FIPS 201-3 Update:
Federation, PIV, and Derived PIV

Justin Richer

Bespoke Engineering

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

FIPS 201-3 Section 7: Federation

- New section in FIPS201-3
  - Contains guidance on how to use federation with PIV
  - Relies on SP-800-63C
  - Does not profile specific protocols
  - Hints at future SP on federation

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

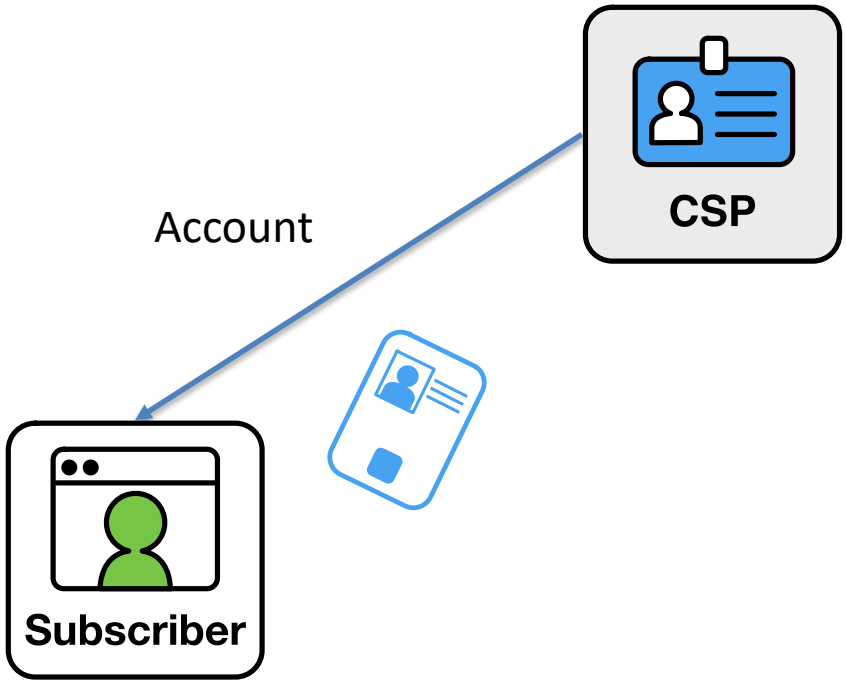
Why do we care about federation?

Federation is the recommended way for an agency to accept and process PIV credentials from other agencies.

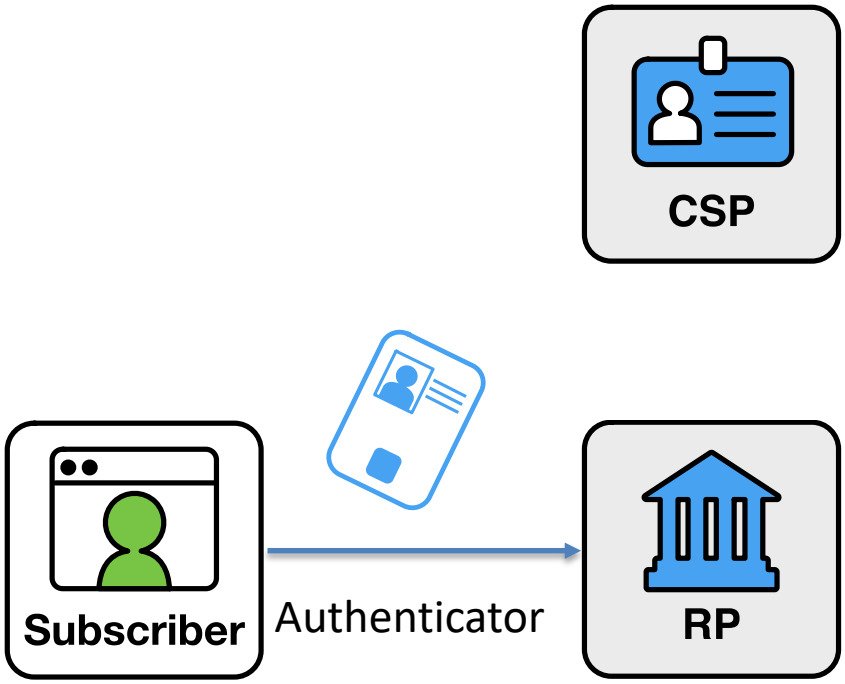
- FIPS 201-3 Section 7.3

A PIV Account in 3 Acts

Issue

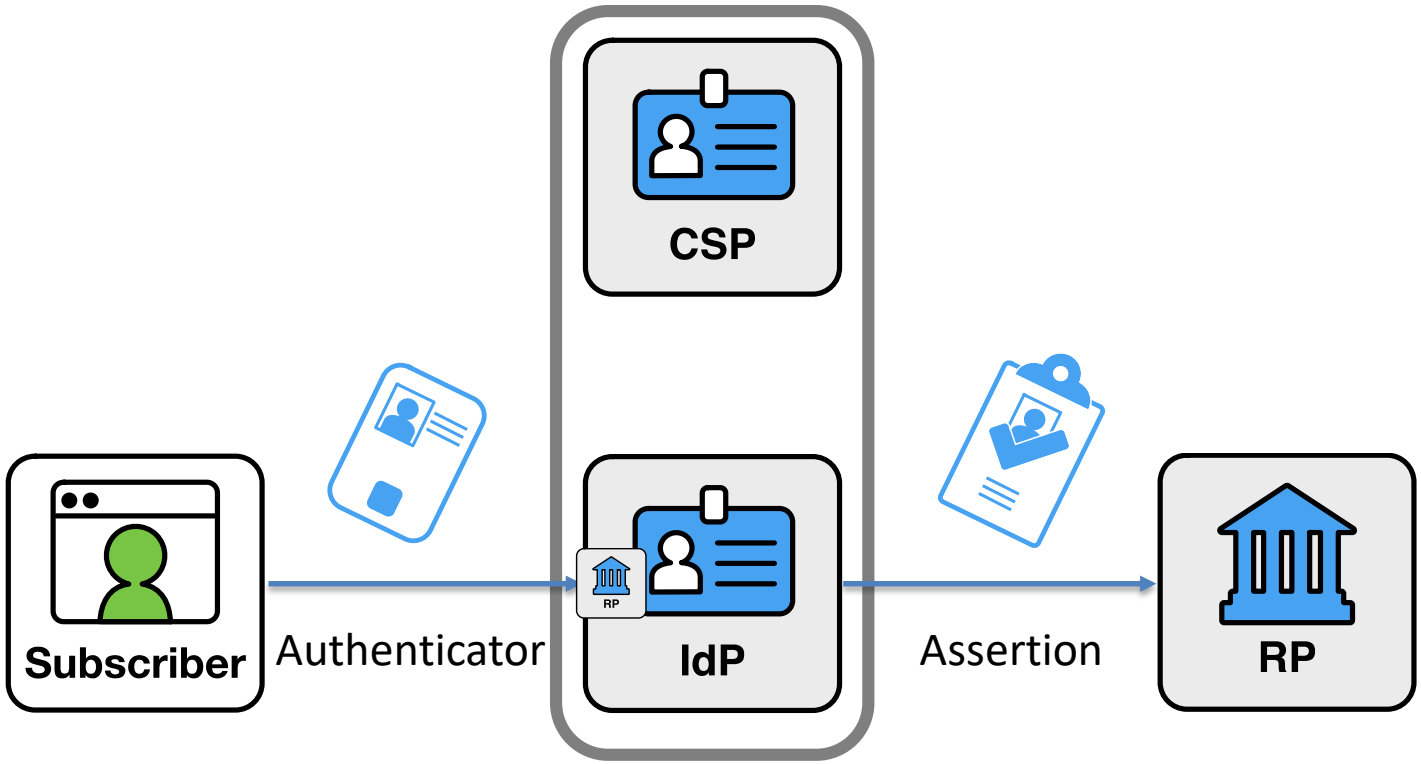


Authenticate



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

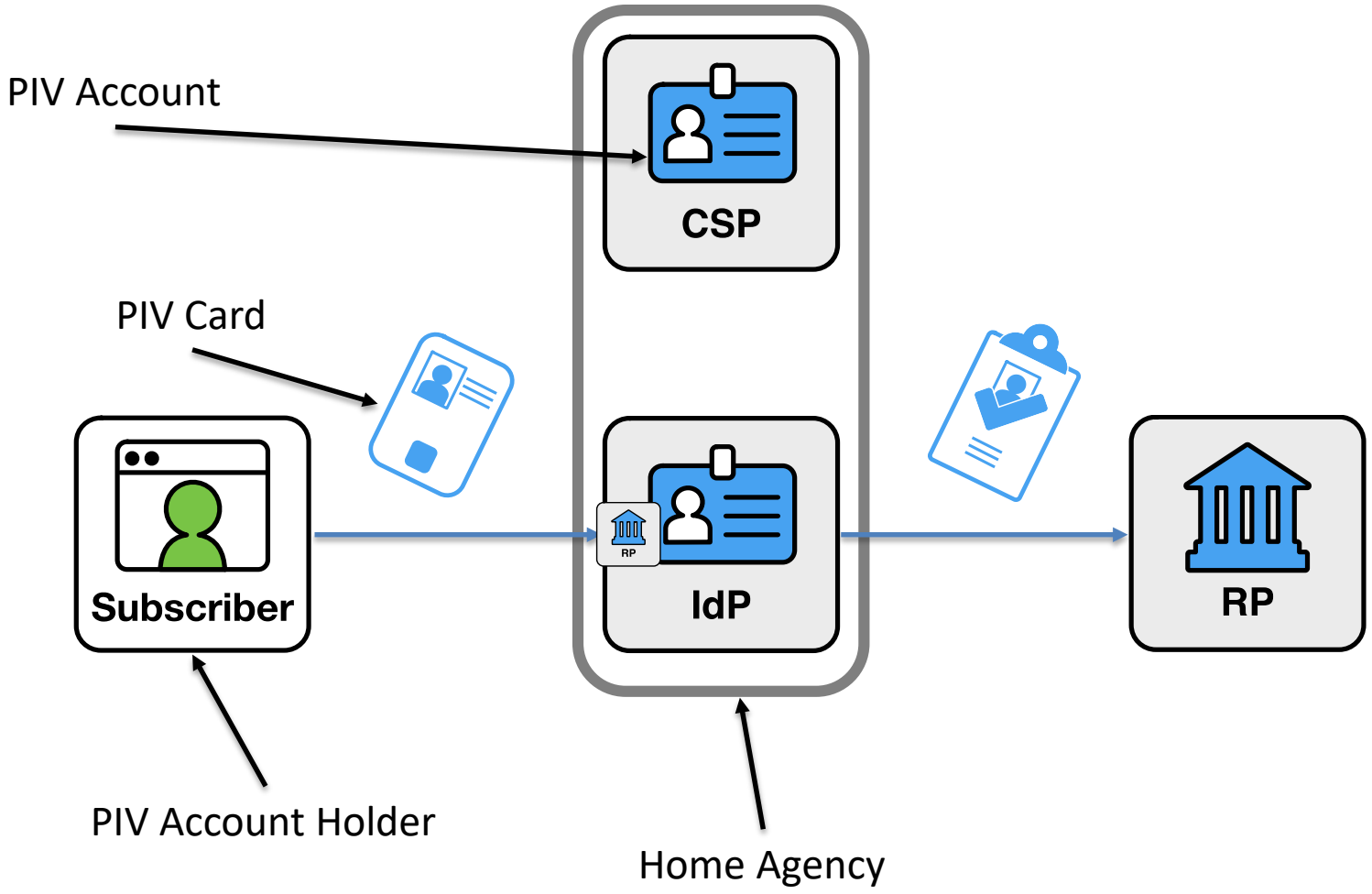
Federate



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

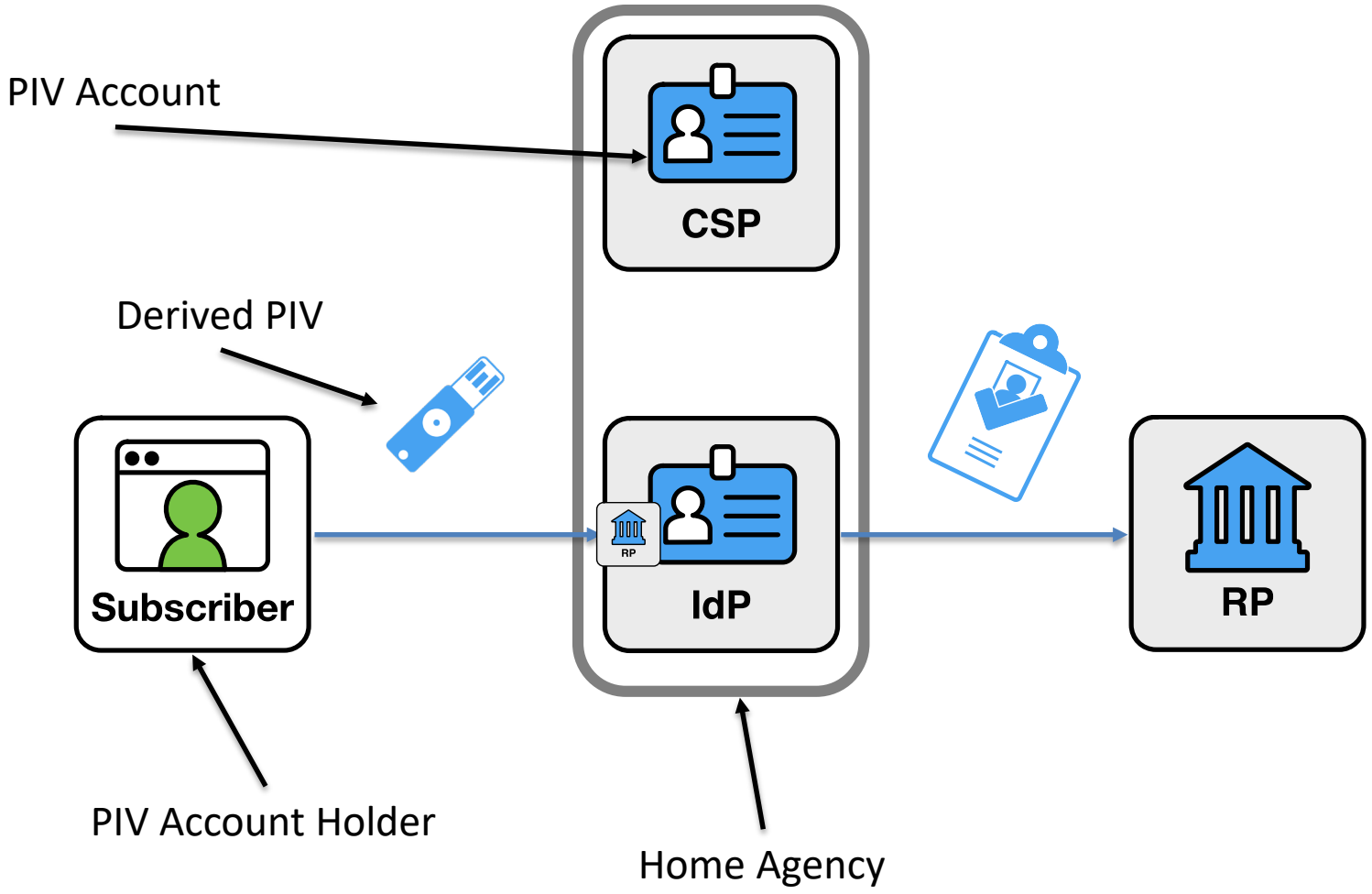
What does this mean for PIV?

PIV Components



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

Derived Authenticators



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

Proposed PIV Federation SP

- Architecture of PIV/Derived PIV in federation
  - Trust models for components
  - Authenticator binding requirements
  - Session management and log-in requirements
- Attribute requirements
  - Personal attributes
  - Application access rights
- Tradeoffs of federation over direct authentication
  - How and when to use federation with PIV
  - Benefits of federation

Defining “PIV Federation”

***PIV Federation**: The use of a federation protocol to facilitate login of a PIV Account to a relying party through the identity provider of the PIV Account’s home agency, where the authentication of the PIV Account to the identity provider is facilitated through either a PIV Card or derived PIV credential.*

PIV Account Federation Architecture

- Clear indication of “home” IdP for each PIV Account
  - Specified by the home agency
  - Could be run directly by the agency or via authority to operate
- Common trust framework of PIV Account verification process
  - Assessment framework for all parties

Not all uses of PIV are PIV Federation

PIV Federation:

- Federation of the **PIV Account** asserted by the **PIV issuer** using PIV Card or Derived PIV for authentication

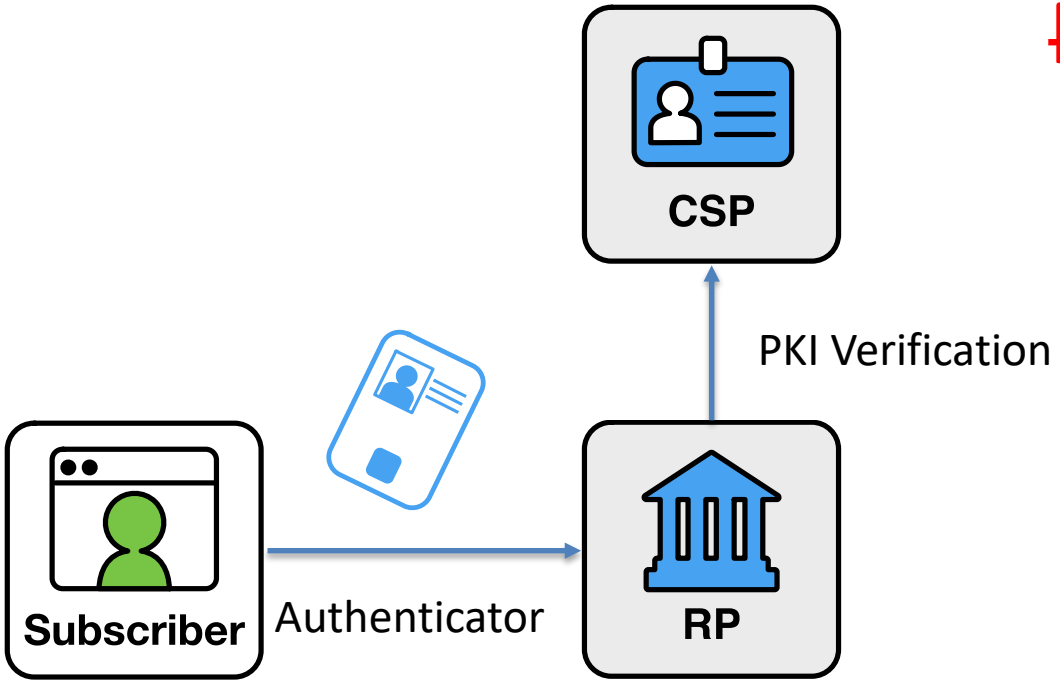
Not PIV Federation:

- Direct PKI Authentication
- IdP provided by someone other than the PIV issuer
- Proxied federation

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

PKI Authentication

~~PIV Federation~~



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

Certificate Credential

Certificate

Subject=

C=US
O=U.S. Government
OU=Department of Commerce
OU=National Institute of Standards and Technology
CN=JANE DOE
UID=93001000268907
E=JANE.DOE@nist.gov
Not Before:
Mar 22 15:37:40 2019 GMT
Not After:
Mar 22 16:04:58 2022 GMT

Public Key=

00:d7:4b:78:00:54:83:c8:ba:b3...

Attributes tied to certificate instance

RP

RP

RP

RPs have to check for revocation

Same certificate sent to all RPs

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

Certificate Credential

Certificate

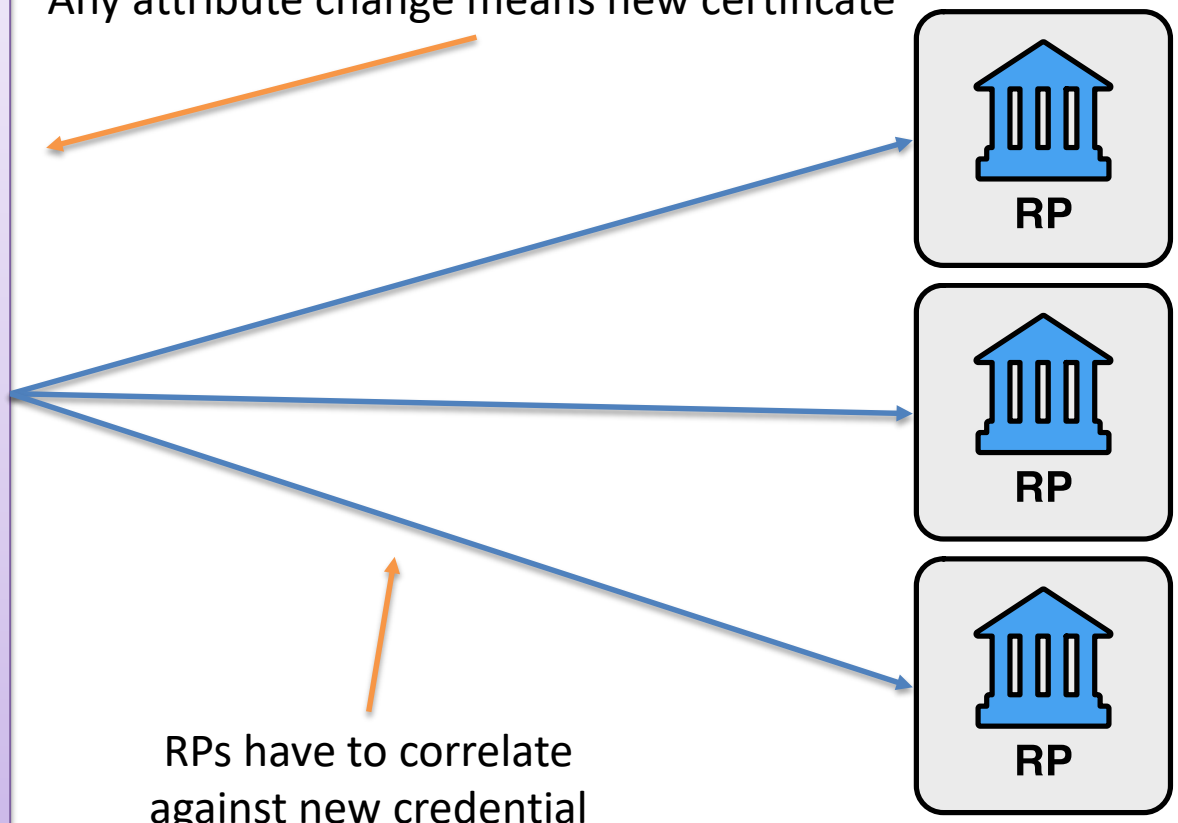
Subject=

C=US
O=U.S. Government
OU=Department of Commerce
OU=National Institute of Standards and Technology
CN=JANE DONT
UID=93001000268907
E=JANE.DONT@nist.gov
Not Before:
Oct 14 15:37:40 2021 GMT
Not After:
Oct 14 16:04:58 2024 GMT

Public Key=

d2:6e:57:94:fa:43:1c:d7
:3e:ae:78:10:9…

Any attribute change means new certificate



RPs have to correlate against new credential

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

Assertion

Assertion

Subject=
- sub: ZDM0N5SNKP
- iss: https://idp.nist.gov/
- email_address: JANE.DOE@nist.gov
- name: Jane Doe

Authentication=
- auth_time: Oct 14 15:37:40 2020 GMT
- exp: Oct 14 15:38:40 2020 GMT
- aud: RP1

Signature=
- SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c…

Created specifically for a single transaction

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

Lifetime: Years vs. Seconds

Certificate

Subject=

C=US
O=U.S. Government
OU=Department of Commerce
OU=National Institute of Standards and Technology
CN=JANE DONT
UID=93001000268907
E=JANE.DONT@nist.gov
Not Before:
Oct 14 15:37:40 2021 GMT
Not After:
Oct 14 16:04:58 2024 GMT

Public Key=

d2:6e:57:94:fa:43:1c:d7
:3e:ae:78:10:9…

Assertion

Subject=

sub: ZDM0N5SNKP
iss: https://idp.nist.gov/
email_address:
JANE.DOE@nist.gov
name: Jane Doe

Authentication=

auth_time:
Oct 14 15:37:40 2020 GMT
exp:
Oct 14 15:38:40 2020 GMT
aud: RP1

Signature=

SflKxwRJSMeKKF2QT4f
wpMeJf36POk6yJV_adQ
ssw5c…

Stable Private Identifier

Certificate

Subject=

C=US

O=U.S. Government

OU=Department of Commerce

OU=National Institute of Standards and Technology

CN=JANE DONT

UID=93001000268907

E=JANE.DONT@nist.gov

Not Before:

Oct 14 15:37:40 2021 GMT

Not After:

Oct 14 16:04:58 2024 GMT

Public Key=

d2:6e:57:94:fa:43:1c:d7

:3e:ae:78:10:9…

Assertion

Subject=

sub: ZDM0N5SNKP

iss: https://idp.nist.gov/

email_address:

JANE.DOE@nist.gov

name: Jane Doe

Authentication=

auth_time:

Oct 14 15:37:40 2020 GMT

exp:

Oct 14 15:38:40 2020 GMT

aud: RP1

Signature=

SflKxwRJSMeKKF2QT4f

wpMeJf36POk6yJV_adQ

ssw5c…

Audience Restriction

Certificate

Subject=
- C=US
- O=U.S. Government
- OU=Department of Commerce
- OU=National Institute of Standards and Technology
- CN=JANE DONT
- UID=93001000268907
- E=JANE.DONT@nist.gov
- Not Before:
- Oct 14 15:37:40 2021 GMT
- Not After:
- Oct 14 16:04:58 2024 GMT

Public Key=
- d2:6e:57:94:fa:43:1c:d7
- :3e:ae:78:10:9…

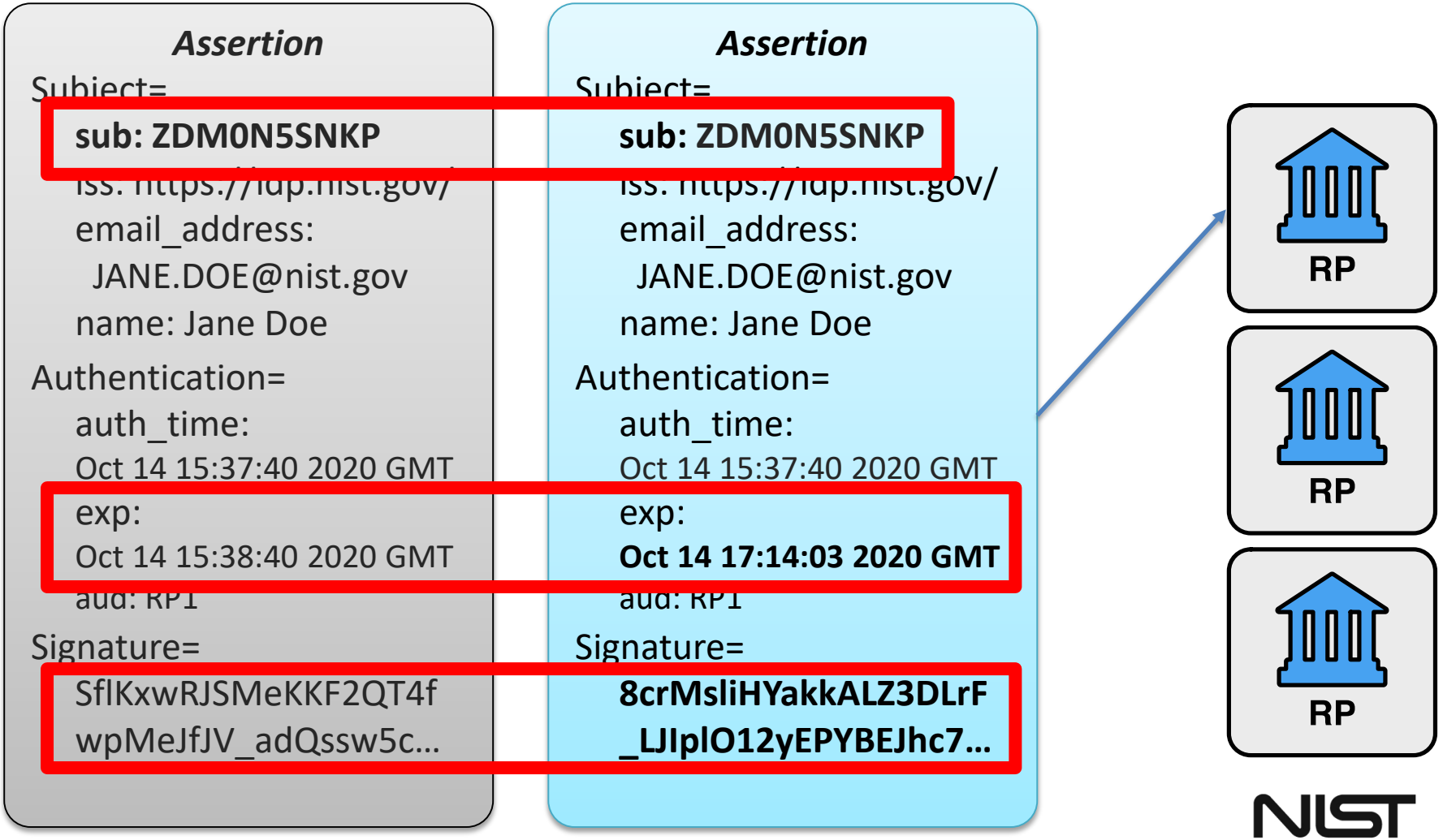
Assertion

Subject=
- sub: ZDM0N5SNKP
- iss: https://idp.nist.gov/
- email_address:
- JANE.DOE@nist.gov
- name: Jane Doe

Authentication=
- auth_time:
- Oct 14 15:37:40 2020 GMT
- exp:
- Oct 14 15:38:40 2020 GMT
- **aud: RP1**

Signature=
- SflKxwRJSMeKKF2QT4f
- wpMeJf36POk6yJV_adQ
- ssw5c…

Consistent Identifier



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

Audience Restriction

Assertion

Subject=
- sub: ZDM0N5SNKP
- iss: https://idp.nist.gov/
- email_address: JANE.DOE@nist.gov
- name: Jane Doe

Authentication=
- auth_time: Oct 14 15:37:40 2020 GMT
- exp: [illegible]
- aud: RP1

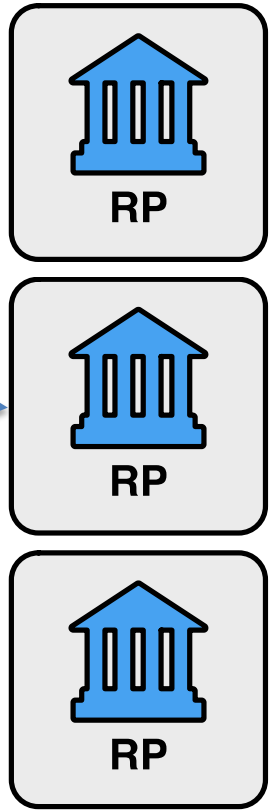
Signature=
- SflKxwRJSMeKKF2QT4f
- wpMeJfJV_adQssw5c…

Assertion

Subject=
- **sub: ZDM0N5SNKP**
- iss: https://idp.nist.gov/
- email_address: JANE.DOE@nist.gov
- name: Jane Doe

Authentication=
- auth_time: Oct 14 15:37:40 2020 GMT
- exp: [illegible]3:06 2020 GMT
- **aud: RP2**

Signature=
- O12JSMeBE8kALZ3Dcr
- MsliHYakLrF_LJIplJhc7…



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

Per-provider Identifiers

Assertion

Subject=

sub: ZDM0N5SNKP

iss: https://idp.nist.gov/

email_address:
JANE.DOE@nist.gov

name: Jane Doe

Authentication=

auth_time:
Oct 14 15:37:40 2020 GMT

exp:
Oct 14 15:38:40 2020 GMT

aud: RP1

Signature=

SflKxwRJSMeKKF2QT4f
wpMeJfJV_adQssw5c…

Assertion

Subject=

sub: SNCGKBFBSY

iss: https://idp.nist.gov/

email_address:
JANE.DOE@nist.gov

name: Jane Doe

Authentication=

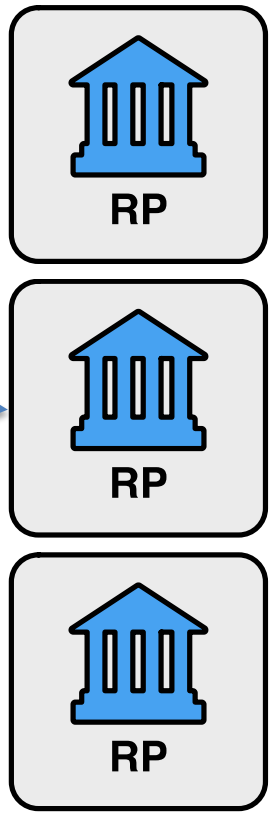
auth_time:
Oct 14 15:37:40 2020 GMT

exp:
Oct 14 15:43:06 2020 GMT

aud: RP2

Signature=

O12JSMeBE8kALZ3Dcr
MsliHYakLrF_LJIplJhc7…



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

Limited/unique attributes

Assertion

Subject=

sub: ZDM0N5SNKP
iss: https://idp.nist.gov/
email_address:
JANE.DOE@nist.gov
name: Jane Doe

Authentication=

auth_time:
Oct 14 15:37:40 2020 GMT
exp:
Oct 14 15:38:40 2020 GMT
aud: RP1

Signature=

SflKxwRJSMeKKF2QT4f
wpMeJfJV_adQssw5c…

Assertion

Subject=

sub: GBFNCKBSSY
iss: https://idp.nist.gov/

Authentication=

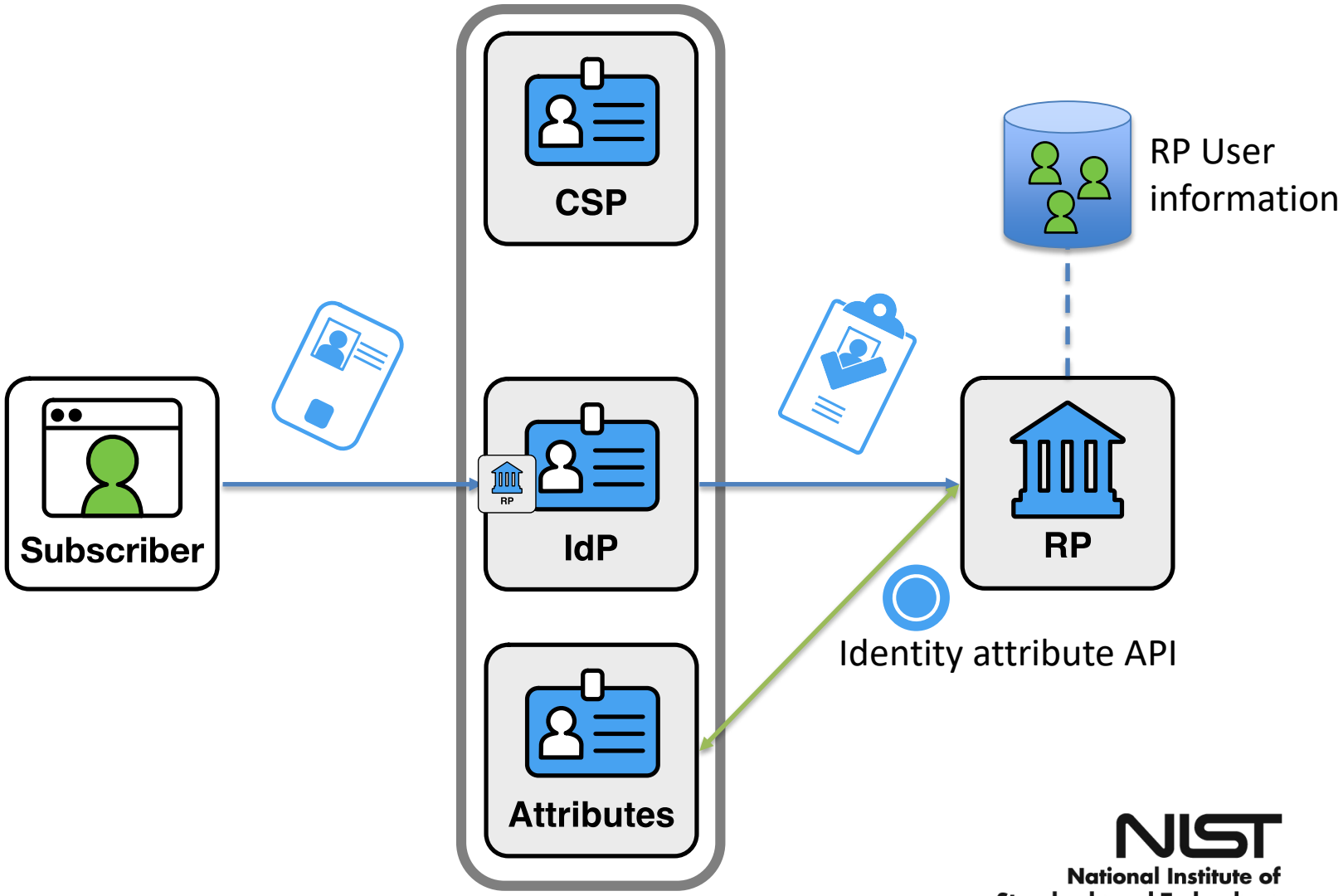
auth_time:
Oct 14 17:47:40 2020 GMT
exp:
Oct 14 17:53:06 2020 GMT
aud: RP3

Signature=

Xcu_FiEUwWI2kXRcNLC
nKvtWc34S3BuNxPSk…

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

Identity Attribute API



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

What's the difference?

Credential (Certificate)

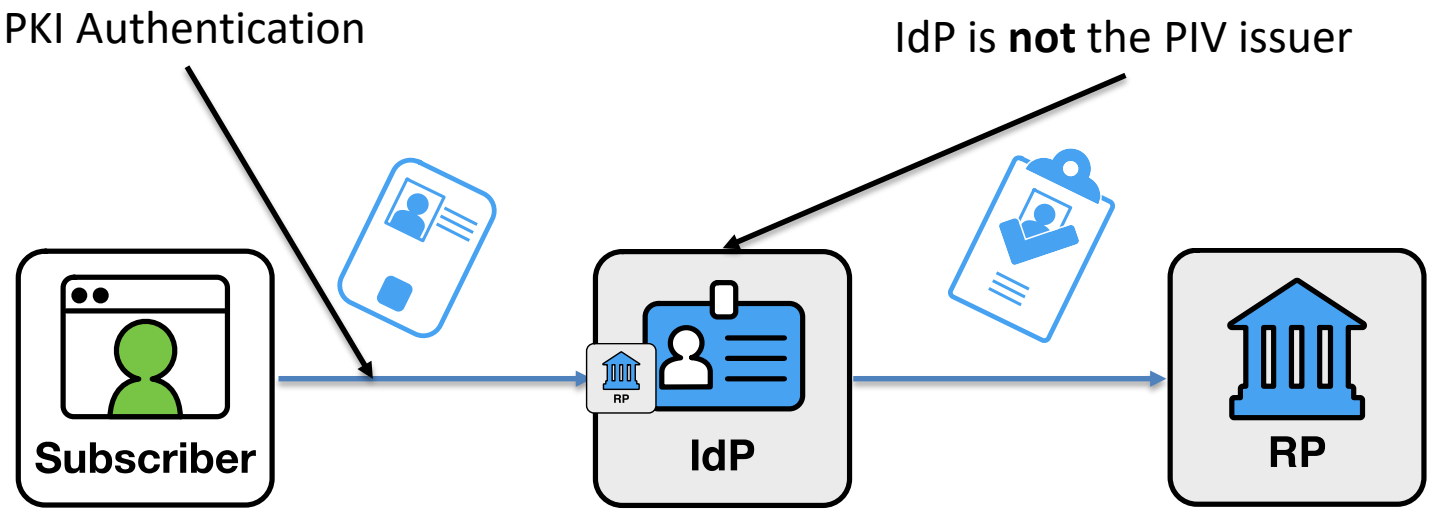
- Same for all RPs
  - Created once, installed on card
  - Fixed set of attributes
- Long lived (years)
- Requires certificate processing

Assertion

- Different for each RP/request
  - Created new each request
  - Different attributes per RP/request
- Short lived (minutes)
- Can be bound to many authenticators
- Can associate with identity APIs for additional attributes

Federation of PKI Credential

~~PIV Federation~~



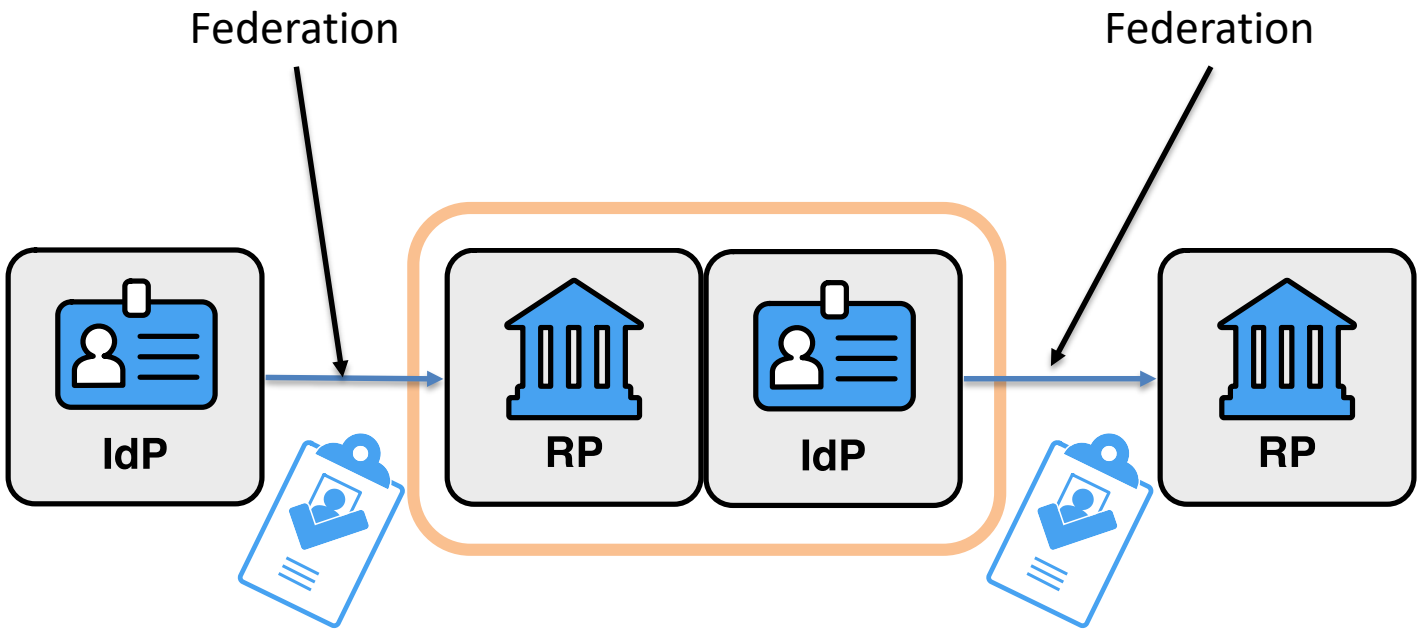
National Institute of Standards and Technology
U.S. Department of Commerce

Why not?

- IdP is not authoritative for the PIV account
- Could be tied to alternative (non-derived-PIV) credentials

Proxied Federation

~~PIV Federation~~

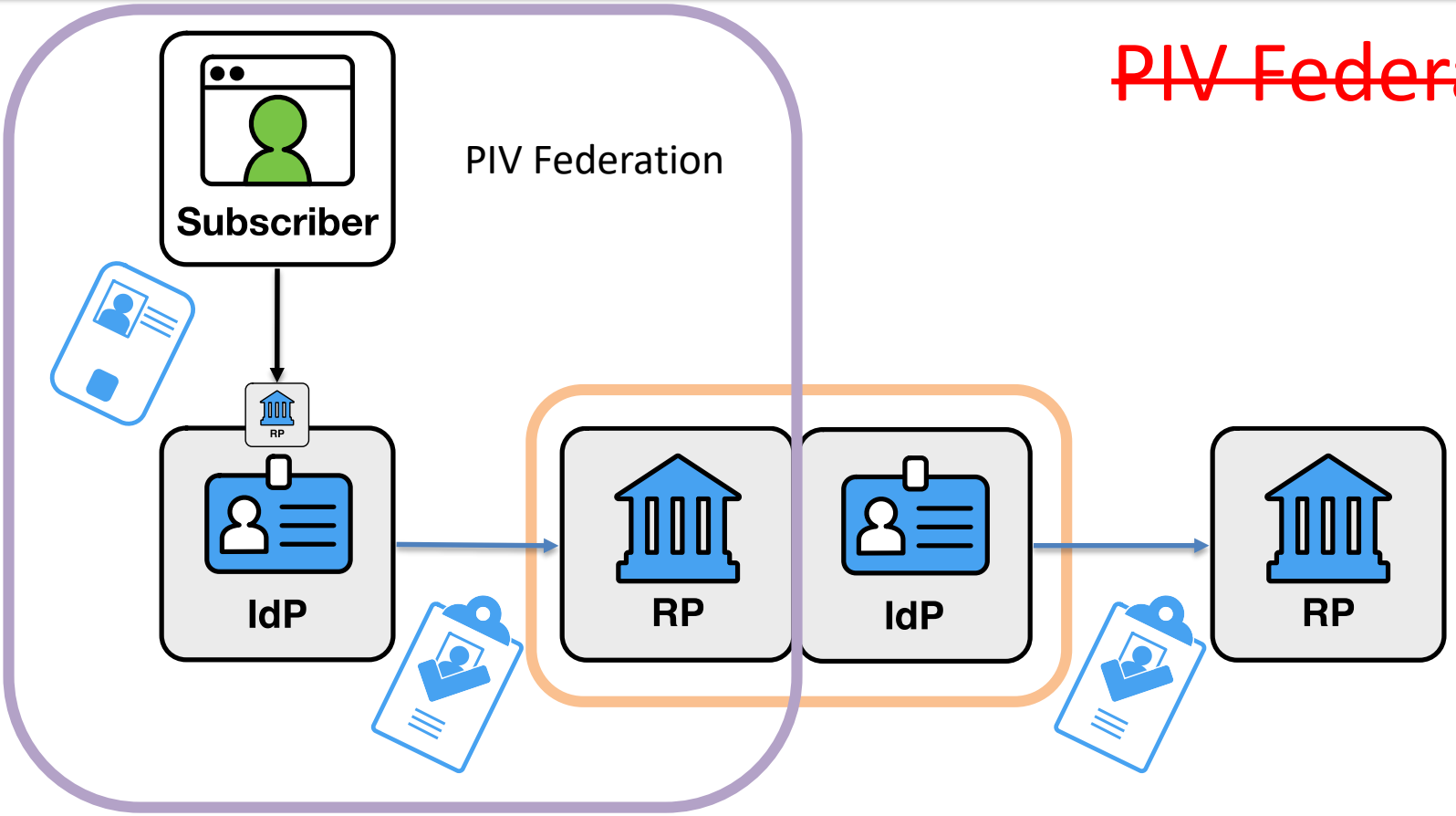


National Institute of Standards and Technology
U.S. Department of Commerce

Why not?

- Proxy IdP is not authoritative for the PIV account
  - Proxy must be fully trusted by the RP (as any IdP would be)
- PIV Account IdP is blinded from RP (and vice versa)

Proxied Federation



~~PIV Federation~~

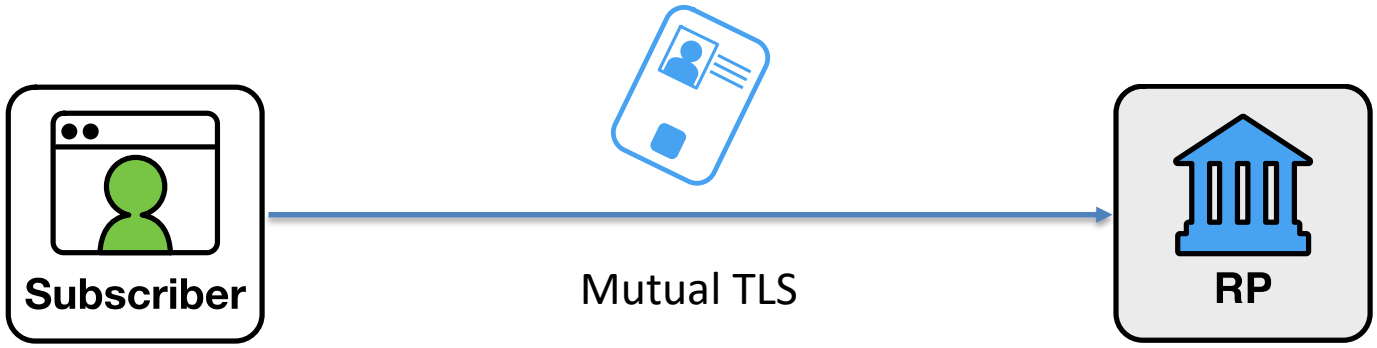
National Institute of Standards and Technology
U.S. Department of Commerce

Alternate Models Are Not Bad Things

Alternate models of PIV credential usage are not inherently bad, and in many cases can be the most appropriate approach for an RP. However, they are not defined by PIV Account Federation guidelines.

PIV Federation and Session Management

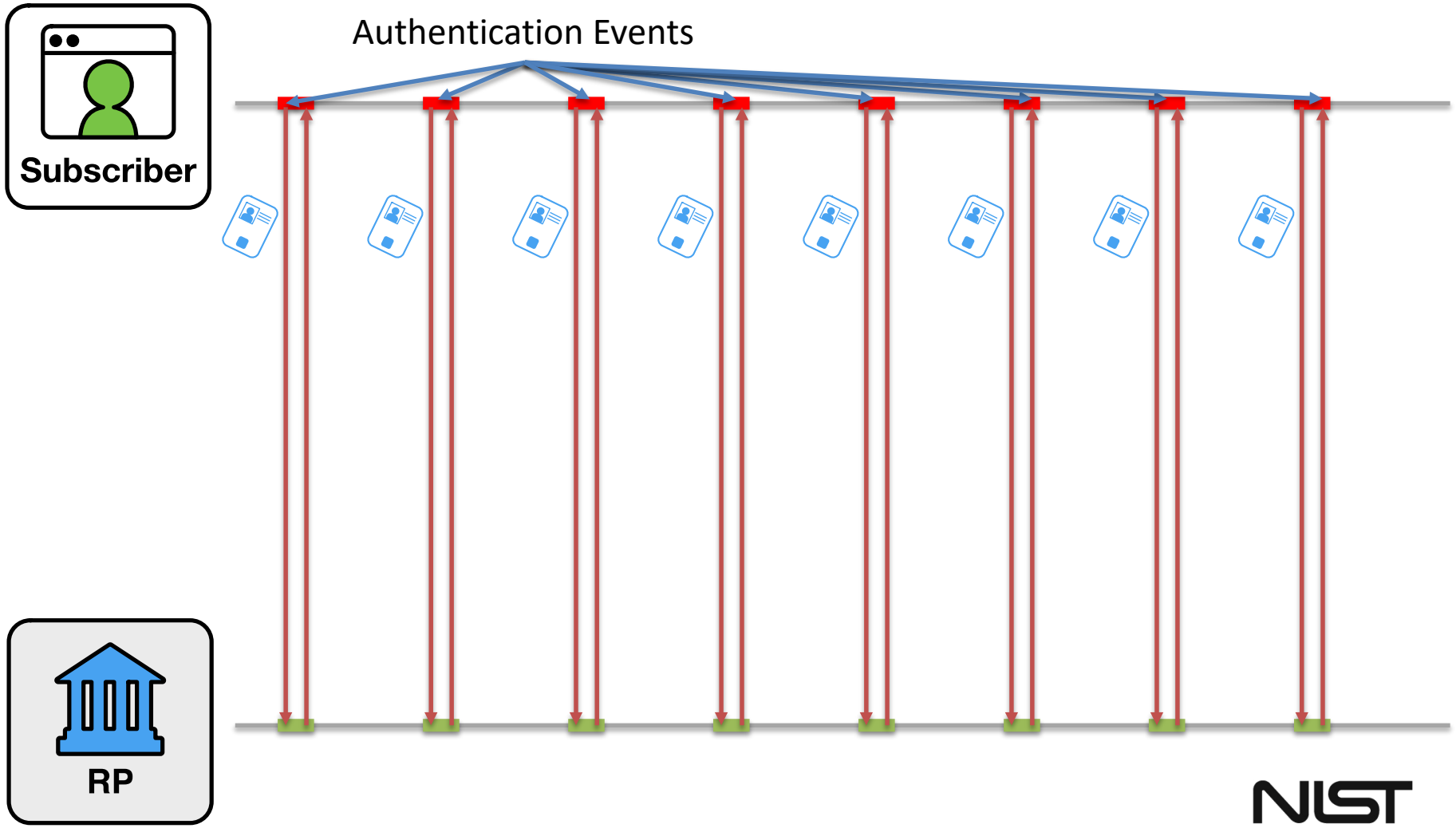
PKI Authentication (In Theory)



The web is made of pieces

Status	Method	Domain	File
200	GET	www.nist.gov	/
200	GET	www.nist.gov	nanoday20.jpg?itok=4cvu1TGl
200	GET	www.nist.gov	Kartik visible rainbow of wavelengths_0.jpg?itok=VohzFZ8M
200	GET	www.nist.gov	Screen Shot 2020-10-13 at 2.24.03 PM.png?itok=K6EQyVBn
200	GET	www.nist.gov	css_Uy_-zl29rJ4PVx1JZCdmUUOqNDo8jxCJ5By92dtFf-4.css
200	GET	www.nist.gov	css_jYZv5rK868ELAkTtTYz_L4rZFhD_zJ1SIs2OJ3R2pqg.css
200	GET	www.nist.gov	css_Wmk7cHp8tUe6LbVg3R63qxW01aH9Q-8Q4W2Hu6mxCwE.css
200	GET	www.nist.gov	css_QjJJwK3xM9GhvZw2QHpjt4tWAyRDr0y8WumNzjT6XCw.css
200	GET	www.nist.gov	css_RKukl929AesFR305ocVuW0ic-sFxKwfgb0PJLfUM_VY.css
200	GET	www.nist.gov	js_LvRAUPThLNI3oFbPPVRjrzRahHN6nwkrwEr_I3SAeco.js
200	GET	www.nist.gov	us_flag_small.png
200	GET	www.nist.gov	icon-dot-gov.svg
200	GET	www.nist.gov	icon-https.svg
200	GET	www.nist.gov	nist_logo_sidestack.svg
200	GET	www.nist.gov	nist_logo_sidestack_rev.svg
200	GET	www.nist.gov	nist-homepage-callout-1.png
200	GET	www.nist.gov	nist-homepage-callout-2.png

What actually happens

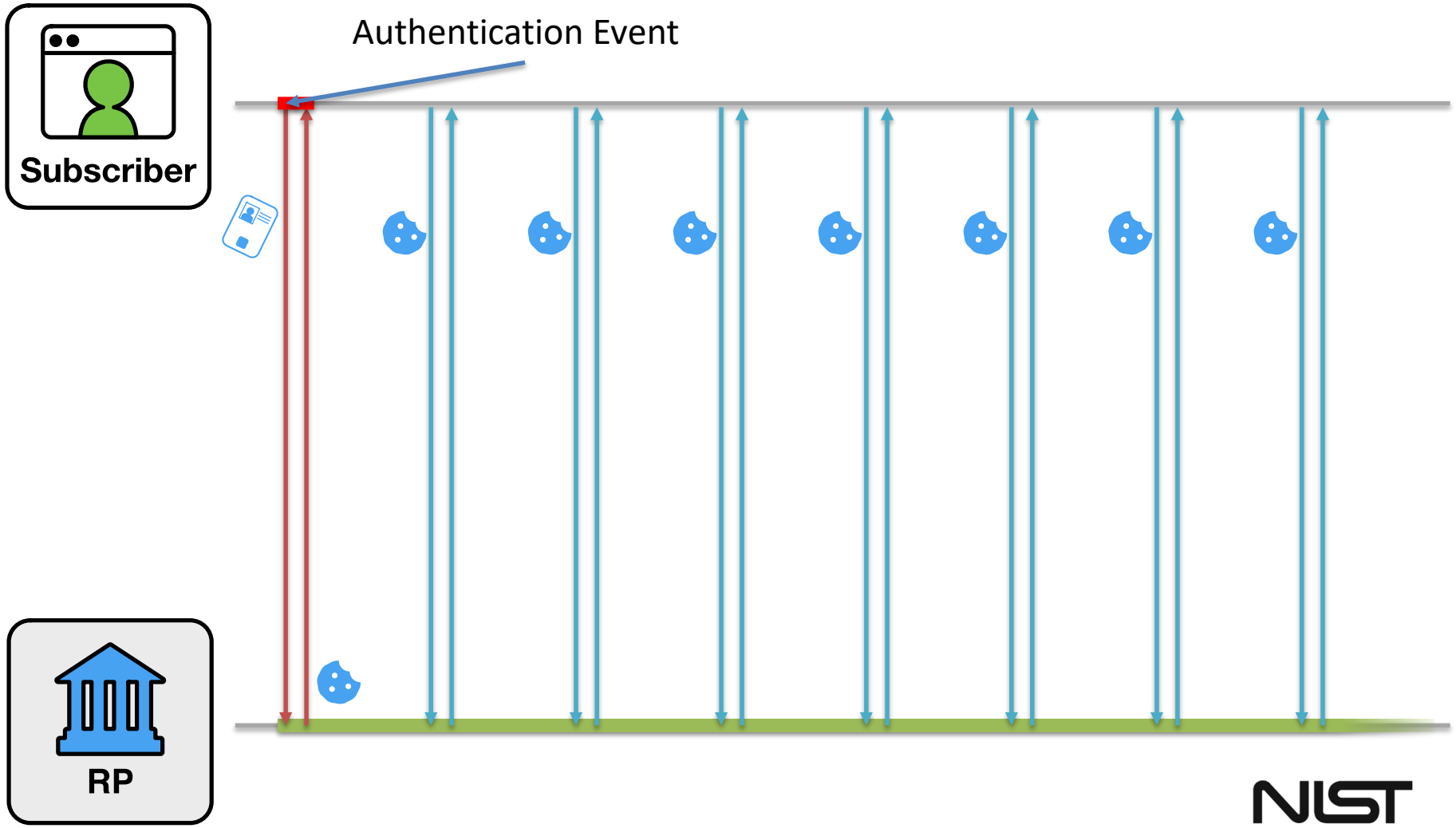


NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Session Management

- User begins session at RP
- RP challenges for credential to authenticate user
  - Capture authentication intent
- RP binds ongoing session to authenticated user

With Session Management

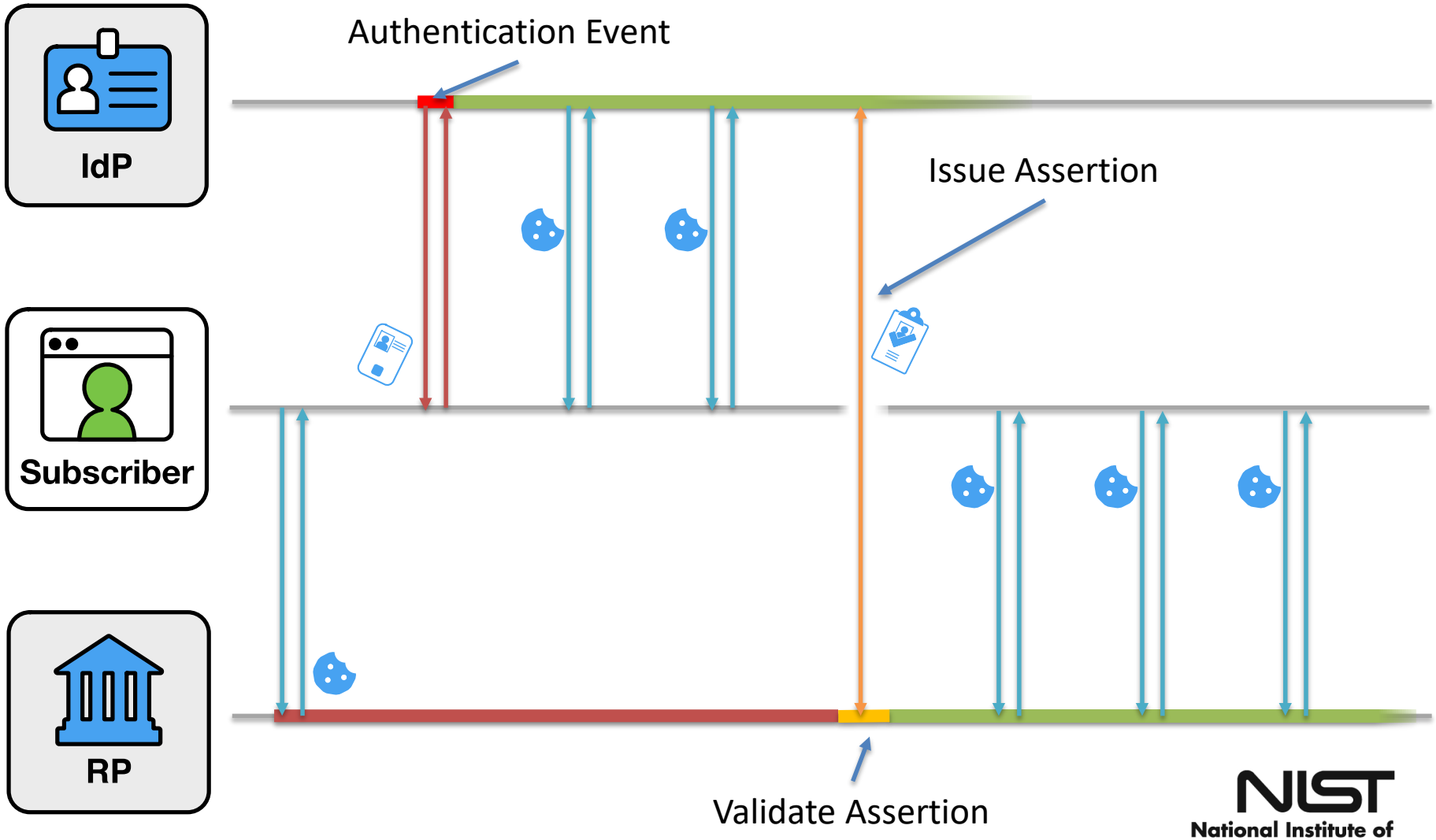


National Institute of Standards and Technology
U.S. Department of Commerce

Session Management with IdPs

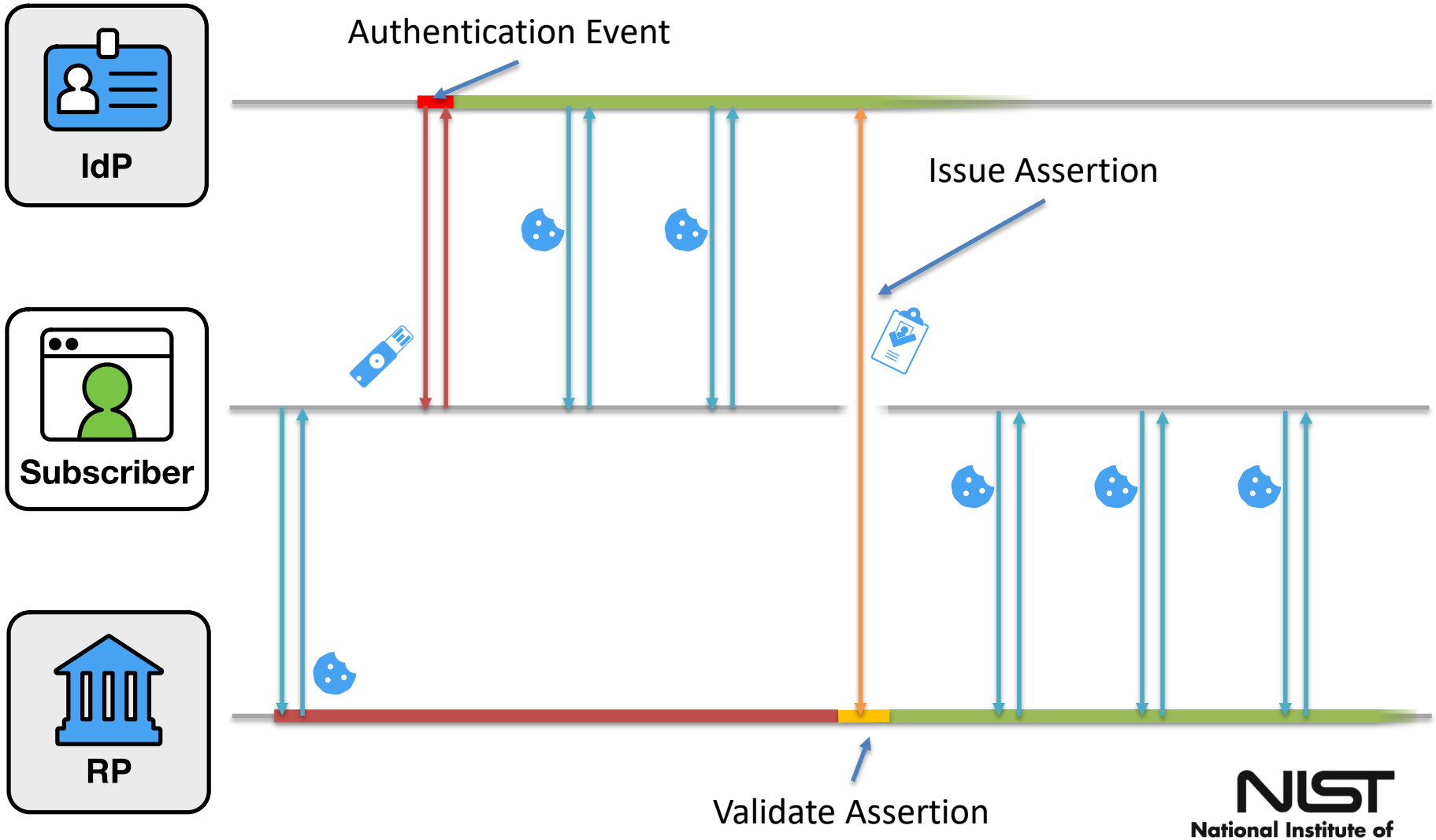
- User begins session (1) at RP
- RP sends user to IdP
- User being session (2) at IdP
- IdP challenges for credential to authenticate user
- IdP binds ongoing session (2) to authenticated user
- IdP creates assertion and sends to RP
- RP validates assertion
- RP binds ongoing session (1) to authenticated user

With Federation



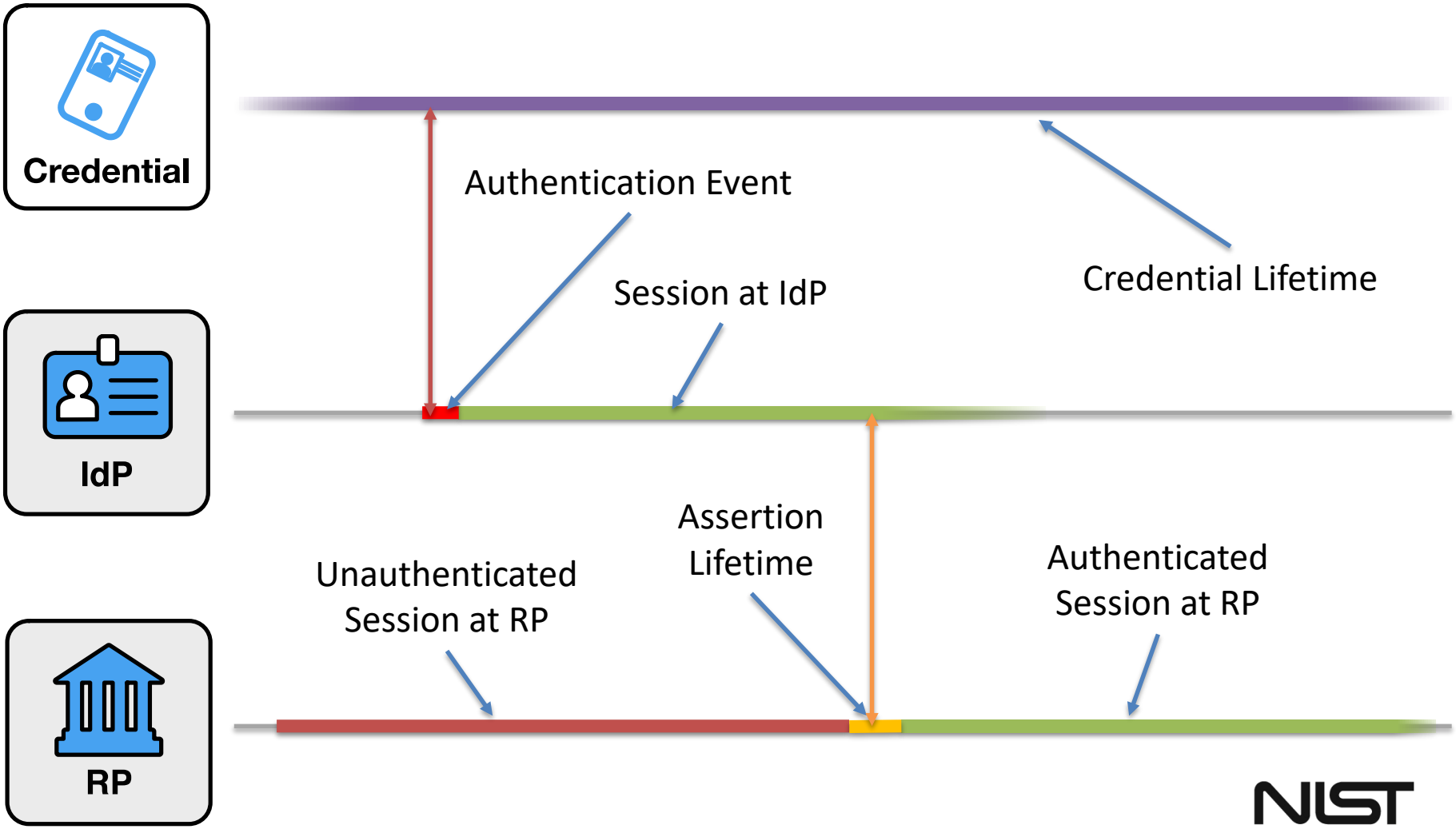
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

With Federation + Derived PIV



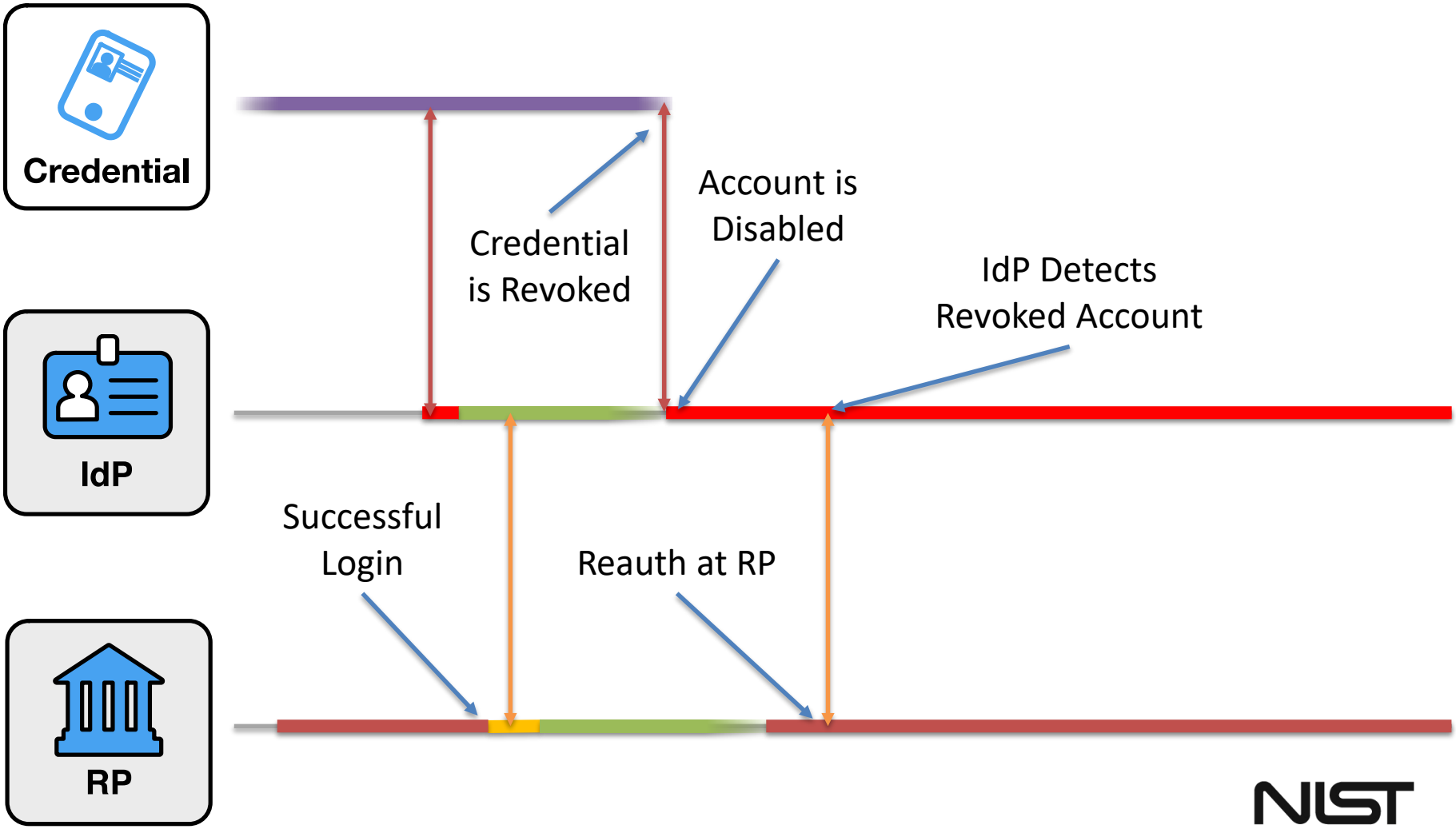
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Comparing Lifetimes



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

Credential Revocation



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

In Conclusion

Use federation technologies to connect to PIV accounts from different agencies, take advantage of derived PIV credentials, and build a more robust identity architecture.