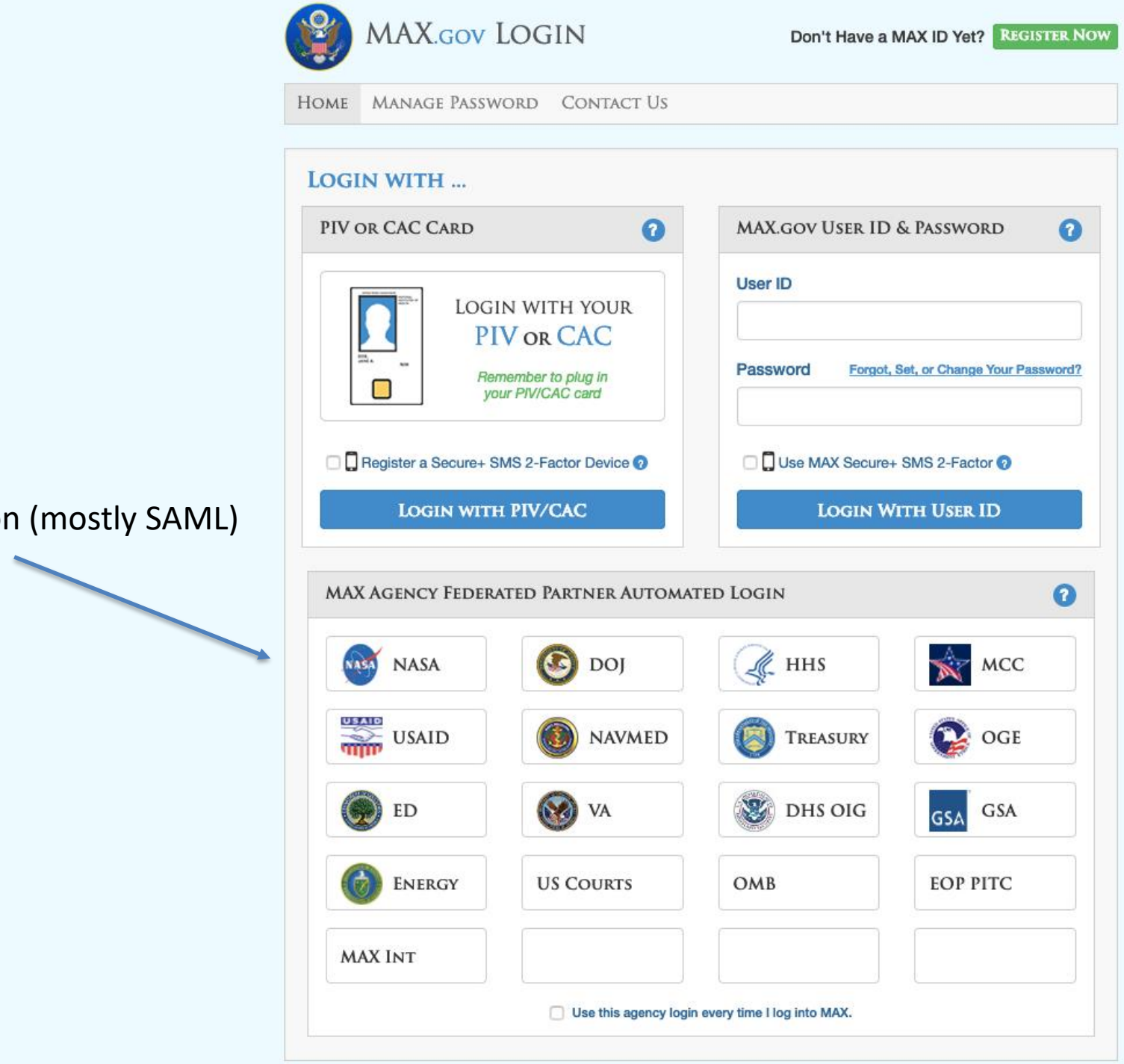
LOGIN WITH USER ID

MAX AGENCY FEDERATED PARTNER AUTOMATED LOGIN

NASA	DOJ	HHS	MCC
USAID	NAVMED	TREASURY	OGE
ED	VA	DHS OIG	GSA
ENERGY	US COURTS	OMB	EOP PITC
MAX INT			

Use this agency login every time I log into MAX.

Federation (mostly SAML)



Assurance Levels

- IAL: How strongly someone is proofed for an account
- AAL: How trustworthy the authentication event is
- FAL: How strongly an assertion is conveyed between federated systems **using a federated protocol**

FAL Considerations

- Aspects of the federation protocol
  - Protection of the assertion
  - Protection of subscriber attributes
- Requirements change based on how assertions are presented
- *Does not account for federation agreement*

Federation Assurance Level (FAL)

	FAL1	FAL2	FAL3
Assertion type	Signed	Signed & Encrypted	Signed, Encrypted, & Holder-of-Key
Subscriber attributes	Yes (if backchannel)	Yes	Yes
Examples	OIDC SAML artifact binding	OIDC with encrypted ID token SAML with encrypted assertion	OIDC or SAML plus secondary key-based authenticator (certificate, FIDO, etc)

Which FAL?

- **FAL1 is good for most use cases**
  - Requires signatures, audience restriction, replay protection, etc.
  - Especially when subscriber attributes are sent in the backchannel, separate from the assertion
- FAL2 increases audience restriction
  - At the cost of key management
- FAL3 is forward-looking
  - Multiple keys and presentations
  - Hard to reach (by design)

Interoperability

- In the past: interoperable authenticators
- Now: interoperable federation profiles

Using federation protocols

- OpenID Connect (OIDC)
  - Supports browser and mobile
  - iGov profile from OIDF
- Security Assertion Markup Language (SAML)
  - Profile available for browsers
  - eGov profile from Kantara

iGov

- OpenID Foundation draft standard
- Increase security and interoperability of OIDC
- Require all clients to have and use keys
- Restrict less secure options (implicit flow, URL matching)
- Require discovery and registration support

eGov

- Kantara Initiative profile
- Increase security and interoperability of SAML
- Require metadata for discovery
- Require signatures and verification

Are you federating today?

- Which protocol and profile are you using?
  - As an IdP or an RP or both?
- What is the trust agreement?
- Do you comply with SP 800-63-3 C?
  - If so, at which FALs?

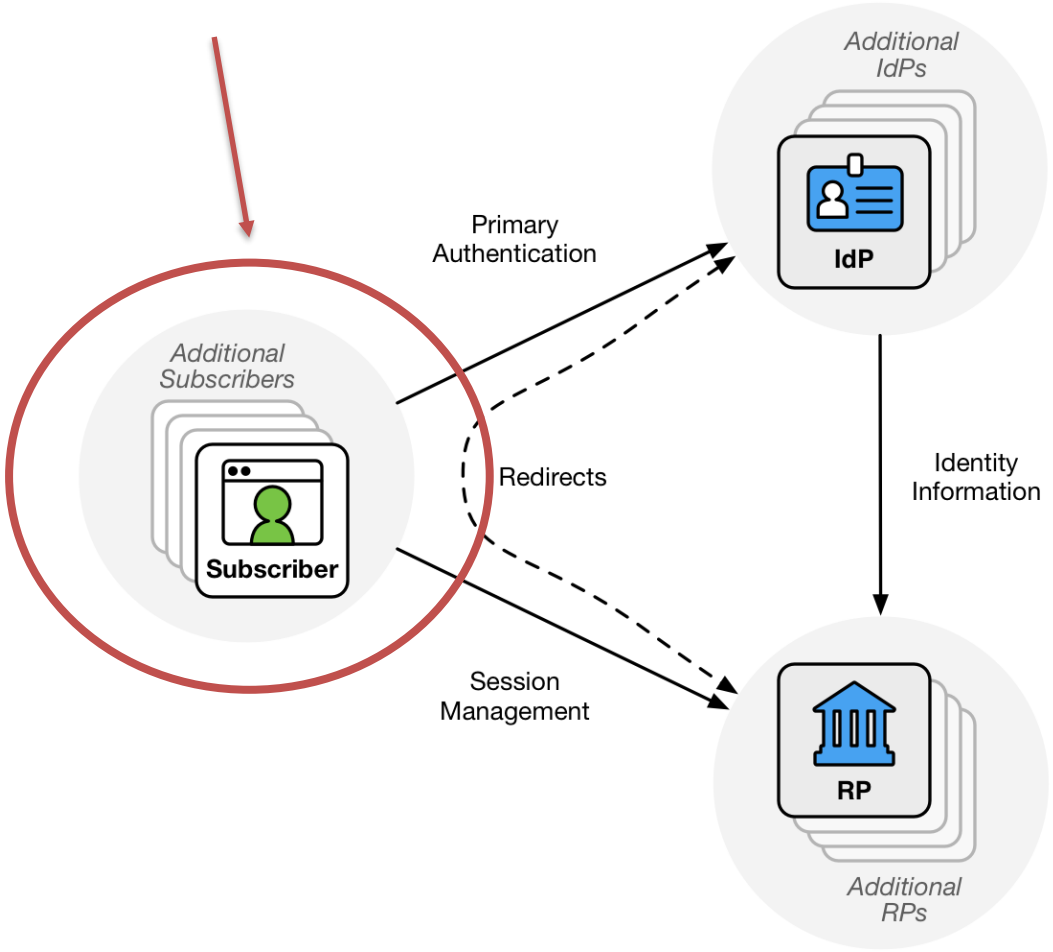
Moving forward

- What would a USG/FIPS-specific federation profile contain?

Questions?

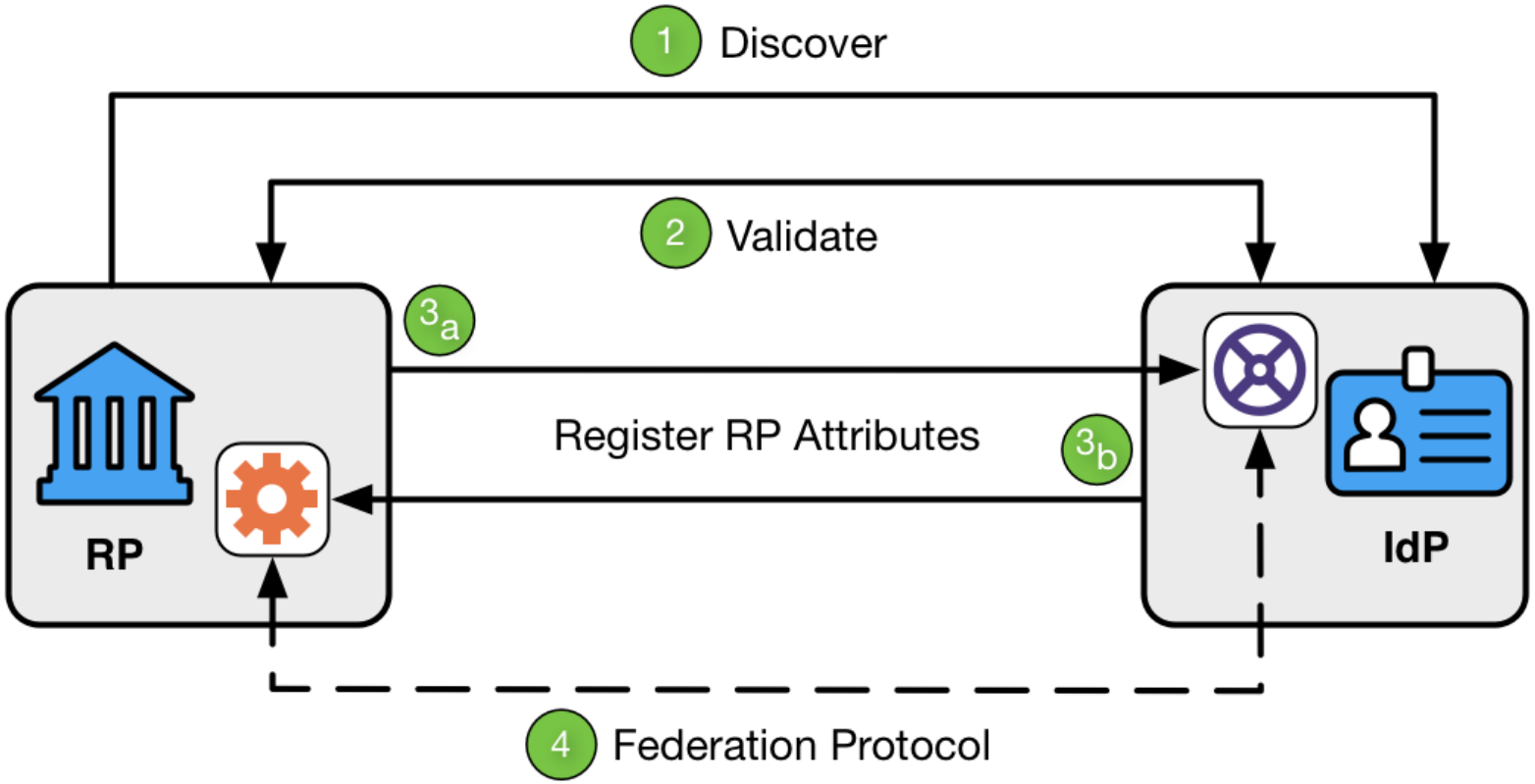
National Institute of Standards and Technology
U.S. Department of Commerce

Users are here



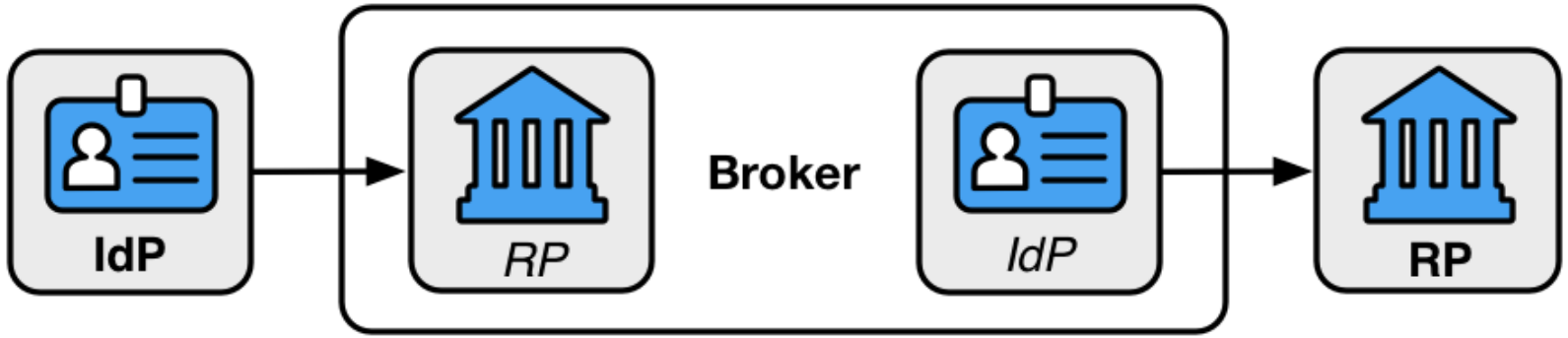
National Institute of Standards and Technology
U.S. Department of Commerce

Dynamic Registration

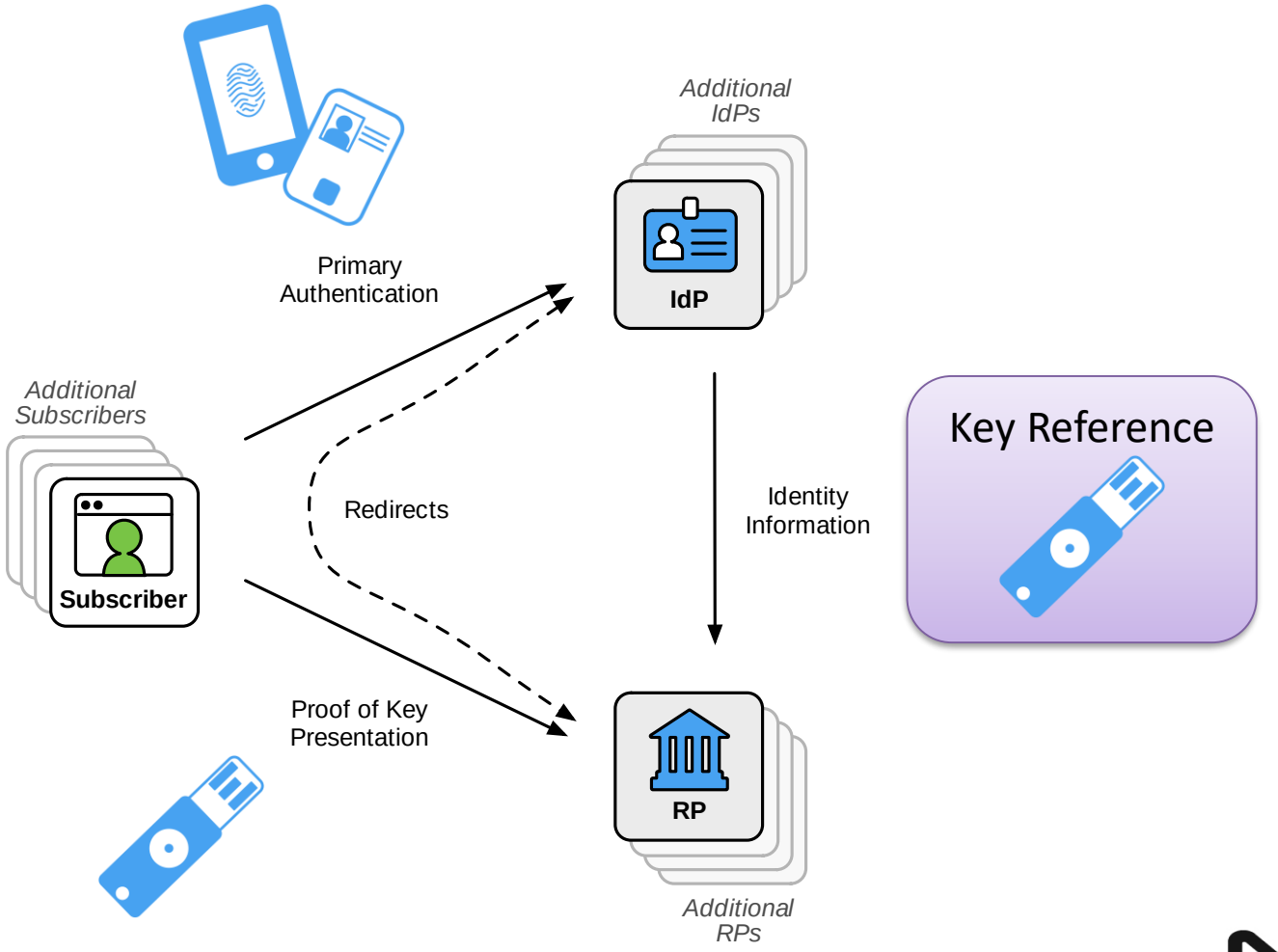


National Institute of Standards and Technology
U.S. Department of Commerce

Identity Broker



One example of FAL3



National Institute of Standards and Technology
U.S. Department of Commerce