Editorial

Emanuele Bellini*

Telematic Applications Lab,
PIN – University of Florence,
Piazza Giovanni Ciardi 25,
Prato Firenze 59100, Italy
Email: emanuele.bellini@unifi.it
Email: bellini@rinascimento-digitale.it
Email: belliniema@gmail.com

Paolo Ceravolo

Università degli Studi di Milano,
Via Festa del Perdono, 7, 20122 Milano, Italy
Email: ceravolo@dti.unimi.it

Biographical notes: Emanuele Bellini, PhD is Senior Researcher and Project Manager at PIN – University of Florence. He is expert in Knowledge and Data Management, Persistent Identifiers and Digital Library. He deals with the development of the Italian NBN service.

Persistent Identifiers (PI) of internet entities is a crucial issue for almost all the sectors of the future information society.

In particular, in domains such as Cultural Heritage, e-Government, e-Health, e-Science, Multimedia and so on, the instability of URLs reduces credibility and prevents the use of the internet as a platform for searching, discovering and accessing reliable online digital assets like datasets, scientific articles, editorial products, library and archive digital objects, etc.

Persistent Identifiers (PI) were designed to make stable this reference (URL) to digital entities in the long term, contributing to secure information reliability over the internet, but now the needs and expectations of user communities are growing. In fact, digital entities are becoming even more complex. For instance a publication can be composed of several parts like the article, the datasets used for the experiments, a number of authors that need to be identified univocally, the references, etc. Moreover, the resulting scientific product has a complex lifecycle as well. In fact it involves several actors (research founders, publishers, authors, libraries, archives, etc.), services (rights management, search and discovery, digital preservation), business models (open access, annual fee, etc.), rules and so on.

In this scenario, the mere entity identification can no longer be the unique service provided to the user community. The persistent identification is now considered a commodity and current solutions need to enrich their offer with features and approaches oriented towards trustworthiness.

In fact Persistent Identifier solutions can become crucial in supporting trust-enabling services such as resource authorship, authenticity and provenance certification, digital rights management, e-identity management, interoperability, and so forth.

Currently the major PI providers of identifiers like DOI, NBN, DATACITE, ISNI, ORCID are working to extend their service in order to cope with the new community needs and this special issue aims to investigate the new conceptual approaches, trends and promised services aimed at implementing trustworthiness in PI infrastructures over different domains.

This special issue aims to collect both theoretical and experimental results in order to gain a wide understanding of the impact of trusted PI infrastructures at technological, social and economical levels in different communities of reference and in the information society in general.

For instance a new tool to manage authority and provenance verification in PI systems is discussed in 'A modular infrastructure for the management of authenticity and persistent identifiers in long term digital preservation repositories'.

Moreover, the standards also need to be aligned to the current requirements. The result of the revision of those most important in the PI domain is presented in 'Revision of the URN standards'.

Another important step ahead towards trustworthiness is given by the interoperability enabled among complementary PI services as experimented between DATACITE (PI of datasets) and ORCID (PI for researchers). The results are discussed in 'ODIN: the ORCID and DataCite interoperability network'.

Moreover, user communities are now aware that no technology is reliable per-se, and no technology can last forever or grant a level of service without a trustworthy organisation: it is well known that 'persistence' requires that other factors such as funding, responsibilities, sustainability, community/institutional mandate, etc. need to be considered and addressed. In particular in the 'ISNI consolidating identities, connecting nodes' the ISO-based initiative to identify authors is presented. Finally in 'NBN:IT The Italian trusted persistent identifier infrastructure' a general model for the PI infrastructure trustworthiness is described and how this model is applied at the National Central Library of Florence for the NBN infrastructure.

I would express my gratitude to all the authors for their interesting contribution. I also thank the editorial team and reviewers for their support and contributions in putting together this special issue.