

UX Sprint Review #42

Account – Lockout functionality

How to handle the workflow regarding what happens when user locks their account

Amable Rodríguez
v2.0 / 2018-07-17

Digital Collaboration Division, Chief Information Officer Branch
Treasury Board of Canada Secretariat / Government of Canada

Division de la collaboration numérique, Direction du dirigeant principal de l'information
Secrétariat du Conseil du Trésor du Canada / Gouvernement du Canada

Document revisions

Version #	Comments	Author	Date
1.0	Document creation	Amable Rodríguez	2018-07-10
2.0	Migrated content to the new UX Document template, added explanatory texts	Amable Rodríguez	2018-07-17

Table of contents

1. Team	4
2. Needs	5
3. Initial conditions	6
4. Design process	8
5. Deliverables	31

1. Team

Product Owner



Bryan Robitaille



Nick Pietrantonio

Development

Development



Stéphanie C. Lefebvre



Amable Rodríguez

UX Design

Technical Writing



Marianne Aubrey

Help-Desk



Krista Lecuyer

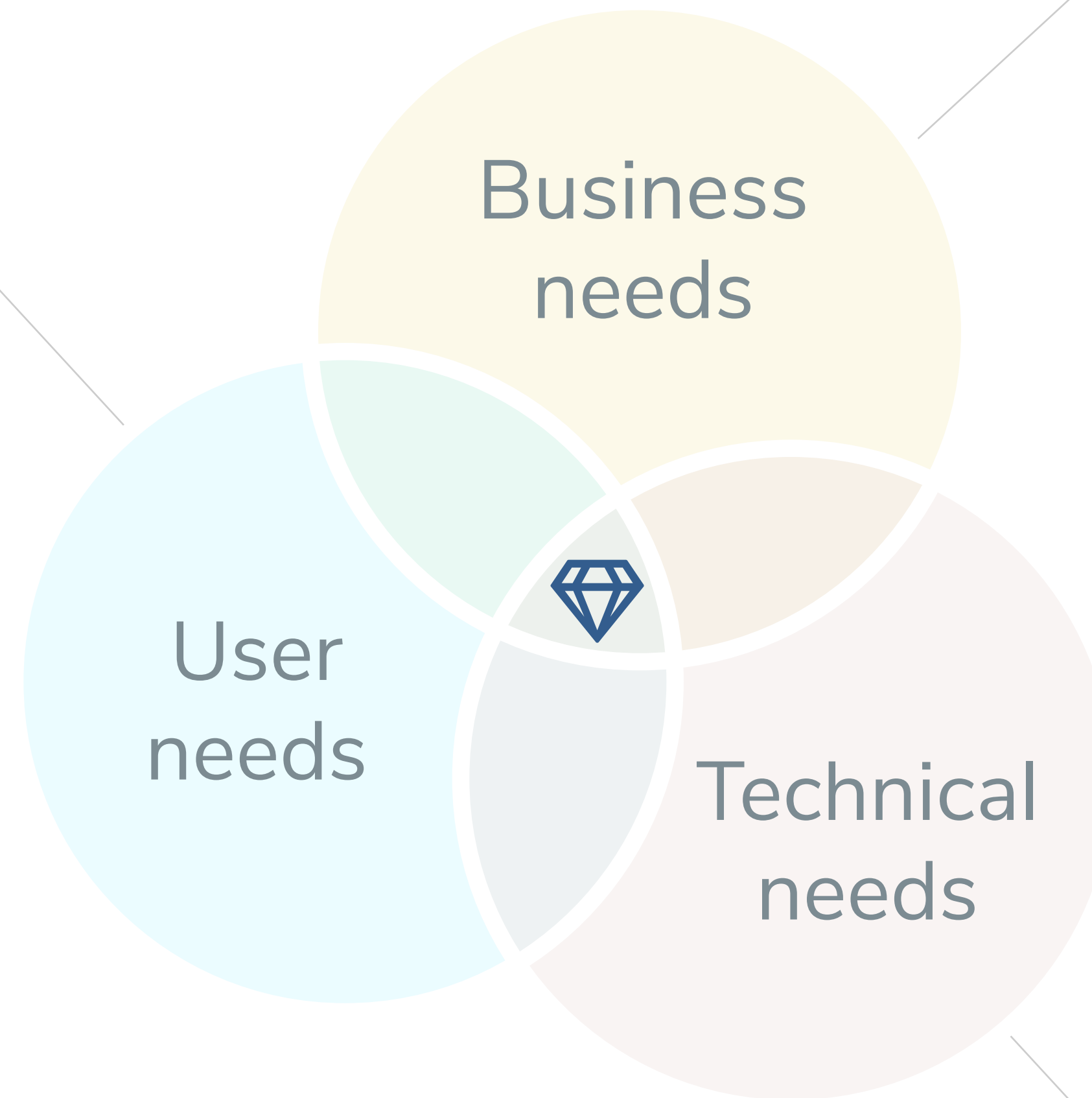


Donna Monbourquette

UX Research

2. Needs

- User needs to be able to recover his/her account by himself/herself
- User should be able to get help-desk help if it is impossible for him/her to recover the account



- Time consumed in help-desk on accounts recovery protocols needs to be reduced (currently between 10 ~15 tickets per day)

- Solution has to make use of the default lockout functionality already in the system

3. Initial conditions

Task, containing:

#2724

conclerage #57

May 9

No Priority

No Points

Account lockout functionality

As specified in the vulnerability report this PR is to address the brute force vulnerability identified.

How it works

1. When someone tries to login, we first check to see if they are currently blocked. We check the username they are trying to use, as well as the IP address. If they are blocked, goto step 5. If not blocked go to step 2.

2. They are not blocked, so we check to see if the login was valid. If valid go to step 6. If not valid go to step 3.

3. Login attempt wasn't valid. Add their username and IP address for this attempt to the cache. If this brings them over the limit, add them to the blocked list, and then goto step 5. If not over the limit goto step 4.

4. login was invalid, but not over the limit. Send them back to the login screen to try again.

5. User is blocked: Send them to the blocked page, telling them they are blocked, and give an estimate on when they will be unblocked.

6. Login is valid. Reset any failed login attempts, and forward to their destination.

The solution leverages the package django-defender and redis alpine image for cache. The lockout template can use some UX review and changes to language as required. The settings are currently set in the config.py file however should be moved to the Django admin interface.

Discussion Needed On

1. Should be include the movement of the defender setting to the django admin interface in this PR

2. UX / Layout of locked_out.html template when informing users their account has been locked. Will add screen shot of template tomorrow

Created by Bryan Robitaille

Labels

Project: Account Stack: UX

Type: Enhancement

Sprint

No Sprint

Epic

No Epic

Milestone

No Milestone

Assignees

Bryan Robitaille

Upvotes

0 upvotes

Move to Triage

Move to Done

Archive Card

Conversation unlocked

Subscribe

Related Cards

#3052 (gctools-outlaga/conclerage #61) Implement Account Lockout functionality in progress

Add a Comment

WRITE PREVIEW

Add a comment

Attach files via drag and drop, select from your computer or paste from clipboard.

Comment

Timeline

Show: comments events

Troy-Lawson added the label Stack: UX Jun 28

Troy-Lawson added the label Project: Account Jun 25

Troy-Lawson removed the label Status: Pending Jun 6

Troy-Lawson added the label Status: Pending May 17

Troy-Lawson removed the label Security May 17

Troy-Lawson added the label Type: Enhancement May 17

Nick - May 14

Leaving some thoughts on the experience and UI for discussion.

Should we send an email to the user when their account has been locked? The email could give more information about the lockout, how to contact helpdesk or how to recover the account. It could also inform users of others trying to get into their account.

After a certain number of incorrect attempts, just before the lockout, could the error message contain links to recover password? I'm not sure if there is a potential security risk with that. We can just let them wait a short amount of time (10mins seems reasonable).

Do we want to give users the option of password recovery while their account is locked? We may get a flood of help desk requests asking to be unlocked.

If the site customisation does not have a help desk link (others using generic account) what steps do users take to unlock their account?

I'll take a look at the UI in a bit and add more feedback. Again just adding thoughts for discussion.

UX Sprint Review #42 - Account - Lockout functionality

6

3. Initial conditions

Task, containing:

- Bryan description of default functionality
- Nick comments on how it could be better



Bryan Robitaille



Nick Pietrantonio

Review pull request on GitHub

#2724 condegrace #57 May 9

Account lockout functionality

As specified in the vulnerability report this PR is to address the brute force vulnerability identified.

How it works

1. When someone tries to login, we first check to see if they are currently blocked. We check the username they are trying to use, as well as the IP address. If they are blocked, goto step 5. If not blocked go to step 2.

2. They are not blocked, so we check to see if the login was valid. If valid go to step 6. If not valid go to step 3.

3. Login attempt wasn't valid. Add their username and IP address for this attempt to the cache. If this brings them over the limit, add them to the blocked list, and then goto step 5. If not over the limit goto step 4.

4. login was invalid, but not over the limit. Send them back to the login screen to try again.

5. User is blocked: Send them to the blocked page, telling them they are blocked, and give an estimate on when they will be unblocked.

6. Login is valid. Reset any failed login attempts, and forward to their destination.

The solution leverages the package django-defender and redis alpine image for cache. The lockout template can use some UX review and changes to language as required. The settings are currently set in the config.py file however should be moved to the Django admin interface.

Discussion Needed On

1. Should be include the movement of the defender setting to the django admin interface in this PR

2. UX / Layout of locked_out.html template when informing users their account has been locked.

Will add screen shot of template tomorrow

Created by Bryan Robitaille

Related Cards +

#2082 (sylvain-williams/condegrace #61) Implement Account Lockout functionality

In progress

Add a Comment

WRITE PREVIEW

Add a comment

Attach files via drag and drop, select from your computer or paste from clipboard

Comments

Timeline

Show comments events

Tray-Lawson added the label Stack UX Jun 25

Tray-Lawson added the label Project Account Jun 25

Tray-Lawson removed the label Status Pending Jun 9

Tray-Lawson added the label Status Pending May 11

Tray-Lawson removed the label Security May 17

Tray-Lawson added the label Type Enhancement May 17

None May 14

Leaving some thoughts on the experience and UI for discussion.

Should we send an email to the user when their account has been locked? The email could give more information about the lockout, how to contact helpdesk or how to recover the account. It could also inform users of others trying to get into their account.

After a certain number of incorrect attempts, just before the lockout, could the error message contain links to recover password? I'm not sure if there is a potential security risk with that. We can just let them wait a short amount of time (10mins seems reasonable).

Do we want to give users the option of password recovery while their account is locked? We may get a flood of help desk requests asking to be unlocked.

If the site customisation does not have a help desk link (others using generic account) what steps do users take to unlock their account?

I'll take a look at the UI in a bit and add more feedback. Again just adding thoughts for discussion.

Labels

Project Account Stack UX

Type Enhancement

Sort

No Sort

By Date

By Size

Milestone

No Milestone

Assignees

Bryan Robitaille

Upvotes

0 upvotes

Move to Stage

Move to Done

Archive Card

Conversation unlocked

Subscribe

UX Sprint Review #42 - Account - Lockout functionality

7

4. Design process

We took the Bryan's description of default behavior



Bryan Robitaille

How it works

1. When someone tries to login, we first check to see if they are currently blocked. We check the username they are trying to use, as well as the IP address. If they are blocked, goto step 5. If not blocked go to step 2.
2. They are not blocked, so we check to see if the login was valid. If valid go to step 6. If not valid go to step 3.
3. Login attempt wasn't valid. Add their username and IP address for this attempt to the cache. If this brings them over the limit, add them to the blocked list, and then goto step 5. If not over the limit goto step 4.
4. login was invalid, but not over the limit. Send them back to the login screen to try again.
5. User is blocked: Send them to the blocked page, telling them they are blocked, and give an estimate on when they will be unblocked.
6. Login is valid. Reset any failed login attempts, and forward to their destination.

4. Design process

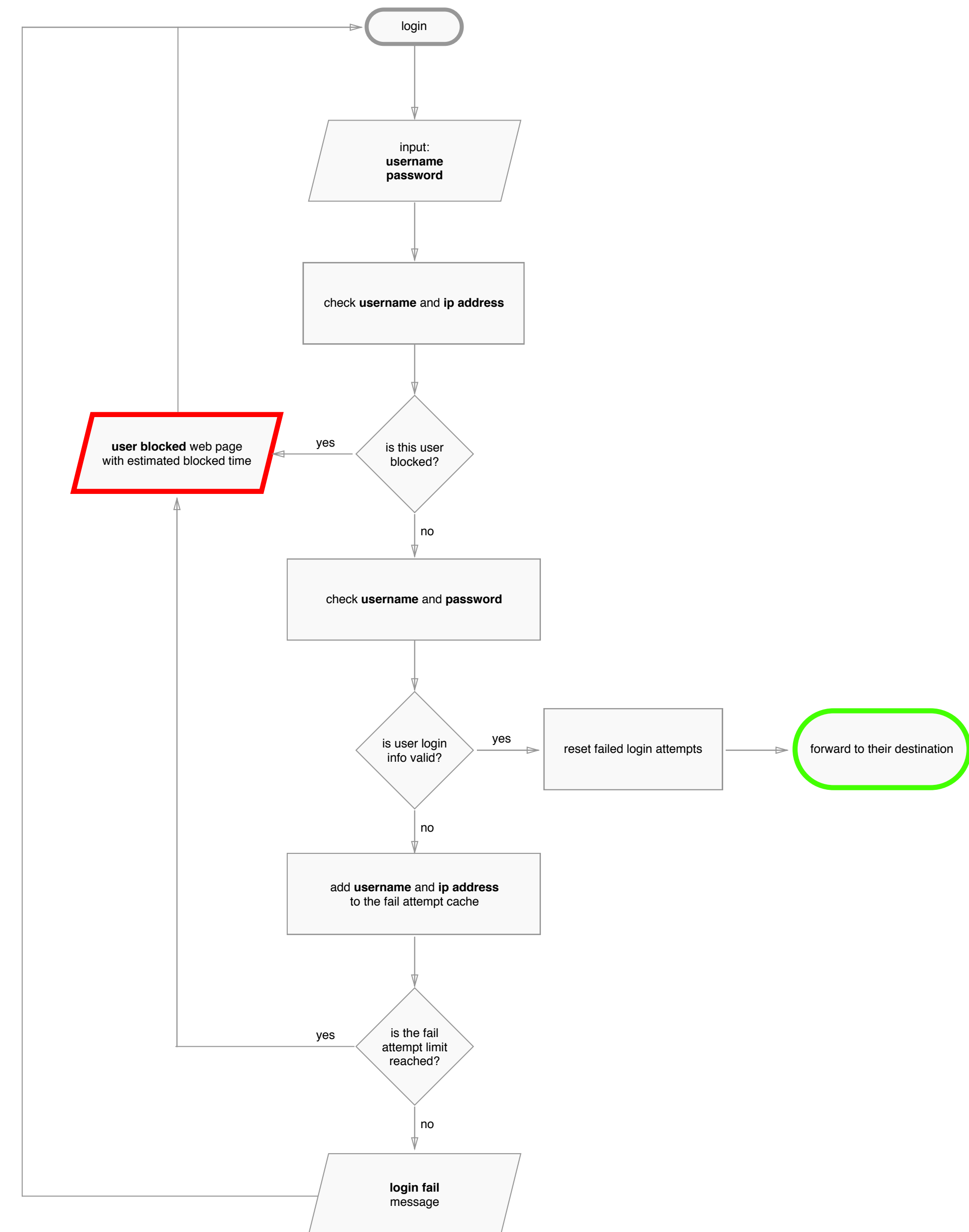
We took the Bryan's description of default behavior and we create the basic flow-chart.



Bryan Robitaille

How it works

1. When someone tries to login, we first check to see if they are currently blocked. We check the username they are trying to use, as well as the IP address. If they are blocked, goto step 5. If not blocked go to step 2.
2. They are not blocked, so we check to see if the login was valid. If valid go to step 6. If not valid go to step 3.
3. Login attempt wasn't valid. Add their username and IP address for this attempt to the cache. If this brings them over the limit, add them to the blocked list, and then goto step 5. If not over the limit goto step 4.
4. login was invalid, but not over the limit. Send them back to the login screen to try again.
5. User is blocked: Send them to the blocked page, telling them they are blocked, and give an estimate on when they will be unblocked.
6. Login is valid. Reset any failed login attempts, and forward to their destination.



4. Design process

We took the Bryan's description of default behavior and we create the basic flow-chart.



Bryan Robitaille

How it works

1. When someone tries to login, we first check to see if they are currently blocked. We check the username they are trying to use, as well as the IP address. If they are blocked, goto step 5. If not blocked go to step 2.
2. They are not blocked, so we check to see if the login was valid. If valid go to step 6. If not valid go to step 3.
3. Login attempt wasn't valid. Add their username and IP address for this attempt to the cache. If this brings them over the limit, add them to the blocked list, and then goto step 5. If not over the limit goto step 4.
4. login was invalid, but not over the limit. Send them back to the login screen to try again.
5. User is blocked: Send them to the blocked page, telling them they are blocked, and give an estimate on when they will be unblocked.
6. Login is valid. Reset any failed login attempts, and forward to their destination.

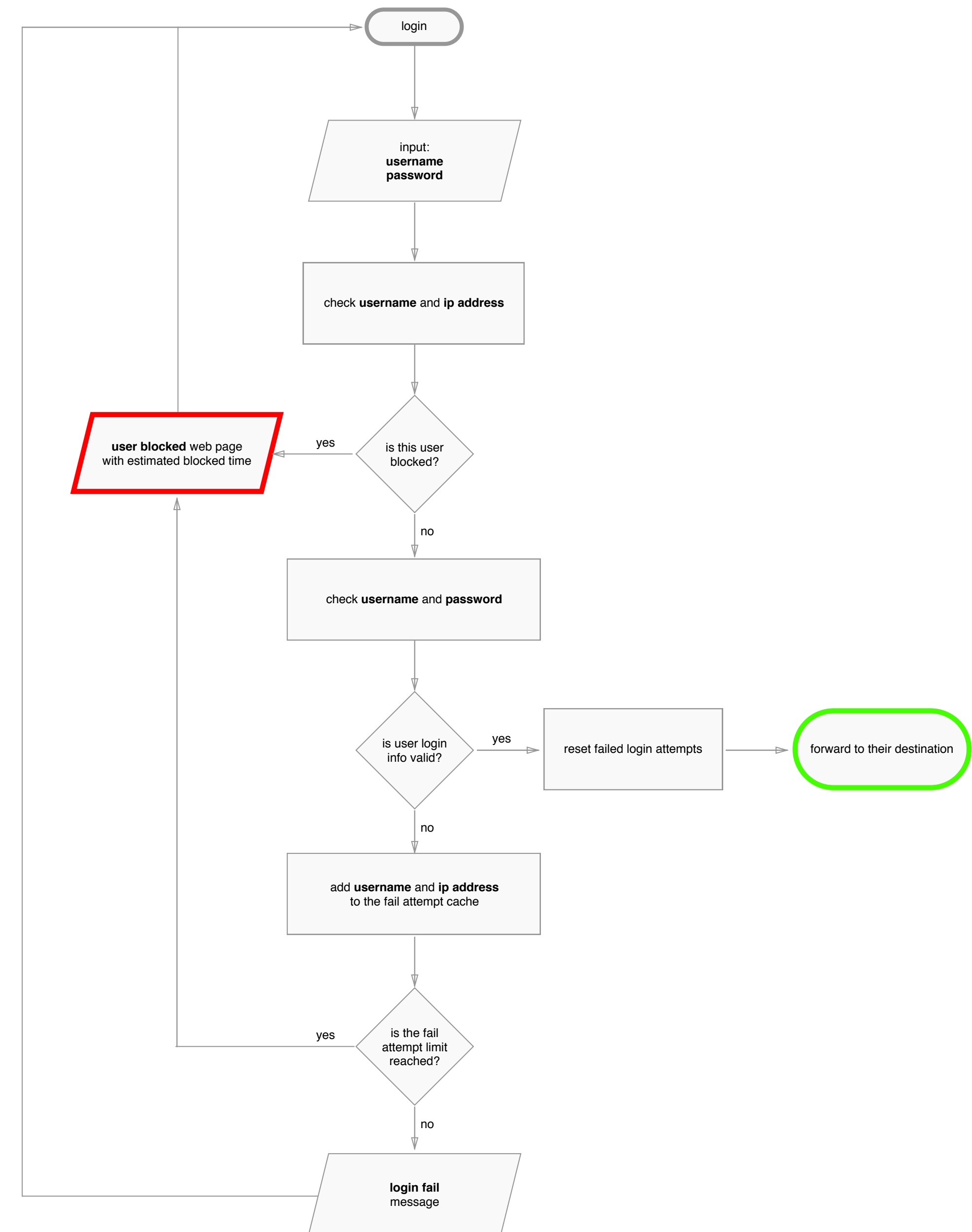
After some discussions with Stéphanie,



Amable Rodriguez



Stéphanie C. Lefebvre



4. Design process

We took the Bryan's description of default behavior and we create the basic flow-chart.



Bryan Robitaille

How it works

1. When someone tries to login, we first check to see if they are currently blocked. We check the username they are trying to use, as well as the IP address. If they are blocked, goto step 5. If not blocked go to step 2.
2. They are not blocked, so we check to see if the login was valid. If valid go to step 6. If not valid go to step 3.
3. Login attempt wasn't valid. Add their username and IP address for this attempt to the cache. If this brings them over the limit, add them to the blocked list, and then goto step 5. If not over the limit goto step 4.
4. login was invalid, but not over the limit. Send them back to the login screen to try again.
5. User is blocked: Send them to the blocked page, telling them they are blocked, and give an estimate on when they will be unblocked.
6. Login is valid. Reset any failed login attempts, and forward to their destination.

After some discussions with Stéphanie, adding Nick's comments,



Nick Pietrantonio

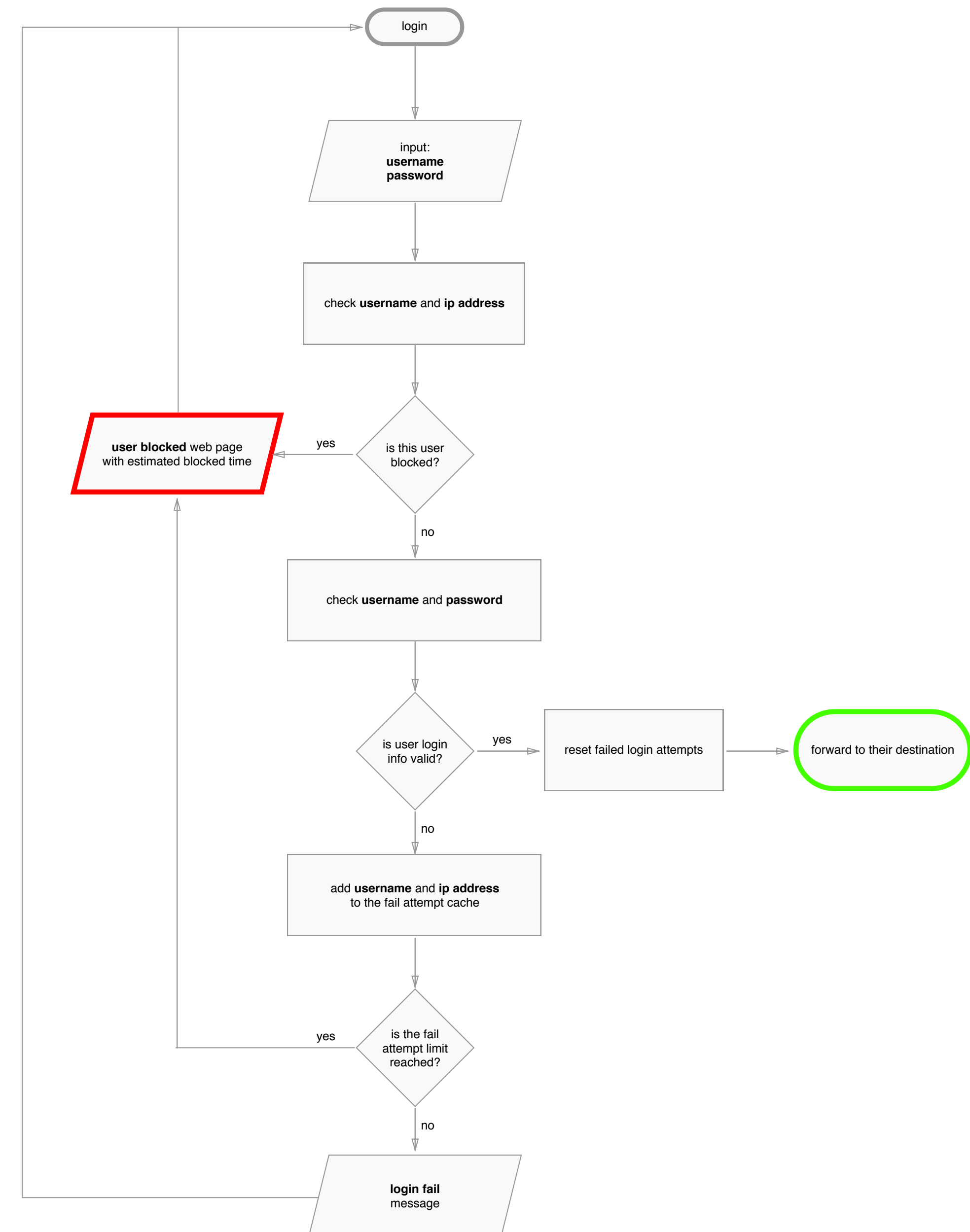
- Should we send an email to the user when their account has been locked? The email could give more information about the lockout, how to contact helpdesk or how to recover the account. It could also inform users of others trying to get into their account.
- After a certain number of incorrect attempts, just before the lockout, could the error message contain links to recover password? I'm not sure if there is a potential security risk with that. We can just let them wait a short amount of time (10mins seems reasonable).
- Do we want to give users the option of password recovery while their account is locked? We may get a flood of help desk requests asking to be unlocked.
- If the site customisation does not have a help desk link (others using generic account) what steps do users take to unlock their account?



Amable Rodriguez



Stéphanie C. Lefebvre



4. Design process

We took the Bryan's description of default behavior and we create the basic flow-chart.



Bryan Robitaille

How it works

1. When someone tries to login, we first check to see if they are currently blocked. We check the username they are trying to use, as well as the IP address. If they are blocked, goto step 5. If not blocked go to step 2.
2. They are not blocked, so we check to see if the login was valid. If valid go to step 6. If not valid go to step 3.
3. Login attempt wasn't valid. Add their username and IP address for this attempt to the cache. If this brings them over the limit, add them to the blocked list, and then goto step 5. If not over the limit goto step 4.
4. login was invalid, but not over the limit. Send them back to the login screen to try again.
5. User is blocked: Send them to the blocked page, telling them they are blocked, and give an estimate on when they will be unblocked.
6. Login is valid. Reset any failed login attempts, and forward to their destination.

After some discussions with Stéphanie, adding Nick's comments, and discussion with Krista,



Nick Pietrantonio

- Should we send an email to the user when their account has been locked? The email could give more information about the lockout, how to contact helpdesk or how to recover the account. It could also inform users of others trying to get into their account.
- After a certain number of incorrect attempts, just before the lockout, could the error message contain links to recover password? I'm not sure if there is a potential security risk with that. We can just let them wait a short amount of time (10mins seems reasonable).
- Do we want to give users the option of password recovery while their account is locked? We may get a flood of help desk requests asking to be unlocked.
- If the site customisation does not have a help desk link (others using generic account) what steps do users take to unlock their account?



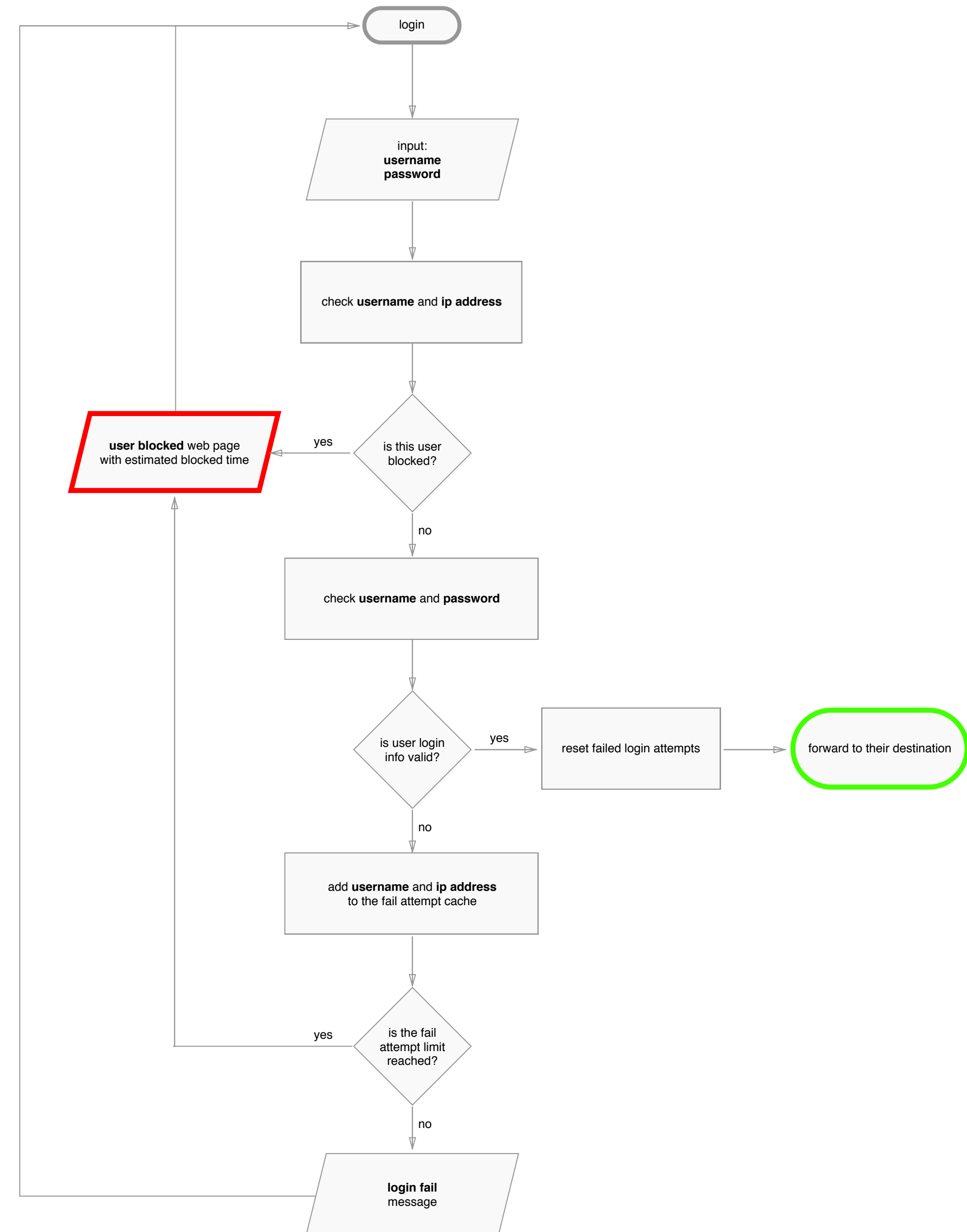
Amable Rodriguez



Stéphanie C. Lefebvre

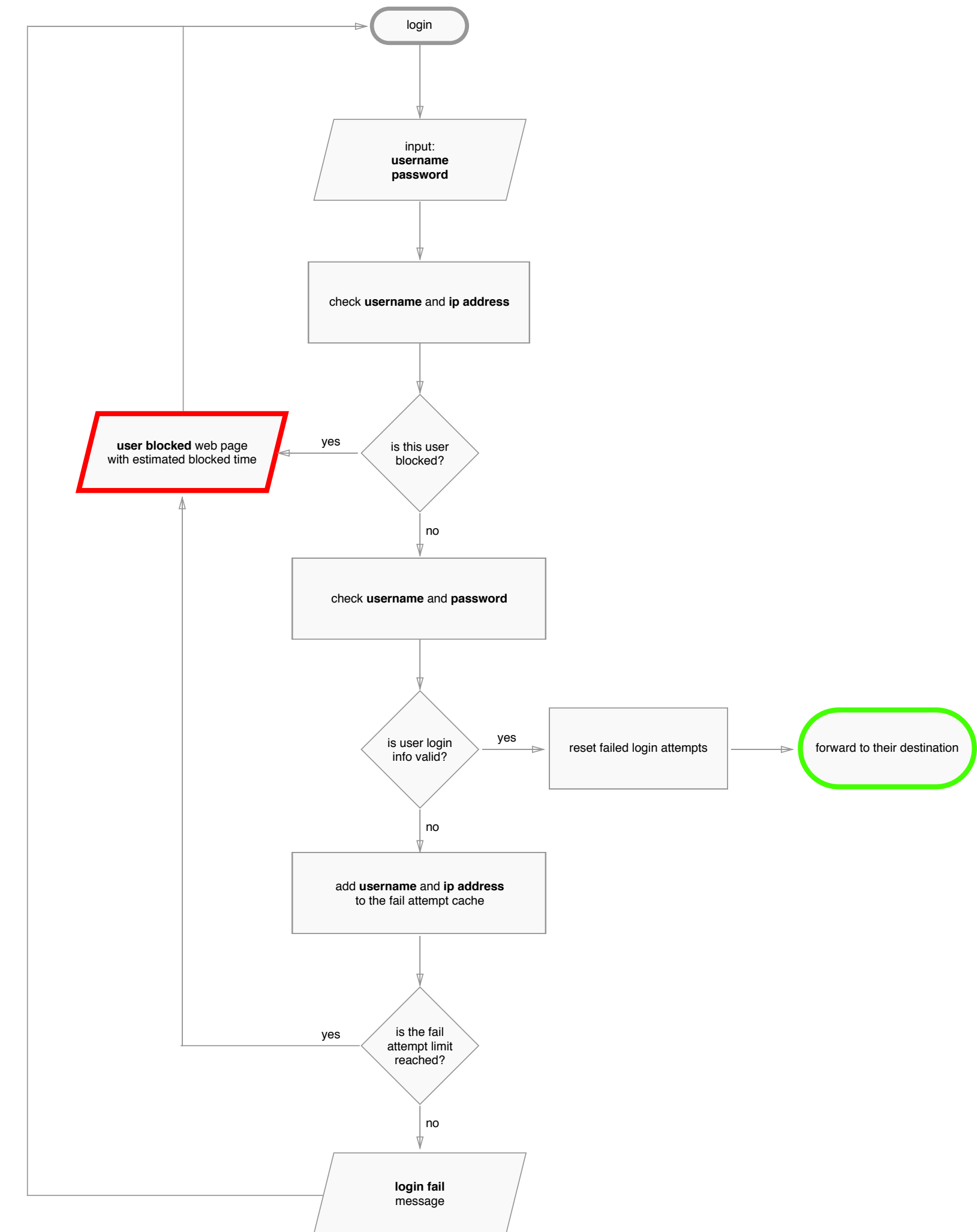


Krista Lecuyer



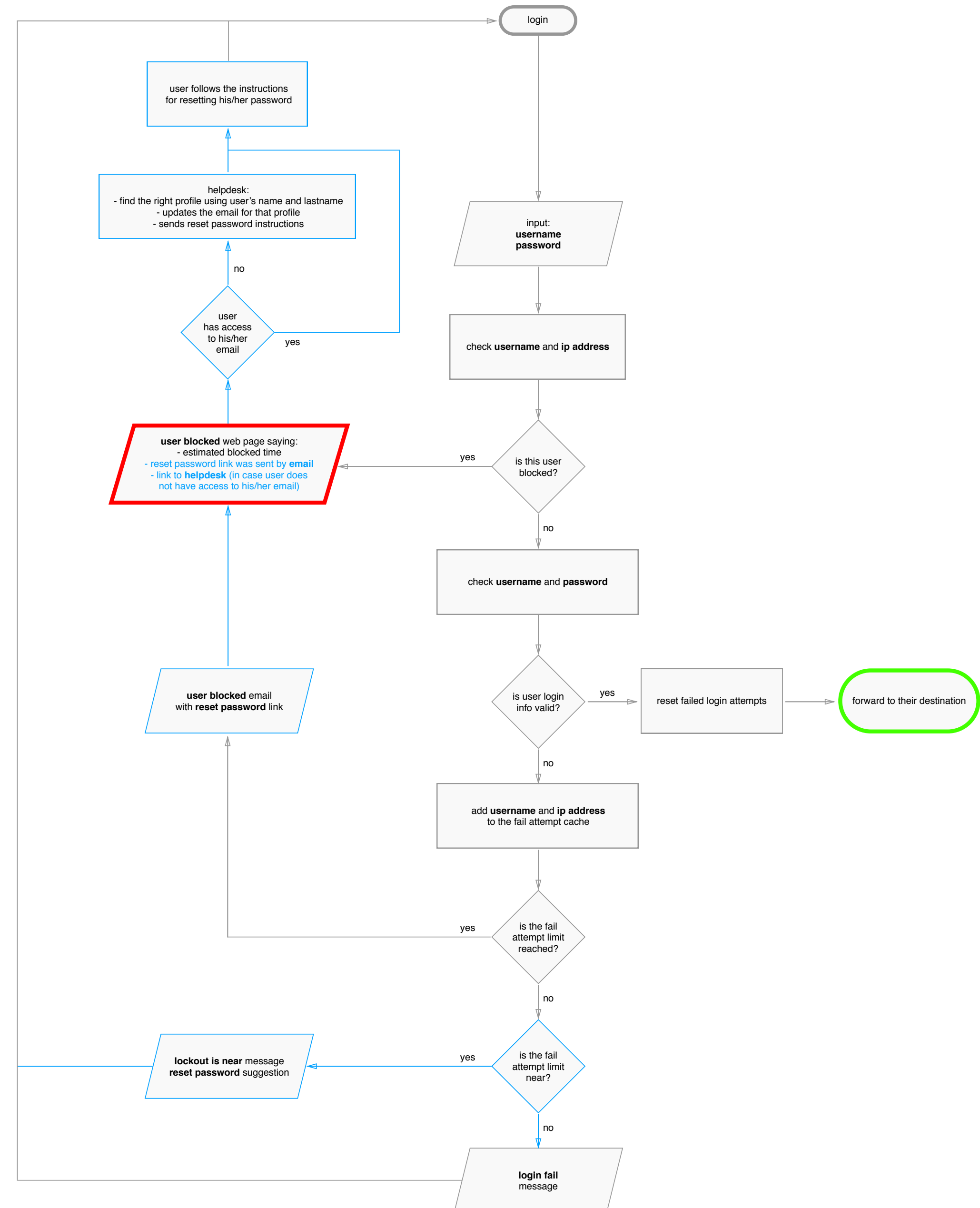
4. Design process

Initial flow-chart



4. Design process

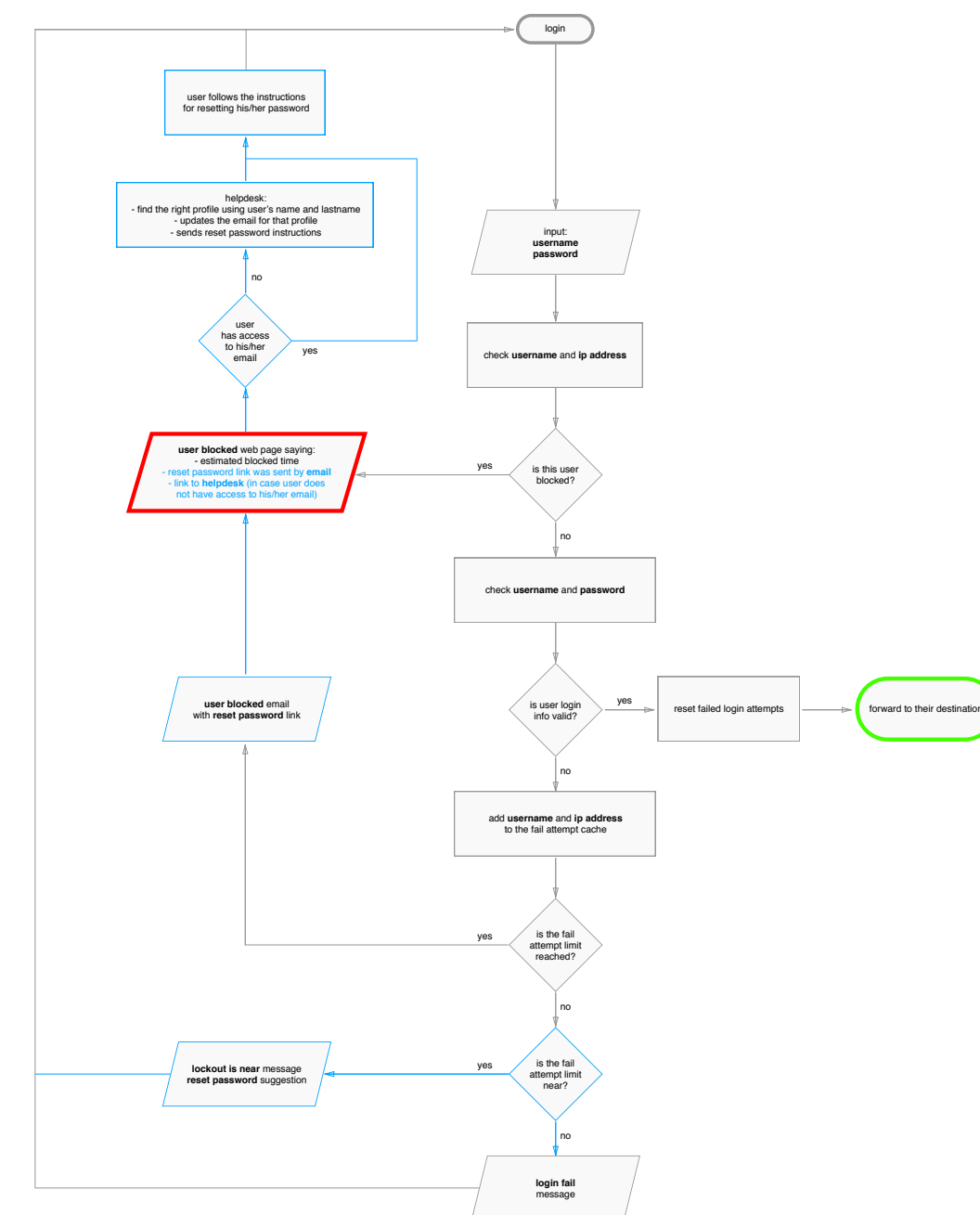
Initial flow-chart got its first upgrade:



4. Design process

This version became
in fact only a first
iteration,

- Iteration #1
- “lockout is near” warning
 - password reset link by email
 - link to helpdesk

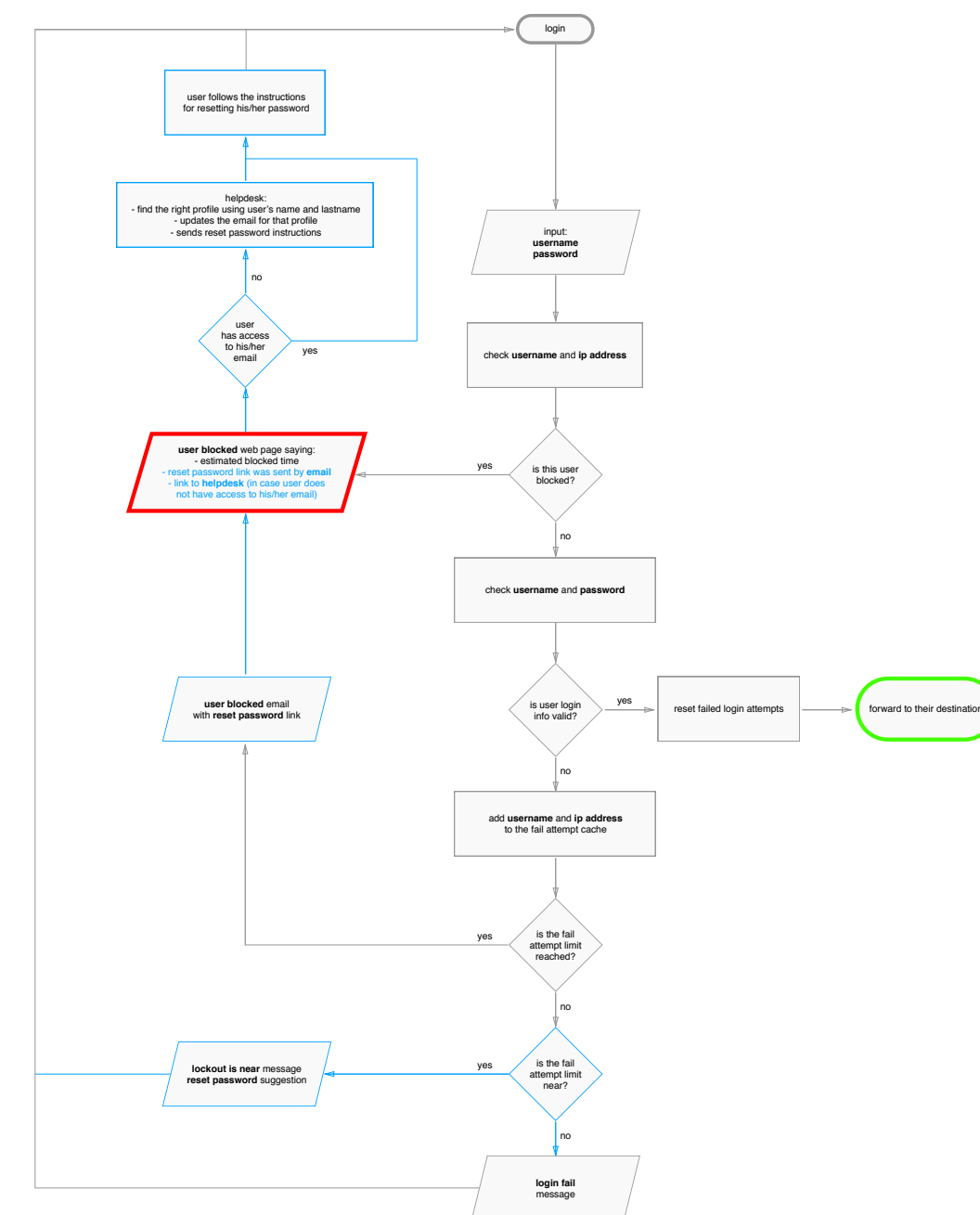


4. Design process

This version became in fact only a first iteration, but other two were generated as well.

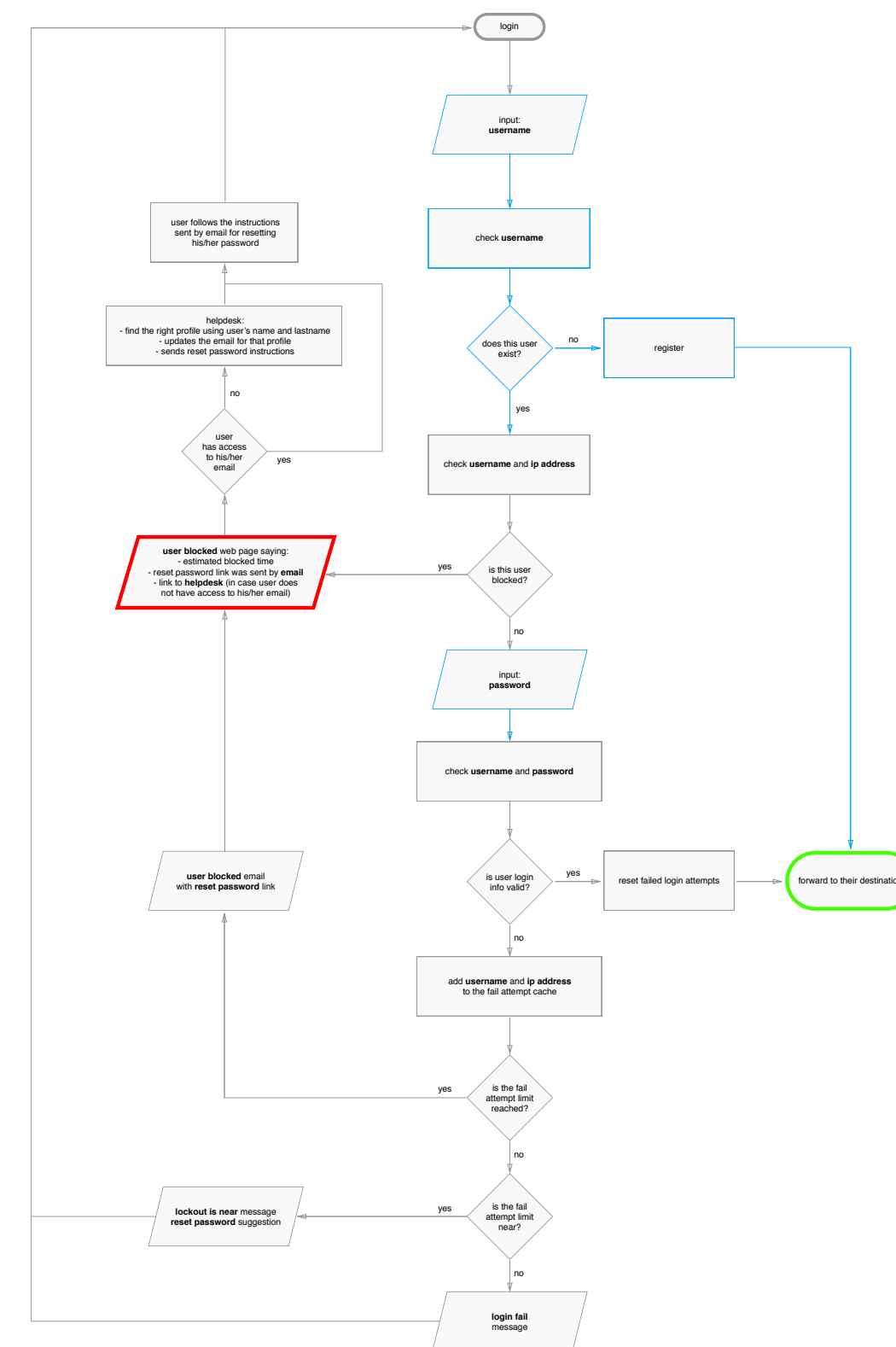
Iteration #1

- “lockout is near” warning
- password reset link by email
- link to helpdesk



Iteration #2

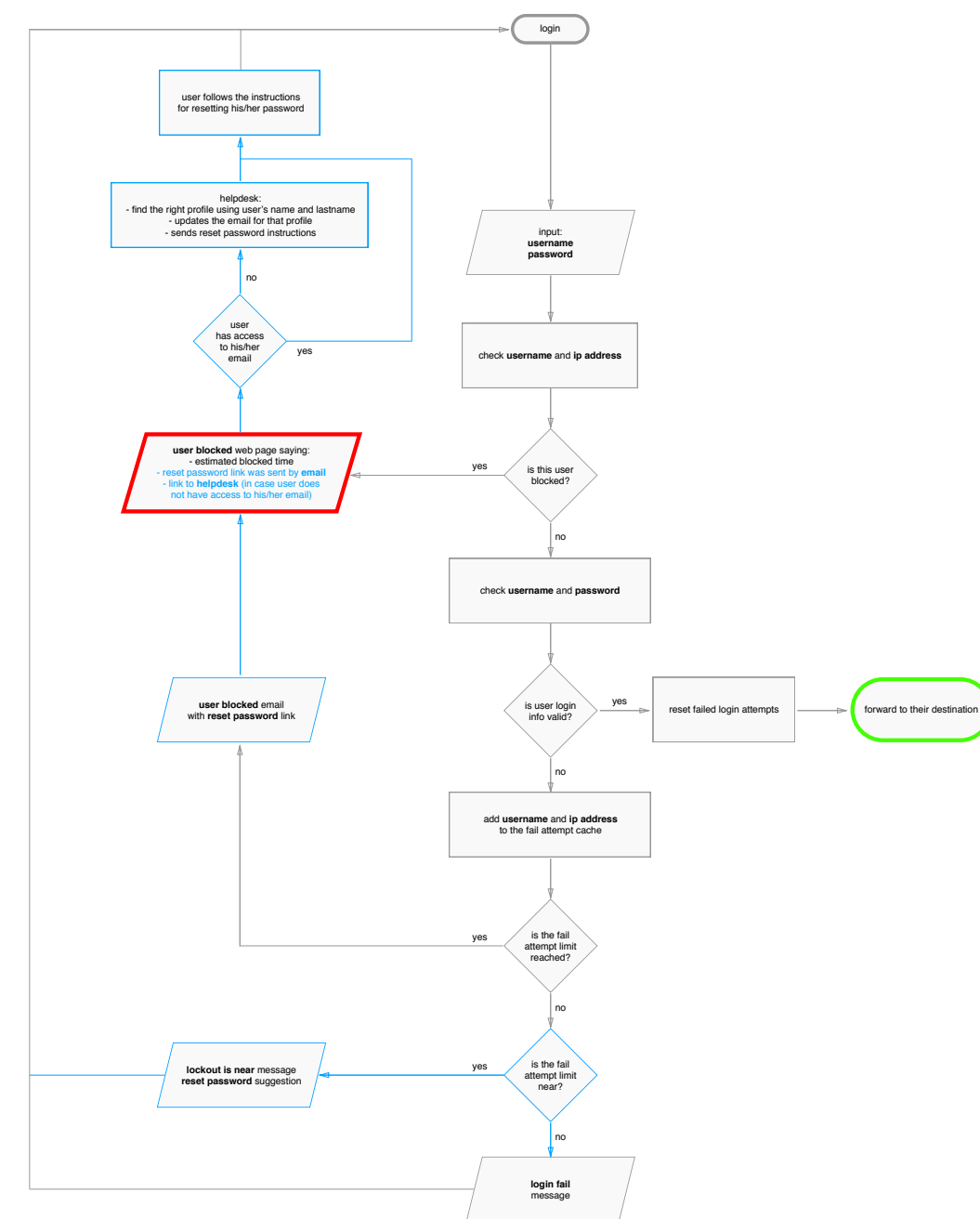
- username and password separation
- inexistent account easy detection
- register added as natural part of the flow



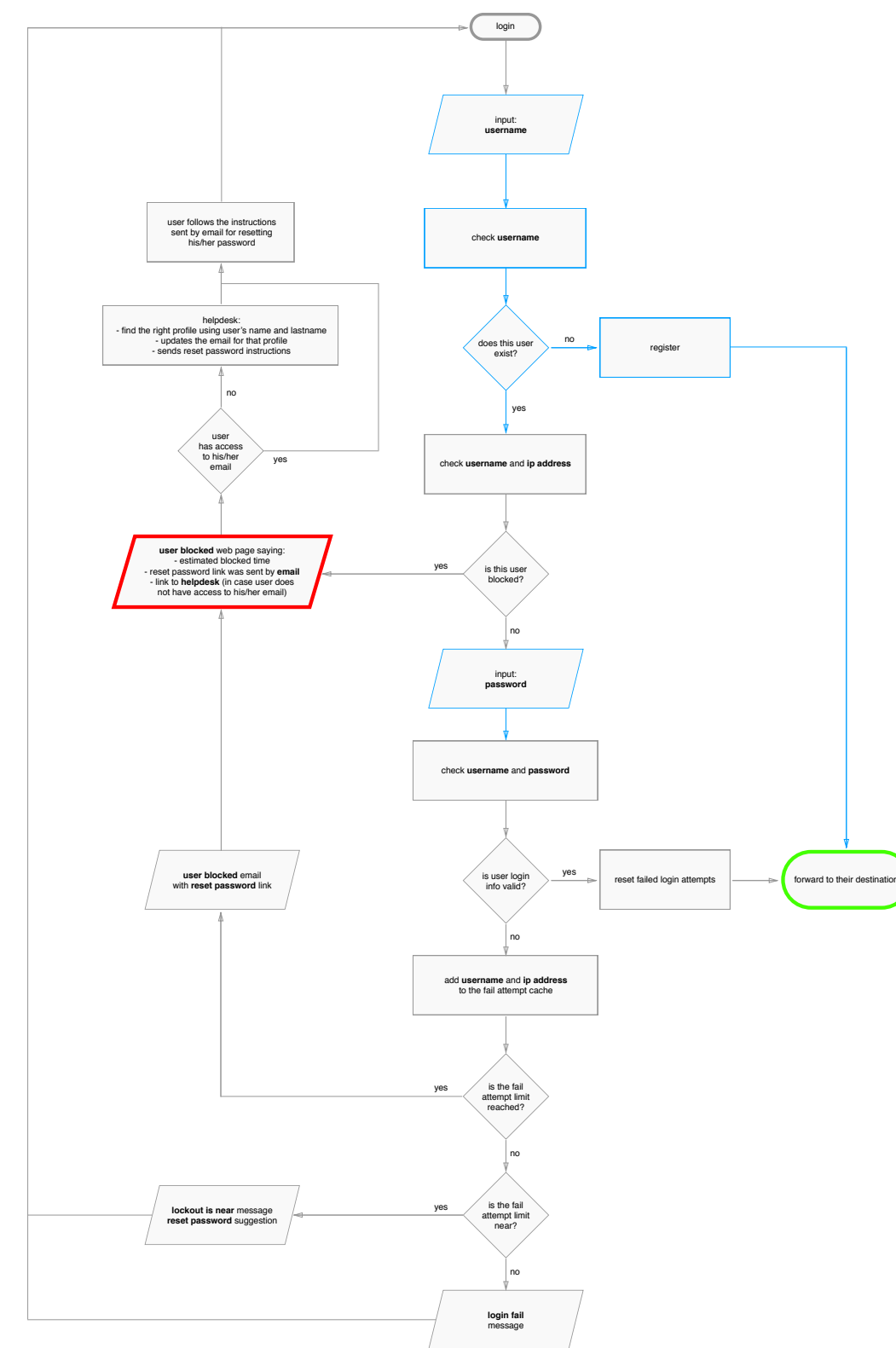
4. Design process

This version became in fact only a first iteration, but other two were generated as well.

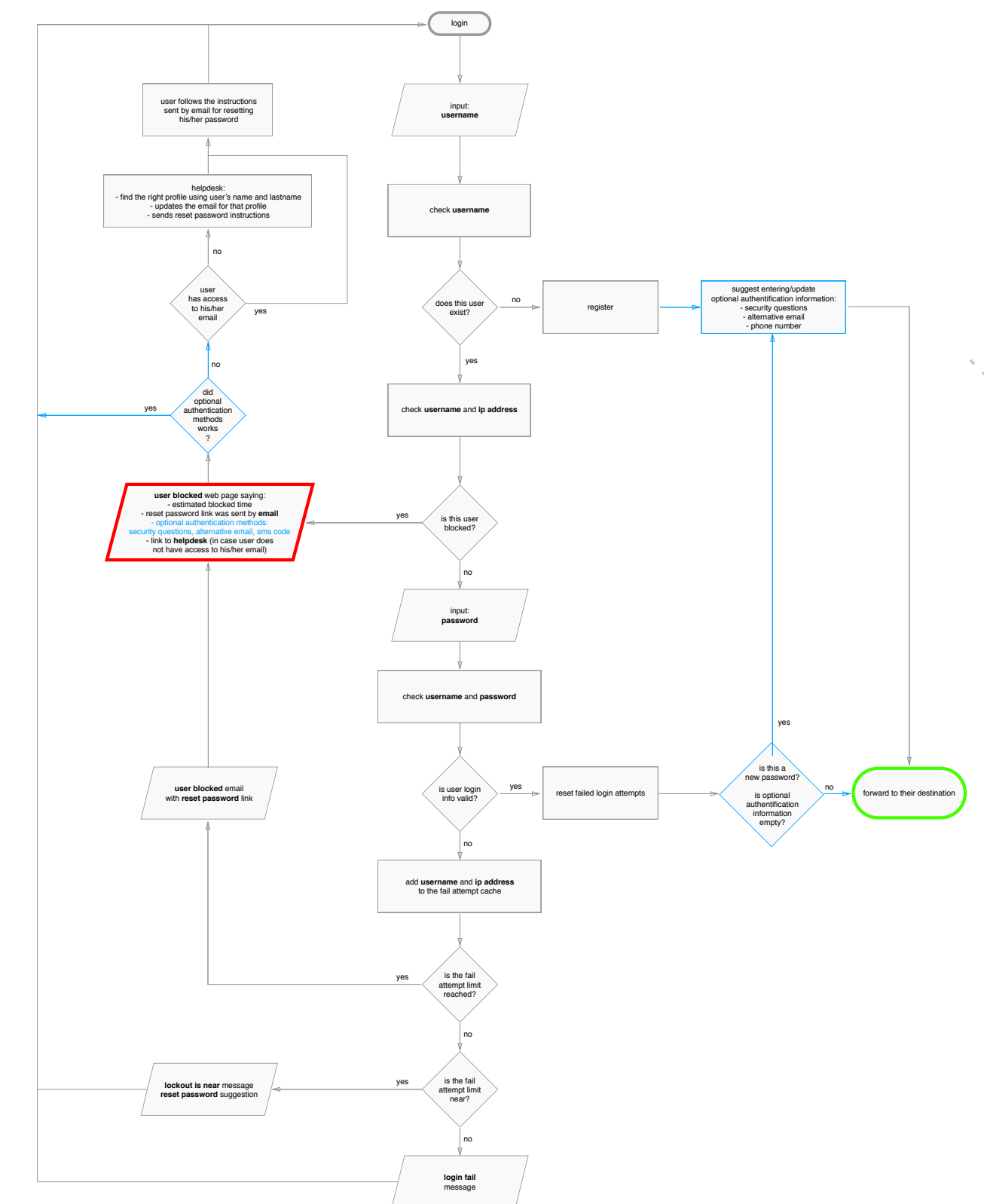
- Iteration #1
- “lockout is near” warning
 - password reset link by email
 - link to helpdesk



- Iteration #2
- username and password separation
 - inexistent account easy detection
 - register added as natural part of the flow

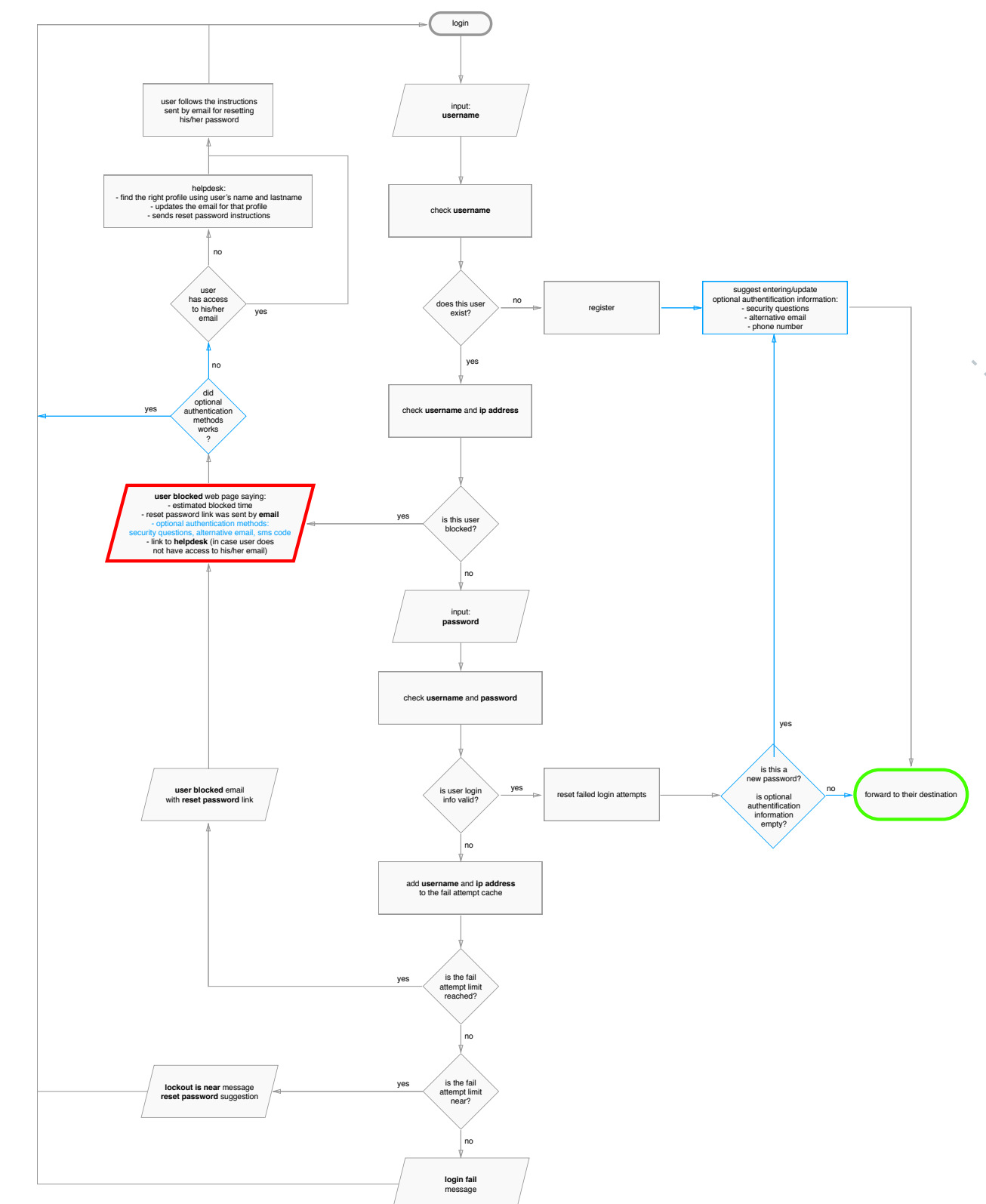


- Iteration #3
- added optional authentication information
 - increase user power to unlock his/her account by himself/herself



From this **road-map**
to the complete
solution

- Iteration #3
 - added optional authentication information
 - increase user power to unlock his/her account by himself/herself



4. Design process

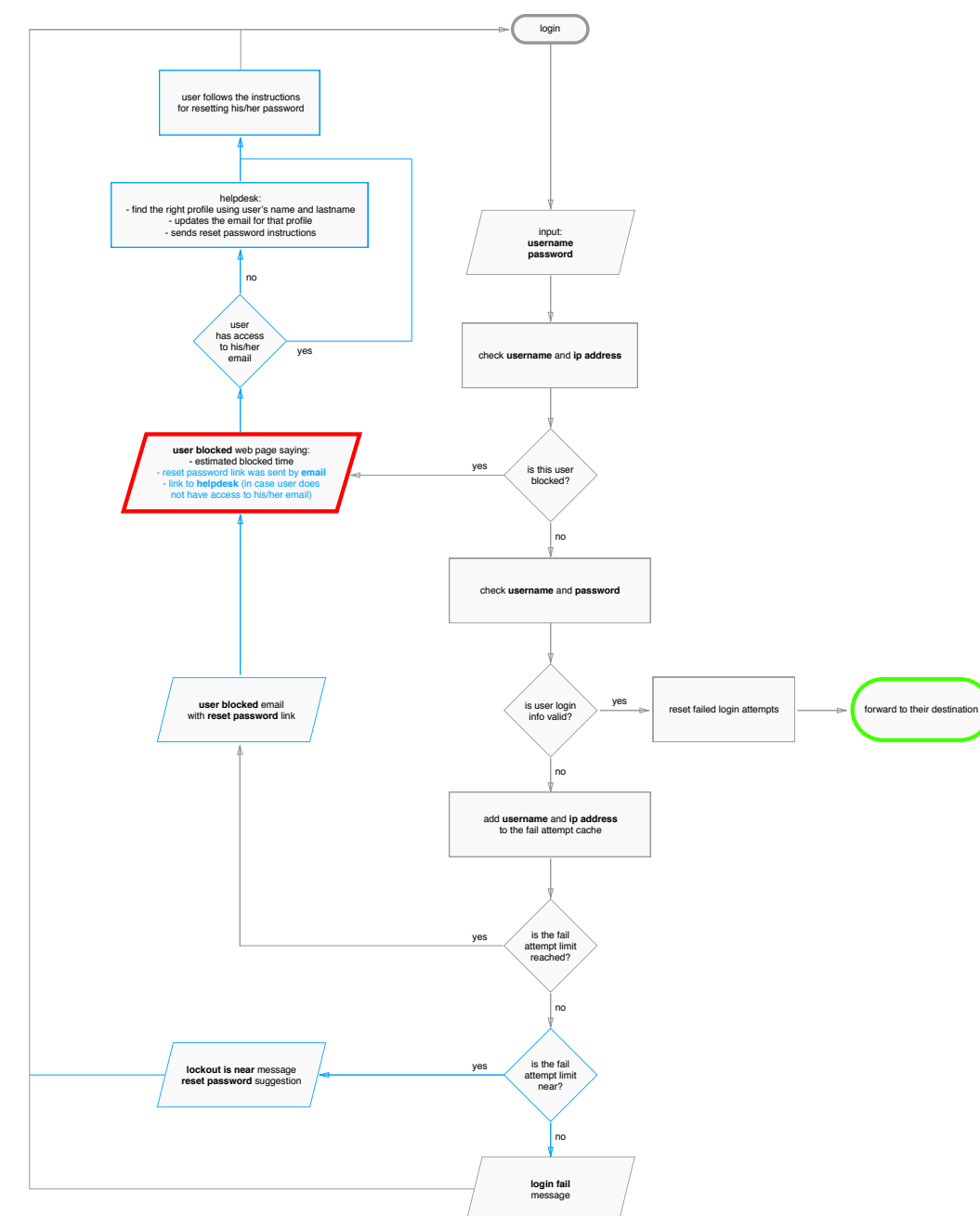
This version became in fact only a fist iteration, but other two were generated as well.

From this road-map to the complete solution, Bryan as Product Owner choose to concentrate efforts on the **first iteration for the current sprint.**

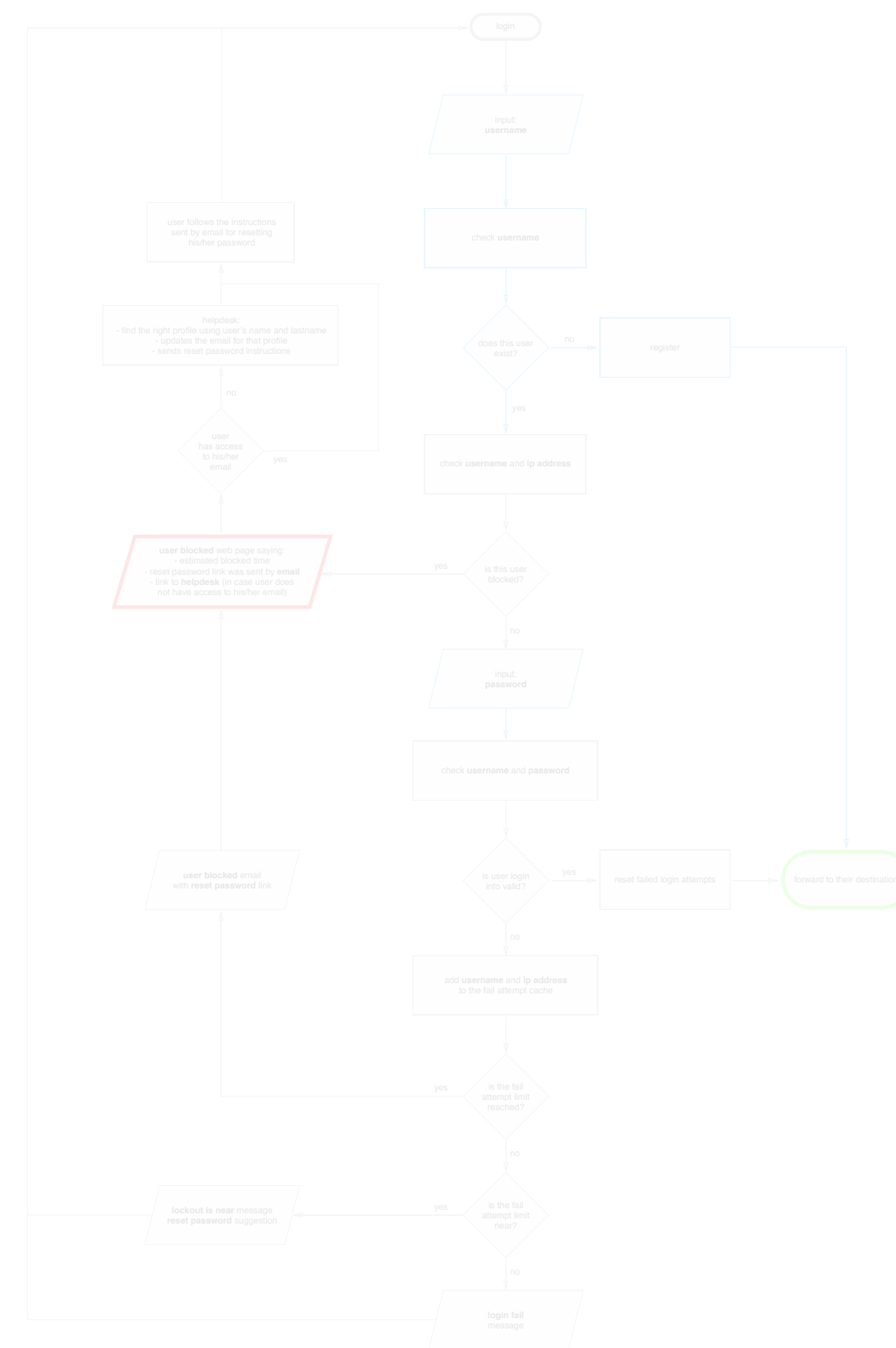
- Iteration #1
- "lockout is near" warning
 - password reset link by email
 - link to helpdesk



Bryan Robitaille



- Iteration #2
- username and password separation
 - inexistent account easy detection
 - register added as natural part of the flow

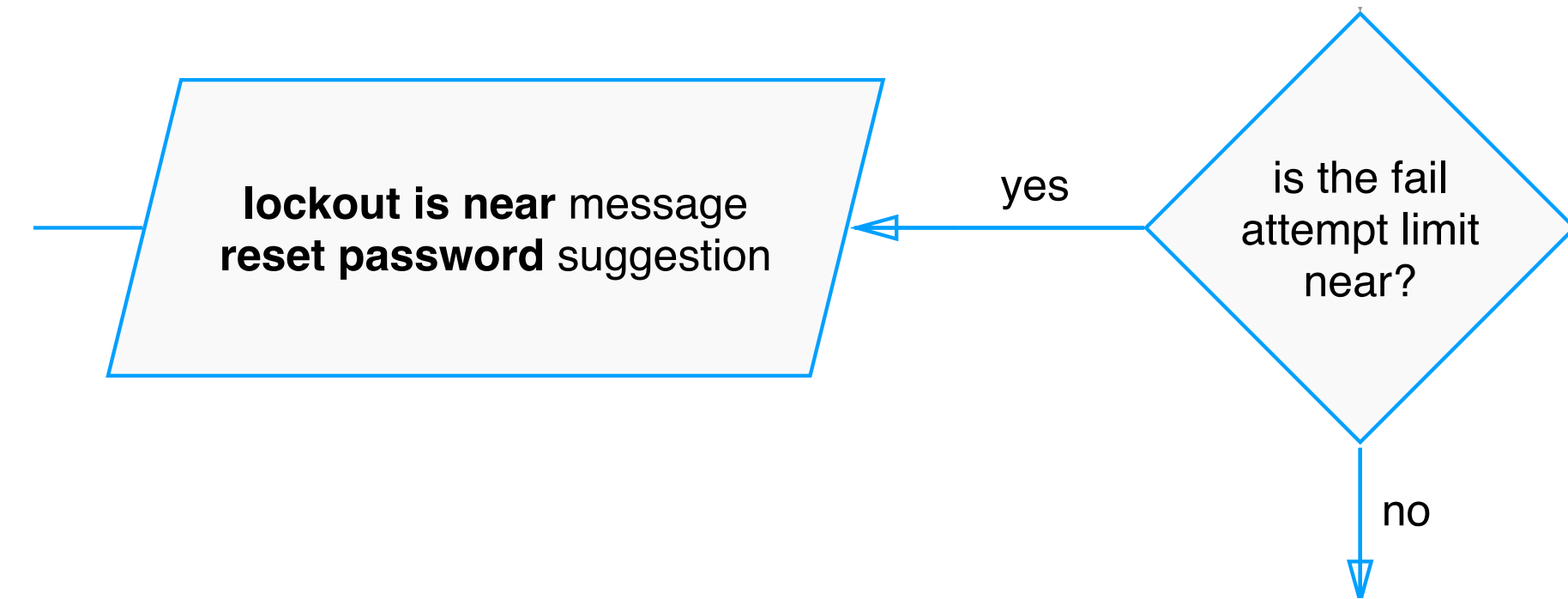
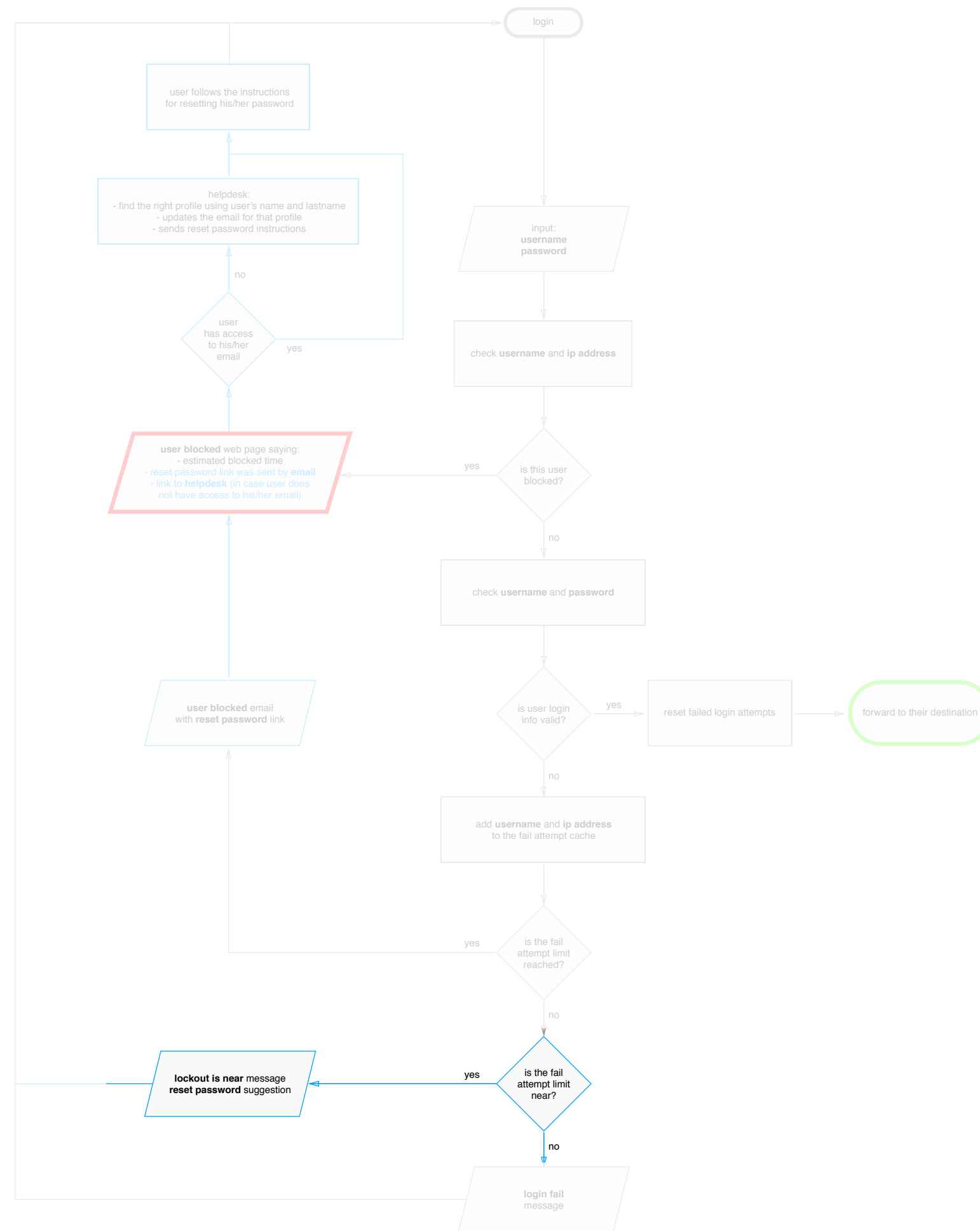


- Iteration #3
- added optional authentication information
 - increase user power to unlock his/her account by himself/herself



4. Design process

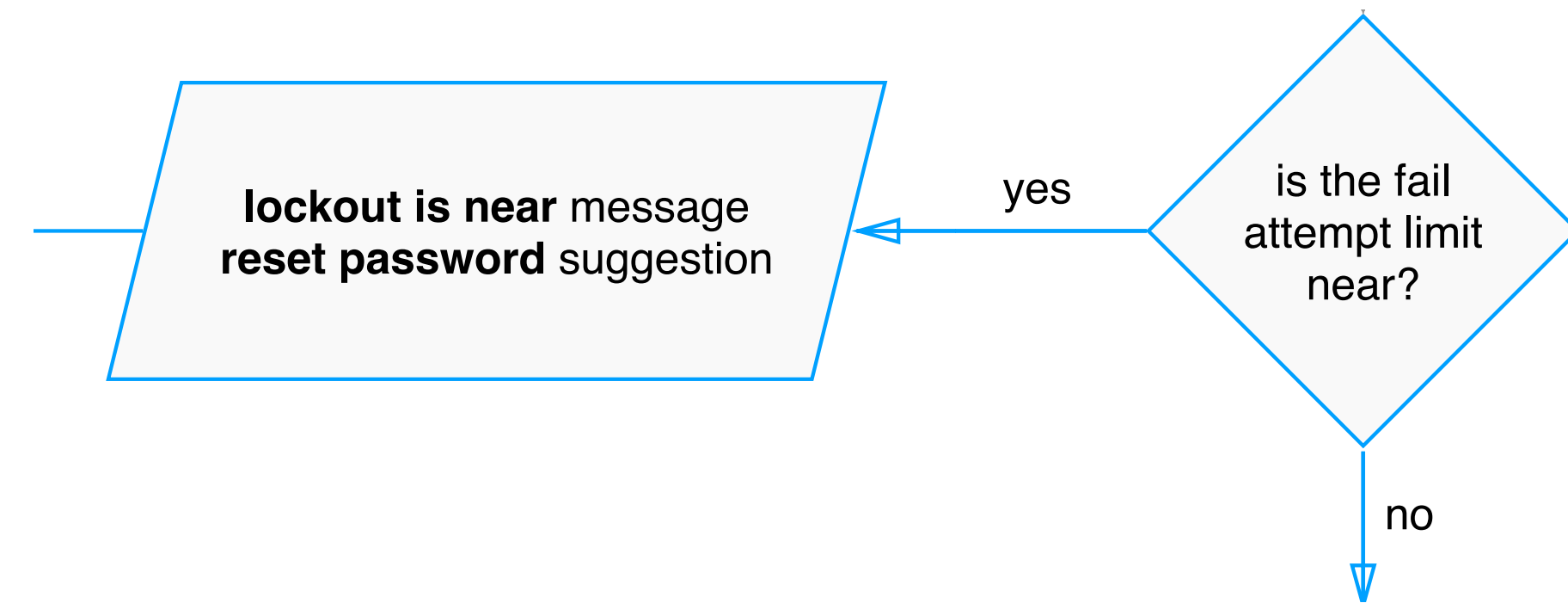
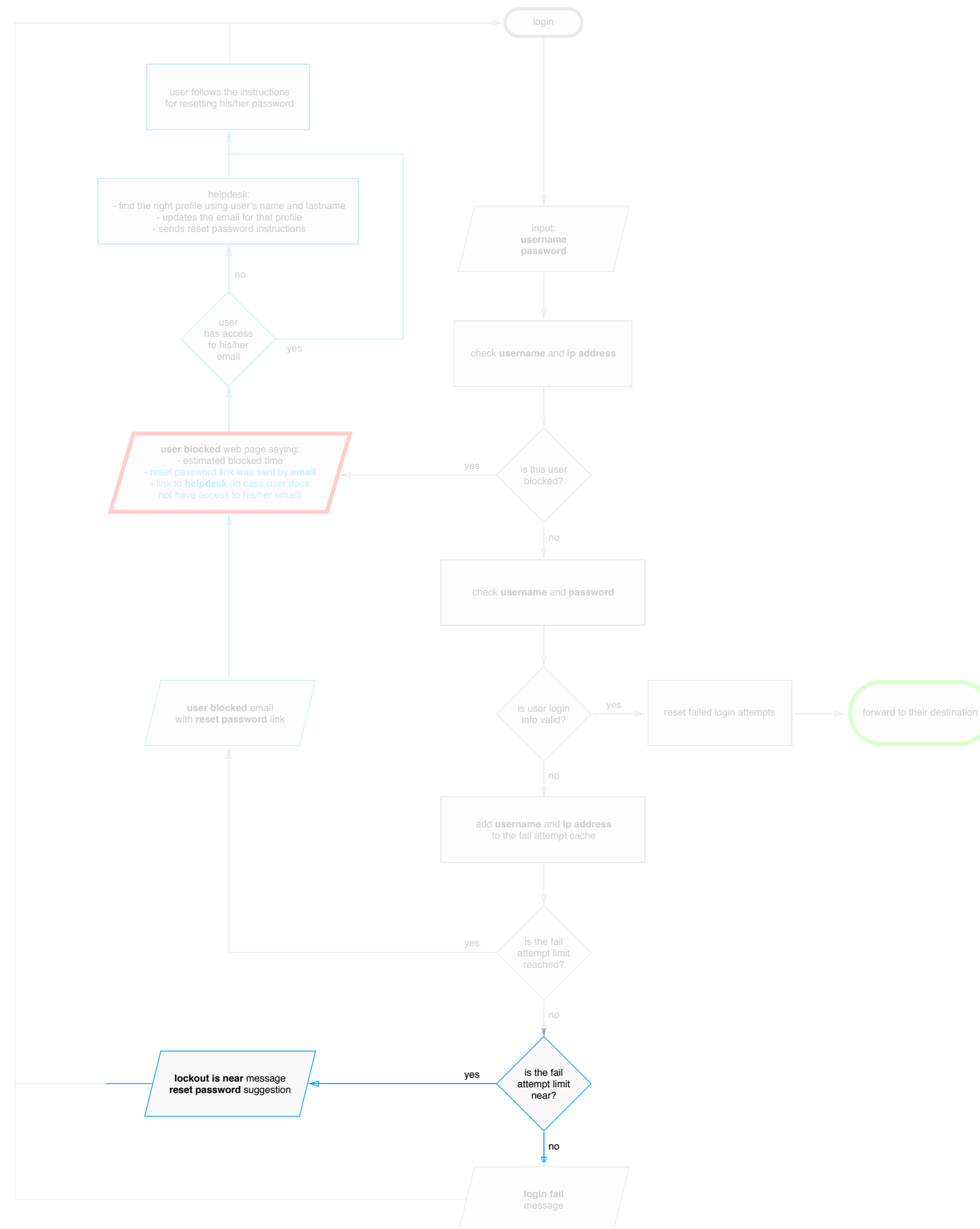
Are we near to lock the account?



4. Design process

Are we near to lock the account?

Based on current login fail message,



Sign in
with your account

Please enter a correct email and password.
Note that both fields may be case-sensitive.

Email address

amable.rodriguez@tbs-sct.gc.ca

Password

••••••••••

Forgot password?

Login

Don't have an account? [Register](#)

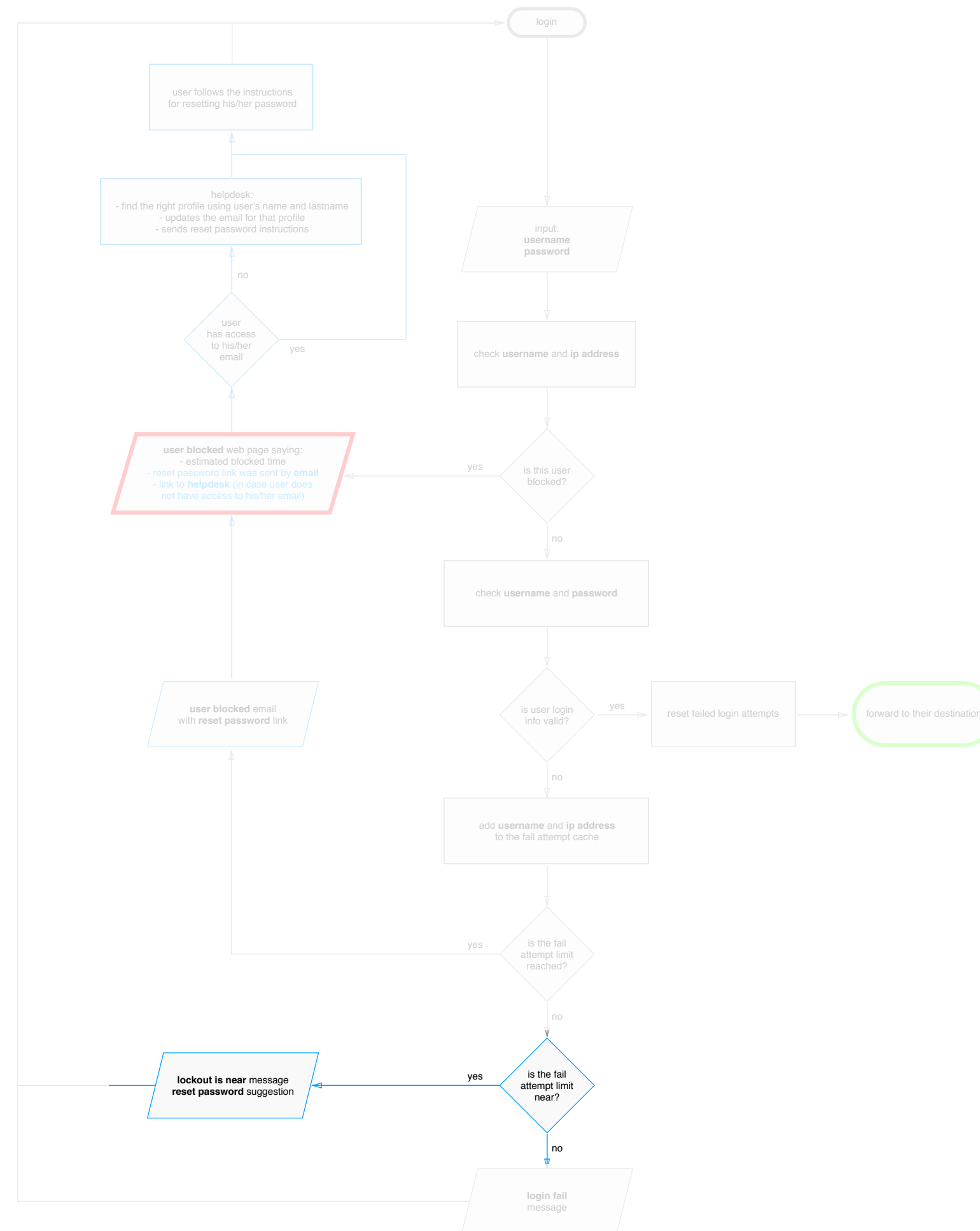
4. Design process

Are we near to lock the account?

Based on current login fail message, we created a warning message indicating the number of attempts left, a reminder to reset the password and a link to help-desk if needed.

Marianne and Donna worked on the texts and details like adding a password structure help reminder.

UX Sprint Review #42 - Account - Lockout functionality



Sign in with your account

The password you entered does not match the email's set password.

You have 2 attempts left before your account will be locked for 5 minutes.

If you have forgotten your password [click here](#) to reset it.

If you no longer have access to amable.rodriguez@tbs-sct.gc.ca you can contact [help desk](#) and an agent will help you regain access to your account.

Email address

amable.rodriguez@tbs-sct.gc.ca

Password

••••••••

[Forgot password?](#)

Note: Your password contains at least 8 characters: 1 lowercase letter, 1 uppercase letter, 1 special character and 1 number.

Login

Don't have an account? [Register](#)



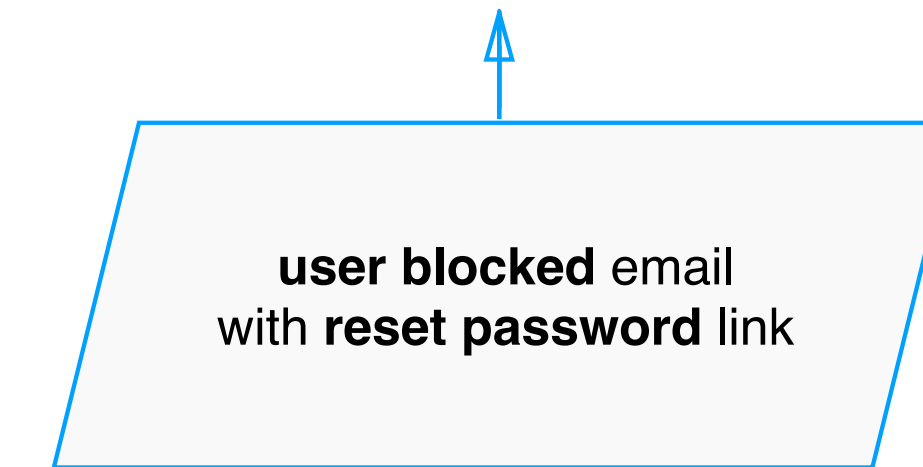
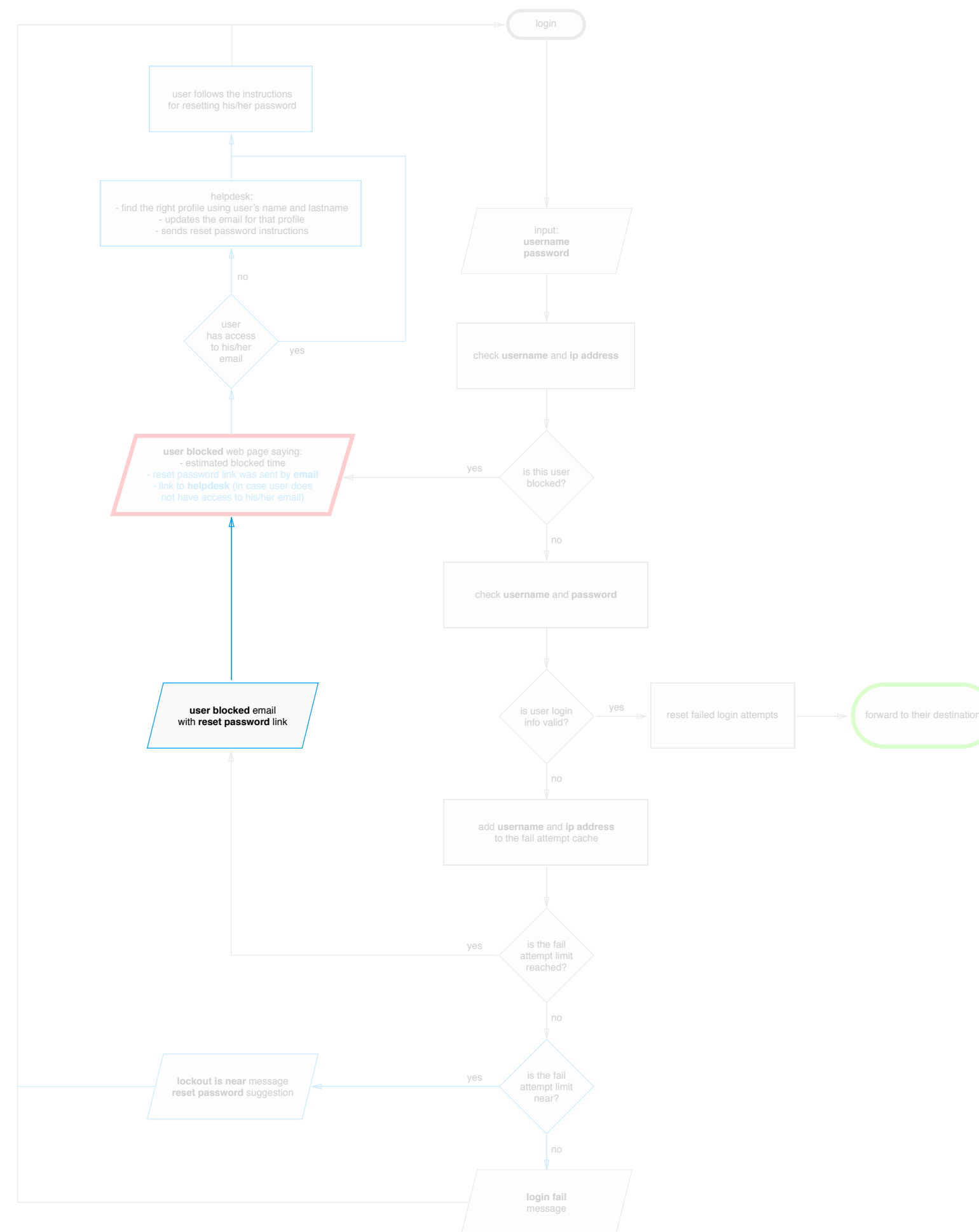
Marianne Aubrey



Donna Monbourquette

4. Design process

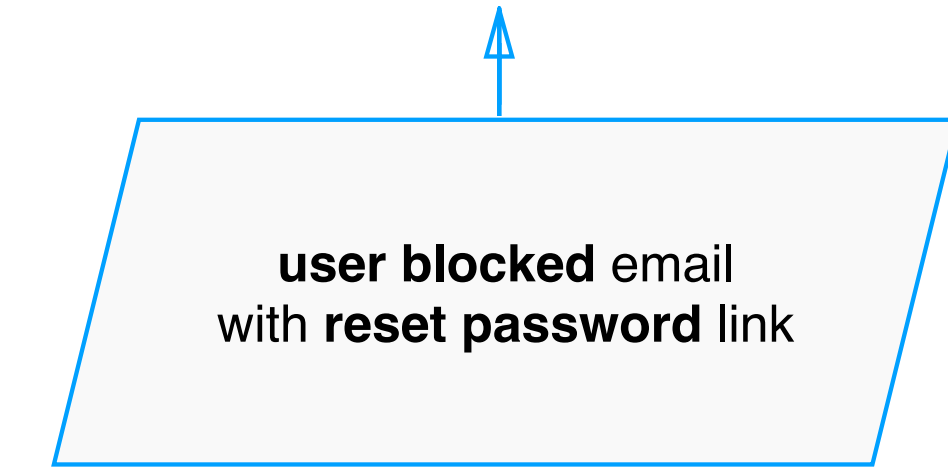
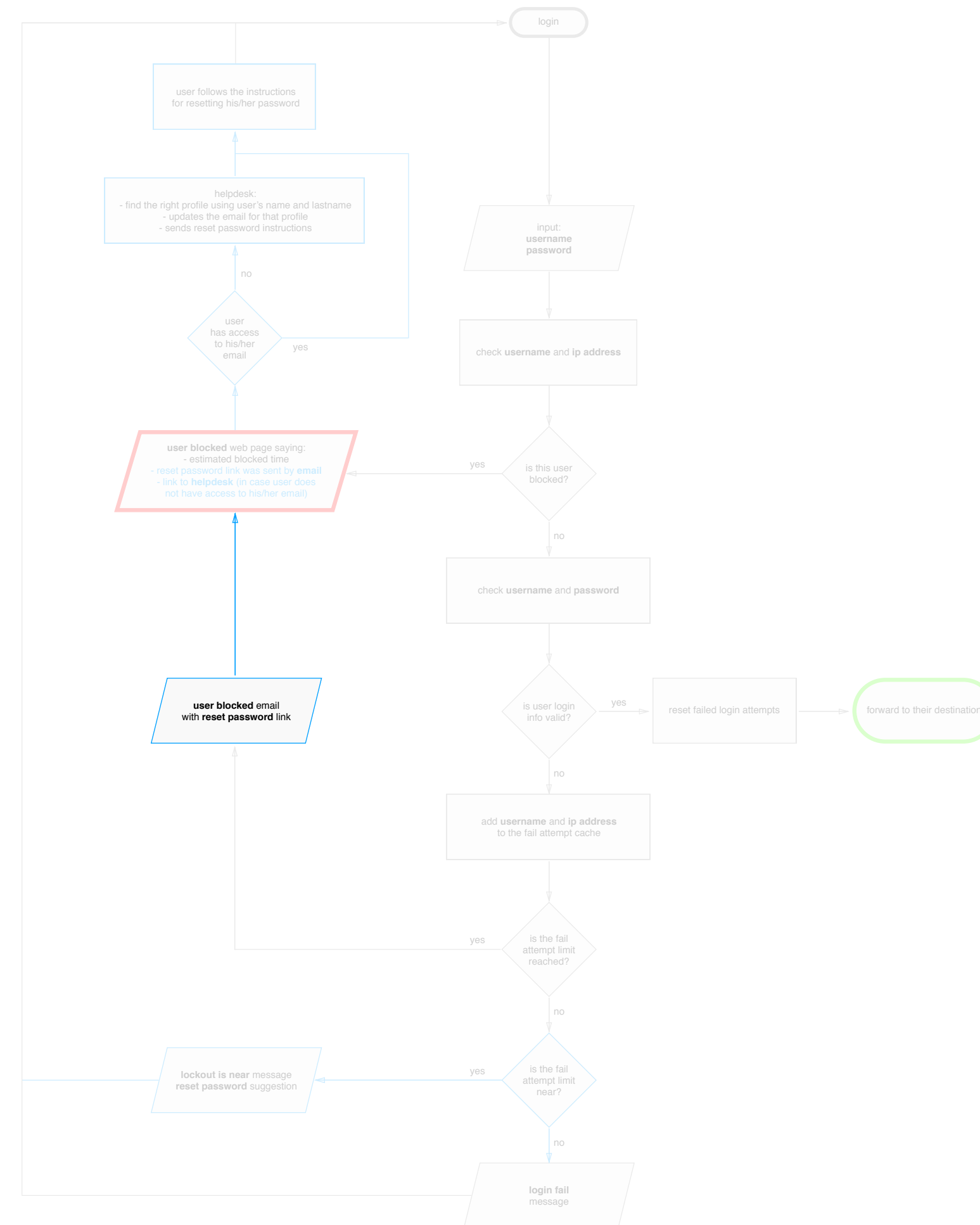
Once the user account is locked, a reset password email is automatically sent to his email address.



4. Design process

Once the user account is locked, a reset password email is automatically sent to his email address.

Starting from the current recovery password email,



From: security@server.com
to: amable.rodriguez@tbs-sct.gc.ca

Hi amable.rodriguez,

You asked to change your password. Please follow this link to set a new password.

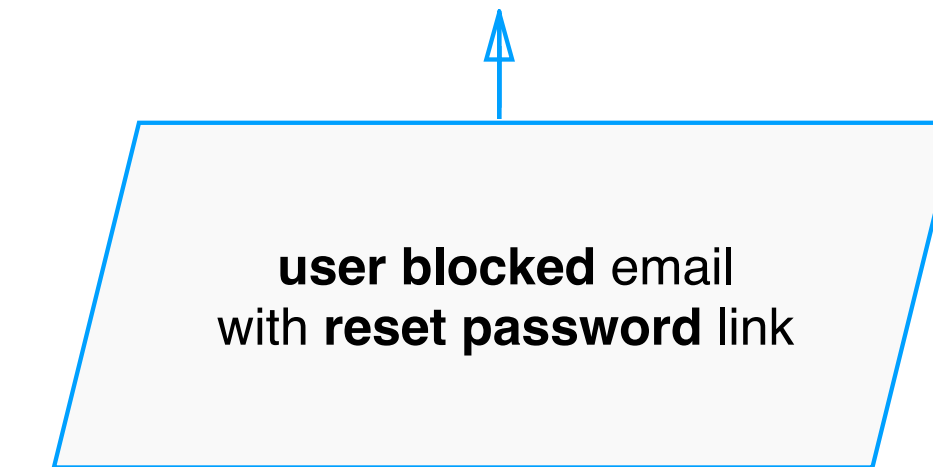
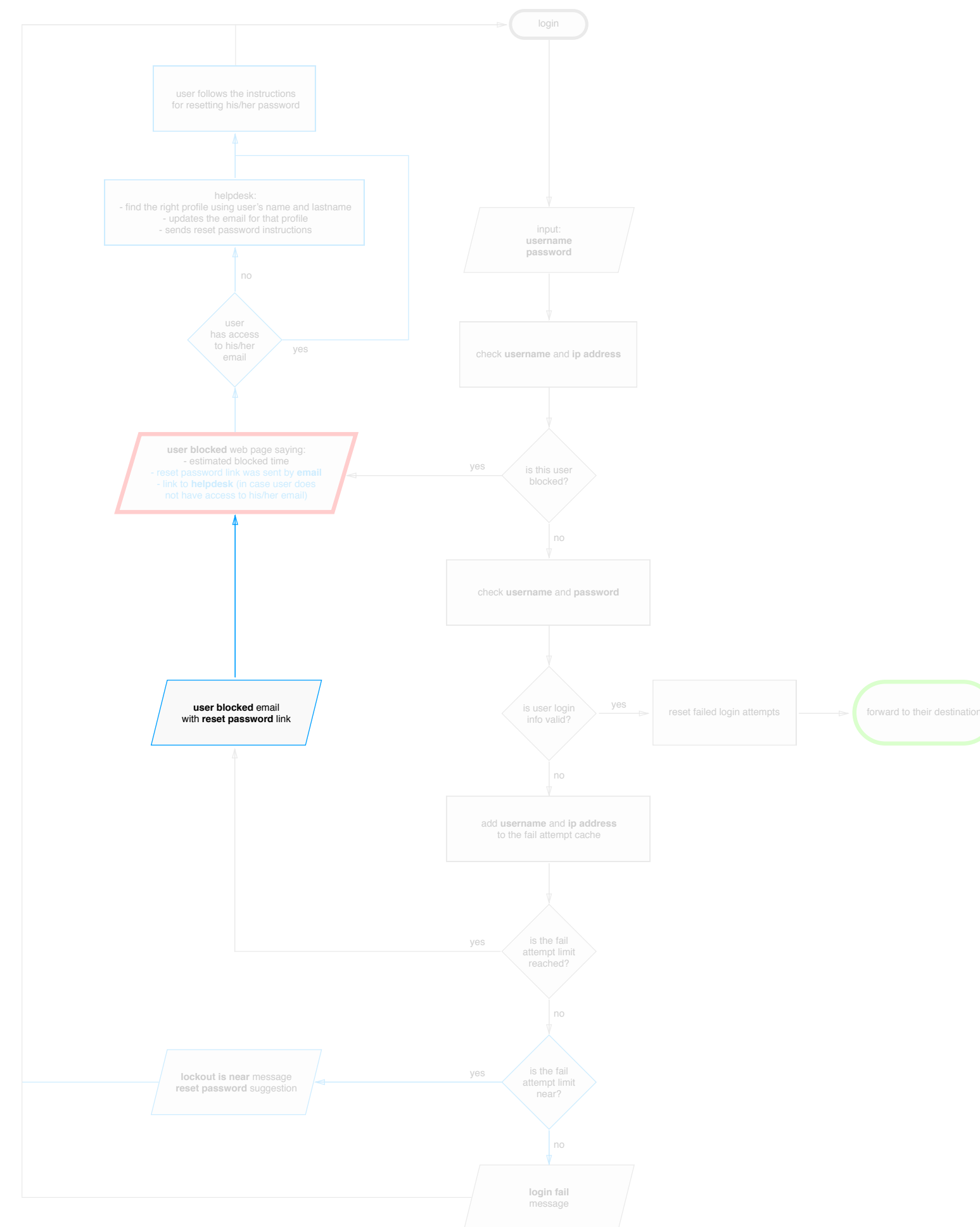
<https://security.passwordrecovery.org/50498478370740738378740387208723>

You can ignore this email if you have not requested to change your password.

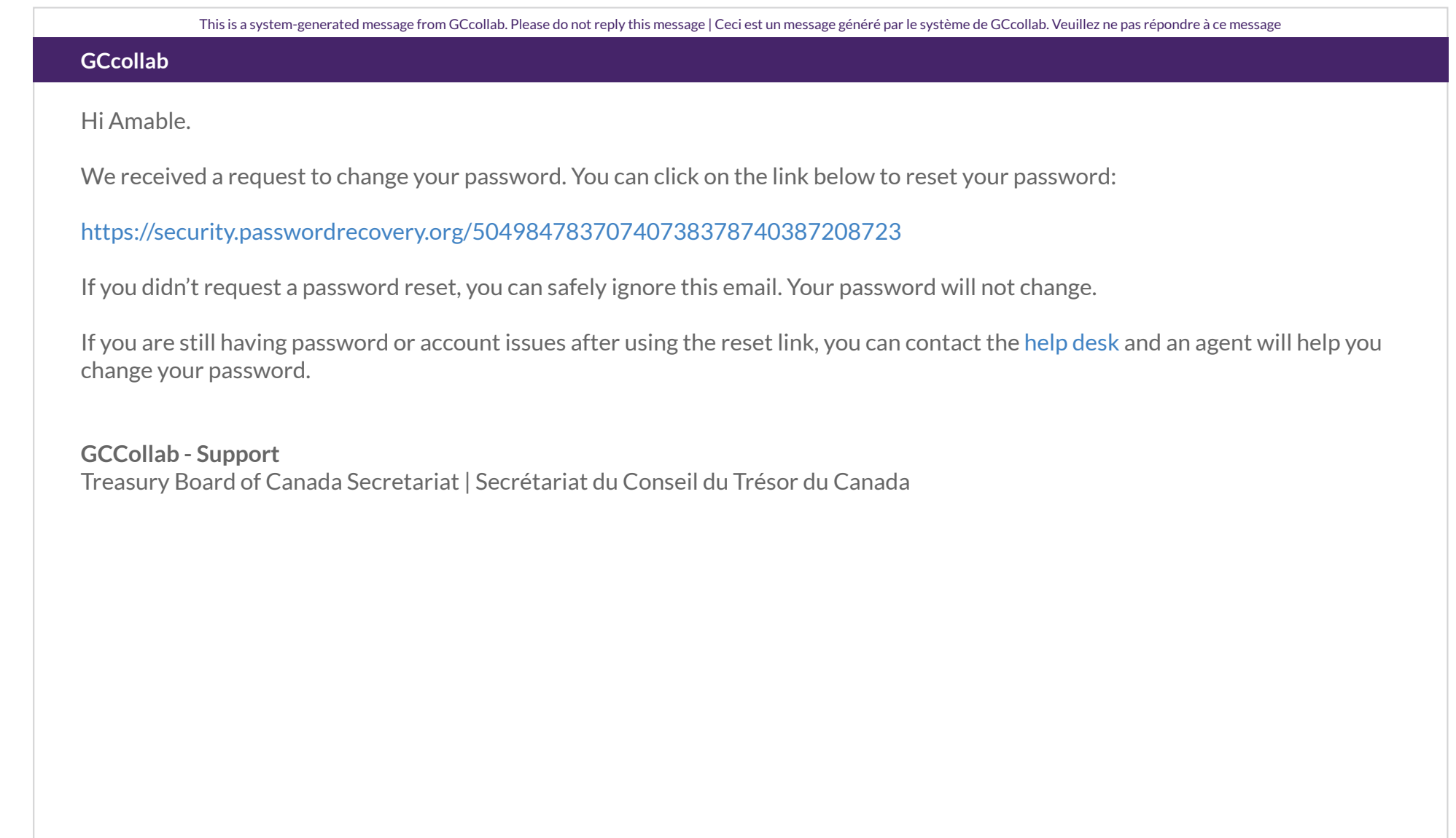
4. Design process

Once the user account is locked, a reset password email is automatically sent to his email address.

Starting from the current recovery password email, Marianne and Donna contribute to making it better,



From: security@server.com
to: amable.rodriguez@tbs-sct.gc.ca



Marianne Aubrey

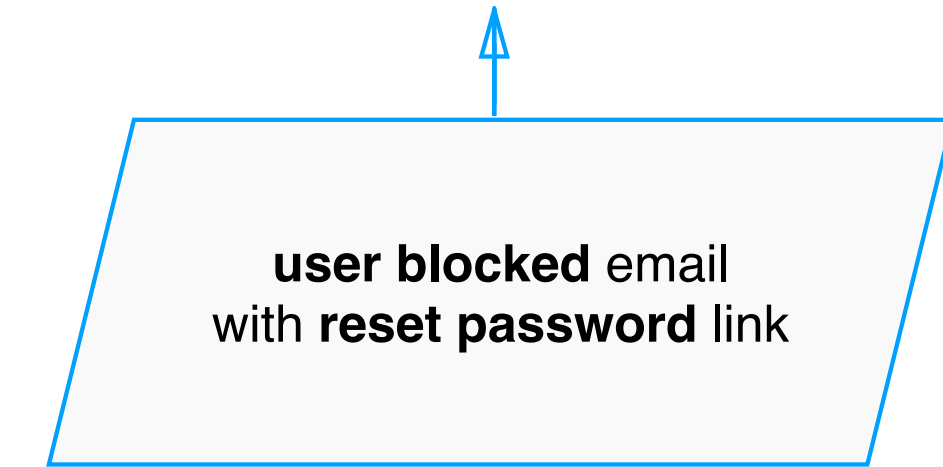
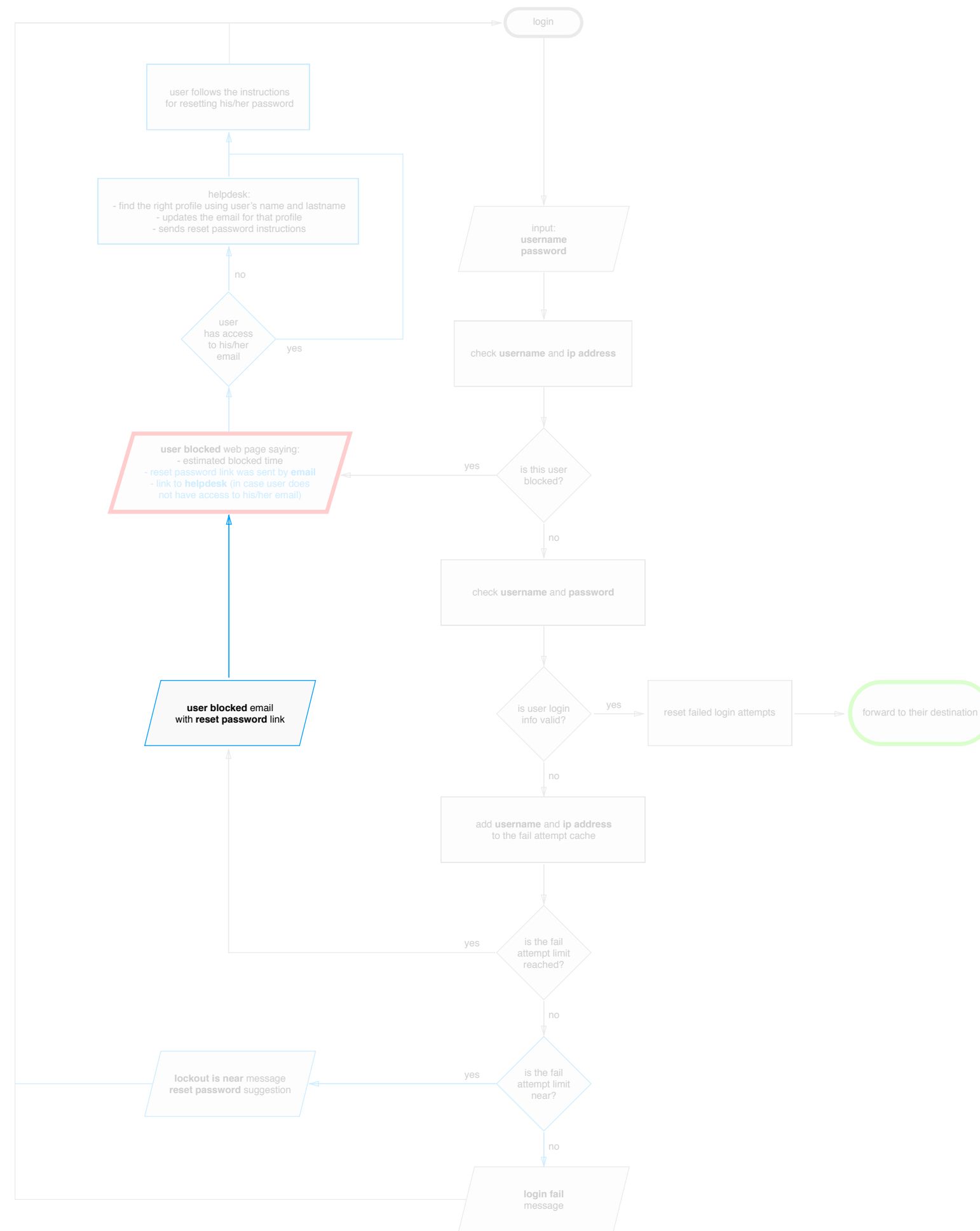


Donna Monbourquette

4. Design process

Once the user account is locked, a reset password email is automatically sent to his email address.

Starting from the current recovery password email, Marianne and Donna contribute to making it better, and we used to create the new account locked email.



From: security@server.com
to: amable.rodriguez@tbs-sct.gc.ca

This is a system-generated message from GCCollab. Please do not reply this message | Ceci est un message généré par le système de GCCollab. Veuillez ne pas répondre à ce message

GCCollab

Hi Amable.

Your account has been locked as the incorrect password had been entered too many times. You will need to reset your password, which you can do by clicking the link below.

<https://security.passwordrecovery.org/50498478370740738378740387208723>

Your account will be unlocked after resetting your password, and you should be able to log in normally.

If you are still having password issues after using the reset link, you can contact the [help desk](#) and an agent will help you change your password and get back into your account.

GCCollab - Support
Treasury Board of Canada Secretariat | Secrétariat du Conseil du Trésor du Canada



Marianne Aubrey



Donna Monbourquette

4. Design process

After account is locked, a message showing the possible alternatives the user has is a very important and delicate stage of the process.



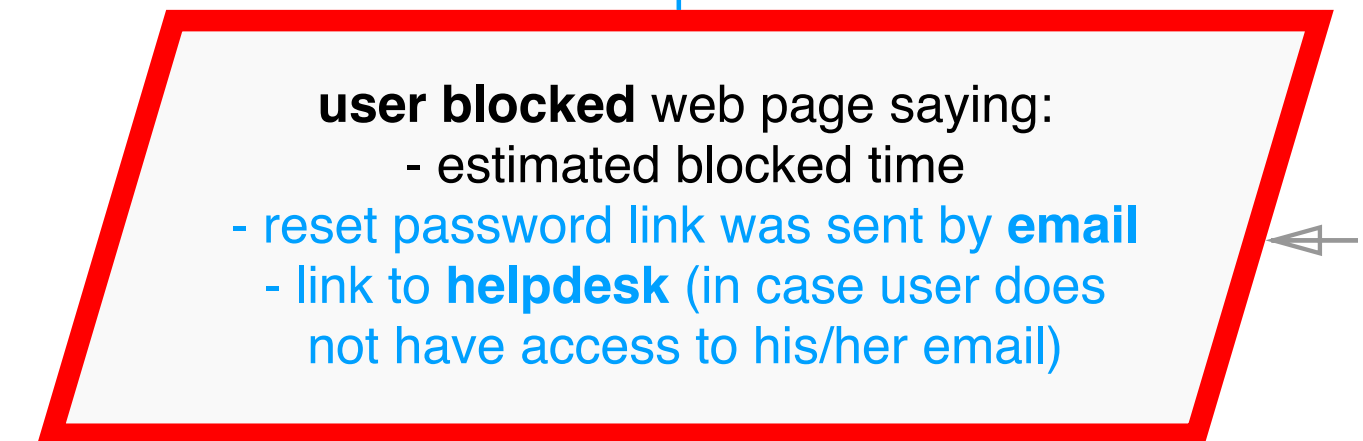
user blocked web page saying:

- estimated blocked time
- reset password link was sent by **email**
- link to **helpdesk** (in case user does not have access to his/her email)

4. Design process

After account is locked, a message showing the possible alternatives the user has is a very important and delicate stage of the process.

Based on the default account locked message,



Security Alert

3 or more failed login attempts
Account locked for 10,0 minutes

[Return to login](#)

4. Design process

After account is locked, a message showing the possible alternatives the user has is a very important and delicate stage of the process.

Based on the default account locked message, the team came up with a more informative and useful message.



user blocked web page saying:

- estimated blocked time
- reset password link was sent by **email**
- link to **helpdesk** (in case user does not have access to his/her email)

Security Alert

Account locked

Your account has been temporarily locked for 5 minutes as the incorrect password has been entered 5 times.

An email has been sent to **amable.rodriguez@tbs-sct.gc.ca** to reset your password and unlock your account.

If you no longer have access to **amable.rodriguez@tbs-sct.gc.ca** you can contact **help desk** and an agent will help you get back into your account.

[Back to Login](#)



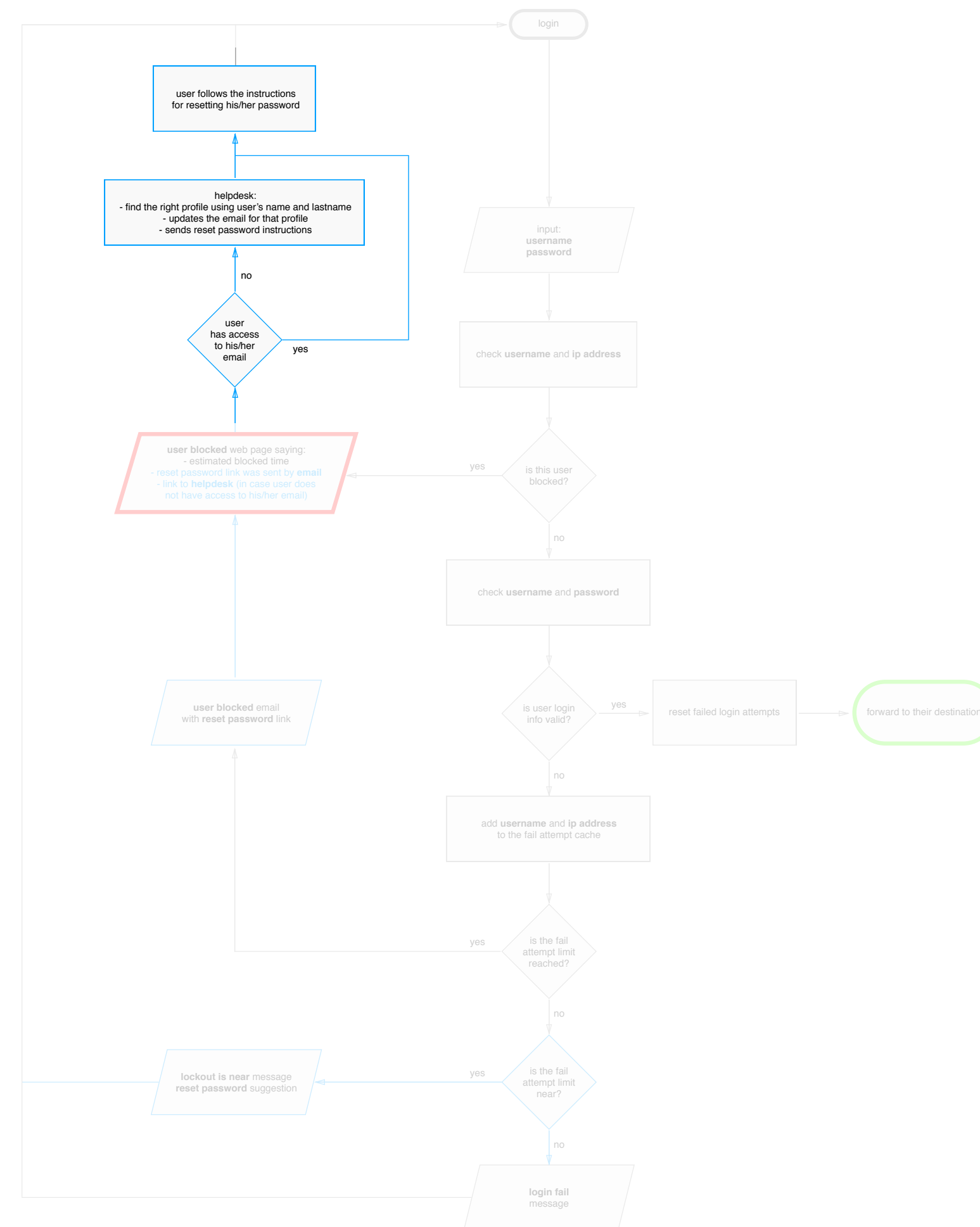
Marianne Aubrey



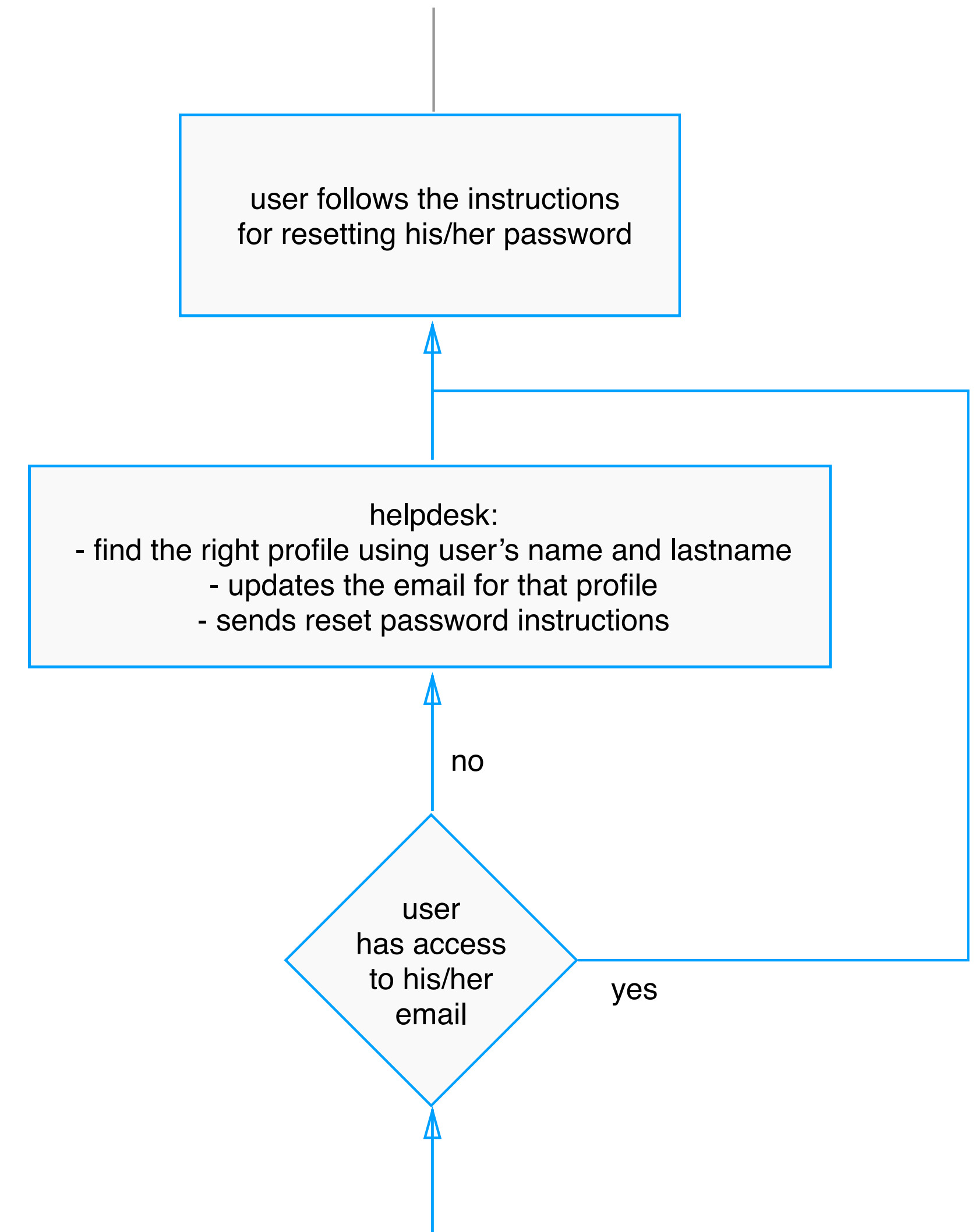
Donna Monbourquette

4. Design process

If the user does not have access to their account, they will contact help-desk in order to manually change the email address of their account and, after receiving the reset password email, follow the steps to regain access to their account.



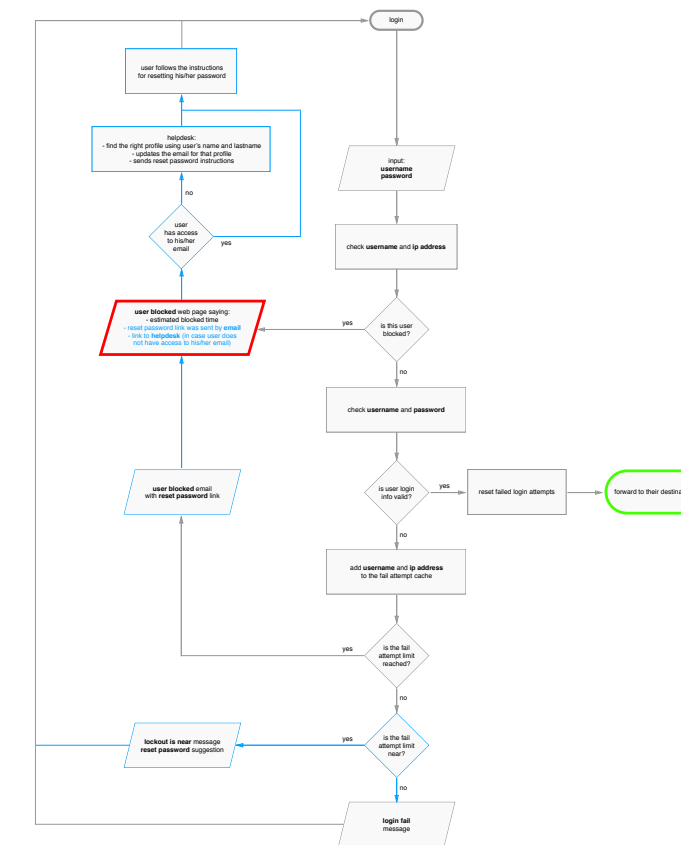
Krista Lecuyer



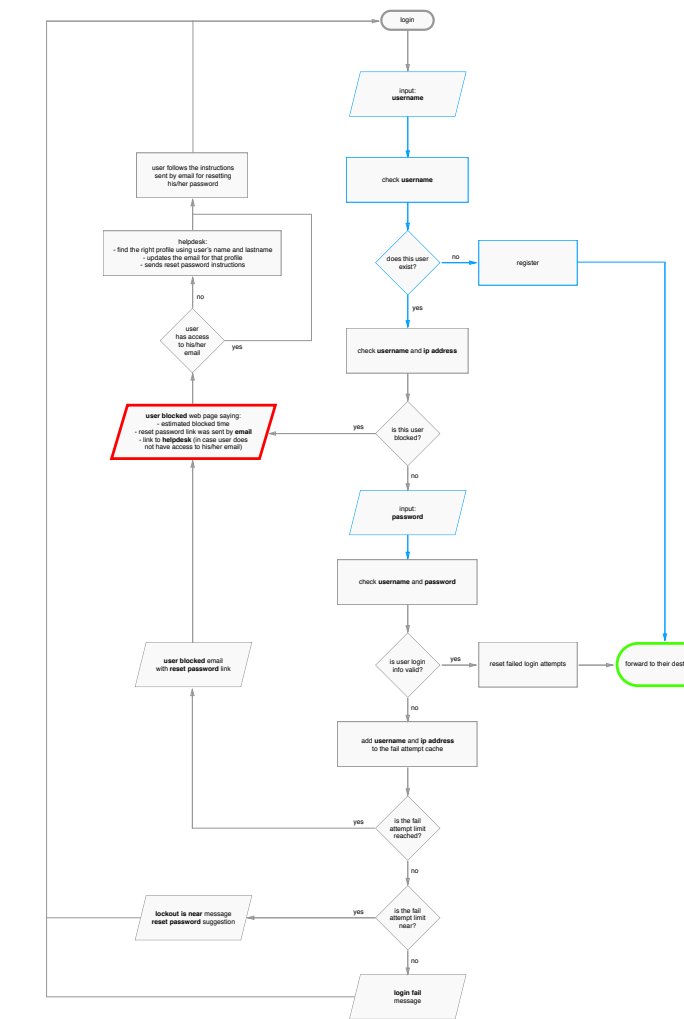
5. Deliverables

For this sprint, a work-flow containing 3 iterations was created.

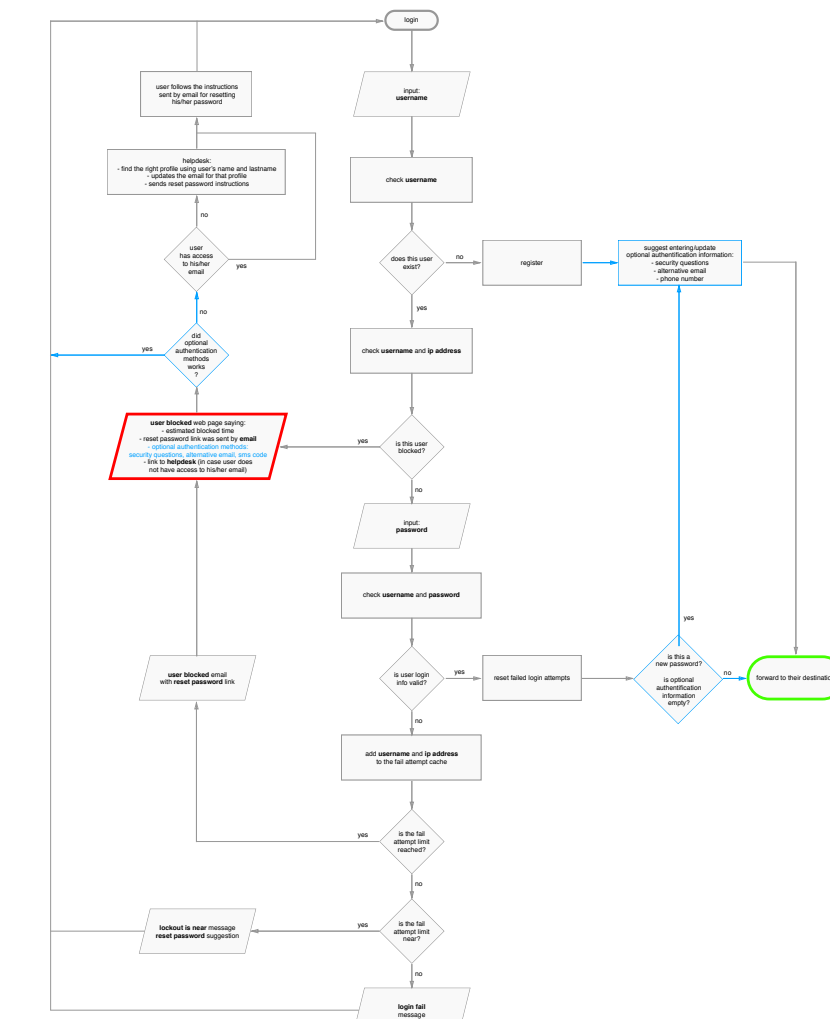
- Iteration #1
- "lockout is near" warning
 - password reset link by email
 - link to helpdesk



- Iteration #2
- username and password separation
 - inexisting account easy detection
 - register added as natural part of the flow



- Iteration #3
- added optional authentication information
 - increase user power to unlock his/her account by himself/herself



5. Deliverables

For this sprint, a workflow containing 3 iterations was created.

All the new screens needed to implement the first iteration were created as well.

Sign in with your account

The password you entered does not match the email's set password.

You have 2 attempts left before your account will be locked for 5 minutes.

If you have forgotten your password [click here](#) to reset it.

If you no longer have access to amable.rodriquez@tbs-sct.gc.ca you can contact [help desk](#) and an agent will help you regain access to your account.

Email address

amable.rodriquez@tbs-sct.gc.ca

Password

••••••••

[Forgot password?](#)

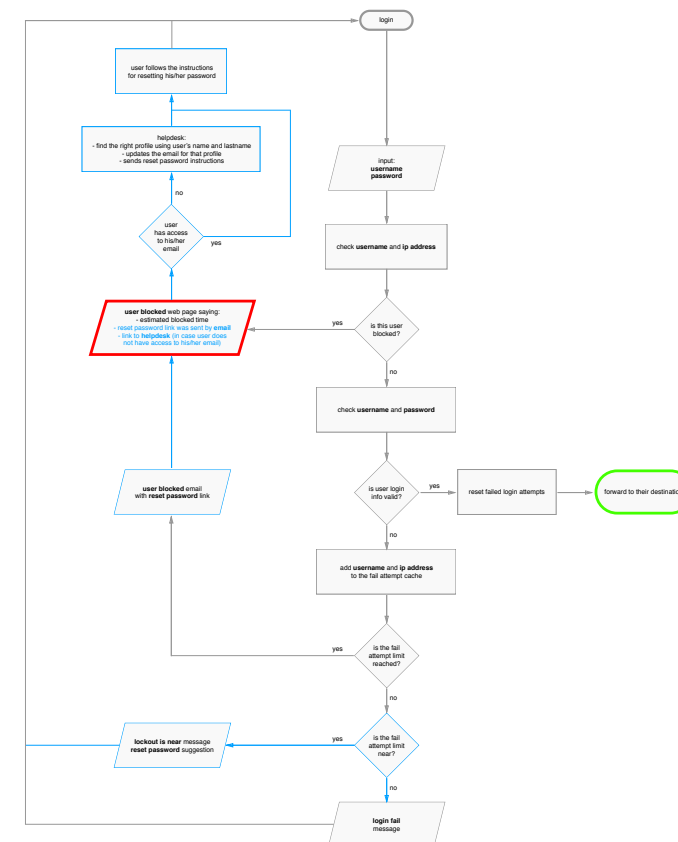
Note: Your password contains at least 8 characters: 1 lowercase letter, 1 uppercase letter, 1 special character and 1 number.

Login

Don't have an account? [Register](#)

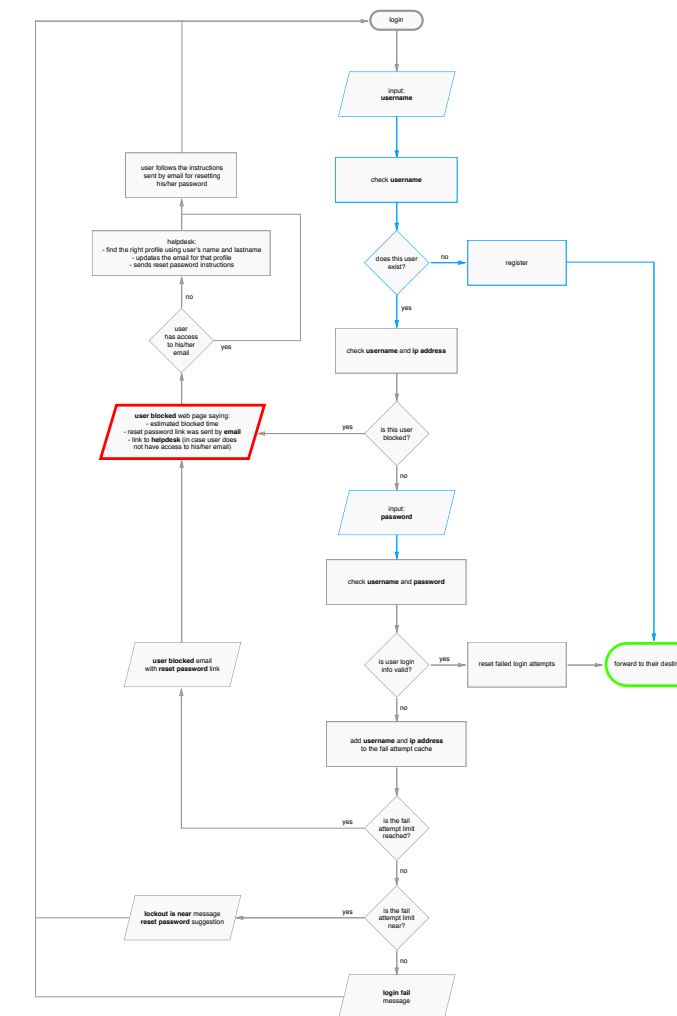
Iteration #1

- "lockout is near" warning
- password reset link by email
- link to helpdesk



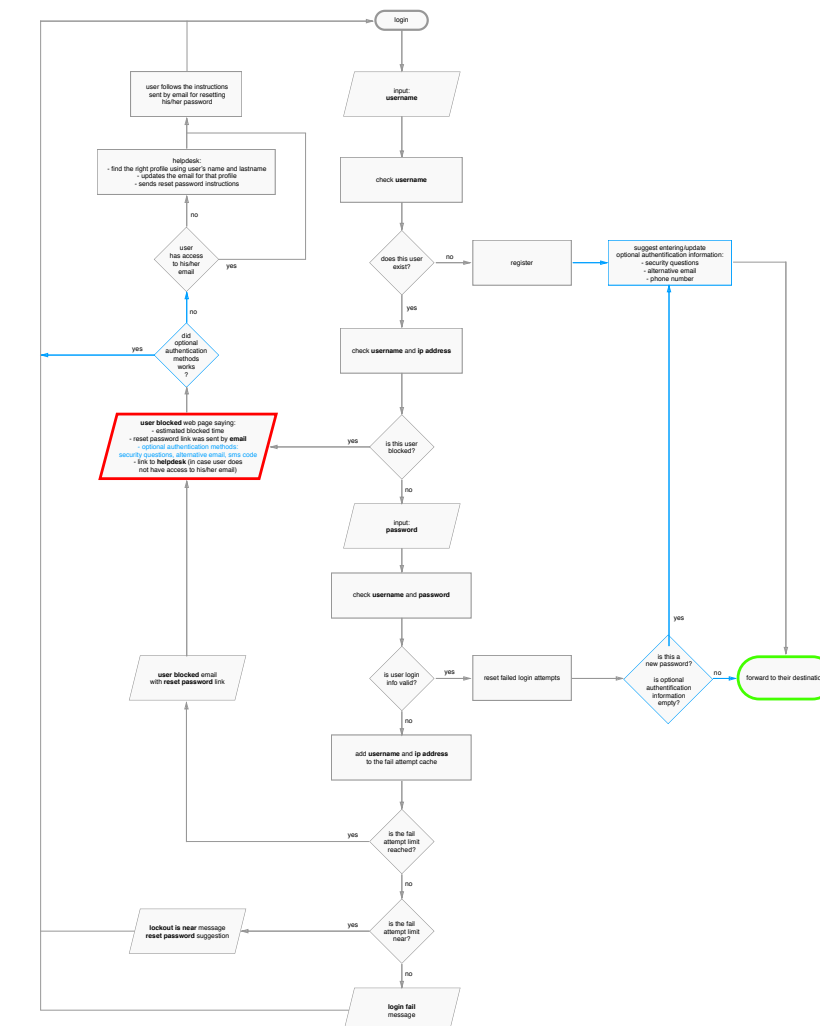
Iteration #2

- username and password separation
- inexisting account easy detection
- register added as natural part of the flow



Iteration #3

- added optional authentication information
- increase user power to unlock his/her account by himself/herself



From: security@server.com
to: amable.rodriquez@tbs-sct.gc.ca

This is a system-generated message from GCcollab. Please do not reply this message | Ceci est un message généré par le système de GCcollab. Veuillez ne pas répondre à ce message

GCcollab

Hi Amable.

We received a request to change your password. You can click on the link below to reset your password:

<https://security.passwordrecovery.org/50498478370740738378740387208723>

If you didn't request a password reset, you can safely ignore this email

If you are still having password or account issues after using the reset change your password.

GCcollab - Support
Treasury Board of Canada Secretariat | Secrétariat du Conseil du Trés

From: security@server.com
to: amable.rodriquez@tbs-sct.gc.ca

This is a system-generated message from GCcollab. Please do not reply this message | Ceci est un message généré par le système de GCcollab. Veuillez ne pas répondre à ce message

GCcollab

Hi Amable.

Your account has been locked as the incorrect password had been entered too many times. You will need to reset your password, which you can do by clicking the link below.

<https://security.passwordrecovery.org/50498478370740738378740387208723>

Your account will be unlocked after resetting your password, and you should be able to log in normally.

If you are still having password issues after using the reset link, you can contact the [help desk](#) and an agent will help you change your password and get back into your account.

GCcollab - Support
Treasury Board of Canada Secretariat | Secrétariat du Conseil du Trésor du Canada

Security Alert Account locked

Your account has been temporarily locked for 5 minutes as the incorrect password has been entered 5 times.

An email has been sent to amable.rodriquez@tbs-sct.gc.ca to reset your password and unlock your account.

If you no longer have access to amable.rodriquez@tbs-sct.gc.ca you can contact [help desk](#) and an agent will help you get back into your account.

Back to Login

The background features abstract blue geometric shapes, including a large triangle on the left and a stepped shape on the right. Faint dashed lines form a grid-like pattern across the white background.

Questions and comments
Questions et commentaires

The background features abstract blue geometric shapes, including a large triangle on the left and a jagged shape on the right. Dashed lines form a grid-like pattern across the white background.

Thanks
Merci