



Trust Services Market Overview

 ANDREA CACCIA

 @eudigitalsme

 office@digitalsme.eu

 www.digitalsme.eu



WHO WE ARE

Europe's first and largest
ICT SME association

30 members

Representing more
than 45,000 digital
SMEs across Europe



The context of eIDAS2

- DIGITAL SME is following the eIDAS Regulation since some years and observed with the pandemic an increasing interest from SMEs
- The crisis has made clear that digital technologies are a strategic asset for the economic resilience and it is essential to be in control of them
- Cybersecurity and digital sovereignty in general are essential, but there is awareness of the opportunities (see [DIGITAL SME manifesto](#))
- DIGITAL SME published a [position paper on eIDAS](#) and contributed to the Commission public enquiry
- In EU enterprises employing less than 49 persons represent 98.9% of all enterprises, employing between 20 and 149 persons represent 0.9% (Eurostat, 2017)

The role of SMEs in the eIDAS ecosystem

- The role that SME can play is twofold:
 - As user of eID, trust services or related solutions and components, either as end users or using trust services as components of their services (EU SMEs are 22.5 millions)
 - A provider for eID services (where allowed by national eID schemes) or trust services, a key enabler for eIDAS
- The roles are not mutually exclusive: SMEs can provide solutions and components or even full outsourcing services to other SMEs or larger organizations that provide eID and trust services

SMEs as users of eID and Trust Services

- Historically the most important driver for a SME to use eID and Trust Services was compliance with legal requirements (e.g. identity or specific attributes, legal obligations with the Public Administration, security and non-repudiability of transactions, etc)
- The eIDAS Regulation eID framework supports mainly the public sector requirements and there are still different approaches to TSP supervision at national level (e.g. for identity proofing)
- The main drivers and area for improvement are:
 - additional compliance requirements such as anti-money laundering and “Know your customer” but increasingly maintaining full control on data,
 - opportunities to innovate and increase productivity, and
 - improving the user experience

SMEs as providers of eID and Trust Services

- EU Qualified Trust Service Providers are >200 (many are SMEs) but including non qualified TSPs, Identity Providers and the suppliers of related solutions, components and services greatly increase this number
- Qualification is a key tool for SMEs to aspire to be able to provide their services on an equal footing with larger providers however, it is necessary to ensure a more uniform and as much as possible standards-based approach to conformity assessment and supervision
- The provision of identity services is not and probably will not be possible in all member states, however the possibility of interfacing the new European Digital Identity Wallet features in trust services (and in services in general) is the greater opportunity
- New trust services such as electronic attestations, remote signatures, eArchiving, electronic ledgers are expected to be very welcomed by SMEs (also as users)

Some recommendations for eIDAS2 (1/2)

- DIGITAL SME recognizes the eIDAS2 proposal as an important step forward from the point of view of the market, not only for SMEs, both for users and providers
- Some suggestions for improvement were made in the public consultation:
 - Remote identification become an evident priority issue during the pandemic, however this practice is not currently accepted and implemented by all Member States, where different rules are in place. This should be addressed urgently with common standard-based good practices as it is also one of the main obstacles to an effective single market for trust services, especially for SMEs.
 - The planned certification of the identity wallet is a major concern for the short timeframe given to set standards: involvement of standard bodies and maximum reuse of existing certification schemes is of paramount importance. Server-side key management has proven to be a secure and rapid deployment solution with qualified signatures: it should be foreseen since the beginning also for the wallet keys.

Some recommendations for eIDAS2 (2/2)

- The concept of technical baseline is fundamental for interoperability: not only standards for policy and security requirements, but also protocols and formats are required for interoperability and should be considered in the implementing acts, as is already the case for signature formats; baseline should not limit, in any case, the competition based on implementation of added value features.
- The double role of SMEs as providers and users of trust services should be taken into due account: the flexibility of SMEs in introducing innovative trust services can also create the conditions and boost the adoption of that services by SMEs.
- The proposed NIS2 directive also is modifying the eIDAS Regulation by deleting Article 19 and being directly applicable to them. There is a high risk of disrupting the existing framework of standards for conformity assessment that already proved to be effective. Trust services should remain directly regulated by the eIDAS Regulation and aligned – as needed – to the NIS2 Directive.
- A transition period for the application of new rules and standards should be foreseen for existing qualified trust service providers.

