3P Credential Creation in Webauthn

Lisbon Plenary
2020-02-05
Use case

Gadgets!!
Buy this gadget.

Buy

gadgets.com
Use case

Your PISP

You gonna buy dis?

Price: $45
FoS: BoA ****1234

Buy

pisp.com
boa.com
Use case

Gadgets!!

You bought it!

Buy more stuff

gadgets.com
Your PISP

You gonna buy dis?

Price: $45
FoP: BoA *****1234

Buy

pisp.com
boa.com
Your PISP

You gonna buy dis?

Price: $45
FoP: BoA *****1234

Buy

Is the real user authorizing this transaction?
Your PISP

You gonna buy dis?

Price: $45
FoP: BoA *****1234

Is the real user authorizing this transaction?
Your PISP

You gonna buy dis?

Price: $45
FoP: BoA *****1234

Buy

pisp.com
boa.com
Requirements

- No pre-existing trust between PISP and “bank”
- “Bank” wants to directly authenticate endpoint.
- No additional network connections (other than to pisp.com)
Proposal:

“Bank” directly creates FIDO credential at client, but scoped to PISP... at KYC-time.
Your PISP

Welcome to your brand new PISP!

Let’s get started!

Name: Bob Smith
Bank: BoA
Acct#: 87611234

Go
Hey Bob, pisp.com sent you here, let's make sure it's you!

Shoe size: 11
CVV: 123
DoB: 1991-11-1

It's really me!
Hey Bob, pisp.com sent you here, let's make sure it's you!

Shoe size: 11
CVV: 123
DoB: 1991-11-11

create() for pisp.com
Hey Bob, pisp.com sent you here, let's make sure it's you!

Shoe size: 11
CVV: 123
DoB: 1991-11-1

Learns public key and credential id
Welcome to your brand new PISP!
You are all set!
FoP: BoA *****1234
Yay!

Credential can be used by PISP.
Credential ID was forwarded by “bank” during redirect.
at transaction time...
Gadgets!!

Buy this gadget.

Buy
gadgets.com
Your PISP

You gonna buy dis?

Price: $45
FoP: BoA *****1234

Buy

```javascript
fido.get({
  credId: credId,
  rpId: pisp.com,
  challenge: hash(txId, price, ...)
})
```
Your PISP

You gonna buy dis?

Price: $45
FoP: BoA *****1234

Buy

FIDO assertion

pisp.com

boa.com
Your PISP

You gonna buy dis?

Price: $45
FoP: BoA *****1234

Buy

pisp.com
boa.com

FIDO assertion
Your PISP

You gonna buy dis?

Price: $45
FoP: BoA *****1234

Buy

pisp.com
boa.com

Trusts credential and can verify assertion because it knows public key
Gadgets!!

You bought it!

Buy more stuff

gadgets.com
Proposal:

RP A can create a FIDO credential for RP B.
Proposal:

RP A can create a FIDO credential for RP B.

Whoa! - what about tracking/correlation???
Proposal:

RP A can create a FIDO credential for RP B. But:

- RP A can’t exercise the credential afterwards. Only RP B can.

- Credential must not be resident-key.
  - This ensures that no new channel is created between A and B.
Proposal:

RP A can create a FIDO credential for RP B.

Can be done through extension or simply by relaxing the spec.
Benefits of the proposal

- Meets the requirements
  - No pre-existing trust between PISP and “bank”
  - “Bank” wants to directly authenticate endpoint.
  - No additional network connections (other than to pisp.com)

- No change in CTAP/authenticators needed
  - (just change in platform)

- “No resident-key” requirement has side effect of precluding DoS attacks
What’s next?

- Feedback from WG
- PR to webauthn spec