protected inbox scenario

Scenario: Protected Inbox(pending)

Submitted by: Joe Andrieu

Problem Addressed

Individuals often want to receive incoming communications from companies but do no wish to release general contact information which could allow anyone to engage in unwanted spam, telemarketing or junk mail. The problem with existing correspondence channels are that there is no incoming access control, so once an endpoint is revealed (an email address, phone number or postal address), all control over incoming messages is relinquished. The result is an unending mess of unwanted and illegimate messaging, this is particularly problematic online, where the marginal cost of sending email is negligible and the enforcement of fair practices essentially non-existent.

Proposed Solution

To address this, the protected inbox presents an incoming service endpoint for ongoing communications, protected by an UMA authorization manager. Individuals can establish incoming policy based either on specific authorizations, group permissions, or other role-based access. In an enhanced scenario, users could also establish policy based on frequency and type of messages, for example, allowing a particular vendor to send a monthly promotional message on a limited schedule while allowing that same vendor to contact at any time for safety or quality recalls or alerts. In such a scenario, users could also allow the vendor in question the opportunity to view the nature of their authorization, so that the vendor could align their outgoing attempts at communication and thereby avoid unnecessary failed attempts to reach the individual.

Although out of scope for the initial UMA specification, one could easily see scenarios where the access control is also used for non-http-based services such as SMTP or RSS.

For the attached diagrams, we assume that the Terms requested by the Authorization Manager simply require sufficient credentials to authenticate the vendor. We do not specify how those authentication credentials are generated. Further, we do not specify how a vendor would self-assert terms regarding the purpose of communications, as this capability will likely be deferred to a future version of UMA.

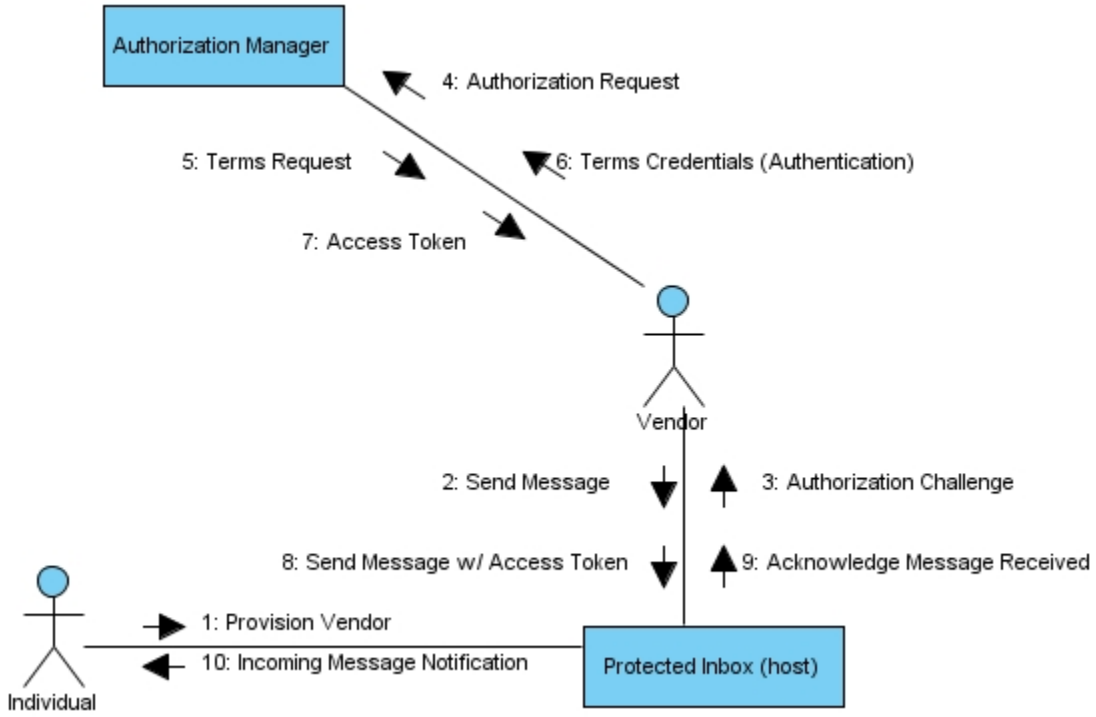
Distinctive Aspects

1. The protected resource is an always-on incoming communications endpoint, rather than "content" or "data" to be released to the Requester.
2. Users may disable a Requesting Party's ability to contact them through the protected inbox simply by updating the policy at the Authorization Manager.
3. (future) the policy for allowing access to the protected resource could be group or role based.
4. (future) the policy for allowing access may specify purpose requirements and limit frequency of access.
5. (future) users may allow the Authorization Manager to reveal to the vendor the purpose requirements and frequency limits associated with their use of the service.

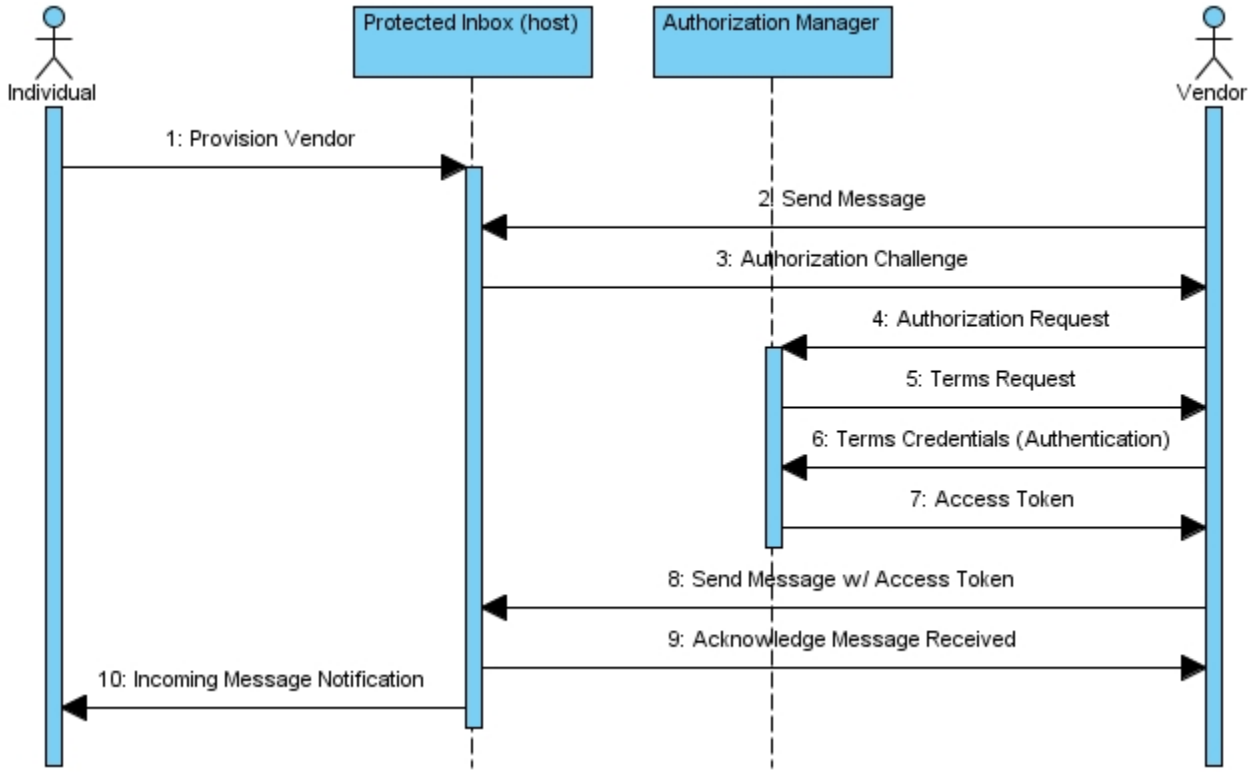
Actors

1. Individual as User
2. Vendor as Requesting Party
3. Communication Service Endpoint as Host (hosting the protected resource of the endpoint)
4. Authorization Manager

Communications Diagram



Sequence Diagram



User Story

Sally recently used a fourth party pRFP Broker, "BuyingNow", to post a personal RFP for a new car. The RFP was distributed to a specific list of contacts or "Vendors" with return communications to Sally's protected Inbox at "Messages, Inc.". Each Vendor is known to BuyingNow and are able to access BuyingNow's web services with an authenticated identity. When Sally published the pRFP, she provisioned BuyingNow as an Authorization Manager for her Messages, Inc. service.

After receiving notifications of the pRFP, several Vendors accessed the pRFP, hosted at BuyingNow as a UMA protected resource. One such Vendor, "Cars R Us", uploaded the details of the Sally's request into its CRM system and, after automated analysis of Sally's reputation and financial credentials (provided as part of the pRFP), escalated the request to a Customer Contact Specialist, aka, a sales person.

Through their internal CRM system, the Specialist researched their inventory and sent a question to Sally to better understand her needs. To send that message, the Cars R Us CRM system accessed a protected SMTP resource hosted by "Messages Inc.".

BuyingNow authenticated the CRM system and authorized access to the SMTP server, which accepted the incoming message for Sally. Sally was notified through her phone that she had an inquiry – as per her standing preference at Messages, Inc. for messages coming through Buying Now. She activated her mobile app and answered the Specialist's question.

Unfortunately, the subsequent proposal from Cars R Us didn't meet Sally's needs and she removed Cars R Us from the authorized vendor list at Buying Now. After that, Cars R Us was unable to contact Sally, as the only contact information they had was the protected SMTP resource. Sally was able to winnow her list of vendors down and negotiate a great price for her new car without exposing her email address to potential SPAM leaks.

New Questions

1. This use case suggests the possibility for multiple AMs for a single resource. Sally wants to authorize BuyingNow as an AM for her Messages, Inc. service while she's shopping for a new car, but most of the time, she uses "MyFriends" to make sure only her friends can send her messages. Can the current system handle multiple active AMs for a given protected resource?