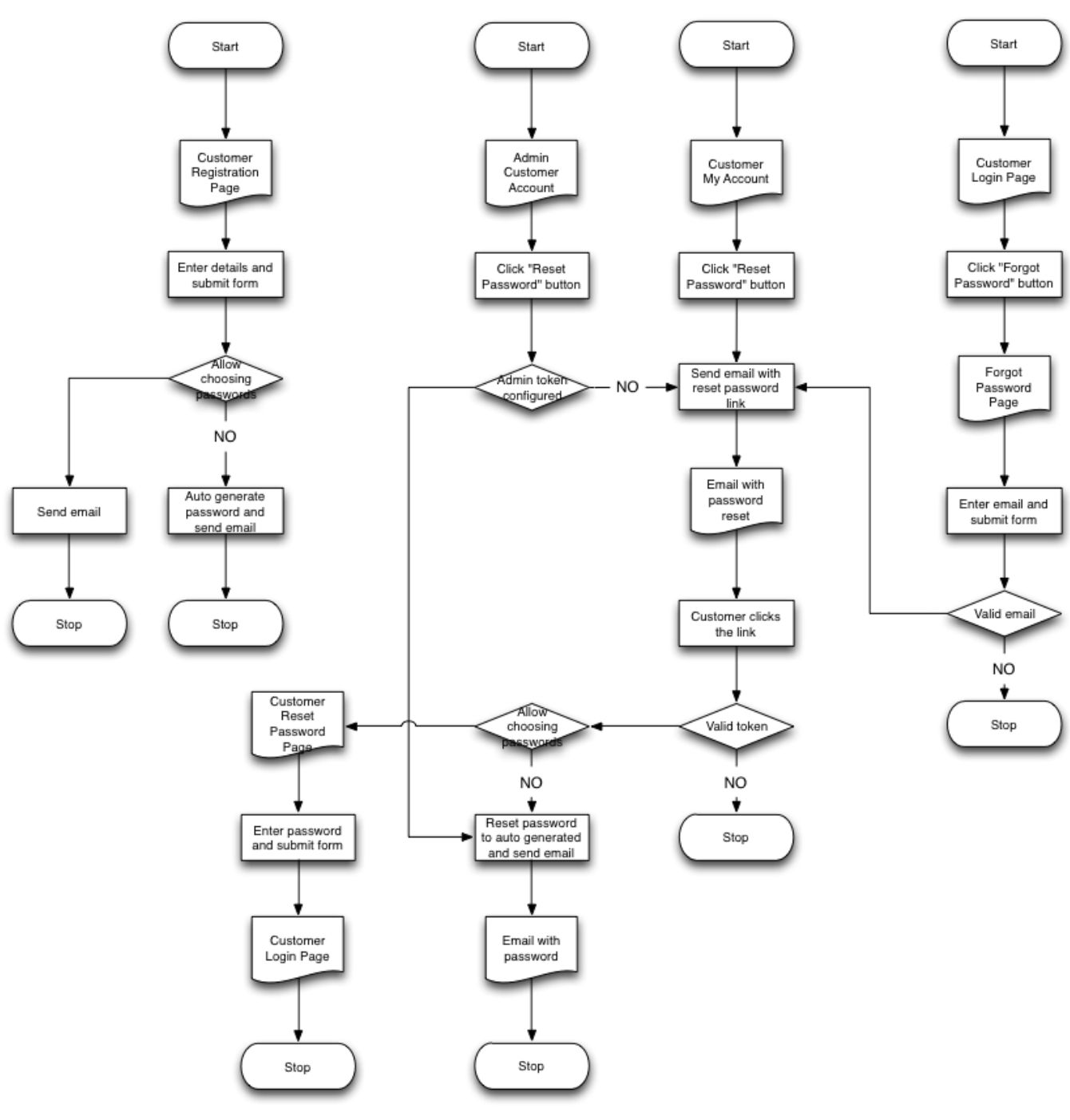
Cookbook - Password Management

- Overview
- Automatic Password Management
    - Customer
    - Business user
- User Controlled Password Management 3.5.0+
    - Customer
- Business user

Overview

Password management is tightly connected with user's email be it customer of a shop or business user using admin application. In both cases user login would be an email address. All password communication will done directly to users email address.

Basic representation of all flows for customer is depicted below:

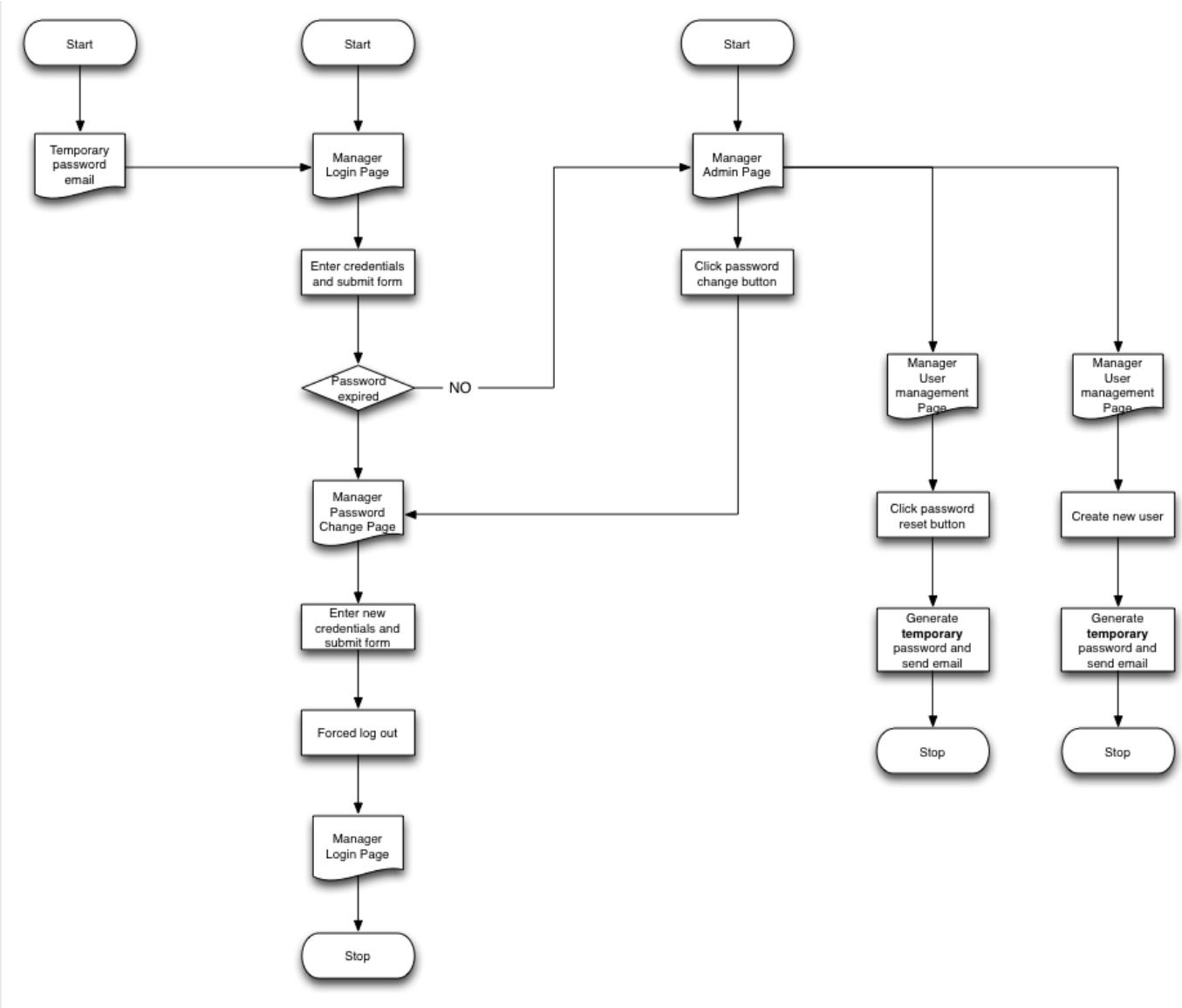


Briefly to outline the process:

- Whenever customer registers they receive an email, which may contain an auto generated password
- Whenever customer or call centre operative resets the password there could be either automatic password reset or a two step password reset whereby first email contain the link to actual reset of the password. This is done purposefully to prevent unwanted password reset (say if someone knows user's email)

Feature for allowing customers to choose their own password is available starting from version **3.5.0**. Platform versions prior this will only have automatic password management capabilities.

Business user password management can be depicted below:



It is a bit simpler since access to admin application is restricted. Thus features such as forgotten password functionality are not available and self password reseting is therefore simplified since it does not contain the token link communication to verify the request.

Key point for business user password managers are:

- Business users receive password in the account registration email (This password is temporary and will force password reset on first login in versions **3.5.0+**)
- Business user can change their passwords using password change page (available in versions **3.5.0+**)
- Business user with user management role can reset passwords for other users which will result in email with password being sent.

Automatic Password Management

Out of the box the platform provides automatic password management. This means that there is no option for customer or business user to change their password, they can only reset the password.

Customer

As depicted on on the diagram in the overview section in automatic mode customer receives their initial password when they register in shop. The password is automatically generated and send via email. Password can be included using the **password** variable in email templates.

Thereafter customer has the option to reset their password from the account using reset password button, which results in password reset link being sent to their email. Alternatively if they forgot their password they can use the forgotten password form to trigger this email. If the shop does not provide a forgotten password functionality customer has option to contact call centre and business user with access to customer accounts can trigger password reset from the admin application. In version **3.5.0+** the origin of the request can be established using **additionalData.callCentrePasswordReset**.

Business user

As admin application is restricted to organisation users the password management is somewhat simplified. Upon new user creation business users receive email with their password specified in a similar way customers do. The password can be reset by business users with user management role which triggers an email with new password.

In versions **3.5.0+** the generated password is temporary, which means upon its use the business user will be promoted to choose another password.

User Controlled Password Management 3.5.0+

Starting from version 3.5.0 password management can be setup to be fully controlled by business user thus providing flows to allow both customers and business users to change the password.

Customer

Allowing customers to choose passwords if fully controlled via shop's registration attributes that provide list of attributes that determine the contents of the registration form. These shop attributes have the following form **SHOP_CREGATTRS_XXX** where XXX represents customer type (e.g. SHOP_CREGATTRS_B2C, SHOP_CREGATTRS_B2G) and contain CUSTOMER type attribute definitions (effectively it is a per customer type list of attributes that need to be captured at registration). Out of the box there are two default attribute definitions **password** and **confirmPassword**, thus including them (e.g. SHOP_CREGATTRS_B2C=email,firstname,last name,password,confirmPassword) will result in password fields being available when customer registers. Note that the attribute code is not important but rather that attribute definition **value**, which is set to password and confirmPassword respectively. Therefore it is possible to create alternative attribute definitions and use them in **SHOP_CREGATTRS_XXX** as long as their values are correctly set. This allows for multi tenant server to define per shop password configurations (e.g. for different validation purposes).

Note that even though the passwords are chosen by customer the email templates will still have **password** variable available (if business still decides to print it in the registration email). It is however recommended not to use this variable as there is no need for exposing this data in user controlled password management mode.

For call centre initiated password resets there are two options. If shop attribute **SHOP_CUSTOMER_PASSWORD_RESET_CC** is set (which represents the business user customer password reset token) this will still trigger the auto generated password flow. Thus it is recommended to leave this value empty when this mode is enabled. Alternatively you can use a condition statement in email templates to distinguish between two types of password resets.

```
<% if (additionalData.callCentrePasswordReset) { %>
Your new password is: <b>$password</b>
<% } %>
```

Observing the customer password reset from from my account page it is noted that there is no password reset form even for the logged in customer. This is done purposefully in the core implementation in order to prevent unwanted password changes say if customer left without logging out on a public computer.

Thus even in user controlled flow the first step is email to the customer with the password reset link.

Once the customer clicks the password reset link in the email this will take them to the password reset form.

> Note that link for reseting password is the same in both password management modes. Thus at the point of using the link the platform will check again the registration form configurations in order to establish of password fields are available for this type of customer. If not then auto generated password will be issued instead.

Business user

The initial password management (i.e. for creating new user and for reseting their password) remained the same in the sense that business user will still receive an email with password specified. However since version **3.5.0+** this password is temporary (i.e. already expired) which forces business user to change the password on first login to the admin application.

Thereafter business user can use the password reset button from the top toolbar to change their password at any time. This process does not involve any new emails being sent.

Note that strength of the password is determined by system preference **MANAGER_PASSWORD_REGEX** which by default is set to (?=.*[0-9])(?=.*[a-z])(?=.*[A-Z])(?=.*[@#$%^&+=])(?=\S+$).{8,} (At least 8 characters, 1 upper A-Z, 1 lower a-z, 1 digit 0-9 and one special character @#$%^&+=). Thus each organisation can create their own regular expression for strength of business user passwords.