## Hyperty Trust and Security Model

This document gives an overview on the Hyperty Trust Model as well as on Hyperty Sandbox runtime execution environment.

It should be noted, that [Hyperty Service Development Framework](development-of-hyperties.md) to be used to create new Hyperties, abstracts Developers from the Hyperty Trust and Security Model described in this document including lower level Identity Management APIs. Details about how to develop Hyperties is provided in [this](development-of-hyperties.md) document.

Hyperties are securely associated to User Identities selected by the end-user himself. Hyperty Users are human beings (including group of human beings e.g. corporation) or things (including group of things and physical spaces e.g. a smart home or smart building).

Hyperty Trust Model extends [WebRTC Identity model](https://w3c.github.io/webrtc-pc/#sec.identity-proxy) where Identity tokens are generated, inserted in intercepted Messages sent by Hyperties and validated by recipient Hyperty Runtimes before delivered to the target Identity. These identity management procedures are performed according to applicable policies managed by the end-user.



Hyperty Trust Management

### Identity

As the necessity to manage identities over the internet has increased, so does the number of solutions to help achieve that objective. Not only for the Internet, but also for large companies with a great number of workers exists the necessity to do a proper Identity management of all them. This digital identity as will be explained below is an identity created from the need to provide an authentication from someone or something, and is used in different ways by diverse systems that requires some sort of identity. Over time several solutions emerged, to fulfil specific problems in projects, mainly because distinct obstacles require different approaches. The following introduces the concept of Identity, and how it can be used.

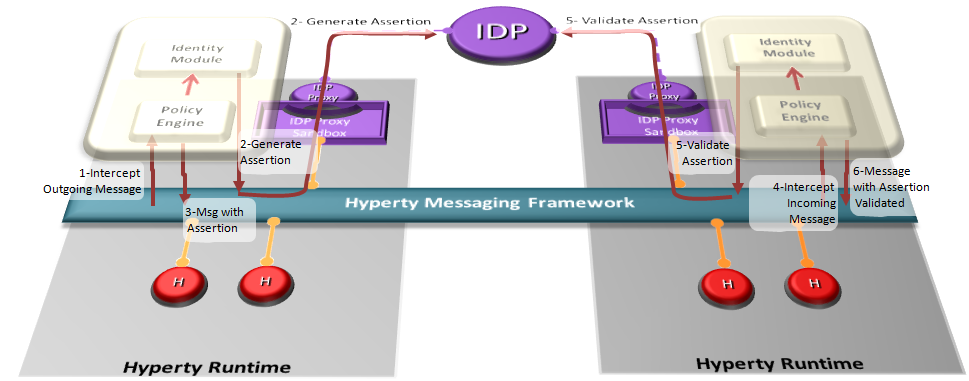
### User Identity

In our modern society, technology is ubiquitous, and transactions are evermore accomplished using digital technologies without the need to involve physical contact. An example of this situation can be observed in money transactions, where a few years ago if someone needed to make a bank transfer, it would require that person to move personally into a bank agency to order it, and in current days these money transfers can be performed using a smartphone. Since identification binds a person identity with the respective individual attributes, an authentication of identity is required. Given this, and since the majority of the current transactions are performed digitally, we need, a sometimes called, digital identity to prove who we are in remote communication. This concept of Identity comprises two important information security mechanisms, the authentication and authorization. In a short description, the authentication is an identification followed by verification. In this identification process an entity supplies its identity, while in the verification process, the identity provided is checked before the system. Therefore, the correctness of an authentication strongly depends on the verification procedure employed. The authorisation is the decision to allow a given identity to execute or access a certain resource. Access control to a service or system, can be achieved based on authorisation mechanisms, where is possible to define the access rights or policies for each Identity, thus making it possible to decide to allow or deny a particular action based on an identifier or attribute. This appears as an interesting solution if the system requires having access restrictions. Traditionally, the authentication is performed with something a user knows (like a PIN or a password) or holds (such as a key, or a magnetic card). But there is another method, biometrics, which can be used to authenticate users. Biometrics are automated authentication methods based on measurable human characteristics, such as voice samples, fingerprint, or facial features. However, biometric methods do not typically allow for remote authentication. As such, it is herein not considered.

### Identity Module and IdP Proxy

The Identity Module (Id Module) is the [Hyperty Core Runtime](https://github.com/reTHINK-project/dev-runtime-core) component responsible for handling the user identity and the association of this identity with the Hyperty instances, in order to make Hyperty instances identifiable. The identity in the reTHINK project is not fixed to a unique Identity Service Provider, but obtained through several different Identity sources. With this approach, the Id Module provides to the user the option to choose the preferred method for authentication. This module will thus able to support multiple Identity acquisition methods, such as OpenID connect 1.0, Kerberos System, or authentication through smart cards. For example, a user with a Google account can use the Google as an Identity Provider to provide Identity Tokens, which can be used by the Identity Module to associate it with a Hyperty instance. Identity proxies are considered to act as intermediaries between the Identity Module and the specific Identity Provider Proxies (IdP Proxy), promoting a more flexible and adaptable solution. The IdP Proxy is the [IDP ProtoStub](hyperty-messaging-framework.md#protocol-on-the-fly-protofly-and-protostubs) that is responsible to handle the communication between the Identity Providers and the Identity Module.

The following figure illustrates this interaction:



Interaction between the Identity Module and the Identity Provider

### Runtime Sandbox

The hyperty runtime implements sandboxing mechanisms that ensure the correct isolation of client JavaScript code (i.e., Hyperties, ProtoStubs, and Applications). Isolation means that client code is confined to execute within the address space of an independent sandbox. As a result, sandboxes prevent potentially malicious code from interfering with client code instances in co-located sandboxes or from accessing external resources in the surrounding environment (e.g., files, network, etc.). Communication outside the sandbox is possible through well defined channels. Both sandboxing mechanisms and communication channels implemented by the hyperty runtime are available to the application programmer throught specific APIs and are dependent on the targeted platform.

For the browser platform, sandboxing is enforced by leveraging native mechanisms provided by the browser API. The core runtime components execute inside an iFrame. The iFrame implements the core sandbox by isolating the code of the core runtime from the main window in which the application javascript code is executed. Application code is therefore prevented from accessing directly to the memory address space of the core runtime. Communication between application and core runtime is possible only through a single and well defined entrypoint which allows them to exchange messages: method postMessage(). Hyperties and protoStub execute as independent Web Workers. Web Workers effectively isolate their internal states from each other and from the core runtime. The postMessage() method constitutes the only communication bridge between the these components.

For the standalone platform, the sandboxing mechanisms we employ are similar to the browser platform. The main difference is that, instead of using a browser, we leverage Crosswalk to support standalone applications. Crosswalk is an HTML application runtime that allows us to execute the hyperty runtime as native mobile applications in Android and iOS devices without the need to install a full-blown browser. Mobile applications only need to be bundled with both Crosswalk webviews and the hyperty runtime code. Since a Crosswalk webview implements a Chromium-based runtime, it can seamlessly execute the hyperty runtime code that was implemented for the browser platform.