What is the problem/issue being addressed?

The FutureTrust project aims at providing reliable and secure implementations of software components that are essential to the success of the “Regulation (EU) No. 910/2014”, which is commonly known as the “eIDAS-Regulation” (https://eid.as/) in the public sector as well as in private organizations across Europe and beyond:

- Global Trust Service Status List (gTSL). The trust anchor for eIDAS-based trust services is an electronically signed XML document containing the trusted certificates used by the eIDAS services.
The gTSL service has been implemented on the basis of Ethereum Smart Contracts to support internationalization of this trust anchor. gTSL is used in ValS, and through ValS in all pilots/demonstrators supporting ValS.

- Comprehensive Validation Service (ValS). Due to the large variety of electronic signature formats and security token standards, the secure validation of a large number of these formats/standards is a non-trivial task. In ValS standards like XAdES, CAdES, PAdES and ASIC, plus the well supported industry standard tokens SAML and OpenID Connect have been implemented as a RESTful web application. ValS may use the gTSL and returns an XML-based validation report according to the OASIS Digital Signature Verification report standard.

- Scalable Preservation Service (PresS). To avoid a situation where the legal status of a document or signature may become unclear, the eIDAS-Regulation requires to implement appropriate preservation measures, as outlined in ETSI SR 019 510. The FutureTrust project has contributed to the (delayed) standard ETSI TS 119 512 v0.0.2. As a result of this delay in standardization, the implementation of PreS will be slightly delayed, which is not critical for the success of FutureTrust.

- Remote Signing and Sealing Service (SigS). SigS has been implemented and supports a large variety of different signature formats (XAdES, CAdES, PAdES and ASIC). After successful authentication of a client device, SigS will generate a signature on the provided document using the private key associated with the client, and the requested signature algorithm.

- Identity Management Services (IdMS). The FutureTrust IdMS will offer the possibility for clients to authenticate against the IdMS is implemented and supports a wide variety of European and international eID tokens, and will issue an identity token out of a small list of interoperable standards. These core services have been integrated into the Portuguese and Georgian demonstrators, the Austrian and the German pilot.

Why is it important for society?

Digital services are becoming more and more important in the everyday life of European and non-European citizens. Big Internet companies like Amazon, Google, Facebook and Twitter already dominate private use cases, and they are providing their own identification schemes. eGovernment, despite being a buzzword for quite a long time, is still being underdeveloped. This is due to the fact that for governmental services, a legally binding identification of requesting parties is required, which is not provided by the ad-hoc solutions of Facebook, Google and Twitter. Several countries already have established national eID schemes for this purpose, which are however not interoperable.

The eIDAS-Regulation aims at closing this gap, and providing a large European ‘market’ for eID solutions from the member states. If e.g. a Portuguese citizen would be able to apply for some official license in Poland without being forced to travel there in person (which is expensive and time-consuming), this could provide a big incentive to use national eID solutions.

The existing integrations into pilots/demonstrators show that the FutureTrust services may indeed be building blocks to facilitate eIDAS adoption worldwide:

- eApostille and eInitiative: Digitally signed Apostille documents can be verified globally, and electronic petitions can be made verifiable.
- eMandates: Electronic SEPA mandates for direct debits can be signed and verified cross border by the banking industry.
- eInvoice: Companies can submit electronic invoices to government agencies.
• eEnrollment: Closing an important gap in the trust chain, X.509 certificates can now be enrolled to entities authenticated via eID. These certificates can then be used to secure web servers, email communication, or signed PDFs.

What is the overall objective?
The overall objective of FutureTrust is to enable the use of cross-border digital services in a secure manner, both technically and legally. This is achieved by providing open-source packages and services based on the software modules needed to offer or consume eIDAS-related services, and by showing how to integrate them into more complex pilots.

Lavoro eseguito dall’inizio del progetto fino alla fine del periodo coperto dalla relazione e principali risultati finora ottenuti

<table>
<thead>
<tr>
<th>WP1</th>
<th>All administrative tasks have been completed on time.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WP2</td>
<td>Legal foundations on GDPR use in eIDAS applications have been applied to the demonstrators/pilots. Tools to evaluate the trustworthiness of services have been published.</td>
</tr>
<tr>
<td>WP3</td>
<td>WP3 has been successfully completed in Year 1.</td>
</tr>
<tr>
<td>WP4</td>
<td>Implementation of eIDAS-services is completed, and software quality has been improved through extensive functional testing.</td>
</tr>
<tr>
<td>WP5</td>
<td>Pilots and demonstrators have been successfully implemented and evaluated.</td>
</tr>
<tr>
<td>WP6</td>
<td>Dissemination is focused on the go.eIDAS label, and major contributions have been made to ETSI, OASIS and SEPA (EPC) standardization. Exploitation strategies have been finalized.</td>
</tr>
</tbody>
</table>

Progressi oltre lo stato dell’arte e potenziale impatto previsto (incluso l’impatto socioeconomico e le implicazioni sociali più ampie del progetto fino ad ora)

Progress beyond the state-of-the-art is achieved by providing specifications (WP3) and implementations (WP4) for services which did not exist up to now. The work also heavily influences European and international standardization (e.g. ETSI, OASIS).

The project achieved more than claimed in the GA. By finding vulnerabilities in several eIDAS services and following the responsible disclosure policy required in the GA and the First Review Report. These results have been communicated to the affected parties and have been discussed internally. In addition, the functionality of the PSDA demonstrator has been extended to cover the eInitiative functionality.

Block chain technology has been integrated in the Global Trust List software, following a recent high-profile trend to build more reliable trust into software.
The socio-economic impact and the wider societal implications of the project have taken place with the inclusion of new associate partners which will help to disseminate the eIDAS services.