Conference Abstract

Interacting FDOs for Secure Processes

Peter Wittenburg[‡], Christophe Blanchi[§]

‡ Unaffiliated, Berlin, Germany
§ DONA, Geneva, Switzerland

Abstract

In modern industry, administration and research there are many processes that involve distributed actors needing to securely create, update and manage information. Typical examples for such processes are supply chains in production industry and treatments in the medical area. Such a process can be characterised by a few key properties:

- they are driven by discrete events in time that need to be recorded
- they allow different authenticated actors contribute to state information
- they must guarantee that existing information cannot be overwritten
- they are characterised by a high degree of automation

Not all applications will require that all properties be met, there are also workflow processes in the research domain, for example. In this paper we will discuss the use case where an FAIR Digital Objects (FDO) is used as a digital surrogate for a physical product, specifically to act as a Digital Product Pass (DPP) which is an electronic document that fully describes the properties of a given product with its own unique global identifier. Each digital object surrogate can then be represented by rendering its ID as a QR code which can then easily be scanned by a client to access information about the object or to interact with that object. To constrain the scope of our example, we will only discuss what happens when a product leaves the factory, is put on a truck together with other products and is shipped to a destination. The requirement in our case is to adapt the DPP so it includes the

greenhouse gas emissions incurred by the product during its shipment. In this process we basically have the following events:

1. the product is identified and its manufacturing details specified.
2. the product enters the truck and is detected and
3. the product leaves the truck.

In all three events some interactions and information updates need to be executed automatically, i.e. we assume that the product is associated with a sensible identity which can be read by a sensor coupled with an IoT edge device on the truck.

In the general case, our model describes interactions between FDOs where any FDO can potentially interact with any other FDO as their physical objects interact in the physical world. Any FDO that can authenticate itself using a Public Key Iinfrastructure challenge and have the proper credentials will be able to add to the state of another FDO. Whenever two FDO interact, each FDO can register the interaction as an event FDO that is recorded at a location specified within each FDO. The ability to register an event can require a different sort of authentication and access control but a simple validated digital signature from the creator of the event is a simple yet effective way to control access.

Our example includes 3 entities the factory (F), the truck company (TC) and a third party that acts as trusted entity (TE) to manage shared information. Each entity is represented as an FDO containing a public key that it can use to authenticate itself as well as a certificate of that key from a trusted entity. The factory instantiates a Product FDO (FDO-Px) for each product and based on an agreement with the trusted entity a DPP for that product-(FDO-Dx). The truck company also instantiates a Truck FDO (FDO-Ty). Each FDO has a public key and a certificate. This certificate would reflect the agreement between the factory and the truck company that authorizes each other to be able to create event FDOs (FDO-Ez) used, record each encounter between their FDOs, and potentially the option to extend the DPP FDO (FDO-Dx). Each FDO also has its own set of methods which can be executed, and which make use of secure communication and exchange their public key.

The first interaction is triggered when the product enters the truck and is detected by the truck's edge device. This edge device is configured to cause the FDO-Ty to register an event by invoking a pre-determined method and passing the ID of the product it detected.

1. FDO-Ty has a few methods that allow it to inform FDO-Fx about the event and will probably have access to create some information in the truck company's database.
2. FDO-Px will have methods to update the appropriate database in the factory so that the factory can trace what happened.
3. FDO-Ty will also be able to create an event FDO FDO-Ex using the FDO-Px event method and trigger clock to wait on a message from FDO-Px.
4. When both FDOs have informed the event FDO that a specific event type happened, the FDO-Ex will use a method to update its event table and the event is signed by both keys.

The second interaction happens when the product leaves the truck and the truck's edge device sensors notice this action. The same procedure will happen again with one extension: (x1) Now the truck FDO-Ty will do some computations according to some algorithm instantiated by the truck company about the additional GHG emissions associated with the transport of the product (x2). This will cause the DPP FDO, FDO-Dx, to update a data structure maintained by a trusted party.

The benefits of this method are as follows:

- All digital surrogates are FDOs and provide a standardized access method.
- All structures are encapsulated and can only be manipulated by tested methods embedded in the corresponding FDOs.
- Methods are extensible and are themselves defined as FDOs.
- All events will be signed by the keys of both parties involved making them authenticated and traceable.
- The systematic use of PIDs makes it possible to follow each action by appropriate analysis functions that have the right to read using methods in the corresponding FDOs.
- The system can be easily extended to different scenarios and different numbers of actors involved

Keywords

FAIR, FAIR Digital Objects, Data Tracking, Digital Twins, Secure Data

Presenting author

Christophe Blanchi

Presented at

First International Conference on FAIR Digital Objects, presentation