D. Hühnlein, H. Roßnagel, C. Schunck, M. Talamo (Eds.): Open Identity Summit 2016,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2016 81

Public Online Services at the Age of MyData: a New Approach to Personal Data Management in Finland

Teemu Rissanen[1]

Abstract: MyData is a framework and model for a human-centric approach for managing and processing personal information in the context of online services. The MyData approach is based on the right of individuals to access all data collected about them in public and commercial records. The core principle driving the MyData effort is that individuals should be in control of their own data. The MyData approach aims at strengthening digital human rights while opening new opportunities for businesses to develop innovative personal data based services built on mutual trust and respect of digital privacy rights in a positive way. The Finnish Trust Network (FTN) is a circle of trust composing of nationally notified Identity Providers (IDP) and notified identity service Brokers. It is a technical and legal framework under which different notified IDP's are mandated to provide strong authentication services for Finnish citizens and residents that can access public online services in Finland, in compliance with the provisions of the eIDAS regulation. As a whole, the FTN and MyData networks offer a new platform for reorganising public online services for the 21st century.

Keywords: eIDAS, eGovernment, OpenID Connect, MyData, open data, public online services, user centric data management, consent management, privacy protection, interoperability.

1 Introduction

When we talk about the knowledge or the information society, we can think of "information" as data about and related to a user, whereas "knowledge" as data that is inherent to a user. Therefore the transition from the information society to the knowledge society cannot be achieved unless information about the user becomes inherent to the user, i.e. as an integral part of how a user interacts online with the society and its services. We can call this a user-centric approach, by which we mean a paradigm shift from personal information that is managed in relation to a user, to personal information managed by a user, or with the consent of the user. It is a paradigm shift because it affects how online services should be delivered, designed and developed.

In this paper we present the MyData approach which offers an innovative and practical framework for delivering online services and managing personal data from a user-centric point of view. We will also introduce the Finnish Trust Network (FTN), which is a cloud-based mechanism for connecting large scale, consumer facing services with trusted identity and service providers. The Trust Network follows the requirements and objectives of the European eIDAS regulation for a network of trust service providers enabling Citizen-to-Business-to-Government secure and trusted

[1] Teemu Rissanen, CISM, EuroConseils SPRL, teemu.rissanen@simplysecure.be

electronic service provisioning. The Network is built upon strong privacy and security principles and enables a user-centric attribute consent model.

The MyData initiative is one of the Finnish Government's Spearhead projects as part of the Big Data initiative that is funded by the Ministry of Transport and Communications [HK15]. As a part of the Government's strategic planning with regards to the adoption of policies defining use of Big Data in public services and overall in the regulated society, MyData is seen as a key component in the development of next generation public online services. One of the aims of this policy work is to align it with the EU's forthcoming Digital Single Market initiative, which should address the issues of data ownership, access, interoperability and accessibility as barriers to free movement of data and services across the EU.

In the Finnish eGovernment architecture, the FTN forms the backbone for all trusted, notified and officially accepted ID's in Finland. The aim of the FTN is to offer a standard and interoperable framework for IDP's and Service Providers to offer identity and trust-providing and trust-consuming services for both public and private organisations, with support for cross-border services. In the eGovernment context, the MyData infrastructure is aimed at bridging data flow gaps that exist between public and private service domains, by inserting the citizen / user / consumer in the middle of the data flow puzzle.

We argue that together, the MyData infrastructure and the FTN circle of trust for public and private online services, form an innovative solution for delivering public online services and managing trust in an open multi-stakeholder environment. As both the MyData infrastructure and the FTN circle of trust are at a development stage and no public services that build on them is available yet, this paper aims at envisioning how the future of public online services could and should be delivered in a user-centric and identity-driven way.

2 The case for identity driven user-centricity in public online services

User-centricity has been a very important design concept in popular social media services, but public online services have not put serious design efforts to change their traditional service delivery models. Social media services have also successfully implemented user identity-driven solutions where user accounts form the key for service aggregation. These solutions are dominated by strong industry ecosystems such as Google, Apple or Facebook. Public online services have occasionally taken some advantages from service aggregators but their proprietary nature and lack of identity assurance frameworks limit their usability whit regards to public services. Identity-driven integration within public services has been limited in the use of unique identifiers which are used to connect different personal data sets stored in various databases. This model has different implementation models depending on national legislations on the use of unique identifiers.

The main driver for both identity-driven and user-centric online service models is the increasing economic value of personal data in the digital economy. The Boston Consulting Group [Va12] has calculated that the value created through digital identity could increase at a 22% annual growth rate and applying personal data can deliver a 330 billion annual economic benefit for organisations in Europe by 2020. According to the study, the consumer value of digital identity for consumers will be even bigger (670 billion) and the combined total digital identity value could amount to roughly 8% of the EU-27 GDP by 2020.

This value growth is not automatic though as the study also finds that two-thirds of potential value generation in 2020 (440 billion) could be at risk if stakeholders fail to establish a trusted flow of data. Another trust-based obstacle is related to personal data management. The study finds that most consumers don't know what happens to their data and only 30% have a relatively comprehensive understanding of which sectors are collecting and using their data.

Also usability and awareness are an important issue as the study finds that consumers who are able to manage and protect their privacy are up to 52% more willing to share information than those who aren't, but only just 10% of the study respondents had ever done six or more out of eight common privacy-protecting activities (e.g., private browsing, disabling cookies, opt-in/out). Privacy controls need to be easy to use and they should not become an obstacle for getting through online services. The study finds that control and convenience are both highly rated, which means that a truly effective privacy control mechanism should be machine-aided using policy enforcement practices that follow pre-set rules and allows low end-user involvement during normal service use. [Va12] The study gives a positive outlook on personal data sharing: when proper privacy controls and sufficient user benefits are met, most users are effectively willing to share their personal data with public- and private-sector organisations.

Another study done for Orange [Fu14] reaches similar conclusions by stating that while consumers may feel that they no longer govern their data held by organisations, they are increasingly savvy when it comes to the value that they assign to their personal data. The study finds that users not only appreciate that their data has a value to businesses, but that value is variable based on the type of information and the relationship with the organisation. The study states that 80% of respondents think that their personal data has a value to businesses, and it has a higher value when they fit the organisation's customer profile. In conclusion we can state that an important portion of online service users in Europe and in the world want to spend their new "currency" on deals that they like, i.e. consume more personalised online services as long as they are in control of the data, receive adequate benefits from sharing their data and can trust the security of the service.

3 MyData principles

The governing principle for MyData is to provide human centric control and privacy where individuals are empowered actors, not passive targets in the management of their personal lives both online and offline [HK15]. A study conducted for Orange [Fu14] finds that consumers in all parts of the world have a growing mistrust of organisations' ability to protect personal data, even though some services are faring better than others. European consumers feel that there is a vacuum when it comes to the presence of a trusted entity to advise them on how to protect their personal data. The study finds that European consumers struggle to have control over their personal data when organisations are becoming increasingly sophisticated in the ways in which they capture and use this data. With MyData, users have the right and practical means to manage their data and privacy.

The second MyData principle is that data should usable so that personal data is technically easy to access and use in machine readable open formats via secure, standardized APIs. MyData is a way to convert data from closed silos into an important, reusable resource. It can be used to create new services which help individuals manage their own data. The providers of these services can create new business models and economic growth to the society. The Orange study also supports this principle as it finds that consumers feel that, on balance, organisations benefit most from customer

data sharing. [HK15]

The third MyData principle is about creating an open business environment where a shared MyData infrastructure enables decentralised management of personal data, improves interoperability and makes it easier for companies to comply with tightening data protection regulations. This environment should also allow individuals to change service providers without proprietary data lock-ins. [HK15]

4 The Finnish Trust Network

4.1 FTN organisation and objectives

The Finnish Trust Network (FTN) is a circle of trust composing of nationally notified Identity Providers (IDP) and notified Identity Service Brokers. The FTN is not a national identity scheme per se – it is a legal framework under which different notified IDP's are mandated to provide strong authentication services for citizens to access public services in Finland. The FTN is based on the revised law on Strong Electronic Authentication and Electronic Signatures [La09].

Technically the FTN is a cloud-based mechanism for connecting large scale, consumer facing services with trusted identity and service providers. The Trust Network delivers the following benefits:

- For citizens, the FTN delivers a familiar, fast and simple online service sign-on experience
- For online services, the FTN removes the barriers of security and complexity related to implementing strong authentication, which is based on mutually accepted levels of assurance.
- For identity providers that issue authentication credentials, the FTN provides new opportunities to leverage the success of their credentials platform and expand credential usage.

The Trust Network follows the requirements and objectives of the European eIDAS regulation for a network of trust service providers enabling Citizen-to-Business-to-Government secure and trusted electronic service provisioning. The Network is built upon strong privacy and security principles and enables a user-centric attribute consent model.

4.2 FTN members and legal framework

The FTN is a circle of trust whose members are either Identity Providers or service Brokers that notify their respective services in accordance with the provisions of the forthcoming regulation MPS72 [Fi16] and the law on strong authentication and electronic signature [La09]. The members will compose of a mix of Public and Private IDP's and identity service Brokers. The FTN IDP's include banks, mobile network operators and the Finnish Population Register Centre, which is the national CA that issues the Finnish eID. Identity Brokers can be private or public service providers, that enable the integration of Service Providers with Identity Providers and offer a

technical platform for users to access public sector Service Providers. In most cases the IDP takes the role of an Identity Broker, but these roles can be independent from one another.

The Regulation MPS72 defines requirements, amongst others, for FTN IDP's and Brokers, and transfers enforcement obligations for Brokers towards Service Providers. Even though service providers are not directly subjected to the requirements of the regulation, the FTN Brokers are responsible for the service providers to comply with the regulation's secure data processing requirements.

The FTN conforms with the eIDAS technical specifications for cross-border authentication using national PEPS nodes with regards to exchanged attributes and attribute naming, which are kept identical. The security requirements are compliant with the eIDAS technical specifications: all tokens and assertions are encrypted and signed, at the transport level, TLS 1.2 is required. [Fi16]

The FTN providers need to comply with published technical interface standards as defined in the regulation MPS72. These specifications mainly describe the mandatory and optional data exchange protocols, attributes and minimum security requirements. The FTN providers can implement additional features and services or alternative protocols, provided that the interfaces are publicly available, open to implement and comply with the attribute and security requirements. This approach gives the industry the freedom to develop and deploy solutions that best fit the functional requirements. The regulator is confident that all FTN providers will mutually agree on the technical implementation details since there is no business incentive for individual IDP's or Brokers to deploy un-interoperable solutions since they would not be able to attract service providers to sign up and register as customers. The regulation references two alternative FTN service interface protocol specifications, which are published as implementation examples that define the minimum data sets for attribute exchange within the FTN and the minimum security requirements. The specific security implementation requirements are included as references to mandatory national security implementation standards. [Fi16]

The FTN SAML 2.0 interface specification is based on the currently implemented Finnish public sector SAML 2.0 profile, which in turn is based on the SAML 2.0 WebSSO profile. The specification complies with the eIDAS technical specifications for cross-border authentication using national PEPS nodes and it is very similar to the Swedish national eID SAML 2.0 profile.

The FTN OpenID Connect interface specification is based on OpenID Connect 1.0 specification and it follows the US Connect.gov draft specification with the aim of updating the specification in the future in order to comply with the OpenID Connect iGov profile specification, as this will be ready. It is well understood that security wise the OIDC protocol is not as mature as SAML2 and even though it supports strong encryption and electronic signing of Java Web Tokens, other security issues that are addressed in SAML2 by default, are open in the OIDC basic specification. The security requirements will eventually be revised by the regulator as regulation MPS72 updates. The two interface specifications are not published yet, but will be by September 2016.

4.3 Levels of Assurance within the FTN network and the MyData infrastructure

User authentication assurance levels are based on the eIDAS Level of Assurance (LOA) levels. The same assurance levels are implemented in order to simplify the normative referencing of standardised authentication assurance levels. For accessing Finnish public online services, only LOA levels "Substantial" and "High" are accepted. At the current moment all existing and

previously notified national IDP's offer only Substantial level authentication, but the National eID will seek for conformance with LOA level High. [Fi16] The benefit of aligning the FTN with eIDAS node specifications is that IDP's would not need to implement different technologies or methods in a cross-border scenario. Also common language and shared standards limits the need to create and maintain proprietary or domain specific standards and practices.

In the cross-border authentication eIDAS Node context, the Finnish Population Register Centre (PRC) acts as the country Node [Fi16]. As it is also a member of the FTN, the relation with the FTN and the cross-border context is identical. Also mobile network providers will be participating in the trust network. The three main mobile operators Elisa, Sonera and DNA already provide mobile eID services that are usable in a federated mechanism. The FTN can have natural cross-border interactions, due to the cross-national nature of its IDP service providers: Sonera is part of Telia of Sweden, which is a major carrier and mobile operator in other Nordic and Baltic countries, and two of the three major banks that are currently acting as IDP's on a national level (Nordea and Danske Bank) are active IDP providers in other Nordic countries as well. In this context it is foreseeable that a lot of cross-border trust service provisioning could take place in the Nordics, thanks to eIDAS.

As a private sector solution, the MyData infrastructure would require the use of identity services that conform to minimum national requirements and LOA level Low identity assurance. But as MyData also aims at becoming a trusted infrastructure to service citizens in relation to their own data stored and managed in public service records and systems, the need for a MyData / FTN interaction becomes apparent. How this would work in practice is that as some IDP's are already members of both the FTN and the MyData Alliance networks, these IDP's could provide trusted and notified identity services that bridge and link the different components that make up the fabric of online services in Finland; public and private.

The benefit in this approach is that it would combine the goals and benefits of both networks and enable increased added value for all parties involved. The added value for the public services comes from the innovative solutions for service delivery and provisioning for citizens and also intra-administration data exchange, based on the MyData model. An added benefit comes from increased security as the FTN would provide for a strong authentication mechanism that protects user credentials that are used for accessing the user's MyData Account at the MyData Operator.

5 MyData architecture

In this section we provide an overview of the main features of the MyData Infrastructure and key elements for an MyData-FTN integration.

5.1 How MyData works

MyData is an infrastructure-level approach for ensuring data interoperability and portability. The open infrastructure makes it possible for individuals to change service providers without proprietary data lock-ins. MyData is sector independent and offers a consent-based data management and control solution for individuals to store all their data in centralised repositories in order to control the data flow. [HK15]

In practice the MyData approach works as follows: MyData Accounts hold the consents that determine how an Individual's data can flow from data sources to data users in an authorised system. For personal data management it is sufficient for the authorisation consents to be centralised in the MyData account. Data can flow directly between the source and the user.

With the MyData infrastructure data flows become manageable, comprehensive, and transparent, meaning that they include all privacy relevant transaction processes in a uniform way that follows predefined rules and policies, and which can be audited. Users can deactivate information flows and withdraw consent for all or specific services and applications from one single point. The MyData Account holds machine-readable consents that can be visualized, compared, and processed automatically. There is also a possibility to use pre-defined privacy and consent policy rules that respond to different profiles and contexts. [HK15]

5.2 The MyData services and authentication

The primary function of a MyData account is to enable consent management. The individual's data itself is not necessarily streamed through the servers where the MyData Account is hosted. In the MyData architecture, data flows from a data source to a service or application that uses the subsequent data and within the MyData infrastructure, the flow of consents or permissions is separate from the actual flow of data.

There are four defined roles within the MyData architecture include 1) Users, 2) MyData Operators, 3) data Sources that hold personal data, and 4) data Sinks that use and consume personal.

Core parts of the MyData authentication mechanism and the MyData APIs can be realised using the User-Managed Access (UMA) standard created by the Kantara Initiative. The UMA specification and its open-source implementations let individuals control authorisations to share their data and to manage how their data is shared between online services. Just like OpenID Connect, UMA is a profile of OAuth 2.0, which is a standard for controlling access to web API's. As OpenID Connect enriches the OAuth 2.0 data access protocol with Federated Identity and Web Single-Sign-On functionality, UMA enriches the OAuth 2.0 protocol with user-centric authorisation functionality. UMA bring two essential elements to the authorization workflow: asynchronous consent and centralized consent management, which are key for enabling the MyData model to work. [HK15]

5.3 Consent Based Approach for Personal Data Management

A legal framework for protecting personal data online is based on a specific, informed, unambiguous and freely given user consent. Processing of personal data is thus subject to the conscious choice to give consent for an external organisation to process data. Also this consent has to be withdrawable, changeable and readable by the involved trusted parties. Finally the consent should be stored appropriately for enabling validity checking by the parties using or providing personal data.

MyData is focused on consents because consents are a primary legislative framework that defines information processing from the human-centric perspective. The same consent management framework can also be used with minor modification for notifications and assignments. In

additions the human and machine readable standardised consents unite technical data management systems, legislative frameworks, and the human perspective. [My16a]

5.4 MyData Service Linking

The MyData service end-user is also called a MyData Account Owner. To be able to manage access to their data, the Account Owner first has to attach the related service to the MyData Account. MyData Service Linking means the act of adding a service (a Source or a Sink) to a specific Account Owner's MyData Account. A successful Service Linking results in a Service Link Record stored in the MyData Account. A valid Service Link Record is required before any data processing consent authorisation can be issued or used within the MyData ecosystem.

Service Link removal process is initiated when either a) Account Owner wants to remove a service from MyData Account, b) service deregisters from the Operator, or c) Account Owner removes an account at the service and there is no need to keep the Service Link, in which case it's service's duty to remove the unnecessary Service Link. The main purpose of Service Linking is to create a Service Link Record as this record contains keys used to sign MyData Consent Records. Without a Service Link Record, MyData Authorisation is not possible.

Service Link Record can be in Active or Removed state. When a new Service Link Record is constructed, it is in Active state. When a Service Link is removed, the Service Link Record is set to Removed state. There can be only one Active Service Link Record between the Account Owner and a service. [My16b]

In the FTN context the Broker service would need to provide the relevant MyData interfaces so that the user can authorise provisioned services.

5.5 MyData Service Registry

The main feature of the Service Registry is to allow the registration and discovery of available services and to facilitate service developers and service providers to manage registrations and to discover available services. The Service Registry is a component that provides identities to all services registered at a given Operator. Each service has a comprehensive Service Description accessible through the Service Registry. A Service Description consists of multiple parts enabling different types of service discovery.

The MyData architecture comprises of two types of services:

1. Services providing data resources to others are called Source services (data providing service)
2. Services requiring data from other services are called Sink services (data consuming service)

The main difference between these service types is that the Sink services do not expose a service interface for data access whereas the Source services do. The Service Registry is part of the MyData Operator service and it maintains a database of all the accessible and registered services. The service registration phases are as follows:

1. A service provider registers services, receives a unique ID for the service and creates the

required service descriptions.

2. The Service Registry provides identities to all services registered to an Operator and provides access to the required Service Descriptions
3. A service instance is then set up, which implements the described service interfaces. After a successful Service Registration, a MyData Operator is then able to search for compatible services (Service Discovery).

Service Descriptions are defined for each service in the MyData architecture. The service end-users are provided with a Human Readable Description of the service and its purpose, and for computer services, several Technical Descriptions of the service are provided by the service registry. The machine-readable API description of the service interface is essential for service developers for enabling service integration. In addition to providing the identity and description of the different services, the Service Registry also manages the endpoints of the registered services using specific Service Access URI addresses. [My16c]

In the FTN context the Broker service would need to provide the relevant MyData interfaces so that different available services can be discovered and provisioned for the authorised user.

5.6 MyData Authorisation

In the MyData architecture, all processing of personal data requires a legal basis. The term personal data processing is used to describe all data collection, movement and processing. There can be several possible bases for processing, but all data processing that is based on the consents from the Account Owner, can always be changed or withdrawn at will by the user.

The consent mechanism is restricted to processing activities that can be legally subjected to user consent, as defined in the EU GDPR. From a public service provider point of view, consent is only one possible ground for processing personal data and it does not always constitute the most typical ground. The MyData architecture provides a tool for the Account Owners to control the processing of their personal data not only when consent based data processing is grounded, but also in other case by providing a unified vantage point for all types of personal data processing activities.

In the MyData Architecture, when an Account Owner issues a consent this is documented in a MyData Consent Record (CR). A Consent Record is a manifestation of legally valid Consent which enables dynamic changing or withdrawing the user's consent. Consent Records are stored in the MyData Account and at the related service. For authorising data processing within a service, the Account Owner creates a single Consent Record for the related service. For authorising data transfer from a specific Source to a specific Sink, the Account Owner creates a pair of Consent Records (one for the Source and one for the Sink). Then, the Source's Consent Record defines, what data can be provisioned to the specified Sink. The Sink's Consent Record defines how the data can be accessed and it can also include the permissions for data processing. On a more granular level, the consents are managed as Resource Sets, which define specific subsets of data that a particular Source service provisions or processes. [My16d]

In the FTN context the user could authorise and manage consents for the different public online services and hold all the consents in one single MyData Account. Currently these features are implemented in certain services such as the tax service, but the MyData approach could generalise authorisation and consents management to all available services.

5.7 MyData Connection

In the MyData architecture a Data Connection is an authorised transfer of data from a specific Source to a specific Sink. This authorisation is given by the Account Owner in the MyData Authorisation transaction. Multiple Data Connections from a Source to a Sink are allowed as long as the subsequent authorisation is not deactivated or withdrawn. For the Source service the user's authorisation consists of a Consent Receipt which describes what data can be provisioned to the requesting Sink service. For the Sink service, the authorisation consists of a Consent Receipt describing how data can be processed and a access token, which is used to authenticate as an authorised data requester towards the Source service. The token is a Proof-of-Possession / holder-of-key type token, which contains Sink services public key. The data request must be signed with the Operator's corresponding private key. The token is both generated and signed by the Operator. [My16e]

The Data Connection Transactions are the following:

- The MyData Operator delivers an access token to the Sink service
- The Sink service request an access token from the Operator
- The Sink service requests data from the Source service

The FTN requires authorisation and authentication of all data connections and transfers and as such, the MyData infrastructure would enable a user-controlled assurance mechanism for securing data transactions towards service providers, which are not supervised by the national regulator. This feature would benefit the service providers as they would be able to integrate within the MyData and FTN networks in a standardised and compliant way. The FTN Broker would need to assure that the access connection token scopes match the scopes that requested and also that the rules applying the various scopes are met. In the FTN the service Broker defines access token scopes on the behalf of the service provider that describe what personal data is requested and fetched from the IDP. In the MyData context this same mechanism is delegated to the MyData aware Broker.

6 Conclusions: online services and the MyData infrastructure

The FTN forms the backbone for all trusted, notified and officially accepted ID's in Finland. The aim of the FTN is to offer a standard and highly interoperable framework for IDP's and Service Providers to offer identity and trust providing and consuming services for both public and private uses, and also supporting cross-border services. The MyData infrastructure is aimed at bridging data flow gaps that exist between the public and private domains, by inserting the citizen / user / consumer in the middle of the data flow puzzle.

As a private sector solution, the MyData infrastructure would only require the use of identity services that conform to minimum national requirements and LOA level Low identity assurance. But as MyData also aims at becoming a trusted infrastructure to service citizens in relation to their own data stored and managed in public service records and systems, the need for a MyData / FTN interaction becomes apparent. How this would work in practice is that as some IDP's are already members of both the FTN and the MyData Alliance networks, these IDP's could provide trusted and notified identity services that bridge and link the different components that make up the fabric

of online services in Finland; public and private.

The benefit in this approach is that it would combine the goals and benefits of both networks and enable increased added value for all parties involved. The added value for the public services comes from the innovative solutions for service delivery and provisioning for citizens and also intra-administration data exchange, based on the MyData model. For the MyData network the obvious added value is the possible inclusion of major personal data services from the public domain in the MyData infrastructure, hence strengthening its uptake as a new standard solution for user-centric data exchange.

For the MyData community, which comprises of major private, public and semi-public service providers and stakeholders, the added value comes from the possibility to engage with users and consumers in a more meaningful way as the infrastructure enables user-consent based data exchange between all parties involved. In the current silo and verticality bound data contexts, the inter-linking of the public-driven FTN and the private-driver MyData networks would create a totally new way for citizens to interact with all relevant parties that are currently in custody of the citizen's own data.

The possibilities to create and recreate public online services that are based on user-centricity are limitless and they should be regarded as a major innovation enabler for the public services globally. User centricity is seen as key when facing the challenges for citizens privacy, posed by over-exposure to digital services that fail to protect private data when it is linked and utilised and many separate contexts and systems. User centricity is also key for addressing the compliance challenges posed by the upcoming GDPR for the public and private bodies that manage private data in their systems and services. In both contexts the MyData approach offers an infrastructure solution that addresses the needs and requirements of all parties and domains.

The FTN IDP service providers can offer two types of services within the FTN/MyData networks: user identity federation for both FTN service providers and MyData Operators and strong end-user authentication for the MyData Operator. The MyData Operator may choose to opt for different LOA authentication levels, but depending on the MyData Source and Sink services higher LOA levels may be required. The MyData Source service defines the required authentication assurance level and it is up to the MyData aware FTN service Broker to assure that the access token scope rules are met when connecting between a FTN IDP and a MyData Source, through the MyData Account, which acts as the end-user control point. Based on the national legislation, at least a substantial assurance level authentication is required for accessing public sector Source and Sink services.

For the sake of user friendliness, commercial MyData Sink services may be satisfied if a user is authenticated at a Low level. This lower level security option should not endanger the integrity of the integrated FTN/MyData infrastructure since the MyData aware FTN Broker would not accept sending access token requests for FTN service providers when the required LOA minimum assurance level is not satisfied. The FTN service brokers, which connect IDP's with different service providers can specialise in different sectors of online service areas: some brokers would integrate only public sector domains whereas others would only integrate with commercial services, or MyData Operators. In order for service providers to not need to implement separate interfaces for the FTN and MyData Operators, the FTN brokers could provide unique integration points for the different interfaces.

The possibilities to create and recreate public online services that are based on user-centricity are limitless and they should be regarded as a major innovation enabler for the public services

globally. User centricity is seen as key when facing the challenges for citizens' privacy, posed by over-exposure to digital services that fail to protect private data when it is linked and utilised and many separate contexts and systems. User centricity is also key for addressing the compliance challenges posed by the upcoming GDPR for the public and private bodies that manage private data in their systems and services. In both contexts the MyData approach offers an infrastructure solution that addresses the needs and requirements of all parties and domains.

References

[Fi16] Finnish Communications Regulatory Authority, Regulation MPS72. https://www.viestintavirasto.fi/en/steeringandsupervision/actsregulationsdecisions/regulations.html, https://www.viestintavirasto.fi/attachments/maaraykset/Luonnos_13.5.2016_MPS72_maarayksen_perustelut_ja_soveltaminen.pdf, Stand: 1.8.2016

[Fu14] The Future of Digital Trust: a European study on the nature of consumer trust and personal data, Orange, Loudhouse , 2014. www.orange.com/en/content/download/21358/412063/version/5/file/Orange+Future+of+Digital+Trust+Report.pdf, Stand: 1.8.2016

[HK15] Honko, H; Kuikkaniemi, K; Poikola, A: MyData - Nordic Model for human-centered personal data management and processing – Whitepaper-Ministry of Transport and Communicaitons, Helsinki 2015. http://urn.fi/URN:ISBN:978-952-243-455-5, Stand: 1.8.2016

[La09] Law on Strong Electronic Authentication and Electronic Signatures 2009/617, http://www.finlex.fi/fi/laki/ajantasa/2009/20090617, Stand: 1.8.2016

[My16a] MyData Architecture - Consent Based Approach for Personal Data Management, v1.1, http://hiit.github.io/mydata-stack, Stand: 1.8.2016

[My16b] MyData Service Linking Specification, v1.1, http://hiit.github.io/mydata-stack, Stand: 1.8.2016

[My16c] MyData Service Registry Specification, v1.1, http://hiit.github.io/mydata-stack, Stand: 1.8.2016

[My16d] MyData Authorisation Specification, v1.1, http://hiit.github.io/mydata-stack, Stand: 1.8.2016

[My16e] MyData Data Connection Specification, v1.1, http://hiit.github.io/mydata-stack, Stand: 1.8.2016

[Va12] The Value of Our Digital Economy, Liberty Global, Inc. with The Boston Consulting Group, Inc., 2012. www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf, Stand: 1.8.2016