General Overview

Version 1.2 – 26. March 2018
Author: Vittorio Bertola – vittorio.bertola@open-xchange.com

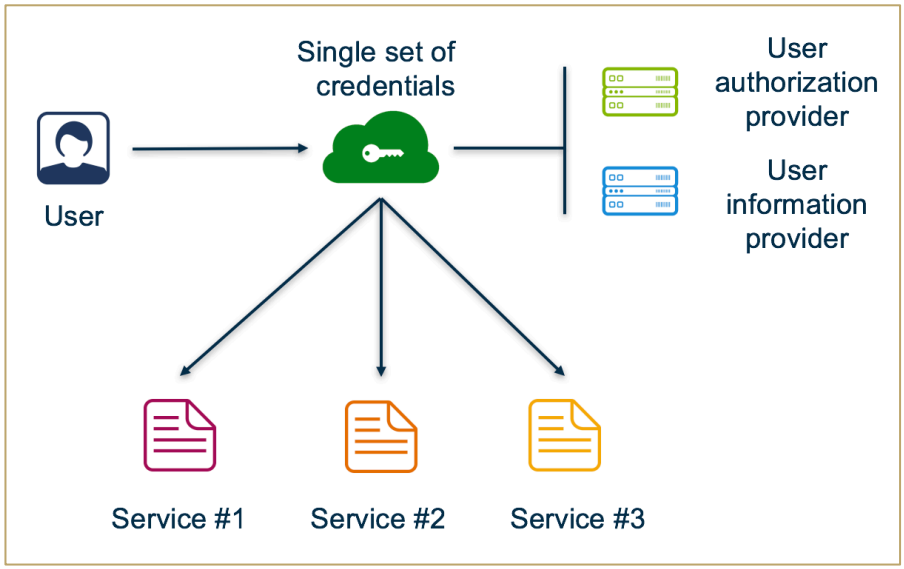
SCOPE OF THIS DOCUMENT

This document describes the basic features, motivations and advantages of the proposed ID4me system.

THE BASICS

ID4me is a public, open, federated digital identity service that aims to provide two main functions:

- Authorization of a user for access to any third party accepting ID4me identifiers ("single sign-on" on an Internet scale);
- Controlled communication of the user's personal information to the third parties accessed by the user.



THE PROBLEM

The main problem addressed by ID4me is how to manage the hundreds of usernames and passwords for online services that each of us has; most people solve this by re-using passwords across services, which is an insecure practice, and even impossible due to varying password requirements. Also, every time you want to use a new service you need to register and enter all your information again; and if you want to change your password, you need to change it manually dozens of times, one for each different service.

Existing global single sign-on services have several shortcomings. The government-run ones (e.g. the European eIDAS project) are usually complex and not widely adopted; also, people do not need (or even want) to provide their complete official personal information to all the websites they visit. The OTT-run ones (e.g. *"login with Google"*, *"login with Facebook"*) are not privacy-friendly, as they come from companies that live off monetizing user information; they allow these companies to track the user's online activities, and require the user to accept the terms and policies of these companies, unilaterally imposed. Also, there are now dozens of competing similar services, up to the point of cluttering the user interface in web login forms, and they do not interoperate.

The ID4me identifier, consisting of a valid DNS hostname (or, potentially, of an email address), would allow users to log into any online service via a single account, similarly to the OTT-run services, but would also allow users to choose the manager of their identifier among any number of compatible providers.

A user that owns an ID4me identifier can use it to log into any website or online service supporting ID4me, even without prior registration; on first access to that service, the service can request access to the user's personal information as entered by him into his profile; if the user consents to this access, the requested information will be made available to the service, which can thus automatically create a local account or profile for the user, associated to his ID4me identifier.

Like email and other public Internet standards, but unlike any existing global single sign-on system, the ID4me service is federated, meaning that multiple interoperable providers of identifiers can exist, including personal providers self-hosted by their users, and that all of them are intrinsically supported by any online service implementing the ID4me standard. Users are free to pick any provider and (if they control the domain name that the identifier is in) to move their identifier to a different one whenever they want, simply by changing a record in the domain name's zone.

ID4me is, in itself, a "weak" identity standard; the purpose is to ensure that the user of a given identifier is always the same that initially acquired that identifier at registration. Accordingly, there is no authentication of the user's identity, and his personal information is entirely self-declared, as it currently happens for most online registration systems. Also, users are free to have multiple identities (e.g. a personal one, a business one etc.). The standard may however be extended to support third-party validation of the user's personal information and thus provide stronger proof of the user's real world identity.

THE BUSINESS VALUE

ID4me wants to promote a free, global, competitive market for the provision of online identity services, including non-profit offerings and self-hosting options. It does not want to rule a closed market, but to promote a public infrastructure and an ecosystem from which the market can evolve freely. Also, as a side benefit, ID4me is meant to promote the use of the DNS and the sales of domain names.

Mimicking the business architecture of the domain name industry, the provision of the ID4me service is broken into two parts; the identifier is jointly managed by an *"identity authority"* (the registry), which acts as trust anchor, manages the user's password, validates the logins and manages consent for data sharing, and by an *"identity agent"* (the registrar), which owns the relationship with the customers and manages their data.

Internet service providers of any kind (domain name registrars, telcos, hosters, access providers…) willing to provide ID4me identifiers to their customers could do so in several ways. They could supply identifiers for free, maybe bundled with other services as an innovative feature, or they could introduce them as a paid upselling offer. They could provide identifiers inside their own domain names, thus promoting their brand in the customer's online identity and gaining some degree of lock-in, or they could sell users a personal domain name, thus creating a new revenue stream. They could choose to only run the agent part, partnering with an existing identity authority and benefitting from their credibility and trust, or they could run both parts on their own, maybe extending their existing internal single sign-on system.

To foster adoption and remove barriers to market entry, ID4me builds on public and open standards (OpenID Connect and DNSSEC) and releases all its specifications as open, royalty-free standards, submitting

them to the appropriate Internet standardization bodies. Entities already running single sign-on systems based on OpenID Connect should be able to extend them to provide ID4me identifiers quite easily.

SECURITY AND PRIVACY CONSIDERATIONS

An important competitive advantage of ID4me, in addition to its simplicity of use, is that it is more secure and more privacy-friendly than the existing solutions. Even if there is a potential security and privacy issue in centralizing all logins into a single sign-on system of any kind, in practice the current typical behaviours are much more insecure and easily trackable than what would happen with ID4me; and ID4me includes several mechanisms to minimize the risks attached to login centralization.

In comparison to the current practice of multiple usernames and passwords, ID4me allows the user to only have one password, so that he/she can focus on memorizing a single, stronger string of characters. The password is never exchanged with any party other than the identity authority; identity agents and online services never get to see it, eliminating the risk of password leaks if a site is cracked, and also preventing online services from stealing the password and trying to use it to impersonate the user elsewhere. Also, any further security measure (e.g. two-factor authentication) only needs to be implemented by the identity authority, and becomes immediately effective for logins to any service. Finally, if the password is leaked in any way, it can be immediately changed in one single place.

In respect to the current OTT-provided single sign-on services, ID4me allows the user to choose and change the provider and the location where his/her data are kept, avoiding vendor lock-in and promoting competition, also in terms of security and privacy. If the identity authority becomes insecure or starts to violate the user's privacy, the user (if controlling the domain name) just needs to move the identifier to another provider; this helps preventing the unauthorized monetization of the user's personal information. Also, users are free to have multiple identities, potentially with multiple providers, and so they can isolate some activities from others or even have pseudonymous identities, while several OTTs require you to only have one account or to validate your true identity.

Finally, ID4me also includes specific features to give the user full control and information over which pieces of information are entered into the account and over which ones are shared with each of the online services that he is logging into, including, in future releases, a way to update or delete the information remotely.