**FutureTrust**

**Trusted Interactions Across Islands of Identity**

How do we extend trusted services beyond eIDAS and the move towards global trustworthy transactions, when the current ‘Islands of Identity’ restrict trust and commerce? We need to find a way past the fear of technology failure, uncertainty over security and doubts over commercial governance if we are to reach the goal of expanding the EU’s trusted transactions across its entire global supply chain.

With the complex eIDAS trust services regulation, there are two differing approaches to its extension beyond its remit within the EU and to global scalability:

1) The integration of other trust schemes within eIDAS
2) The interconnection of eIDAS with other trust schemes

The integration of eIDAS with other trust schemes is covered by eIDAS regulation EU 901/2014 Article 14: “…where the trust services originating from the third country are recognised under an agreement concluded between the Union and the third country in question or an international organisation in accordance with Article 218 TFEU.”

The concept of establishing many bi-lateral collaborative agreements is unscalable in terms of delay and resources. Interconnection, however, it is possible if a mechanism is provided to establish technical availability and visibility between the governance of the respected trust schemes. When both these aspects are addressed, then the ‘islands of identity’ can begin trusted interactions.

**The importance of the FutureTrust project**

FutureTrust is one of two loosely linked EU projects to enable the interaction between eIDAS and other schemes, and to expand the EU’s trusted transactions across its entire global supply chain.

FutureTrust provides accessibility to eIDAS trust services at a technical level and enables services to be built that can exploit eIDAS without a legislative collaboration. The other project is LIGHTest (http://lightest-community.org) which provides underlying transparency of policy and practice between schemes and utilises established internet global infrastructure.

FutureTrust provides a level of abstraction above the core of the main eIDAS services and permits a simpler approach to utilising eIDAS services for credential users that do not use eIDAS notified credentials and that may be geographically external to the EU.

FutureTrust is based on the open-source components that are compatible with the production SKIdentity federated platform operated by ECSEC GMBH and incorporates eID, Signature, Validation and Preservation Services. These services are seen as the primary services required to establish global trust between schemes.

LIGHTest and FutureTrust projects are tackling interoperable trust with two possible approaches, and the further combination of projects should be seen as a set of visionary actions to enable globally trusted transactions to be connected to eIDAS.

**Author:** Jon Shamah, Chair of EEMA (WP6)
Identity Assurance in the UK: technical implementation and legal implications

Identity Assurance in the UK is a paper recently published in the Journal of Web Science. It follows a first paper previously presented at the Web Science Conference of 2016 on Gov.UK Verify, the UK electronic identification (eID) scheme, and its potential implications from a privacy perspective in an eIDAS setting.

Although no formal indication to notify Gov.UK Verify to the European Commission (EC) has been given yet, “Identity Assurance in the UK” explores how Gov.UK Verify could participate to the eIDAS ecosystem and, in doing so, offers a demonstration of how national eID systems can ensure compliance with the eIDAS regulation.

The paper offers an overview of key concepts related to eID. It distinguishes between identification and authentication and explains how eID architectures are evolving to address privacy risks through technological and policy-based solutions.

We then compare eID policies and solutions in the UK and the EU. Looking back at previous attempts to introduce an eID policy in the UK, we note that the main driver behind its failure was an elevated concern of user privacy. We explain how this prism shaped the current eID policy in the UK and how it reflects on the main components of Gov.UK Verify, which incorporates a mixture of public and private entities into its ecosystem.

Next, we look at the eID policy shaped at the European level through the enactment of eIDAS and its associated implementing acts. We explain compliance with eIDAS through the concept of ‘sets of requirements' that eID systems need to satisfy.

We highlight key areas where attention is needed for Gov.UK Verify to participate in eIDAS, in particular in terms of eIDAS’ levels of assurance, interoperability framework and data protection and liability requirements.

Finally, in light of the recent developments in the UK, we look at how a potential exit from the EU could impact Gov.UK Verify and advise on how eID systems from non-EU ‘third countries’ could participate in eIDAS through obtaining legal equivalence.

The paper was written by Tsakalakis, Niko, Stalla-Bourdillon, Sophie and O’Hara, Kieron from Southampton University. For more information about the paper visit: https://eprints.soton.ac.uk/413943/

Author: Dr Sophie Stalla-Bourdillon, Associate Professor in Information Technology / Intellectual Property Law within Southampton Law School at the University of Southampton

Partner Profile: University of Southampton

Dr Sophie Stalla-Bourdillon is Associate Professor in Information Technology / Intellectual Property Law within Southampton Law School at the University of Southampton, specialising in Information Technology related issues. She is the Director of ILAWS, the Institute for Law and the Web and its core iCLIC.

Sophie is the author of several legal articles, book chapters and books on intermediary liability, data protection and privacy, information security and intellectual property. She led the legal work conducted for the purposes of the FP7 research project on operational trustworthiness enabling technologies (FP7 OPTET) examining the implications of a trustworthiness-by-design approach to be applied from the
design phase and comparing it with other value-by-design approaches such as the data-protection-by-design approach to be found in the proposed General Data Protection Regulation (GDPR).

Sophie is contributing to the Horizon 2020 Data Pitch innovation programme and is acting as the legal partner for FutureTrust exploring the potential impact of the GDPR on eID schemes and trust services.

Niko Tsakalakis is a Senior Research Assistant in Southampton Law School and a PhD candidate in the Web Science Centre for Doctoral Training. He has previously completed studies in Law (LLB), with an LLM in International Commercial Dispute Resolution and an MSc in Web Science. He has held positions as an in-house lawyer in a legal firm in Athens and an IT analyst in a HEI London. His current research, supervised by Dr Sophie Stalla-Bourdillon and Dr Kieron O’Hara, examines how privacy-enhancing technologies can be used as compliance techniques for the purposes of eID regulations (eIDAS) and data protection (GDPR).

FutureTrust Project Update in Brussels

FutureTrust consortium members, associate partners and the advisory board convened at the NRW permanent representation in Brussels on 16th and 17th November. The two-day session gave all stakeholders the chance to receive a comprehensive update of all work packages, as well productive networking sessions where many new ideas, opportunities and innovations were shared for the advancement of the project.
FutureTrust Project Partners

Full details of all Partners can be found on Opencard.

Federal Office of Administration (Germany)
EEMA (Belgium)
Arhs Spikeseed (Luxembourg)
Federal Computing Centre of Austria (Austria)
esec GmbH (Germany)
Giesecke & Devrient GmbH (Germany)
LAW trusted Third Party Services (Pty) Ltd (S Africa)
Ministry of Interior Republic of Serbia (Serbia)
Multicert (Portugal)
Public Service Development Agency (Georgia)
PwC (Belgium)
Ruhr-Universität Bochum (Germany)
Secure Information Technology Center (Austria)
Southampton University (UK)
Trustable Ltd (UK)
Türkiye Bilimsel veTeknolojik Arastruma Kurumu TUBITAK (Turkey)

Planned Activities and Events

ETSI - eSignature and eSeal validation workshop 10th January 2018 Sophia Antipolis, France
ReCRED - H2020 project clustering event 31st January 2018 Athens, Greece
FutureTrust GA 10th - 12th April 2018 Belgrade, Serbia

THE PROJECT MANAGEMENT FRAMEWORK EMBODIES A PROJECT LIFE CYCLE AND FIVE MAJOR PROJECT MANAGEMENT PROCESS GROUPS.

OH NO! THE EXTREME LEVEL OF ABSTRACTION HAS MADE US WEIGHTLESS!

THAT DOESN'T EVEN MAKE SENSE.