

ABOUT MAGIC CARPET NETWORK

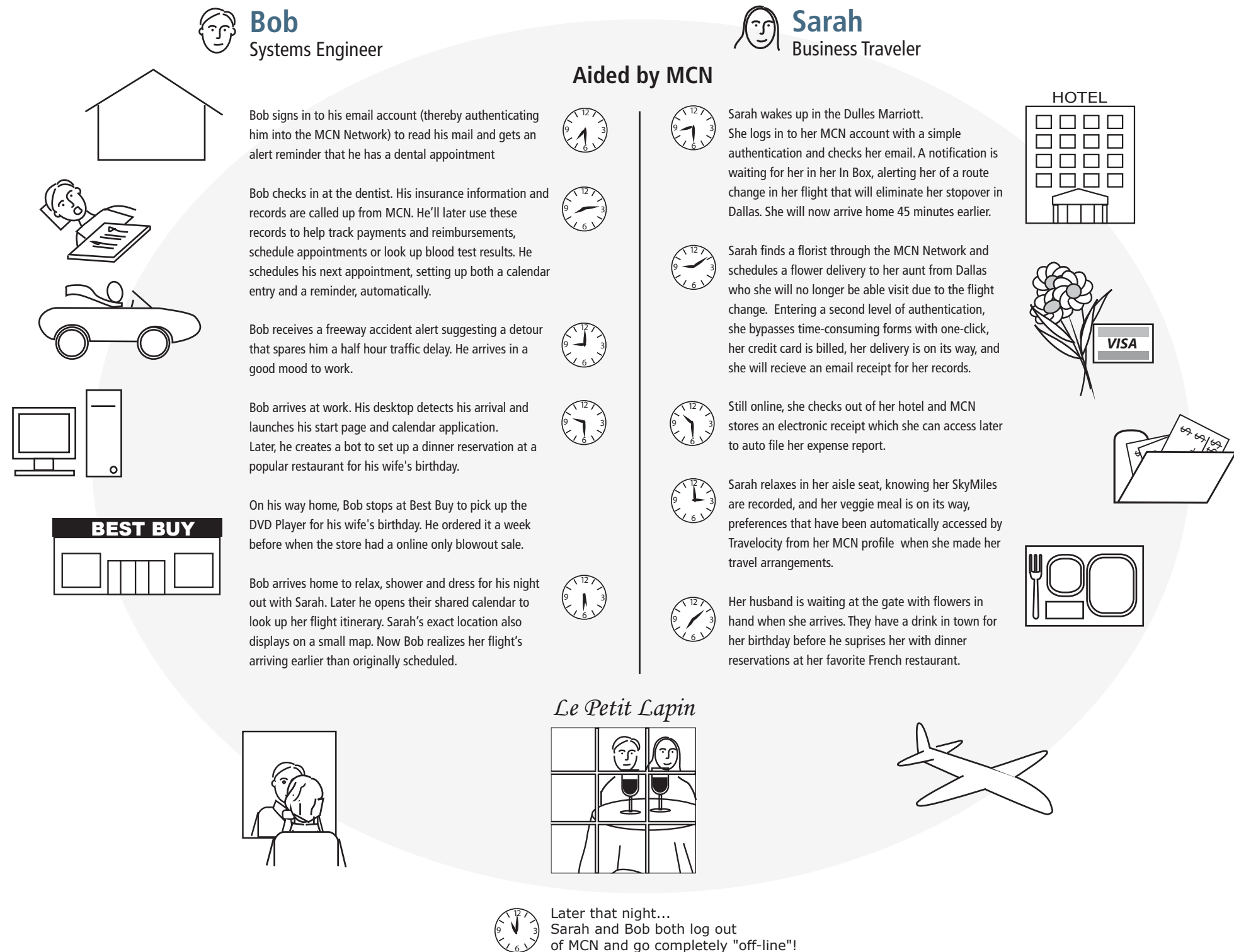
Magic Carpet Network (MCN) is a universal identity service designed for AOL/TW. It allows users to create a unique Digital Presence for securely accessing internet-enabled products and services. MCN Authentication and Profile simplifies traditional web activities such as making purchases or managing financial activities (or their offline equivalents) by providing a secure centralized consolidation of private information (e.g., identity or financial information, etc.). A Near Field Communication device, such as a mobile phone, with an MCN ID becomes a virtual wallet one could use to pay a bridge toll, borrow a library book (and manage overdue fines) or receive flight alerts and pass through airport security.

The heart of MCN is an open source technology with robust development tools and implementation standards. Anyone may freely employ and extend MCN making it a potentially ubiquitous and powerful tool for a mass audience.

About This Document

Included in this document are several examples of design deliverables completed during the discovery and preliminary design phases of this project.

MAGIC CARPET NETWORK
A DAY IN THE LIFE



MAGIC CARPET NETWORK
USER EXPERIENCE FRAMEWORK CONCEPTS v2

CONTENTS

This document outlines the overall user experience framework for Magic Carpet Network (MCN) and serves as a peer to Product and Engineering Discovery documents. It is intended to speak to specific issues and does not represent final product requirements.

03 DESIGN CRITERIA

UE requirements. MCN interaction and screen design will be developed with the goal of meeting the criteria in this section.

04 ARCHITECTURE OVERVIEW

Analysis of MCN from task perspective. UE will refer to this section when buildinginteraction flows as a baseline for coverage. Interaction flows and screen design should enable all tasks represented in Architecture Overview.

07 AUTHENTICATION

Description of major interaction tasks, with models that illustrate key issues. Included:

- Account Creation - the process of registering for an MCN account.
- Entry Points, Browser - methods of providing credentials at the Participant level.
- Authentication Levels, Session Behavior - model for MCN session behavior in the context of Participant configuration, cross-site activity, and portal authentication
- Strength and Freshness - authentication use cases in the context of MCN requirements, Participant configuration, and user preferences.
- Portal Model - illustrates characteristics of portal site
- Tools - interaction models for three different persistant MCN tools (hat, smart client,persistant html popup), includes strength and weekness of each model

13 PROFILE

Model for MCN central outlines a structure that can be configued to meet the requirements of an authentication agency.

14 WALLET

Addresses methods for interaction in the context of the wallet service. Includes components of the authentication service to illustrate potential user flow.

15 BRANDING LOGIC

Models intendend to provide UE flow perspicitive for the branding issue. UE team is working with marketing to resolve brand strategy.

16 MIGRATION PATH

Outlines UE approach to SNS/MCN migration.

CRITERIA

Personalization

- System should know who the user is in order to provide personalized information and services.
- System should provide strong benefits to user when they provide their private information.
- System should store user’s preferences and activities.

Control

- System should allow users to easily add, edit and delete their data.
- System should allow users to understand their authentication status anytime.
- System should allow users to control privacy and security. Users should know where their data are stored and who are sharing their data.

Accessibility

- System should provide clear access to all the functions available to the user.
- System should provide easy and secure access to user’s private information.
- System should facilitate users to navigate to their favorite contents fast.

Coherence

- The system behavior should consistent when users and partners interact each other within the system.
- System should be self-explanatory so that users can easily follow options and paths.

Customization

- System should be customizable to adapt to individual interests, capabilities and goals.

Automation

- System should support user with automated procedures so that they can accomplish their goals more efficiently.

Affordance

- System should allow user to learn the product through visual cues and behaviors, not relying on messages.
- System should provide information that is contextual to the task.

Interoperability

- System should be flexible enough to be operated in different applications or platforms.
- System should allow services to be inter-connected.

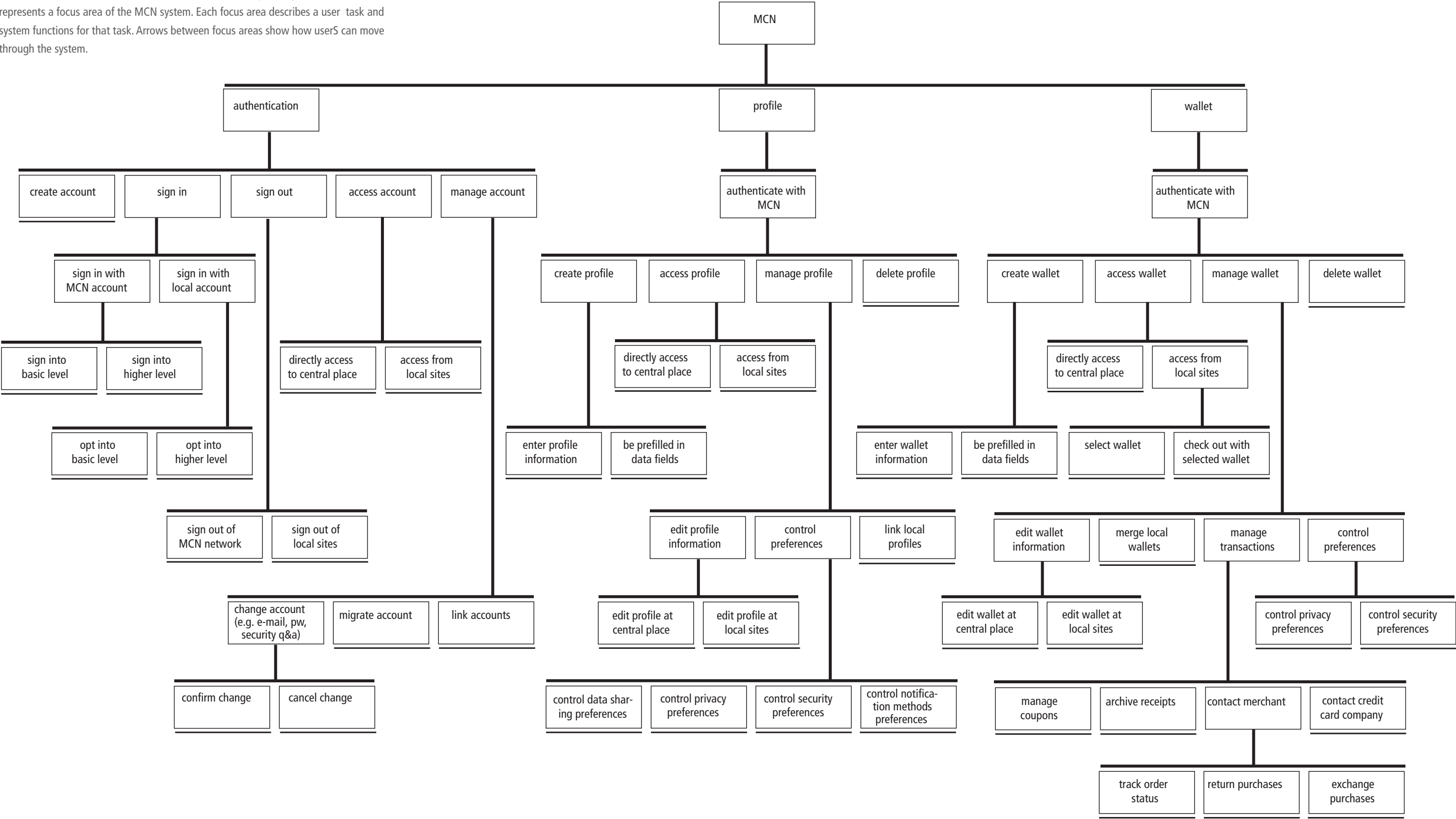
Partner Integration

- Systems should be customizable to meet partner specific needs.
- Partner requirements should be minimal to integrate the system.

Internationalization

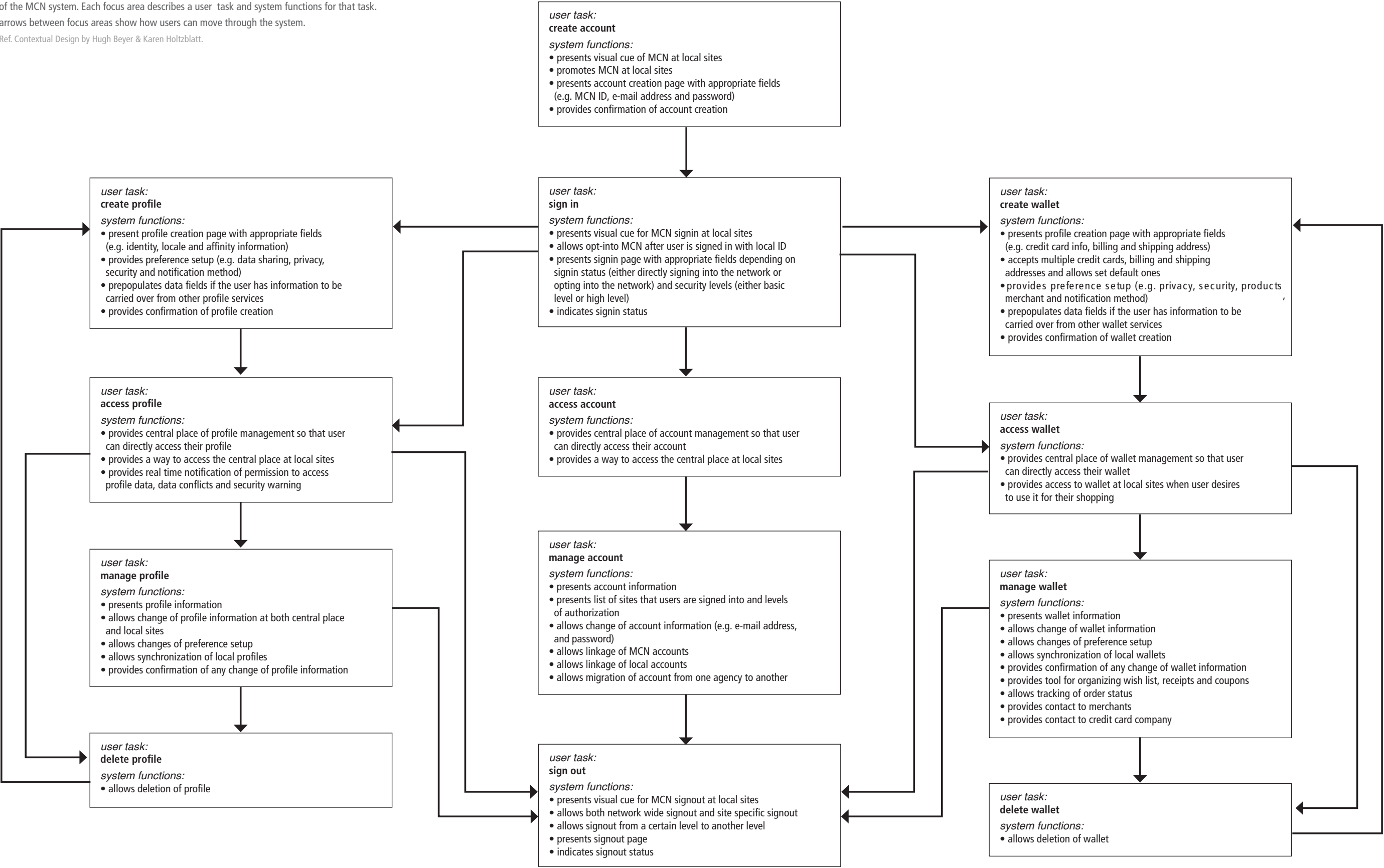
- Systems should support different requirements from target countries, such as different languages, forms of data and legal requirements.
- System should be designed to minimize additional work when it is localized.

This diagram describes system functions that are required for users to accomplish their tasks. User tasks are taken from the Hierarchical Task Analysis diagram. Each box represents a focus area of the MCN system. Each focus area describes a user task and system functions for that task. Arrows between focus areas show how users can move through the system.

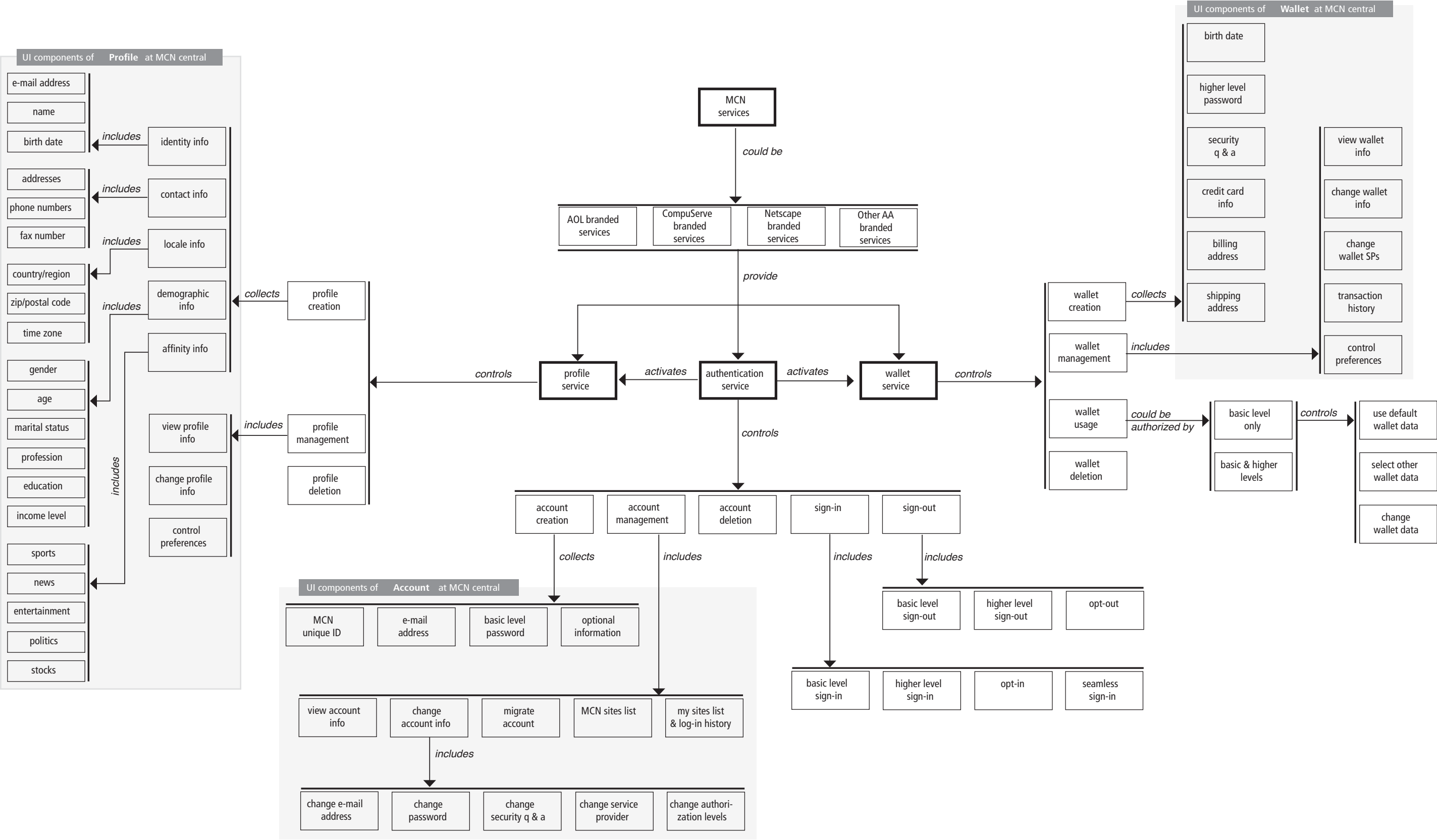


This diagram describes system functions that are required for users to accomplish their tasks. User tasks are taken from the Hierarchical Task Analysis diagram. Each box represents a focus area of the MCN system. Each focus area describes a user task and system functions for that task. arrows between focus areas show how users can move through the system.

Ref. Contextual Design by Hugh Beyer & Karen Holtzblatt.



This diagram illustrates objects required for MCN services and the relationships between them.



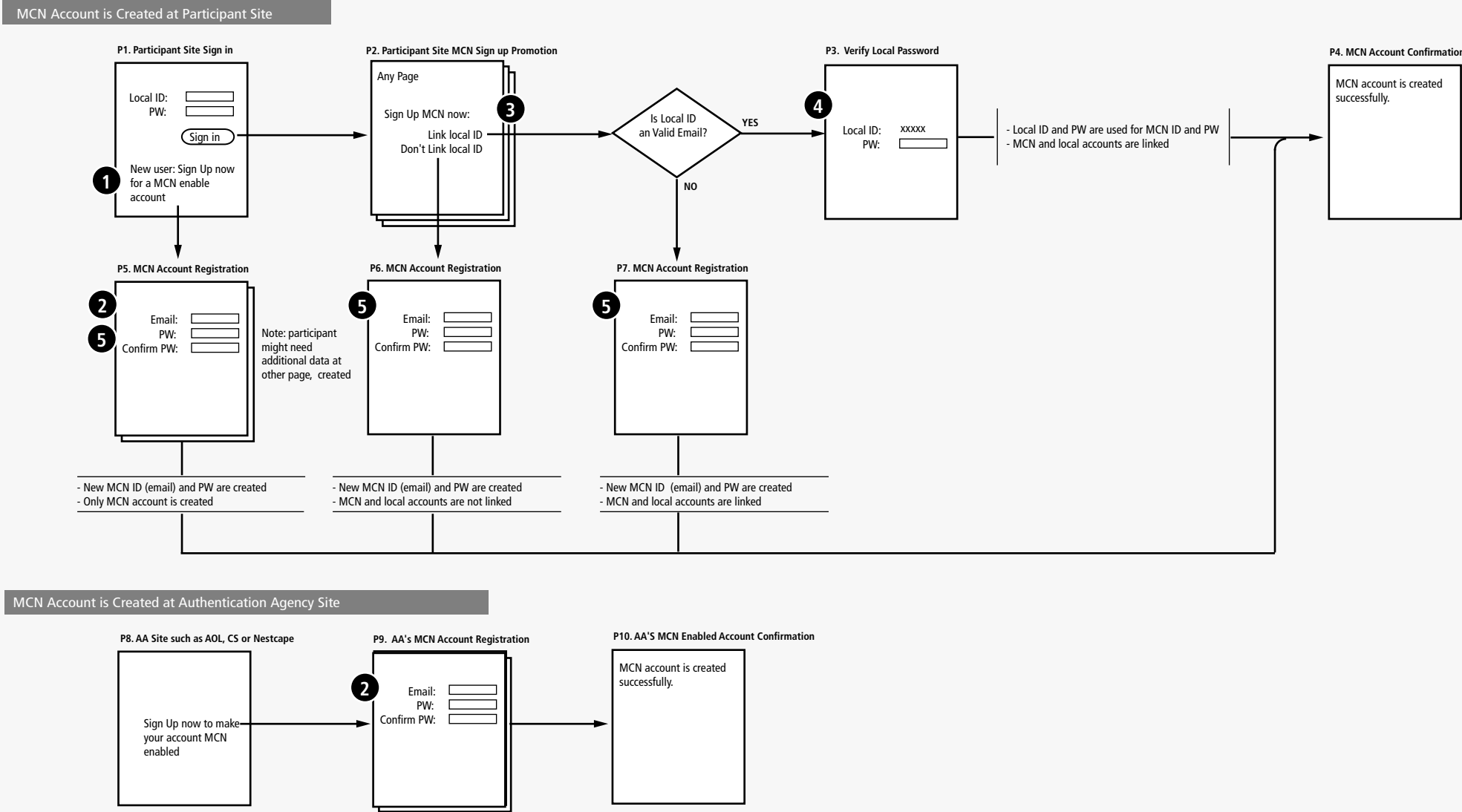
OPERATING ASSUMPTIONS

- MCN account creation should take into account AOL and Web Properties needs.
- Support co-existence and binding/linking of local and MCN accounts.

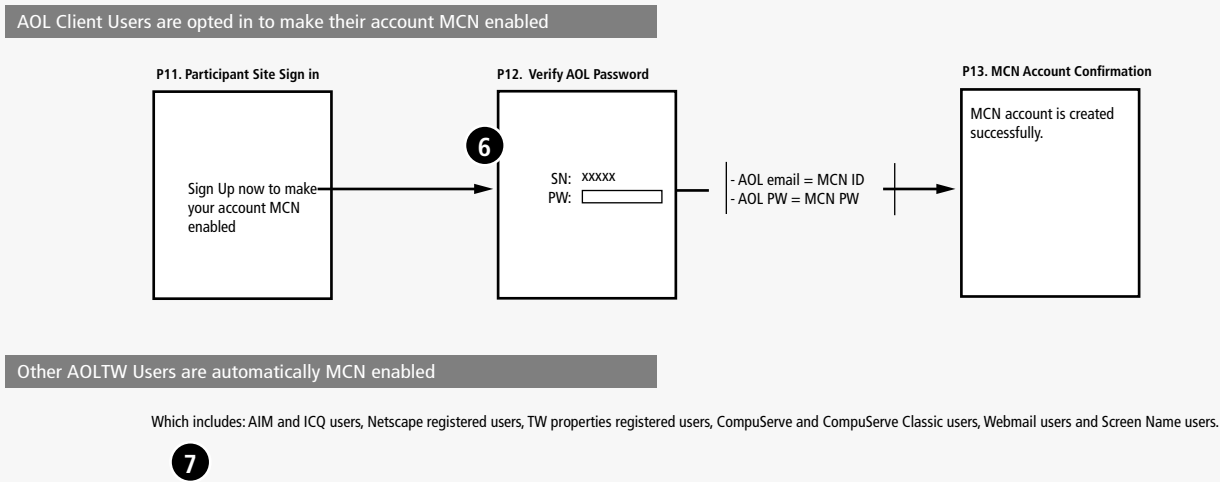
UE RECOMMENDATION

1. Provide Ability for New Users at Participant Sites to Sign Up MCN Account directly. Allowing new users to register MCN account directly will both serve the participant's needs and maximize the MCN adoption.
2. Allow Users to sign up a MCN Account through an One Step Registration. The minimum required fields are email and password. Collection of zip code and birth date is optional. Participants, service providers or authentication agencies might require additional fields for user-entered information. However, these fields will display in another pages after MCN account creation occurs. Detail is covered in the MCN profile flow.
3. Provide Ability for Local User to Opt-in MCN Account with Choice of Linking Local and MCN ID. Participants should promote their local users through an opt-in process to make their account MCN enabled. During the opt-in process, linking of Local and MCN ID should be provided to allow users to leverage their existing local ID, password and profile information for their new created MCN account.
4. Verification of Local password is required for the Linking of Local and MCN ID. Even though local users might be already authenticated in the participant site, they need to verify their local password to link their local and MCN ID.
5. Provide a Default Authentication Agency for MCN Account Creation at a Participant Site. Selection of authentication agencies could introduce difficulty for MCN adoption.
6. AOL Client users need to Opt-in to make their account MCN enabled with Verification of AOL password required. Due to privacy policy, AOL needs to opt-in to make their account MCN enabled. Their AOL email and password will be leveraged to be MCN ID and password.
7. All Other AOLTW Users (except AOL Client users) are Automatically MCN Enabled. Which includes: AIM and ICQ users, Netscape registered users, TW properties registered users, CompuServe and CompuServe Classic users, Webmail users and Screen Name users. Messages need to shown at the MCN participants' sites so that AOLTW users could use their existing ID and password to sign in these MCN sites.

NEW USERS



EXISTING AOLTW USERS



OPERATING ASSUMPTIONS

The authentication process should be flexible in terms of leading the user to the authentication point, but should clearly indicate that the site allows MCN authentication at the authentication point.

UE RECOMMENDATION

1. Allow the partner to utilize local devices to lead the user to an authentication procedure. The partner may be unwilling to implement MCN messaging or authentication mechanisms on their page. This will not improve the chances that the user will find the MCN authentication point. User tests from SNS demonstrate that the scarab can be confusing, particularly if the user is new to the site. Additionally, many partners do not implement the scarab correctly. The example demonstrates that if the user clicks on a protected area, they will be led to the authentication UI.

2. Provide partners with an MCN scarab as an option. The partner may wish to provide a direct path to MCN or to separate a local login process from the MCN process. The partner should still have the option to lead the user to the authentication point through other paths.

3. Allow partners to present MCN authentication UI in a content page. User testing has demonstrated that the easiest way to direct the user to the authentication process is to surface the login UI. MCN branding should be present in this UI. The partner should still have the option to lead the user to the authentication point through other paths.

4. Allow partners to achieve MCN authentication goals via a "hat". The hat has potential to provide status to the user across multiple MCN sites. The partner should still have the option to lead the user to the authentication point through other paths

5. Allow the partner to use local UI to accomplish MCN goals, but recommend MCN flex UI. Partners may not wish to implement MCN flex UI. In this event, local UI may be leveraged to authenticate the user. The partner will be required to implement some MCN branding and messaging to support this task. Optimal implementation is MCN flex UI. The partner's local terminology may conflict with MCN terminology (i.e. "user name" for login ID instead of "email address"), and it may be less clear that the user is interacting with MCN if all interaction is accomplished through local UI.

6. Provide pop-up solution for MCN flex UI. The ability to enable authentication and other MCN tasks via a pop-up will allow partners to complete tasks without taking the user from the context of the page.

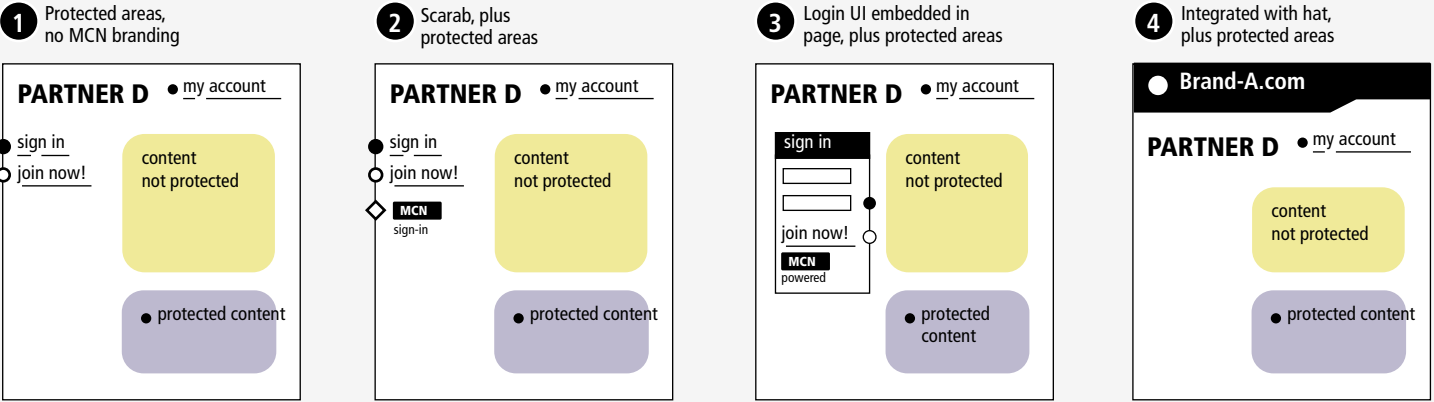
7. Provide an embedded solution for MCN flex UI. Partners may not wish to implement a pop-up flow. The partner should be allowed to embed MCN flex UI in the look and feel of their site.

INTEGRATED PARTNER, BROWSER

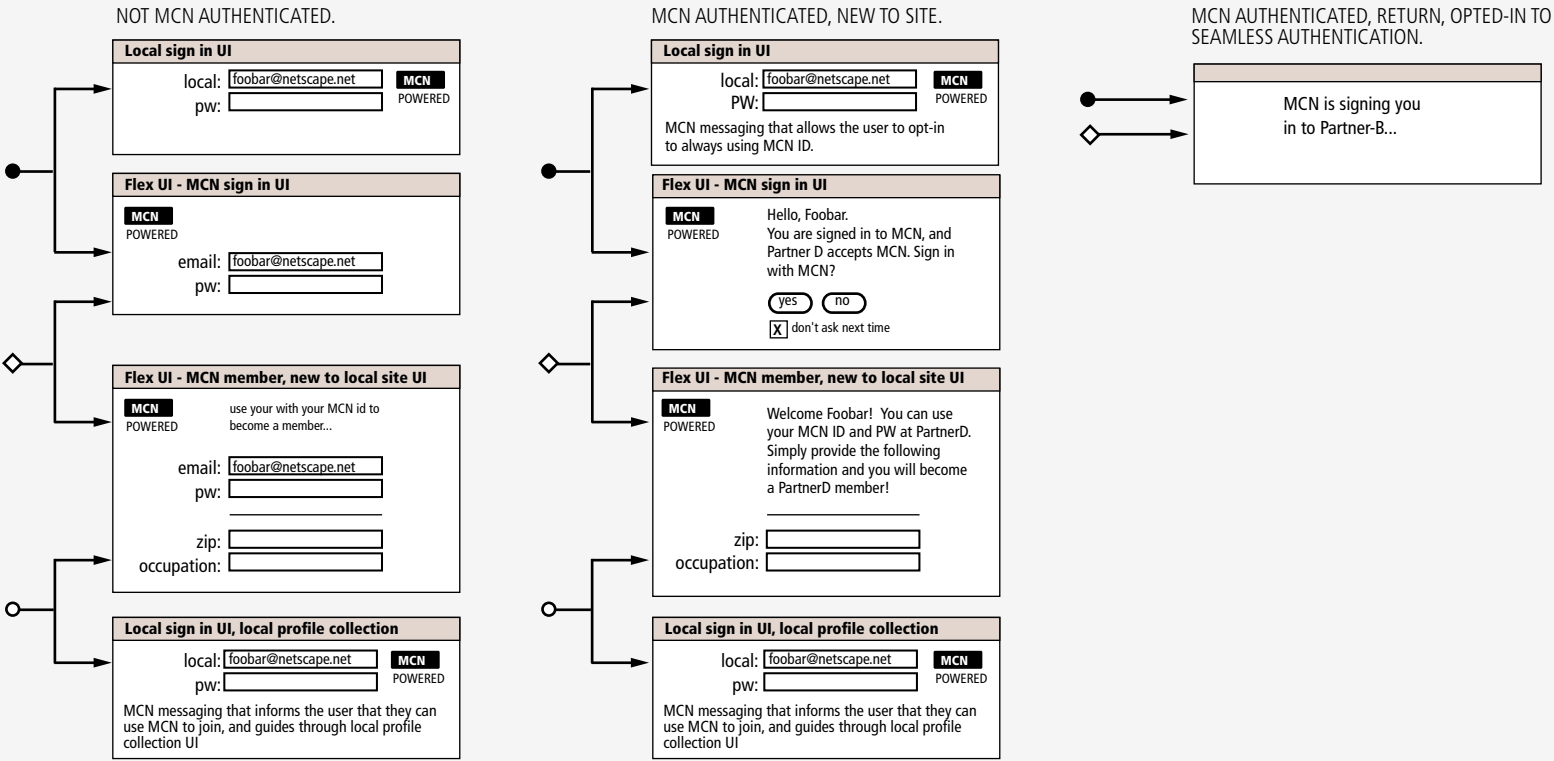
CHARACTERISTICS

- User may visit partner via browser or client that does not allow the use to sign in with MCN credentials.
- Persistent MCN authentication status may not be available.
- Paths to mcN authentication are determined by partner
- MCN messaging/branding is present when challenge is necessary, otherwise not required.

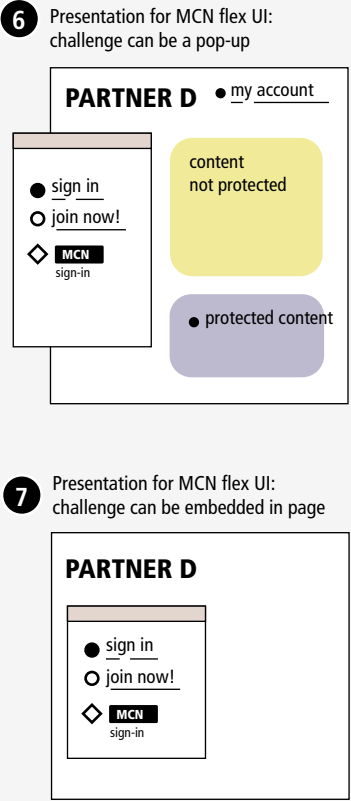
INITIATE AUTHENTICATION OPTIONS



5 AUTHENTICATION UI OPTIONS: LOCAL VS MCN FLEX UI



PRESENTATION OPTIONS



OPERATING ASSUMPTIONS

- MCN requirements determine authentication procedure across different sites during a session.
- Portals count as one site in an MCN session. If MCN requirements are met for any site within the Portal, the Portal can configure the authentication process.

UE RECOMMENDATION

1. Prepopulate MCN member’s loginID in basic challenge UI. Once the user signs into MCN through a client, MCN will always prepopulate the member’s loginID (even if they explicitly sign out of MCN). This creates a connection to the MCN signin process and reminds the user that they are signing in to a participant with their MCN credentials. If more than one member uses the same client, MCN pre-populates most recent loginID. If that loginID is incorrect, members can enter a different one.

2. Require site specific opt-in when the user is new to an MCN site, regardless of auth status. The choice to sign in and share information with a site must be the user’s choice. When the authenticated MCN user lands on an MCN site for the first time during authentication, MCN must inform the user that they will be signed in with MCN credentials. At this point, the user should also be aware that they will be transparently authenticated the next time they arrive as an MCN authenticated user. This can take many forms –i.e. popup, embedded messaging at sign-in point, scarab (see BROWSER ENTRY POINTS REQUIREMENTS).

3. Don’t require site-specific MCN opt-in for sites within a Portal after the user has opted in. Portals are sites or clients that represent a unified site experience, regardless of how many additional sites or partner sites are part of the Portal. Authentication requirements are set by the Portal once the member has provided MCN credentials (see PORTAL SITE MODEL). Example demonstrates that even though the user is new to a "SportsSite" partner within the portal site, the user is authenticated transparently because they authenticated at partner home.

4. Inform that MCN is performing authentication process. Even when transparent authentication occurs, the process can be indicated via messaging –if blank screen is needed, put messaging on screen during the authentication to help the user understand the behavior of the MCN product.

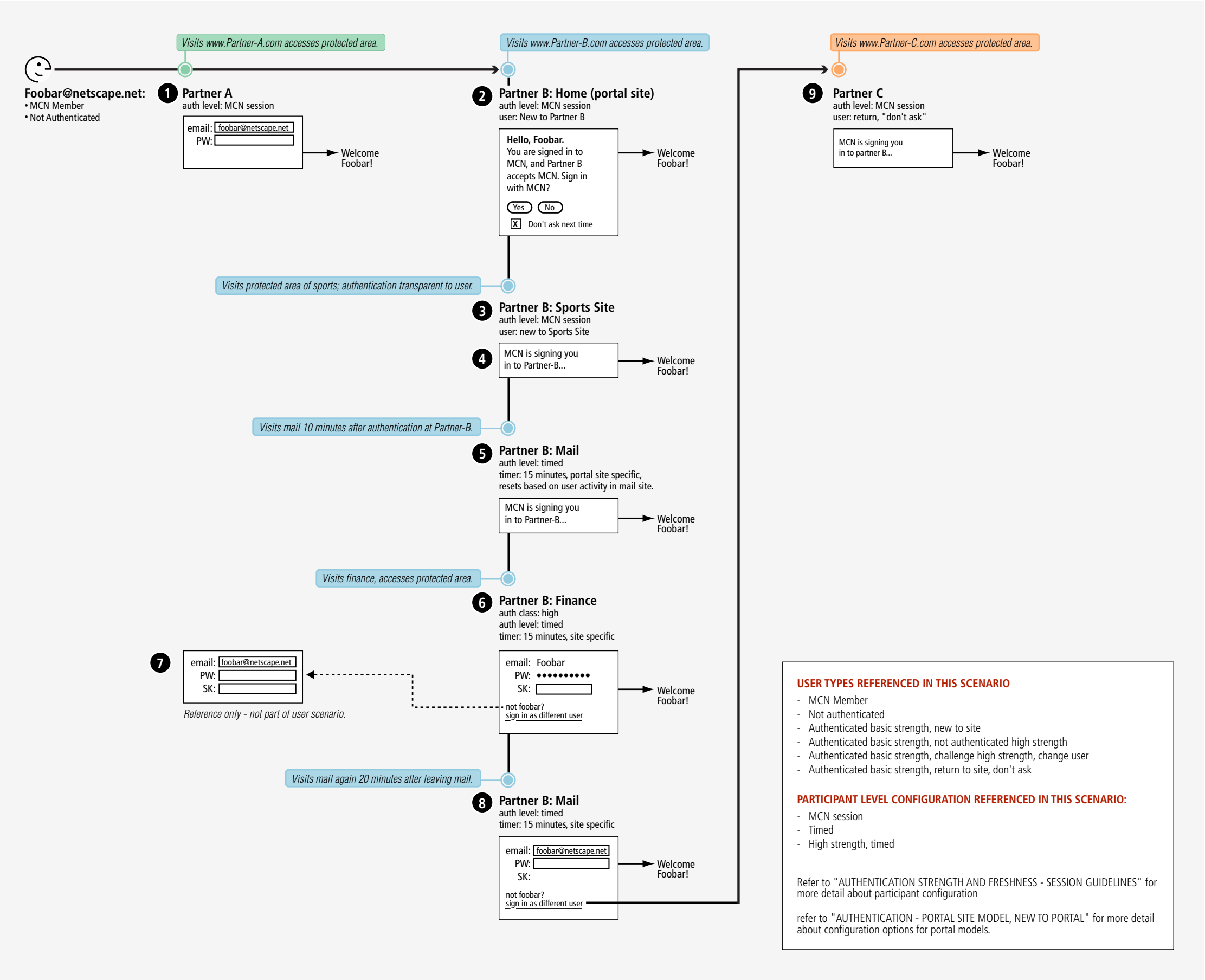
5. Allow partners to configure timer based MCN authentication or site-specific authentication. If the partner site chooses site specific, then MCN session timer should not be a factor. The member should not be challenged until site specific timer expires. Example demonstrates that the user will not be challenged because they have only been at partnerB for 10 minutes (even though the 20 minutes may have passed since the started their MCN session at partnerA). The timer is reset by user activity while in the mail site. The site specific timer starts again when user is inactive in mail site.

6. Prepopulate auth’d MCN user’s loginID and indicate that PW has been entered in high strength challenge UI. High strength auth will be different than the user’s basic strength authentication. Prepopulating SN and PW representation will indicate authenticated at the basic level. Users need the ability to re-sign in as a “different user”. MCN must allow sign out of a site and present a new basic and high strength authentication screen for the user.

7. Prepopulate user’s loginID even when the user chooses to "sign in as different user" from high strength login UI. Prepopulation of the loginID should not be affected by the user’s choice to sign in as a different member - the email address will still be associated with the previously authenticated user until a different user completes authentication. New user’s loginID should be prepopulated. When high strength auth required and use not authenticated at basic strength, PW and SK fields are available to avoid the need to navigate two separate screens to authenticate at high strength.

8. Set timer on initial login. Reset based on activity within the site. Although an authenticated user may be active, timer should reset based on activity within the site protected by the timed level. Example shows an active user; 20 minutes has elapsed since the user was last active.

9. Authenticate an MCN auth’d user transparently once they have opted in. Once users permit MCN to sign them into a specific site, MCN can perform this activity transparently.



STRENGTH	CREDENTIALS	NO.	FRESHNESS	CONFIGURATION	CREDENTIALS NEEDED	SESSION IMPACT
Basic	LoginID PW	1	Single Transaction	MCN	Each Transaction	Does Not Initiate Session
		2	Per Access	Participant	Each Access	Initiates MCN Session, Access Ends When User Leaves Area
		3	Per Access, Timed	Participant	Each Access, and When Timer Expires	Initiates MCN Session, Expired Timer Ends Access But Does Not End Session
		4	Timed	Participant	When Timer Expires	Expired Timer Ends Access But Does Not End Session
		5	Per Participant or Transaction	User	Once per Participant Access, or Transaction	Initiates MCN Session, Will Challenge User Based on User Preferences
		6	MCN Session	Participant	Once for Session	Initiates MCN Session
		7	Shared Computer	User Once for Session	Once for Session	Initiates MCN Session
		8	Client Permanent	User Not Required	Once for Session	Initiates MCN Session
High	LoginID PW SK	9	Per Access	Participant	Each Access	N/A - High Class Authentication Does Not Carry Across Sites
		10	Per Access, Timed	Participant	Each Access, and When Timer Expires	N/A - High Class Authentication Does Not Carry Across Sites
		11	Timed	Participant	When Timer Expires	N/A - High Class Authentication Does Not Carry Across Sites
		12	Per Participant or Transaction	User	Once per Participant Access	Will Challenge User at High Strength Based on User Preferences
		13	Portal Session	Portal or Participant within Portal	Once for Session at Portal	initiates session for high strength authentication only in context of portal site

DESCRIPTIONS

1. Single transaction. Facilitates a purchase by allowing MCN to challenge user without initiating an MCN session.

User experience: When users employ an MCN mechanism to complete a purchase, they are in effect providing credentials in order to complete a purchase. The user does not intend to initiate a session, the user would not expect that they need to sign out.

Example: Quick Checkout wallet behavior. User clicks a QC button in a partner flow to use wallet. Once the shopping password is provided, the purchase is complete. User never needs to sign out from a Quick Checkout transaction flow.

2. Per access. Allows participant to challenge user on access to a sensitive area or to challenge user for each transaction, but also initiates an MCN session. Access to area ends when user leaves page.

User experience: A user may visit a sensitive area such as "my account" or may be in the context of a portal site where transactions may occur. In either case, the user is navigating content or is in the context of a portal experience, and would expect to sign out.

Example: Yahoo challenges the user every time they access account info, regardless of authentication status. eBay challenges the user every time they make a bid, regardless of authentication status. In both cases, there are other areas that are accessible with ID/PW level authentication, therefore it is appropriate to initiate MCN session for seamless access.

3. Per access, timed. Allows participant to challenge user on each access to a sensitive area, and also to end access when user is inactive in protected area for specified amount of time. Initiates MCN session. When timer expires while page is in browser, page refreshes to challenge screen.

User experience: Users are familiar with "timeout" behavior on the web. If the user is going to be challenged each time they access a content area, it would be logical that the access may also be timed. The user also would expect to sign out, therefore it is appropriate to initiate an MCN session.

Example: Site challenges user each time they access account info, and times the user out if they are inactive at that screen.

4. Timed. Allows participant to designate areas that accept MCN session authentication within a specified period of time, but that provides a higher level of protection by challenging the user if time has expired. When timer expires while page is in browser, page refreshes to challenge screen.

User experience: Users may sign into Portals such as AOL Anywhere to access mail. A timed session allows users to sign in and immediately navigate to mail without being challenged again, but provides the extra security that users expect for sensitive information (challenging after inactivity).

Example: AOL Anywhere. Users are encouraged to sign in first at AOL.com, then access mail, calendar, etc.

5. Participant access. Allows user to request to be challenged for entry to specific sites or when completing a transaction based on preferences (can be configurable from My Site List or Security Preferences (i.e. "always ask for my password when shopping").

User experience: Even if a site will allow the user to seamlessly access content based on MCN session level, the user may have security or privacy concerns and therefore may want some sites to challenge them every time even though they are already authenticated.

Example: From SNS 2.5 usability tests, quote "I don't have a problem with Harry Potter signing me in automatically, but I'm sure not comfortable with eBay doing that. It doesn't seem secure."

6. MCN session. Allows participants to accept active user credentials that may have been entered at other sites. Site configured at this level do not require users to enter credentials again. If users visit a new site they must have the opportunity to opt-in to being authenticated at the site (note: for Portal model, user opts in to all sites within portal on portal entry point - see "PORTAL MODEL")

User experience: Sign in once, access multiple sites.

Example: SNS, passport. Today, both models operate on "scarab" model. Users click a button to indicate that they opt-in to sign in to the site. MCN is exploring alternatives that still give the user the ability to opt-in to signing in to sites without requiring the user to find the scarab (see "BROWSER AUTHENTICATION ENTRY POINTS").

7. Shared computer. Allows users to indicate they're using a shared computer. This is a counter to Client Permanent. If activated, this level protects the user by overriding the Client Permanent choice and signing them out of MCN when they end client access. Ideally, this would also be timed (timer configured according to MCN requirements).

User experience: Surfaced at the sign-in point, this option serves as an active prompt for the user to think about a shared computer experience. Provides assurance that system will protect user in this scenario and allows extra protection for users who may not understand the "sign me in automatically on this computer" option.

Example: Passport offers this option on sign-in screens. Yahoo does not, but addresses the scenario in "sign-in help", several levels deep. If user really searches, Yahoo informs the user not to select "remember my ID and PW on this computer" if using a shared computer.

8. Client permanent. Allows the user to indicate that they wish to be signed in to MCN automatically when using a specific client (i.e. browser).

User experience: Surfaced at the sign-in point (i.e. Sign in automatically on this computer), allows users to request that MCN sign them in automatically without the need to provide ID/PW. Option is ended when user explicitly signs out.

Example: Passport and Yahoo offer this option. SNS also offers a "permanent authentication" choice on a site specific basis - the participant has the option to configure their site to accept this option. However, the permanent option for MCN will not be site-specific, it will apply to MCN session.

NOTE:

There are three variables to consider in terms of UE guidelines for authentication strength and freshness:

1. MCN standards.

2. Participant requirements, within context of MCN standards.

3. User experience: preferences, trust, security, and understanding the behavior of the authentication service.

Guidelines are intended to represent use cases within the context of these variables.

The intention of this table is to state the use cases that should be accommodated through the MCN authentication service. It does not necessarily represent technical implementation - for example, one technical implementation may solve several cases.

Note on high strength descriptions:
user must have authenticated at basic strength before reaching high strength - if user authenticated in a "single transaction" mode at basic strength, then there is no MCN session. High strength applies only to specific sites - sites don't have the option to accept high strength from others unless in the context of a Portal.

9. Per access. Allows participant to challenge user at high strength on access to a sensitive area or to challenge user for each transaction. Access ends when user leaves area.

User experience: Represents a higher level of security.

Example: Yahoo also features a higher strength pw, "security key".

10. Per access, timed. Allows participant to challenge user on at high strength each access to a sensitive area, and also to end access when user is inactive in protected area for specified amount of time. When timer expires while page is in browser, page refreshes to challenge screen.

11. Timed. Allows a portal to designate areas within the portal that accept high strength portal session authentication within a specified period of time, but that provides a higher level of protection by challenging the user if time has expired. When timer expires while a protected page is in browser, page refreshes to challenge screen.

User experience: User may be in a portal that offers multiple secure applications or content areas, such as health, finance and wallet. If user authenticates at high strength, they may wish to access multiple areas within a given period, but also may expect the site to protect their information by challenging them again if they are inactive for a period of time.

User experience: Yahoo allows users to authenticate at the security key level once for multiple applications (i.e. wallet and finance). Given level of security, it is probable that participants will want to apply timed access.

12. Per participant or transaction. Allows user to request to be challenged at high strength for entry to specific sites or when completing a transaction based on preferences (can be configurable from "my site list", or security preferences i.e. "always ask for my Security Key when shopping").

User experience: Paranoid users may desire the highest level of security regardless of participant or MCN requirements. If user chooses this option, they will need to provide their SK each time they access a participant or every time they complete a transaction (depending on preference).

13. Portal session. Allows Portals to designate areas within the portal to accept high strength session authentication entered at another area within the portal. Designation of "sites within a portal" must follow MCN guidelines.

User experience: Allows the user to provide SK once and access multiple areas within portal experience at high strength without being challenged again for duration of session.

Example: Yahoo allows users to authenticate at the security key level once for multiple apps (i.e. wallet and finance).

GUIDING PRINCIPLES

Although a portal may consist of multiple sites and applications, MCN perspective treats the portal as a single site that may protect specific areas within the site.

UE RECOMMENDATION

1. Initial entry into portal will follow MCN requirements for authentication strength and freshness. Requirements for sharing data, opting in to the site, and authentication can apply to all sites within the portal (at the portal's discretion) once the user has satisfied MCN requirements at the entry point.
2. Allow portal to configure site so that the process of "becoming a portal member" occurs only once, regardless of entry point. The portal can not predict where a member may decide to become a member (i.e. sign up for calendar, or sign up for mail). Once the user completes portal membership requirements, any subsequent requests for data should be in the context of a known portal member.

OUTSTANDING ISSUES

A portal may have partners that are part of the portal, but also maintain an independent presence or that may also be a part of other portals (i.e. fedex). It may be necessary to be more explicit when sharing data with this type of participant. It would be important to consider how data that is collected within the context of a specific portal may be used outside of the portal context. Permissions may need to be more explicit for this case.

MCN REQUIREMENTS

Additional data can be incrementally collected based on portal requirements. Data collection UI should be flexible - i.e. user impression should not be that they are "registering" for portal again. MCN requirements apply-refer to "Portal Site Model - Data Collection".

PORTAL SITE REQUIREMENTS

MCN POWERED

email: foobar@netscape.net

PW: ●●●●●●●●

SK:

not foobar?

sign in as a different user

P6. www.mail.branda.com

branda.com

Wallet



time expires

email: foobar@netscape.net

PW: ●●●●●●●●

SK:

not foobar?

sign in as a different user

P7. www.finance.branda.com

branda.com

Finance



time expires

email: foobar@netscape.net

PW: ●●●●●●●●

SK:

not foobar?

sign in as a different user

email: foobar@netscape.net

PW:

P8. www.account.branda.com

branda.com

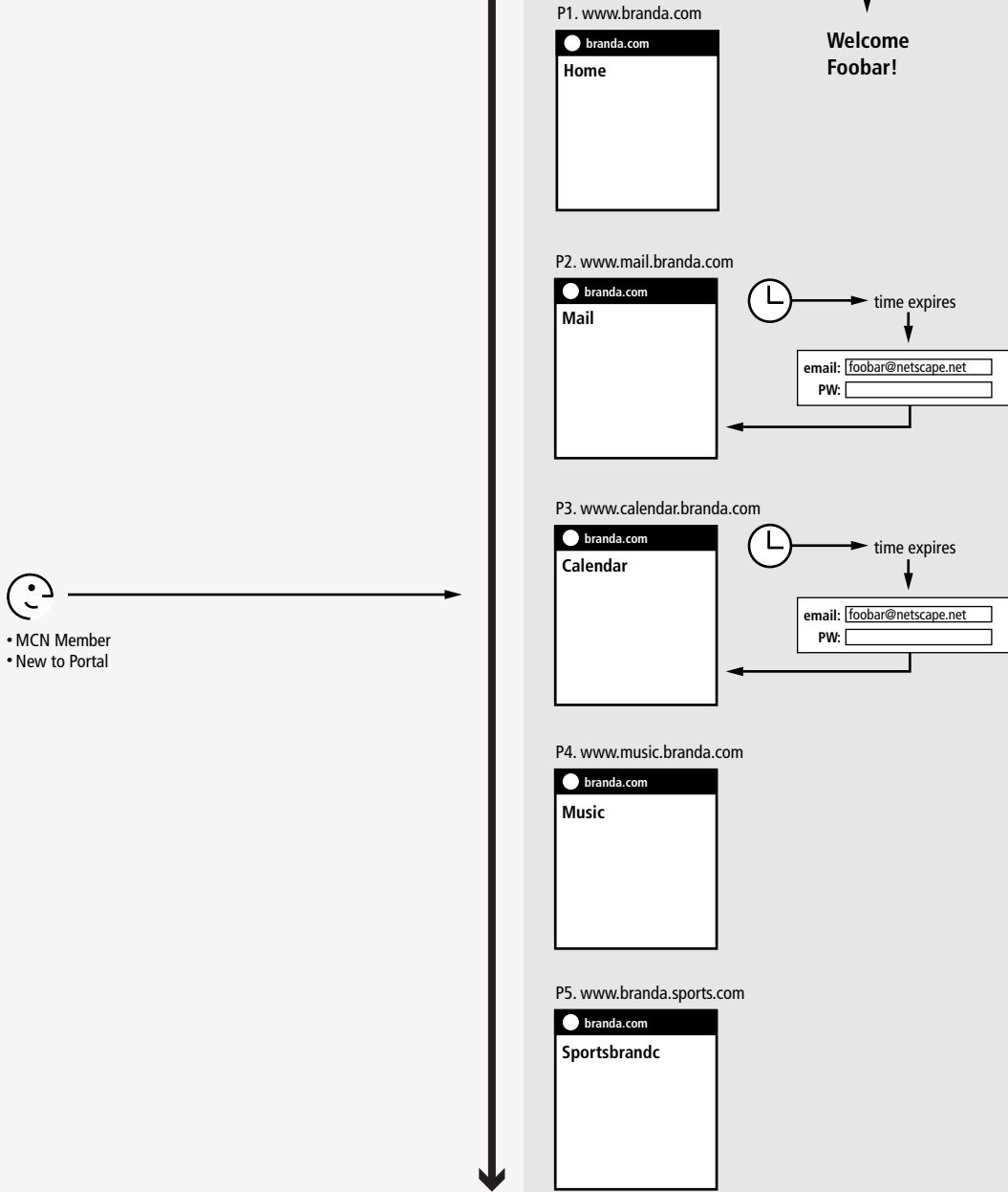
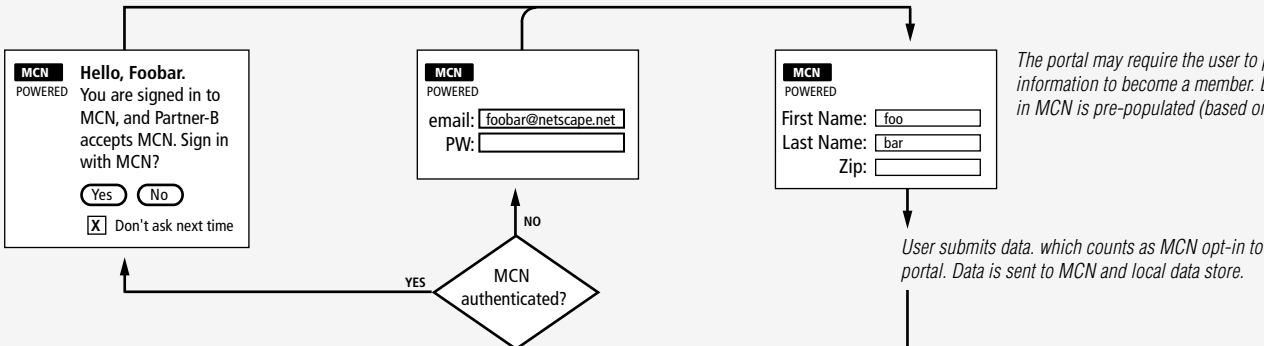
My Account



time expires

email: foobar@netscape.net

PW:



- 😊
- MCN Member
 - New to Portal

MCN Basic Strength required (ID/PW). User can meet this requirement at any site within portal that requires user authentication. Authentication allows user to seamlessly visit any of the sites in this column as authenticated user.

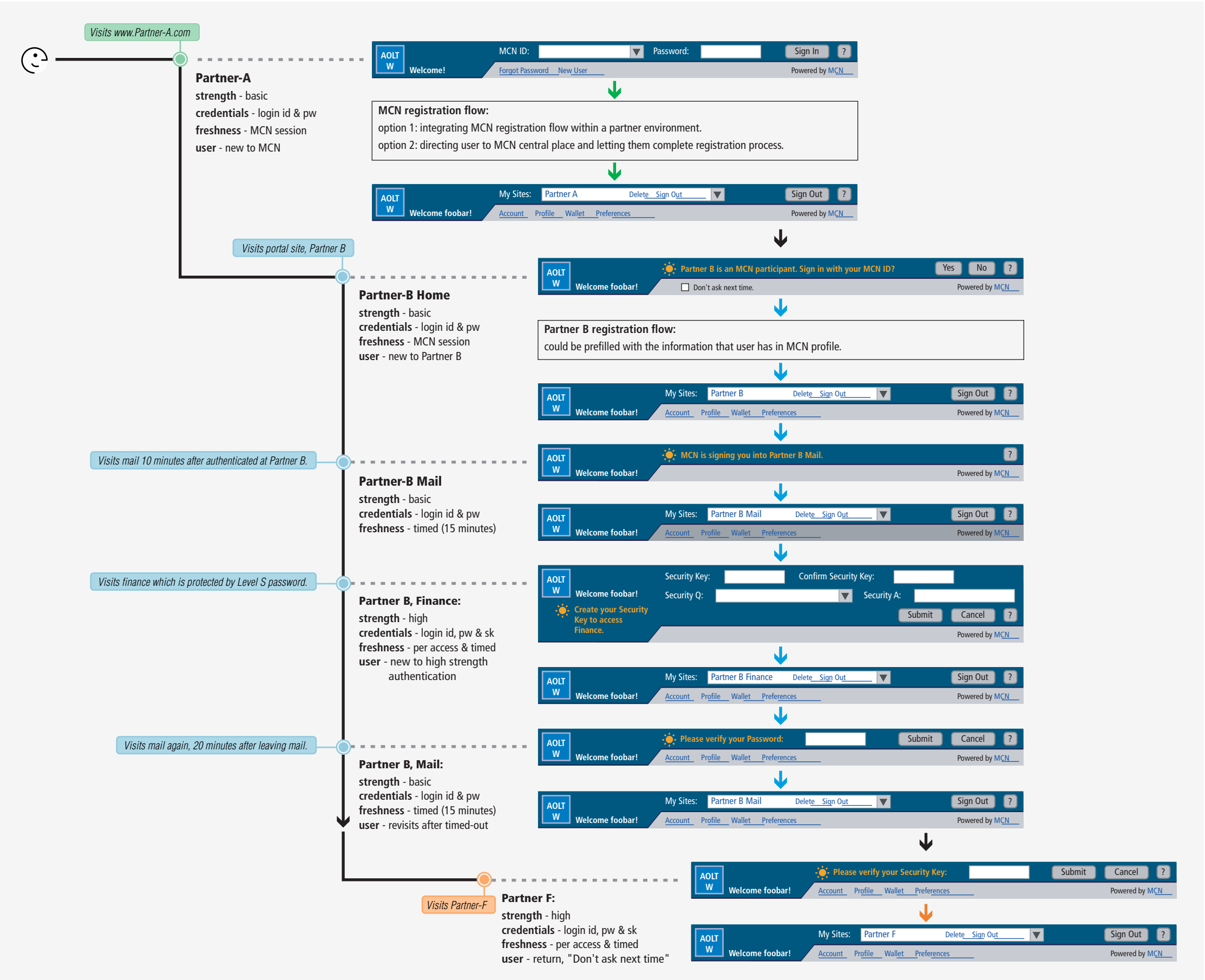
Portal has configured these sites to require high strength (ID/PW/SK). Once user has provided SK, user can move among high class sites without being challenged again, but SK session is timed.

Portal has configured this site as a "per access" level of freshness. The user must provide pw each time they visit this site. Access is also timed.

- BASIC GUIDING PRINCIPLE
- MCN should be consistent in Authentication, Partner Integration and Presentation to users.
 - MCN should clearly indicate user’s authentication status across participant sites and these sites should allow MCN Authentication at appropriate Authentication point.

- CHARACTERISTICS OF HAT
- Hat requires Partner integration and should be inserted above Partner content.
 - Hat appears at first interaction with MCN at Participant and carries across site (see PORTAL MODEL).
 - Authentication applies only to partner sites.
 - Hat provides a persistent authentication status for MCN user throughout participant sites.
 - Hat enables account management during a participant’s flow.
 - Hat has some navigation elements through participant sites.
 - Hat provides access to MCN central place.

- ISSUES OF HAT
- If Hat is integrated with participating sites –not with a browser– it only appears when user is on Participant; i.e. there is no way user can know their MCN authentication status while they are browsing through web sites that are not MCN participants.
 - Hat model could be combined with Smart Client model for Persistence regardless of sites. User Downloads and installs Client, so that it is always via their browser.



OPERATING ASSUMPTIONS (MCN PROFILE GUIDING PRINCIPLES)

- MCN requirements determine authentication procedure across different sites during a session.
- Portals count as one site in an MCN session. If MCN requirements are met for any site within the Portal, the Portal can configure the authentication process.

UE RECOMMENDATION

1. Provide a Central Profile Management Site with a Contextual Navigation Model (MCN Profile PRD Feature 6.2). AOLTW will build one central site for users to manage all preferences. Personal data in is organized into contextual categories (i.e. account management, wallet/shopping, travel and more) with links to specific buckets for detail contextual management level. At the detail contextual management level, a path is provided for users to link to the AOLTW profile central site.

2. Support Core Profile Fields Allowing Users to Enter Data Once and Use in Multiple Context (MCN Profile PRD Feature 1.3). Core Profile Data is expected to be among the most commonly used across participants. Core Profile Data can be gathered through both central site and participants interaction. Data can be placed into extensible logical groups which can consist of one or more fields. Once users arrive to a new contextual area, existing data could be pre-populated in a reasonable sense –i.e. default shipping address in wallet can be pre-populated as ticket delivery address in travel sites.

3. Rules for Updating Data Across Contextual Area (MCN Profile PRD Feature 6.2). Only core profile data can be updated once and be used across all contextual areas. Once users update pre-populated data in the core profile field during a participant interaction, they should be able to update the core profile or just keep the new data in the contextual area. Other non core profile data should be considered to be used only in the related contextual area and not to be extended to other contextual areas. Within a contextual area, data should be able to be used across participants. In general, updating or adding data should be in a manner that makes sense to users.

4. Allow Profile to be Passively Personalized (need to be added into MCN Profile PRD). Profile system will save users' most recent data automatically for future use –i.e. recent shipping addresses in transaction sites, recent travelers in travel sites, etc. For a novice user, this will automatically populate the profile; this helps advanced users reuse recently used data without need to retype or resave.

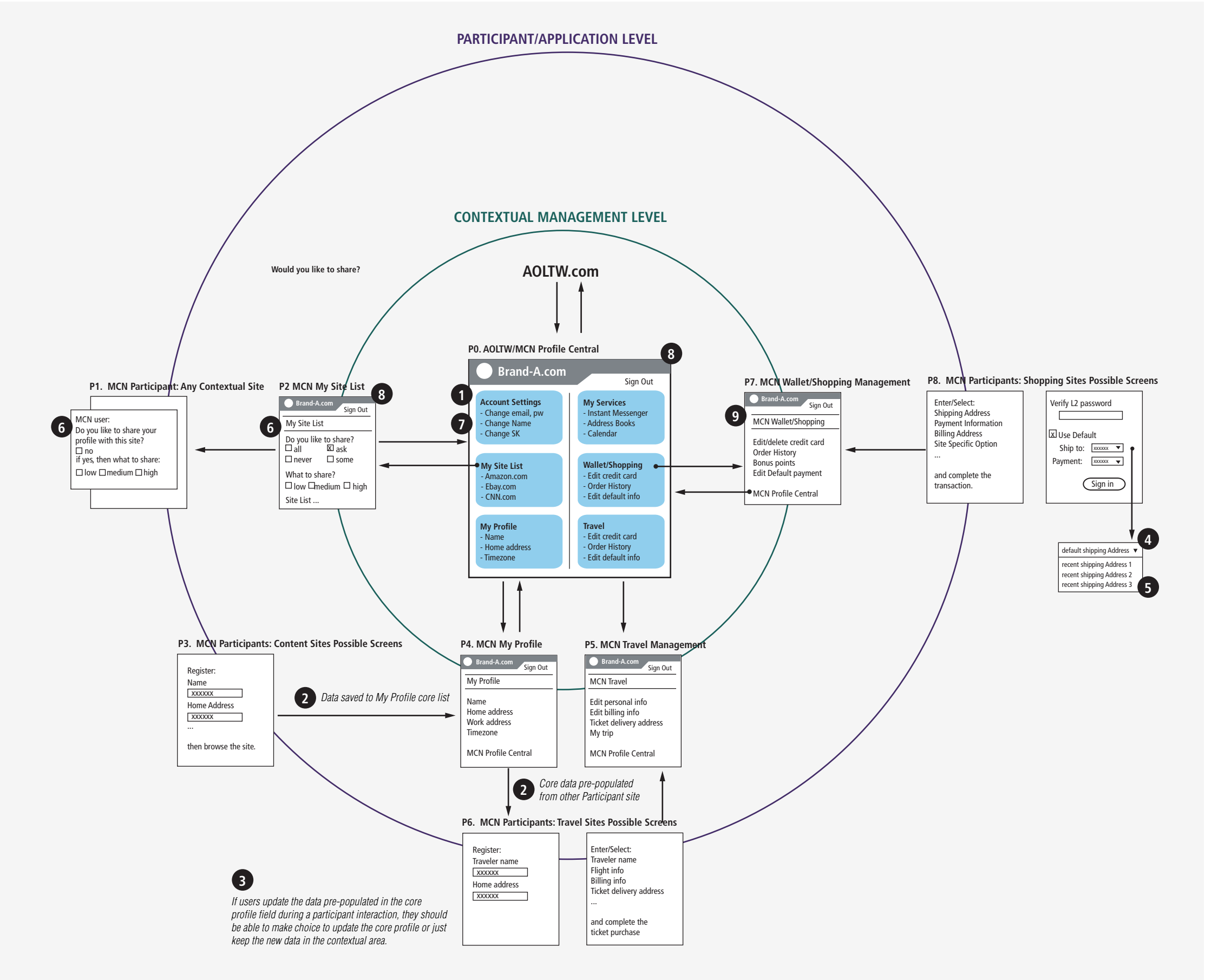
5. Support the concept of Default Information in All Contextual Profile Areas. (Add to PRD). Wallet/shopping profile: this means the credit card, corresponding billing information and shipping address. In travel profile: primary traveler, credit card, corresponding billing information and ticket delivery address. More conveniently, we can provide users a menu with default information associated with the most recent passively saved data. Participants would be delighted that MCN users can use their default payment information and skip the shipping, payment and billing address forms.

6. Provide a Easy to Understand Data Sharing model to Maximize User Control Over their Personal Data (MCN Profile PRD Feature 5.1). Data sharing management can be in the central profile area or in context when data is requested by Participant. At central profile and contextual profile management site, system should support sharing –Always, Ask, Never and Custom– and sharing level if users choose to share (low for all core data, medium and high privacy for some of the core data). By default, sharing class is Ask and sharing level is Medium. Choices are then applied to all Participants.

7. Content to be Considered in the Central Profile Management Site. 1)MCN Account Setting: email, L1 pw , L2 pw and Security Q&A. 2)Contextual area: fields in specific buckets such as wallet/shopping, travel, etc. 3)My services: links to all enabled MCN services such as Alerts, Wallet, Calendar, Address book, etc. 4) participant sites: allows navigation to Participant sites from MCN Central Profile 5) My Site List: Participants that users have signed in or registered with. 6) Privacy and Help.

8. Present AOLTW as Primary Brand for MCN Profile Central and Contextual Management Level Sites. MCN will be secondary branding indicating ubiquitous benefit to MCN members. AOLTW might need to be broken down to AOL, CompuServe or Netscape since those user types are different.

9. Content to be considered at the Wallet/Shopping Management Level –MCN Wallet PRD Feature 5.1. 1)Order history: allows view of wallet purchases. 2)Credit Card and Corresponding Billing Address: allow for same billing address for multiple cards. 3)Shipping Address: allow editing recent addresses. 4)Default shopping info setting: allows for set up of default card, billing and shipping address.

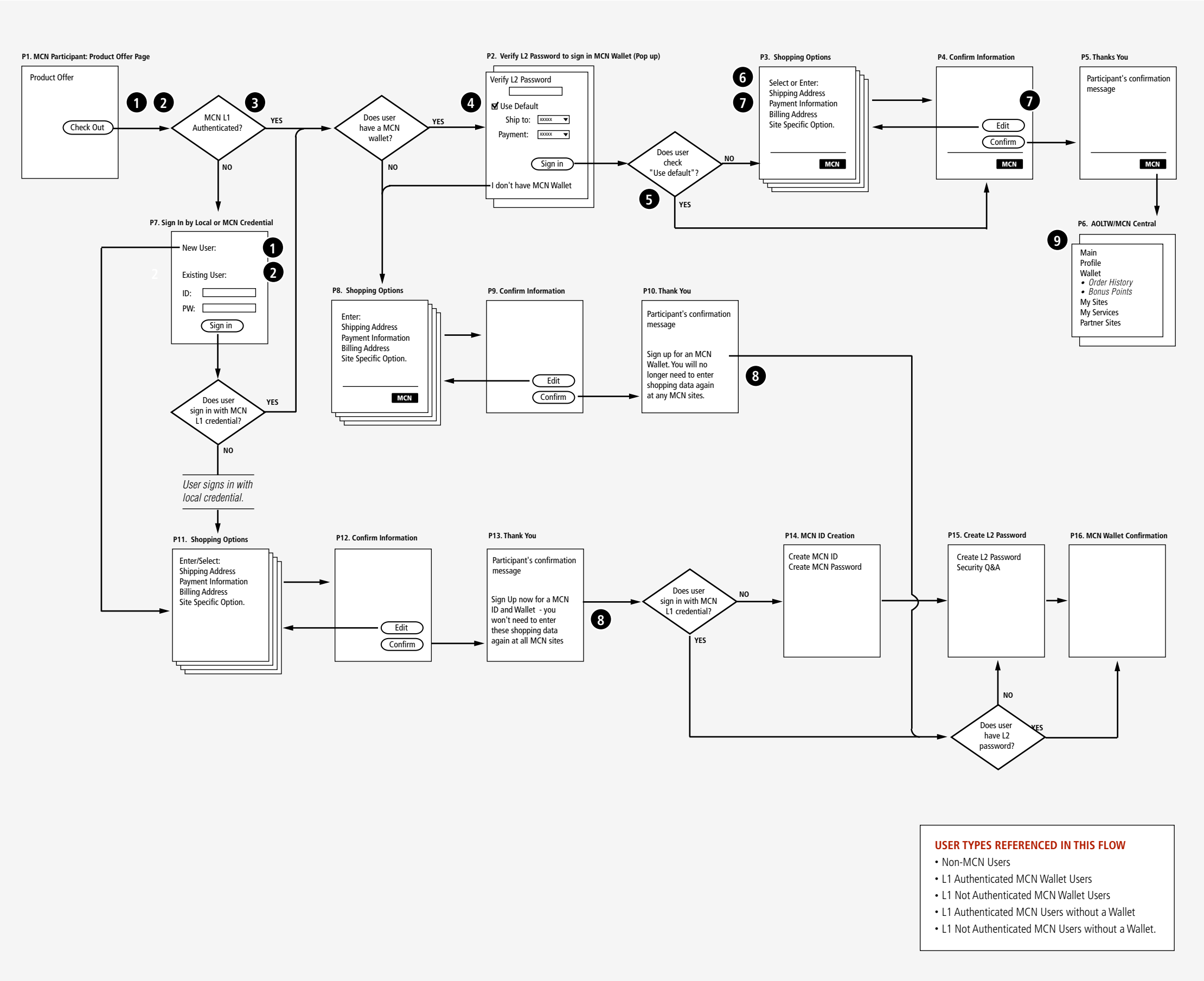


BASIC GUIDING PRINCIPLE USED WHILE DEVELOPING THIS FLOW

- Minimum UE/UI Impact in the Participant's flow
- MCN Wallet is transaction facilitator, not processor

ASSUMPTIONS

1. Present only MCN Brand at the Participant site level. Branding of AA or wallet service providers are not present. MCN brand will serve as a signifier of ubiquitous benefits and the methods of interaction. (Similar to the Visa logo, where the bank branding is not present at the point of interaction. See Colm Nelson's "MCN Brand Issues" document)
2. Support non-Scarab Sign in approach and keep Scarab as a alternative approach. For wide acceptance, a variety of flexible methods are needed. For most participants such as Amazon, Non-Scarab sign in may be used in which MCN users can sign in seamlessly using Participants existing sign in form. This eases the difficulty for MCN users' to find the MCN sign in credential from competing elements (local sign in, join now buttons, etc.). However, for Participants such as Ebay who have already accepted .Net scarab sign in approach, MCN may consider Participant's paradigm.
3. Provide ability for auto-detect authentication status. If an MCN user has already authenticated L1 (e.g., at another MCN site,) then they will not be challenged for their L1 password again when they click "checkout" and wish to access their Wallet information. They will only be required to present an L2 password If it is required by the MCN Wallet service provider.
4. Provide AOLTW/MCN branded "Verify L2 Password" page in Pop Up. AOLTW requires the user to present two levels of authentication at external (non-AOLTW) sites. The first level of authentication will probably use the participant's existing sign-in form. However, the UI for collecting the second level password should be presented in an AOLTW/MCN branded pop-up window. This will help users to understand that they are about to use the AOLTW/MCN Wallet for the transaction without leaving the context of the participant site. In the AOL client, while the first level of authentication is eliminated, UI for collecting the second level password is still be presented in a pop-up window when necessary.
5. Provide "Use Default Shopping Information" choice at "Verify L2 Password" page. If MCN users check it, they do not need to go through screens to select or enter shipping and billing information, default information or a new combination of shooping information is selected. This adds convenience to the users, and they can always change the information in the confirmation page. Default shopping information can be edited in AOLTW central site.
6. Allow Participant to get Wallet data without any MCN or Flex UI. MCN Wallet data is seamlessly inserted into participant's UI on behalf of user without wallet service provider's brand being presented. This improves likelihood of Participant adoption by ensuring minimum UI/UE impact in Participant's existing flow. For Participants who can't receive all MCN Wallet data, Flex UI needed.
7. Update Wallet when users enter or edit new data as long as they sign in with MCN Credentials. If users sign in with MCN credentials, shopping data will be saved in their MCN Wallet for future use.
8. Promote MCN ID and Wallet Sign Up only after transaction completed. If users does not have an MCN Wallet, they need to enter the shopping data to finish the transaction. Once completed, the Participant should promote MCN ID and Wallet. If the users sign up, the shopping data for this transaction will be automatically saved in the MCN Wallet for the future use. If the users do not sign up, the shopping data will not be saved in the MCN for future usage.
9. Provide AOLTW central link for authenticated MCN users to access their global information. Once MCN users sign in, they should be able to access and manage their MCN profile, wallet data (order history, bonus points, etc.) and use other MCN services (messaging, address book, calendar, shopping comparison tool, etc.) to enhance their shopping experience. This also helps Participant close sales and enhance customer support. AOL or Netscape header/toolbar may be added to Participant's page for users to link to their global information after they sign in with MCN (need to check with web property network team). Global information is presented in a pop up so users don't leave the context of Participant environment. AOLTW is presented as the primary brand and MCN is as a secondary brand.



BASIC GUIDING PRINCIPLE

- The MCN brand will be a signifier of benefits.
- The MCN brand will signify a point of interaction with the network tools and services.
- The MCN brand will be agnostic in order to facilitate broad adoption; it not will be associated only with AOLTW, but equally with all authentication agencies (AA).

UE RECOMMENDATION

1. The MCN brand should act as a secondary brand signifier at an authentication agency. Users will most likely trust and become loyal to brands that they already use, such as AOL and Yahoo. Participants who wish to become authentication agents (i.e. AOL, Yahoo) will insist on promoting their own brands whenever their tools and services are used. They will resist promoting and displaying an MCN brand. (See UE Partner Value Proposition and Privacy Best Practices documents in UE Network Specifications).

An MCN brand that is agnostic to AA's should be presented at authentication agency sites as a sub-brand –a brand secondary to the authentication agency brand. This is similar to the VISA logo presented on credit cards or credit card issuers' web sites.

2. The MCN brand strategy should imply MCN powered services. In most cases, users will continue using the tools and services to which they are accustomed. MCN can be presented as augementation to them. Whenever the MCN brand is presented, users will learn to expect a familiar experience that is comfortable and convenient with the added Network benefits.

3. MCN is a contextual entity. MCN is not a destination. MCN is an enabler of online and offline activity. Users will most likely encounter it within the context of some activity such as a book purchase or flight arrival look-up. Although users will require a central location to manage personal information, account management will ideally be an infrequent activity.

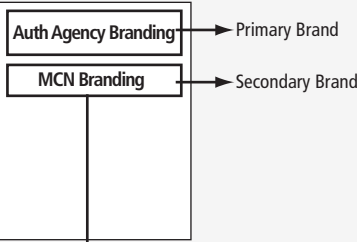
4. The MCN brand should act as an entry point for Network services and tools. AUTHENTICATION

The MCN brand signifier may also serve as a means to access an MCN sign in page. Some partners may choose a scarab approach to authentication whereby users will be directed to a co-branded (flex-ui) sign in page. In such cases, the scarab would not only signify MCN, but also a mechanism for authentication.

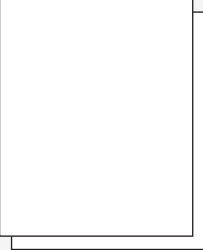
CENTRAL SITE
In the cases where users will seek to view and manage their accounts etc, AA's will need to provide a central management site (see Passport Research Summary and User Values Proposition) that is easily accessible. To succeed, MCN will need to make access to it as ubiquitous as the MCN brand. The MCN brand signifier makes for a natural gateway. (See also the MCN Profile Central Site document within this UE Design Guidelines document).

MODEL

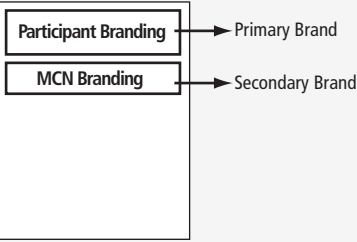
Authentication Agency Central Page



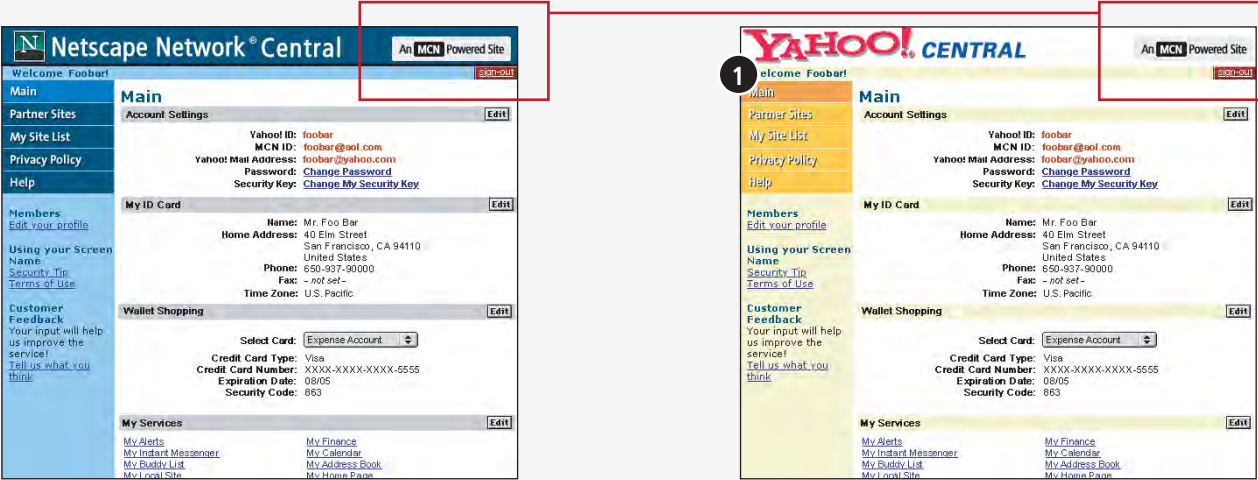
Authentication and Central Pages



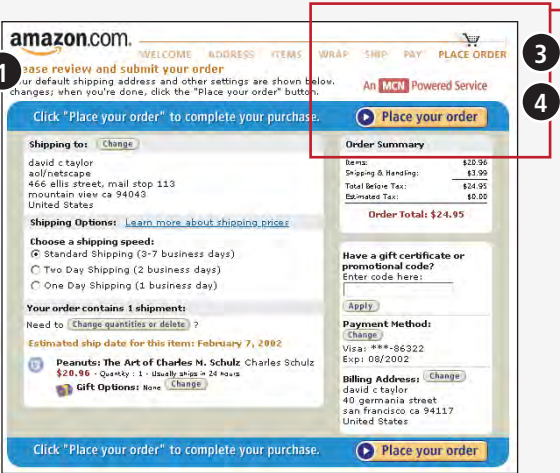
Participant Tool/Service Page



EXAMPLE



MCN Branding Element



MCN Branding Element

OPERATING AASSUMPTIONS

- NETSCAPE.COM requires TBD level of MCN infrastructure. V1 proposes use of ScreenName Service.
- Current ScreenName Service web members automatically become MCN members.
- AOL client users will need to opt-in to MCN.
- All integrated ScreenName Service Partners will not immediately migrate to MCN.

UE RECOMMENDATIONS

1. Add features to SNS that support basic MCN authentication and profile model. AOLTW controls the brand experience for SNS. If these features are in place, then AOLTW can easily rebrand SNS as MCN without significant impact on integrated SNS partners (technical issues?). This will support the "upgrade" concept from the consumer perspective. Partners who do not fully integrate with MCN at launch will at least support enough MCN functionality to support MCN brand proposition via the rebranded SNS product . Potential features include, but are not limited to:

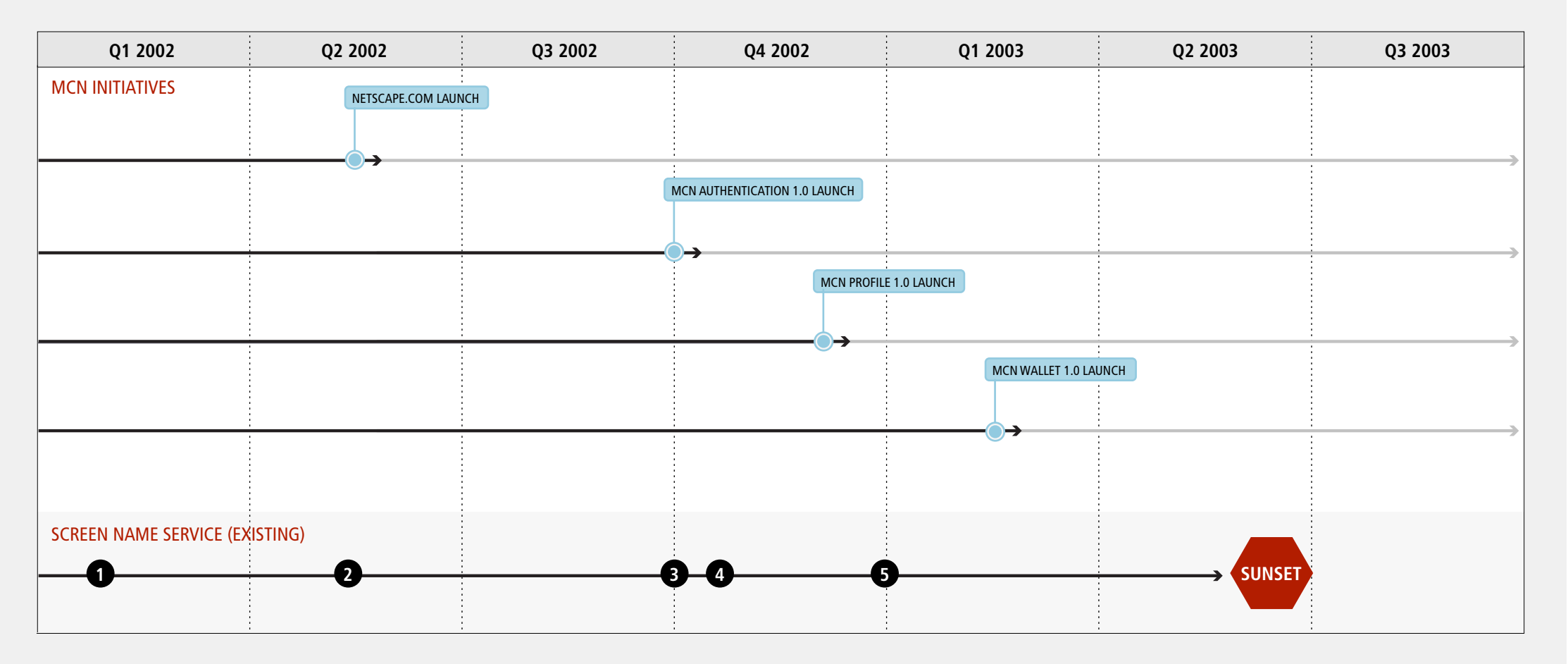
- Support for email address as authentication mechanism
- Member education at SNS home prior to transition
- Authenticate the user for mcn
- Brand affiliation designates need for "opt-in" (i.e. @aol.com requires opt-in)

2. When NETSCAPE.COM becomes an MCN implementation, sunset the SNS brand. When NETSCAPE.COM relaunches, the options are 1) to utilize the SNS and transition to MCN when MCN launches present the authentication process as a strictly Netscape Network (NN) experience and extend beyond the NN experience to external partners when MCN is further along in development. Currently, the path is to utilize SNS and transition to MCN. When the transition is made from the consumer perspective, an MCN brand should be in place so that the SNS product can be rebranded.

3. SNS and MCN should not "co-exist" from the consumer perspective. The concept that MCN is an "upgrade" of the SNS product supports the idea that SNS members will automatically become MCN members. When MCN launches, the member experience should be entirely MCN.

4. Support transition of SNS home to central control for AOLTW properties. The SNS product is modeled as 3rd party authentication and profile product that crosses the three core brands. SNS home (my.screenname.com) is currently positioned as a standalone site with SNS as the primary brand. The consumer will visit SNS home to edit their profile ("my profile"), to view partners that accept SNS credentials ("partner directory"), and to view the sites where they have become members with SNS credentials ("my site list). The MCN model relies on the AA to host these attributes in the core brand experience (see AOLTW central doc) and does not have a concept of a standalone site for central account management. The core brands (AOL, Netscape, CompuServe) should support this transition through messaging or other appropriate methods.

5. Provide new "VISA" style brand that enables the transition of SNS to MCN. The SNS brand was created around the concept of an AOL screen name as the login ID, but MCN will support other login IDs such as an email address or phone number. Ideally, the product will be rebranded as MCN when the new functionality is in place.



END
THANK YOU.

AOL QuickCheckout Shopping Password Evaluation

v2 | 8/22/02 | owner: dtaylor@netscape.com | dtaylor@aol.com

overview

Executive summary

The current implementation of the QuickCheckout (QC) Shopping Password (SP) for AOL subscribers effectively functionals as a barrier to purchase completion rather than a barrier to consumer fraud. AOL should simplify the QuickCheckout experience, potentially removing secondary authentication entirely- and more thoroughly test the revised design with users.

Barriers

- Little or no promotion (exisiting promotion is unfocused and sometimes inacurate).
- Little QC presence on merchant sites.
- Inconsistent partner implementation of QC.
- Users forget their SP.
- Users forget answer to 'forgot password Q and A.
- Users too easily locked out of account during password enty. No recourse if account locked.
- Little or no effective online help - be it by Help section of Shopping Assistant.
- Difficult to access QC and SP knowledgeable Member Services Rep.

1. Premise of Shopping Password Unsettling

That QC requires AOL subscribers to create and use a Shopping Password implies that Screen Name passwords provide inadequate security. "Why not just make sure my Screen Name password is so secure that I don't even *need* a Shopping Password."

2. Shopping Password Creation Burdensome

- Users don't necessary understand the value of a SP.
- Users are wary of undertaking an additional QC 'set-up' procedure.
- Creation process sidetracks users from central goal of making a purchase.
- Some transactions cannot be completed until a SP is successfully created.

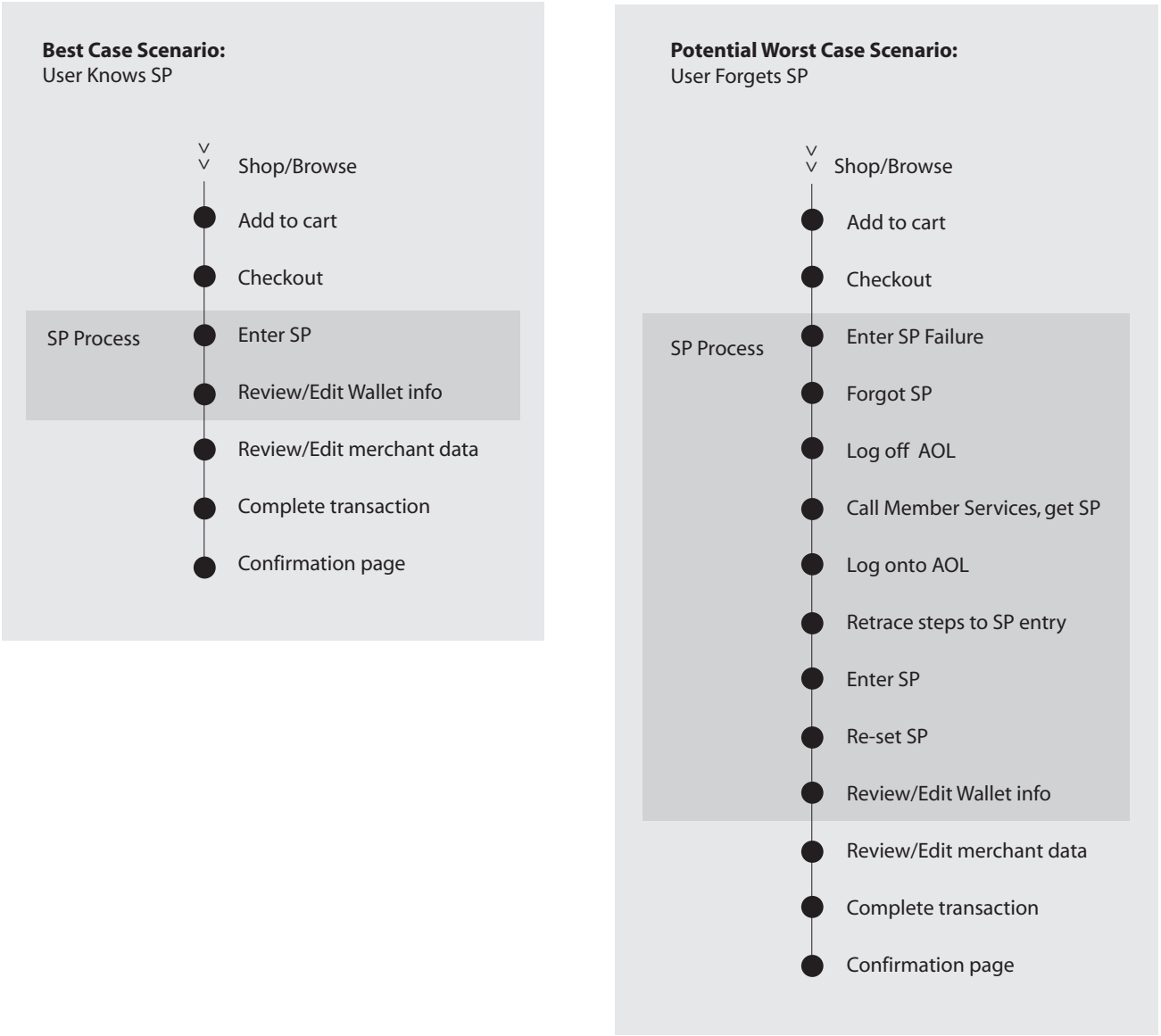
3. Unknown or Forgotten QC Account

QuickCheckout suffers from lack of recognition by AOL subscribers (*and* web users). Users are surprised –sometimes unpleasantly– and confused to discover that they have QC accounts. In a recent study, more than 50% of users *did not even realize* that they had previously set up a QC account, did not know their SP and were forced to retrieve it. Of these, one user was locked out of his QC account and was unable to continue. 25% of users remembered they'd set-up QC accounts, but could not remember their SP. Some confused it with their Screen Name password.

4. SP Retrieval Leads to Drop-off

A forgotten SP may be retrieved via a "Security Q & A" query (ie, "Name the town where you were born) or by telephoning Member Services (MS). This additional step can lead to users becoming sidetracked from the purchase process. For example, users with a single phone line may be forced to sign out of AOL, telephone MS (wait in queue, explain problem, etc) and retrieve SP, then sign back into AOL and retrace their steps to their shopping cart and return to the SP entry page. In another scenario, a user who mis-answers the Security Q & A is locked out of his account for 24hours and unable to complete a transaction

flow analysis



MCN UE Design

MCN Hosting and Entry Points

DRAFT

dtaylor@netscape.com
dtaylor@aol.com

11.20.02

Overview

Document Goal: Define UI approaches that we will support in V1.

In the product definition phase, several approaches (1-4 below) have been identified to support an MCN UI flow. The UE team has been operating under the assumption that all four approaches must be supported but recent discussions indicate that this may not be the case for all products (auth, profile, wallet, alerts).

The purpose of this document is to define the approaches, illustrate some flow issues related to the approaches, and to move towards resolution on which approaches will be supported in V1. The goal of the document is not to move into a granular detail, but to define the key considerations so that the product teams can finalize requirements. This will allow the UE team to eliminate unnecessary tasks and provide a more detailed schedule.

Topics for consideration (these will be defined in the following pages)

MCN user entry points, participant site. Determines whether the user will enter an MCN product flow or a local participant flow.

1. **Scrab approach.** Similar to today's approach with SNS and QC - The partner integrates a branded icon or link on their site. The user must click the branded icon or link in order to use the MCN product.
2. **Non-scarab approach.** Does not require the user to click on a branded icon. The participant can be proactive in leading the user to an MCN flow.

MCN participant flow. The MCN product flow at the participant site that is enabled by the AA and Service Providers.

3. **MCN hosted (flex) UI.** The AA and Service Provider hosts the MCN product flow. The participant can customize the flow to fit the participant look and feel. SNS provides this flow today.
4. **Participant hosted (integrated) UI.** The participant hosts and provides the UI for the MCN flow. MCN feeds data to the participant via server to serve interaction to enable user flow. The participant UI also collects data and writes back to MCN. MCN prompts and visual cues will be present in the flow that inform the user that it is an MCN flow and that provides access to MCN central management tasks.

Each option should be considered and defined in relation to these specific flows:

- Sign In flow
- Registration flow
- Wallet flow
- Wallet edit
- Opt-In flow

Questions

What's the Menu for V1?

The table, left, demonstrate the variations that up for consideration. If the table at right represented a "menu" for MCN, what are the options? Who gets to pick from the menu?

Key questions:

1. Can we absolutely reject an approach for UI flows? For example, if our prime objective is for participants to host the UI, but there are some participants that must implement the "MCN hosted" UI, then we will need to support both. The same is true for scarabs - if some participants or SP's want to support the scarab approach, and some do not, then we still need to define rules for both approaches.
2. In the event that we support both options will the AA and SP be able to define "hybrid" flows. I.E., Authentication team decides that a participant is not trusted to host the sign in UI, but the Wallet team decides that the participant can host the wallet UI.
3. What's the implementation cost of each approach? Is an MCN hosted "flex UI" easier for participants to implement than a server to server participant hosted UI?
4. Would a "hybrid" approach increase implementation costs for the participant?
5. How many participants do we expect to request the "Participant hosted" UI option in the time frame of MCN 2.0? Can we eliminate this option for MCN 2.0 and support it in the next release or when a marquee participant requests the option?
6. Participant choices in relation to which method to implement. Are there elements that will require MCN to host the UI? For example, if trust is an issue, and a participant is not trusted to host the "opti-in" UI, then the participant would not have the choice to enable a fully hosted participant UI.
2. Brand issues for MCN 1.0 to MCN 2.0. We'll introduce the MCN brand in 1.0, which will rely strictly on the scarab approach. If we eliminate the "scarab" approach for MCN 2.0, will participants be able to integrate a "non-scarab approach"? Would they be willing to do so?

Key considerations:

1. Scalability of the product. An "MCN hosted (flex) UI" flow must be standardized to some extent so that participants can implement once for multiple AA/SP's in the future. However, this will place burdens on the AA/SP to conform to standards.

MCN user entry points, participant site

	Scarab Approach	Non-Scarab Approach
Authentication		
Transaction		
Alerts (?)		
Other service (?)		



MCN participant flow

	MCN hosted (Flex) UI	MCN hosted (Flex) UI
Sign In flow		
Registration flow		
Wallet flow		
Wallet edit		
Opt-In flow		
Alerts flow (?)		

MCN user entry points, participant site

Scarab approach

A scarab is a branded element that allows the user to indicate that they wish to use a third party facilitator at a participant site. Today's approach (SNS, QC and competitors) requires the partner to place a branded icon on their site - the user must click the icon in order to use the product at the partner site. Today's approach is flawed because it is inflexible, but an improved scarab approach may still be the cleanest method to enable a user to use the MCN product at a participant site.

UE recommendation

1. Revise the scarab approach to be more flexible. This may mean more types of scarabs for specific purposes (i.e. join, register) and different forms (i.e. branded hypertext link). It also means revising the rules for return visitors (i.e. once user has established MCN relationship with site, enable seamless interactions based on authentication state rather than forcing user to click button).
2. Provide a scarab approach in some form, even if the non-scarab approach is supported at the participant site. Refer to flows, pg (?) for more detail on why this will be necessary.

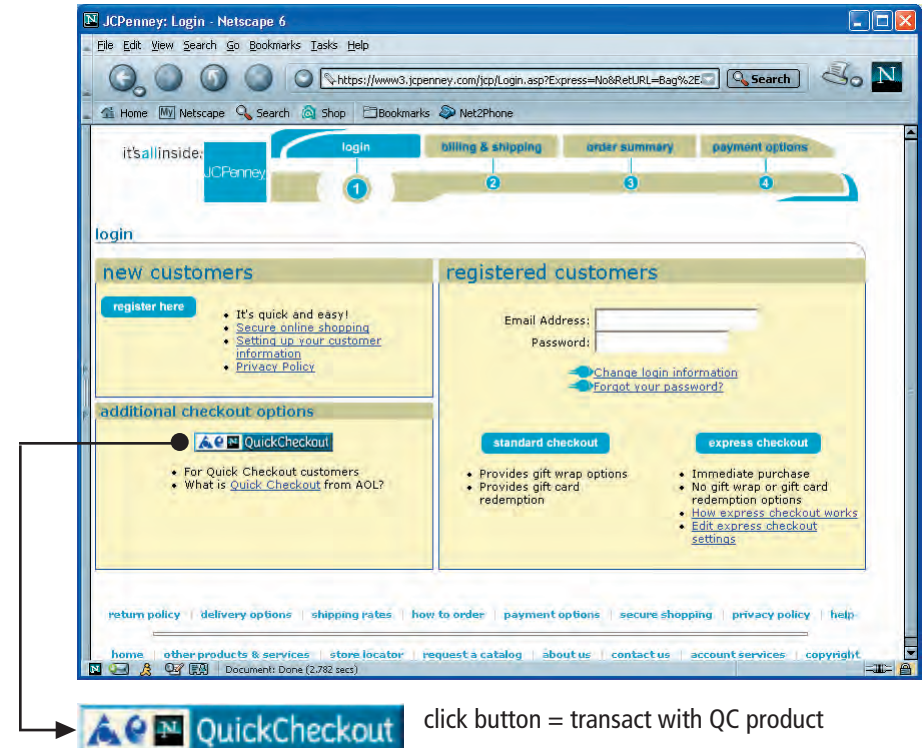
Example of scarab approach, authentication scenario



click button = sign in with SNS screen name

click button = sign out of SNS product

Example of scarab approach, transaction scenario



click button = transact with QC product

Examples of competitor scarabs

Microsoft authentication scarabs



Microsoft transaction scarab



Yahoo! transaction scarab

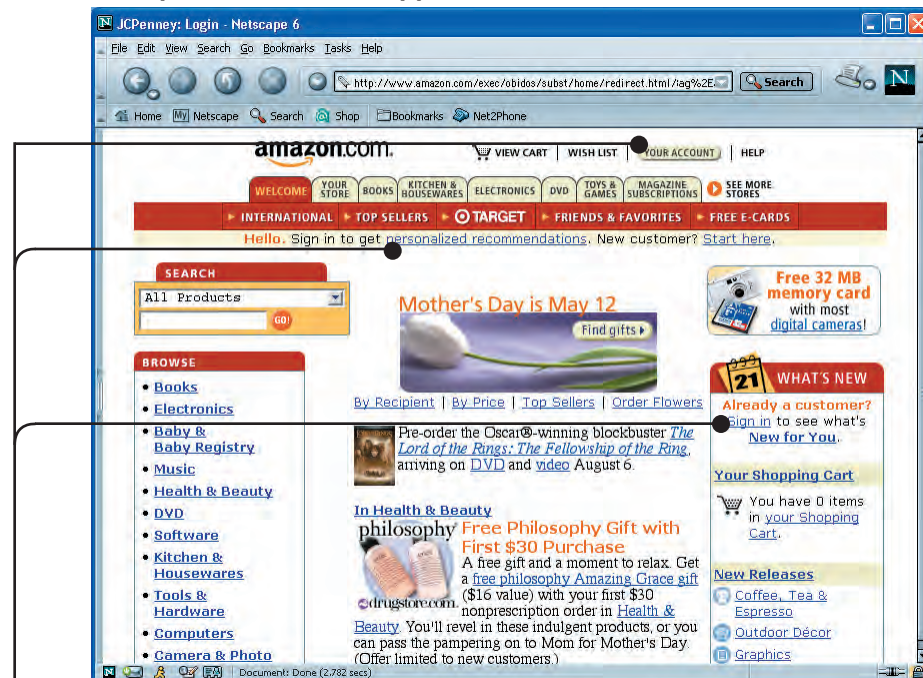


MCN user entry points, participant site

Non-scarab approach, detection based

Enables the participant to lead the user to the MCN flow without requiring the user to click an MCN branded element. For example, the partner may lead the user to MCN through generic "sign in" or "join" links. Another example may allow the user to use the MCN product by clicking the participant's "checkout" button during a standard flow at the participant site.

Example of non-scarab approach, authentication scenario



→ User clicks on any of these links

Based on detection, proactively authenticate the user with MCN credentials. Conditions apply - see "content site flow", pg (?) for more detail.

UE recommendation

1. Utilize this as a supplement to the "scarab" approach. The non-scarab approach can work, but it is too conditional to be successful as the only method (see flows, pg ?). The participant should be allowed lead the user to the MCN product if the conditions are right, but the user should still have a method to choose to use MCN credentials at the participant site if conditions fail.

Example of non-scarab approach, transaction scenario



→ User clicks on "proceed to checkout" button

Based on detection, proactively authenticate user with MCN credentials and provide MCN wallet for transaction. Conditions apply - see "transaction site flow", pg (?) for more detail.

MCN user entry points, participant site

Non-scarab approach, user initiated

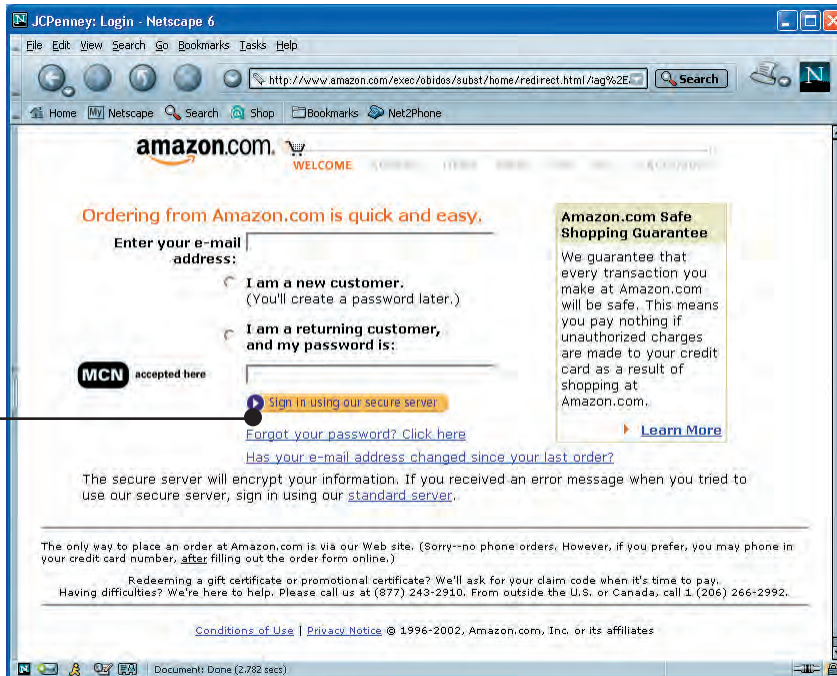
User can enter MCN credentials in the local (participant) sign in fields to authenticate as MCN user at participant site. The participant must implement MCN branding that indicates that the credentials are accepted. The brand should be clickable and provide information about MCN if clicked.

NOTE: Dependent on participant hosted sign in UI.

UE observations (recommendations not yet available)

1. The branding is similar to a "scarab" approach from the participant perspective - it still requires the participant to integrate a brand into their site UI.
2. This approach places a heavy burden on the user to understand the model. The local sign in page could feature any label, and it is not very clear what to do to utilize MCN. Take this example - there is an option for "new customer" and an option for "returning customer". For the MCN user who is new to the site but has an MCN wallet they'd like to use, neither label describes an actionable path.

User enters MCN credentials in participant hosted UI



User enters MCN credentials and clicks "submit" button

An authentication sequence identifies that the credentials are MCN credentials and leads the user to the next step in the MCN flow.

MCN participant flow

MCN hosted (flex) UI

The MCN hosted approach requires the participant to point to an MCN AA or an MCN Service Provider for UI to supports MCN tasks. The “flex” feature allows the partner to host customized templates for the flow, which will be called for the page build to provide the “look and feel” of the participant site during the flow. We already support this with SNS, but QC does not have the “flex” feature for hosted UI.

UE observations (recommendations not yet available)

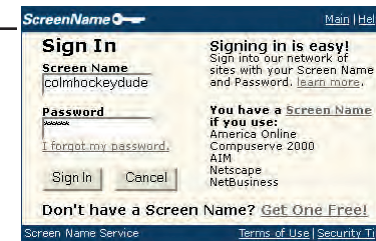
1. The current flex model for SNS is all provided by one product, therefore the UI is all provided by one product, which enables a consistent user flow. Alternatively, the model for MCN treats each AA and Service provider as a separate product. A user path may cross several products in on interaction. In order for this approach to be successful, there may need to be some standard requirements placed on Service Providers.
2. If the flow and modules are not standardized to some extent, it will be very difficult for participants to integrate with MCN (imagine requiring the participant to create custom templates for multiple service providers if the template rules are different for each service provider).

MCN hosts the page, the participant provides customized templates



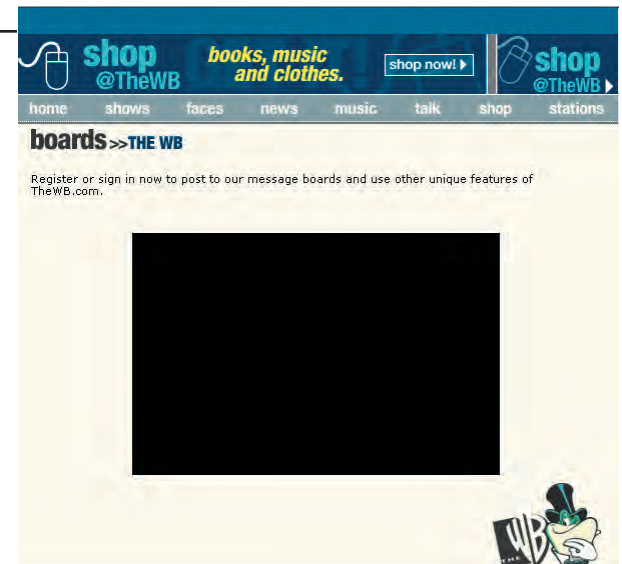
SNS module

SNS provides a UI “module” that is consistent in width. All modules are consistent in width, but vary in height depending on module contents.



Customized Template

The partner builds a customized template and designates a space for module placement.



MCN participant flow

Participant hosted (integrated) UI

The participant hosts the UI for the MCN flow. Data is exchanged on the backend to facilitate the user interaction. In the case of write to MCN scenarios, the participant collects the data in thier form and pushes it to MCN. In the case of read from MCN scenarios, the participant pulls data from MCN and populates in thier form. MCN branding and prompts are available to facilitate MCN aspects of the flow.

UE observations

1. It will be very difficult to achieve consistency related to brand placement and MCN prompts for this type of flow. It is very difficult to enforce brand requirements that rely on participant implementation. This can translate to a difficult user experience if elements are not always available during a participant flow.

MCN provides data to participant, participant populates data in UI

Choose a shipping address
Is the address you'd like to use displayed below? If so, click the corresponding "Ship to this address" button. Or you can [enter a new shipping address](#).

colm c nelson's Address Book

Ship to this address
judy nelson
823 morningside drive
jeffersonville, IN 47130
United States
[EDIT](#)

Ship to this address
colm nelson
2431 richmond drive #4
santa cruz, CA 95062
United States
[EDIT](#)

Or enter a new shipping address
Be sure to click "Ship to this address" when done.

Full Name: _____
Address Line 1 (or company name): _____
Address Line 2: _____

MCN Data provided by MCN

Select a payment method.
Is the credit card you'd like to use displayed below? If so, please select it using the button to the left of the card name. You can also enter a new credit card, pay by check or money order, or use an Amazon.com gift certificate or promotional code. Click Continue when done.

MCN Data provided by MCN (you can review this order before it is final)

Payment Method Credit Card No. Expiration Date Cardholder's Name

☒ MasterCard 18459 04 2003 colm nelson

Or enter a new card

☐ Visa _____ 01 2002 _____

☐ Amazon Credit Account _____ Does not expire _____

Note: Using a Visa Check Card? Select Visa. Using a Eurocard or MasterMoney card? Select MasterCard.

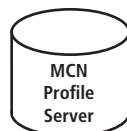
☐ Pay by check or money order (or check funds on account)

Want to pay by purchase order? Learn more about our [Corporate Accounts program](#).



user: Foo

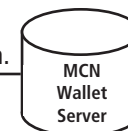
authorization granted to
share data with Amazon



Foo's shipping addresses.



Foo's credit card information.



NOTE: diagram has been simplified to illustrate MCN population of data in participant UI. Diagram may not be architecturally correct, and final model for V1 may not define shipping addresses as coming from the profile service.

Content site

Non scarab approach with MCN hosted Sign In UI

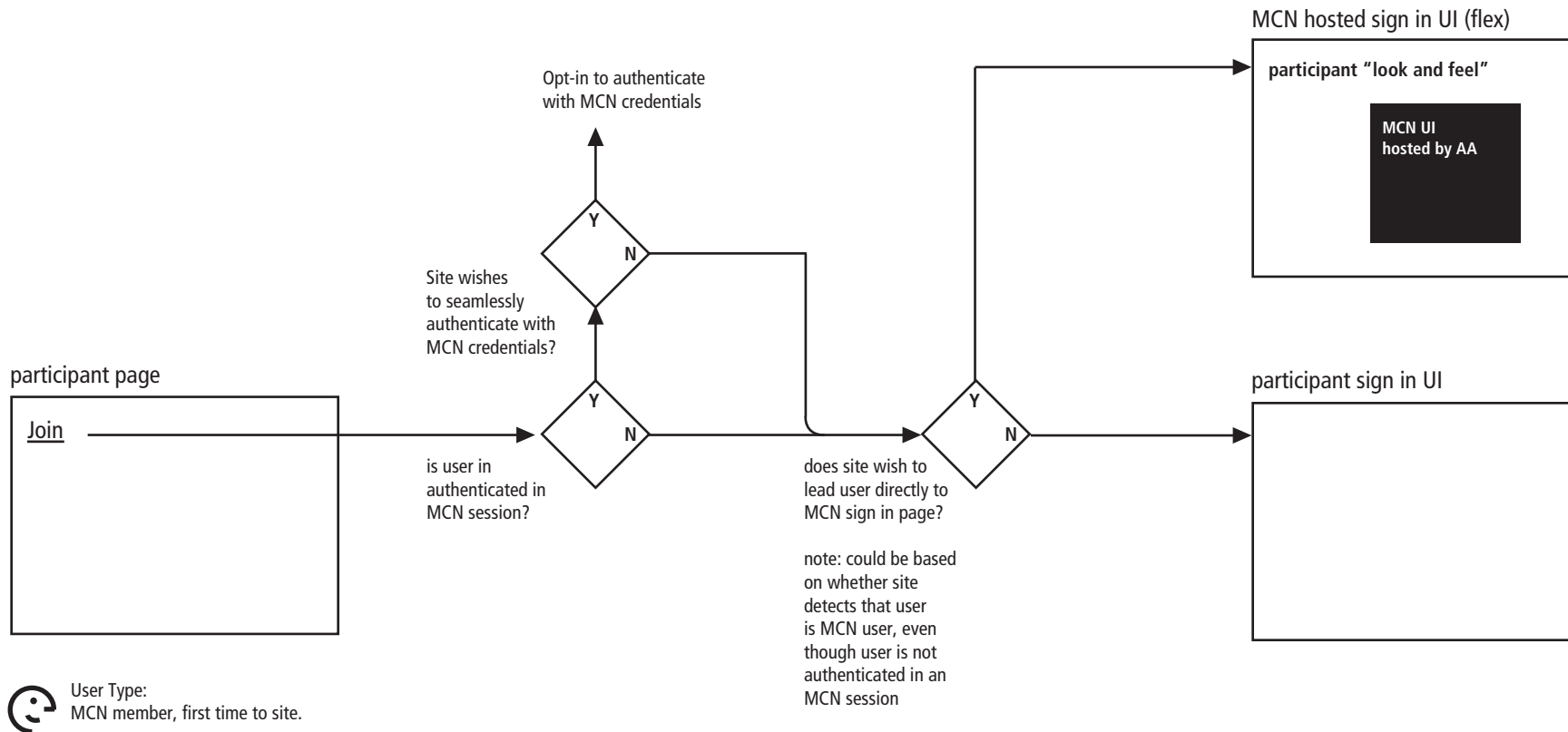
Eliminating the "scarab" requirement allows the participant to choose how to lead the user to the mcn authentication step. For example, the participant can lead the user to the MCN signin page via a generic "Join" or "Sign In" link .

Participant Configuration

- Non-Scarab
- MCN Hosts UI
- Supports Local sign in and MCN sign in

Issues

1. If the user is MCN authenticated, and the site wishes to seamlessly authenticate user, an "opt-in" page will be necessary.
- 2.



END

THANK YOU.