Case Study:
Online Personal Loan Scenario v.01

Author: Domenico Catalano

Introduction

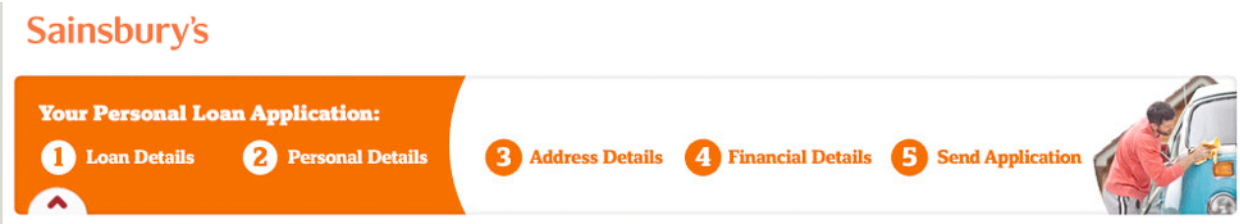
Personal Information sharing is an emerging trend for online personal daily life activities, including the interaction with financial credit, insurance, healthcare, etc..
A typical situation is when a Subject, in order to obtain a specific online service from a Service Provider, must agree for sharing personal information with the SP itself.

This use study analyzes a specific scenario for a financial credit interaction for an online personal loan request.

Problem Scenario

Online Personal loan request is a life typical use case in which a Subject requests for a personal loan to a Financial Service.
The Financial Service, to approve or reject the loan request, must verify many Subject's personal information from different Service Provider (Host). For instance, the amount of monthly user salary (i.e. 3 last monthly salary) from user's Employer, user bank account information (account number, net) and they need to access to the user credit score from a Financial Risk central service.

The following picture shows an example of all the typical steps for an online persoanl loan application by Sainsbury's (UK).



The problems with this scenario are many, and we provide the following classification based on the party which is afflicted.

Financial Service	Subject
Gathering Subject's information from distributed resources.	Multi-step Form-fill based request.
Privacy disclaimer and Subject's consent to manage personal information (depend ing on country's legal framework).	No control on what information will be revealed for what purpose and with which parties (privacy).

Trust relationship based on registration step, or through loyalty card (pre-registered).	Lack of autorization mechanisms to protect distributed personal information.
Human intervention to verify Subject's personal information.	

Proposed Improvements
UMA protocol helps to:
- Reduce sensibly human intervention through automated discovery and gathering of Subject's information.
- Give control of the personal information to the Subject through the Authorization Manager interface and analytics features.
- Introduce a claim-based authorization mechanisms to enforcement Subject's policy to prevent unauthorized access to the resources.
- Enable Trust relationship among the parties through bind obbligation and UMA trust model.

UMA applicability can leverage on three different constellations, depend on how the Subject interacts with the Financial Service:
- Person-to-organization
- Person-to-organization mediated from a human agent
- Person-to-Self

In this study we discuss the Person-to-organization constellation which involves autonomous client application to reduce at minimum the steps of process and human intervention.

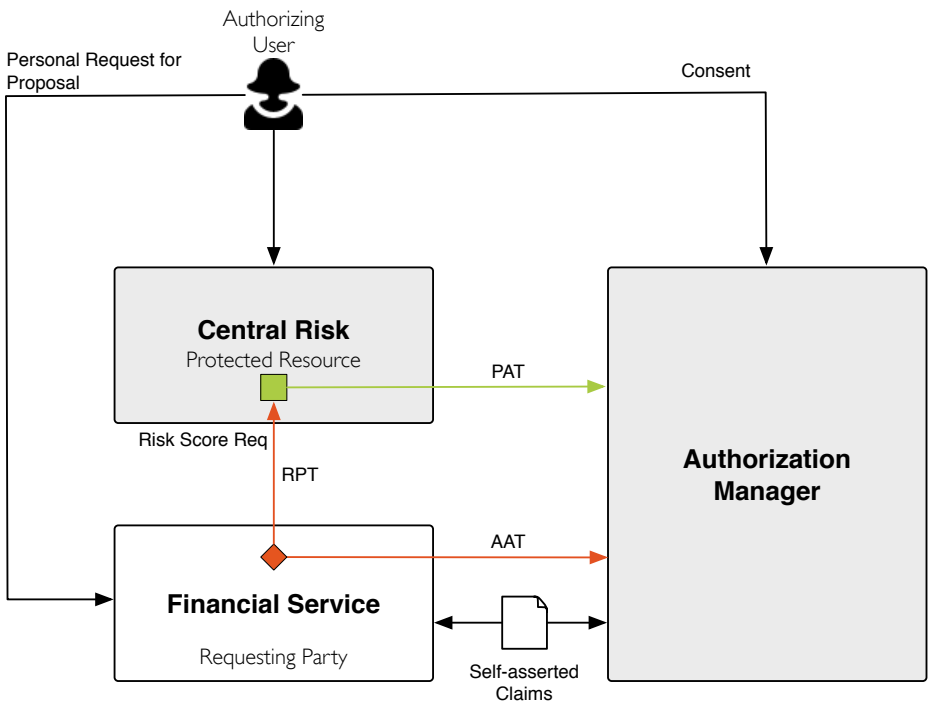
Solution Scenario

Online personal loan request represents an Autonomous person-to-organization sharing UMA scenario.
The diagram below shows the interactions among the parties:

Assumptions:
- The Subject (Authorizing User) has registered the Central Risk host service with the Authorization Manager (AM). The Central Risk obtains a PAT.
- The Subject has definied a claim-based authorization profile at AM for Online personal Loan request or she can leverage a standard profile for "life" activities.

Trust Model
- Central Risk is an accreditated organization by a central financial authority.

- The Financial Service acts on behalf of an operator which must present third party verified claims, or sign a self-asserted claims based on the Subject's profile policy.



Financial Service acts as autonomous web service client and AM should support server-to-server interactions based on JWT, using JSON Web Signature (JWS). The client application creates a JWT and signs the JWT with the private key and then sends the token request (in the appropriate format) to the AM.
Cryptographic materials, including public/private key could be generated by third-party PKI infrastructure, under a trust framework or directly by the AM through a dedicate registration phase.

Solution Flow

The sequence diagram below describe for the Online personal request process, based on UMA solution flow.

1. An unregistered user (Authorizing User) interacts with the online Financial Service for requesting a personal loan.
2. The user select a specific loan target and "apply with copmonkey" Authorization Manager (AM) service, with which he has an account.
3. Financial Service redirect the User to the AM for discovering service and authorization process.
4. The user login with AM and authorize the request
5. AM redirect the User (User Agent) to the Financial Service with references to the protected resource (Central Risk) that they need to access.
6. Financial Service attempts to access to the Central Risk protected resource with not valid Requester Permission Token (RPT).

7. Central Risk creates permission on the AM service for this request and redirect the Financial Service to the AM.
8. Financial Service requests a valid RPT at the AM, using an Authorization API Token (AAT).
9. AM challenges the Financial Service to provide a promissory claims to ahdere at User's authorization policy.
10. Financial Service provides the promissory claims
11. AM releases a RPT
12. Financial Service access to the Central Risk resource with a valid RPT.
13. Central Risk provides the risk score attribute for the user
14. Financial Service approves or rejects the request based on this attribute.

Solution Demo

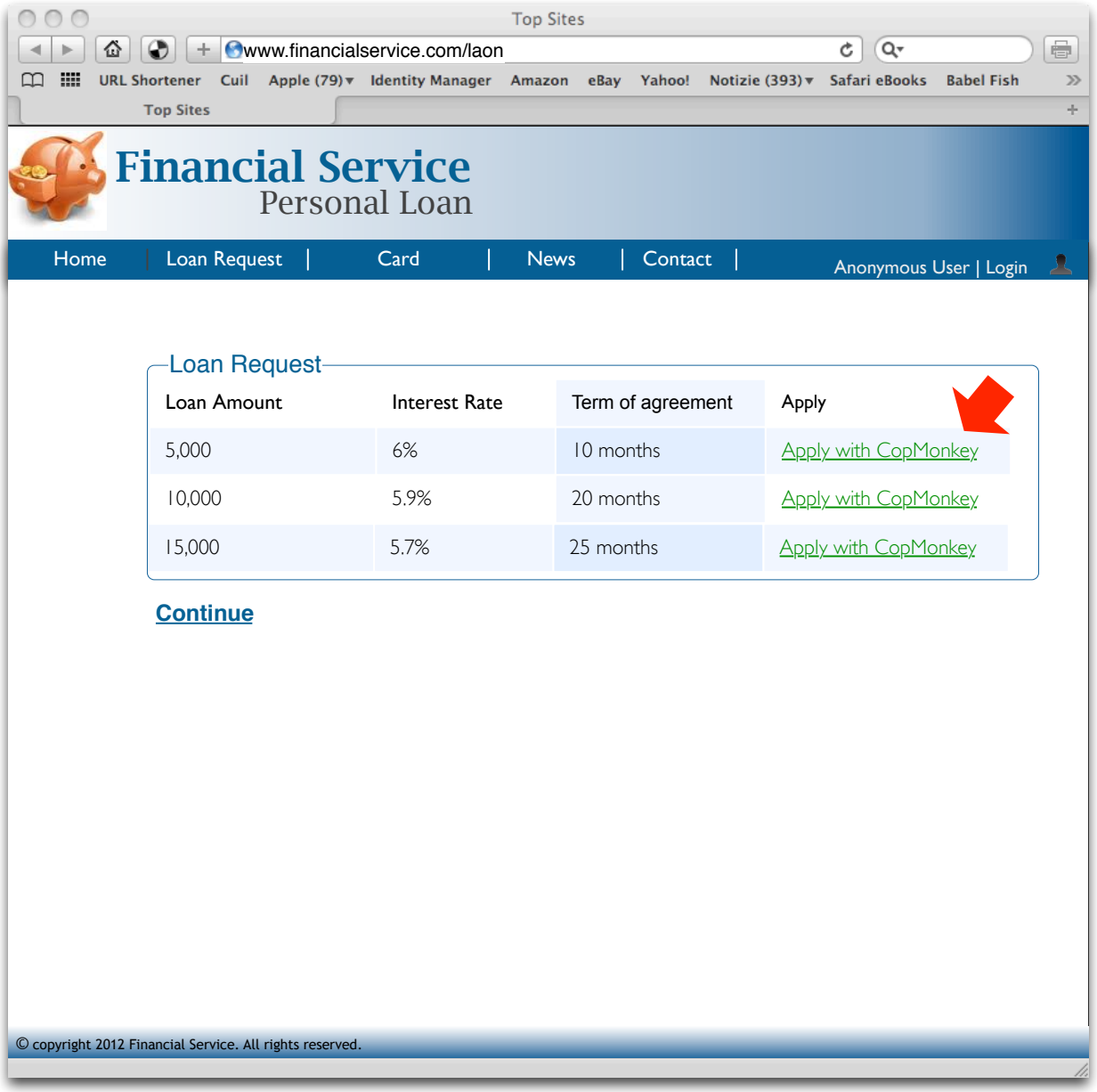
Optional section showing screen shots and/or giving info on existing UMA-based implementations, deployments, etc. for addressing this problem

The following screen shots describes the user experience for the online personal loan request based on the solution flow, including:

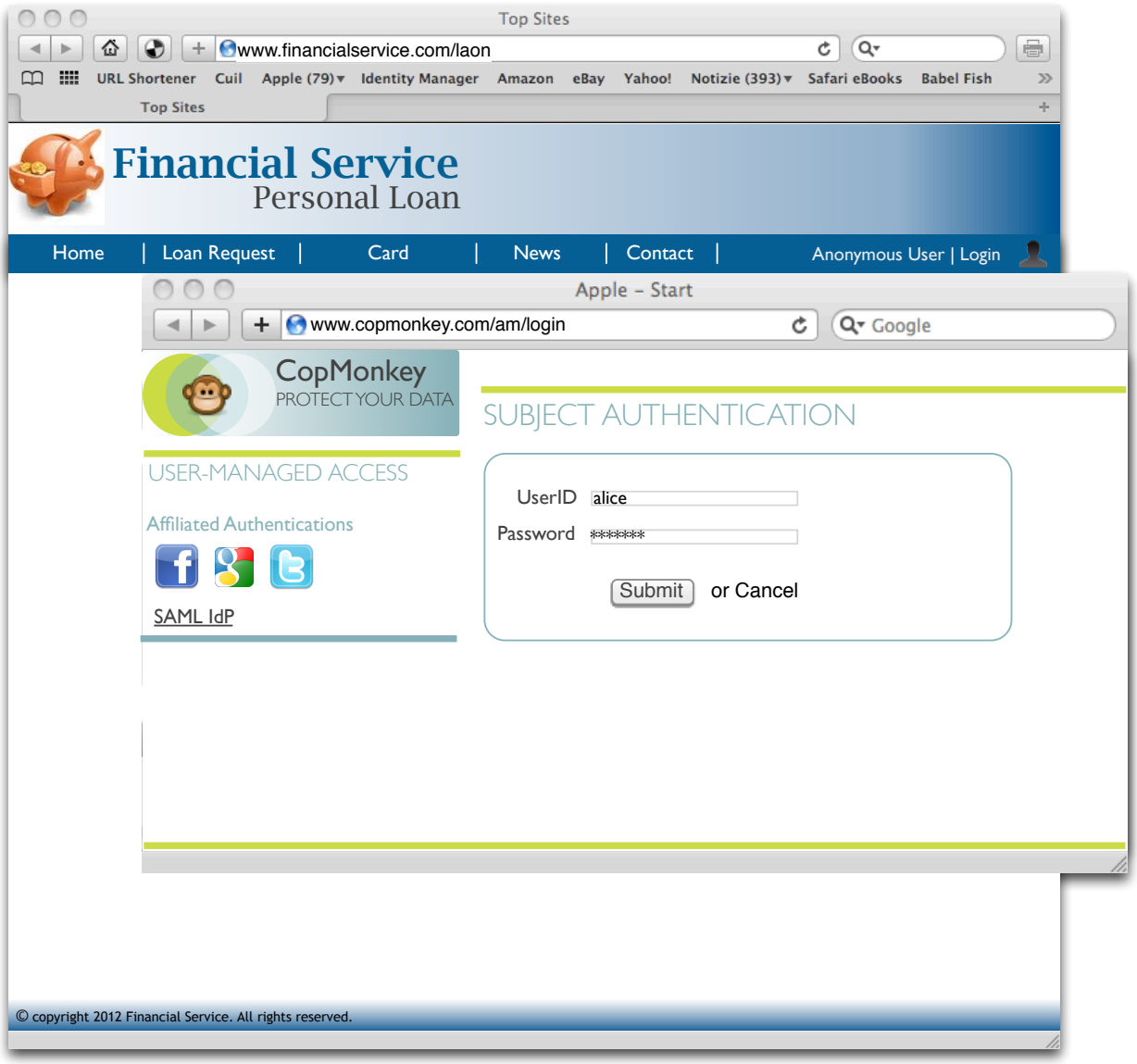
1. The Financial Central Risk protected resource at CopMonkey's Authorization Manager.
2. Financial Service's interface for applying online personal loan request, based on one-click "apply with copmonkey".
3. User Authentication at CopMonkey/AM site.
4. Authorization process and user consent at CopMonkey/AM site.
5. User's personal details visualization at Financial Service.

CopMonkey/AM interface and Protected Resources

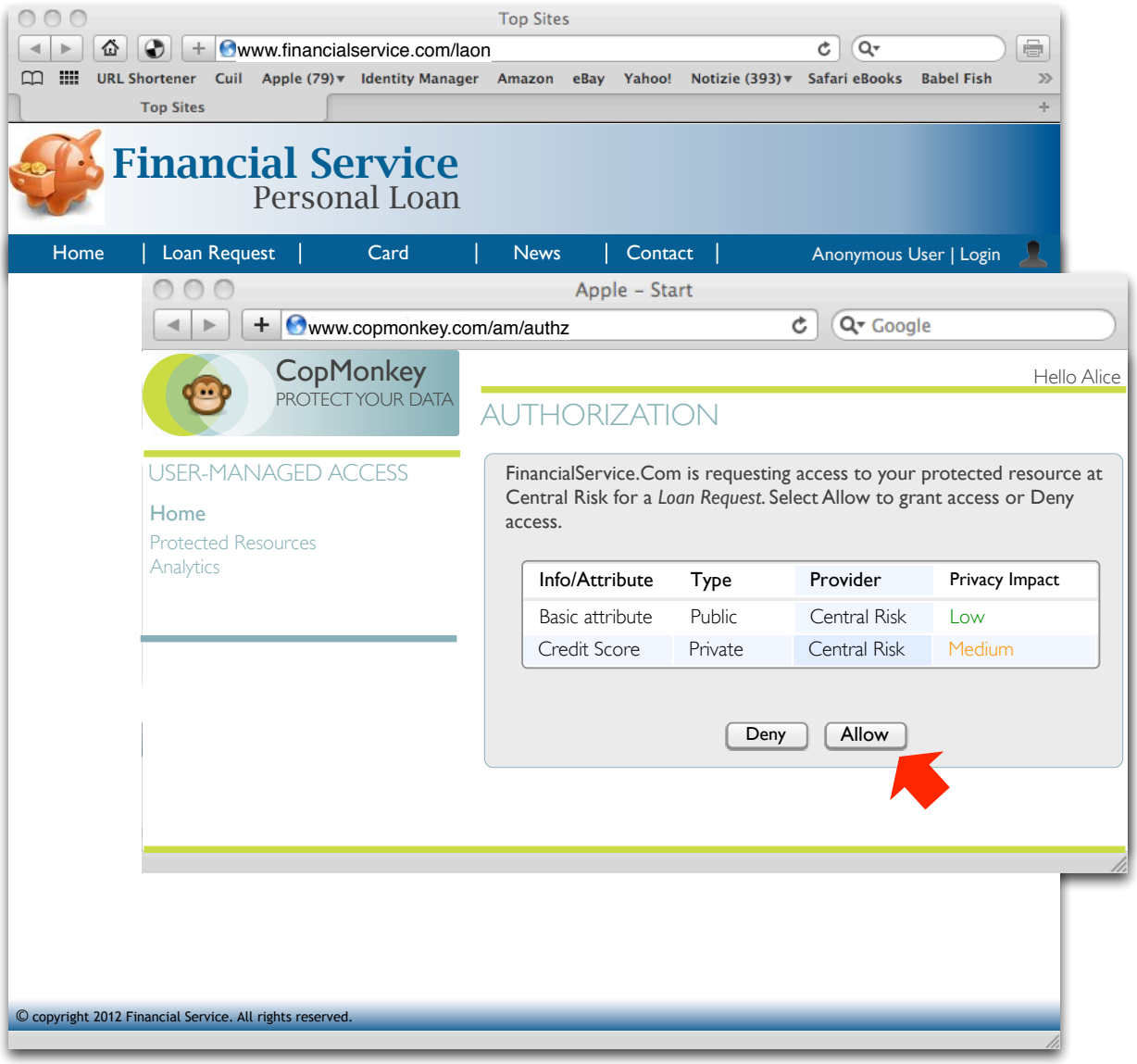
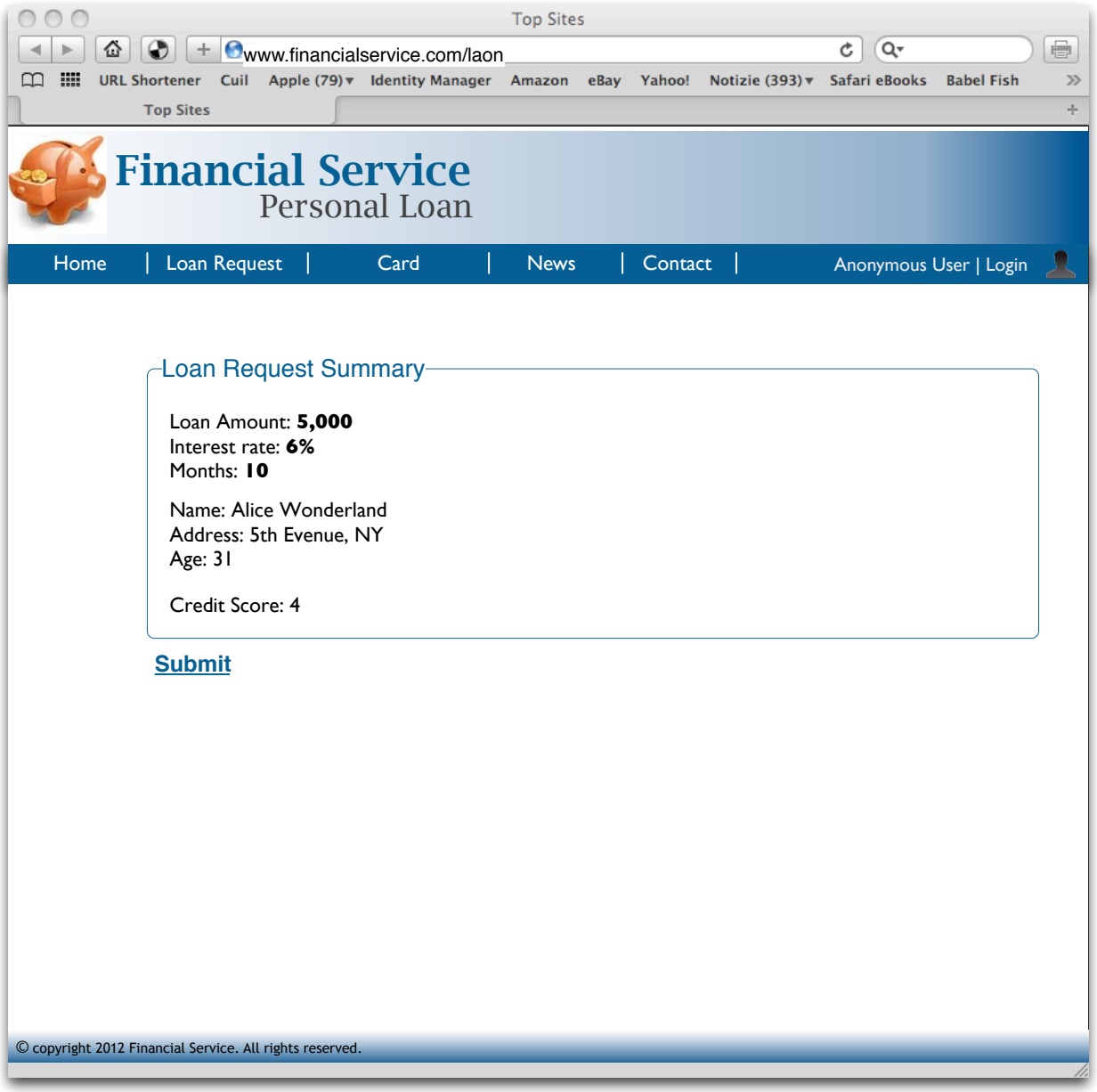
Financial Service's page and Online Loan request process



User Authentication at CopMonkey/AM



User Authorization process at CopMokey



Visualization of the user personal details at Financial Service