Council of the European Union

Brussels, 3 June 2021
(OR. en)

9471/21
ADD 4

Interinstitutional File:
2021/0136(COD)

TELECOM 242
COMPET 457
MI 432
DATAPROTECT 156
JAI 670
IA 108
CODEC 826

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	3 June 2021
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2021) 124 final PART 3/3
Subject:	COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT REPORT Annexes Accompanying the document Proposal for a regulation of the European Parliament and of the Council amending Regulation (EU) n° 910/2014 as regards establishing a framework for a European Digital Identity

Delegations will find attached document SWD(2021) 124 final PART 3/3.

Encl.: SWD(2021) 124 final PART 3/3

EUROPEAN
COMMISSION

Brussels, 3.6.2021
SWD(2021) 124 final

PART 3/3

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT REPORT

Annexes

Accompanying the document

Proposal for a regulation

of the European Parliament and of the Council amending Regulation (EU) n° 910/2014 as regards establishing a framework for a European Digital Identity

{COM(2021) 281 final} - {SEC(2021) 228 final} - {SWD(2021) 125 final}

Table of contents

Table of figures

ANNEX 3: WHO IS AFFECTED AND HOW?

A summary of costs and benefits of the preferred option is given in the following table.

Figure 18 - Overview of benefits (total for all provisions) of the preferred Options

Description	Amount	Comments
	Direct benefits	
Savings in administrative costs related to peer-review processes and notification process of eID	Overall, €63.000 in the first year and €220.000 per year afterwards	***Recipient: Public authorities*** *with regards to baseline which provides to simplify and improve the notification and peer review procedures.*
	Not quantified	***Recipient: Citizens / end-users*** *with regards to baseline which provides to simplify and improve the notification and peer review procedures.*
Reduced operational costs linked to identification procedures (onboarding procedures, KYC procedures etc.)	Sectoral yearly savings: ● Financial services (overall): €0.68 billion - €1.36 billion ● eHealth: €1.26 billion – €2.51 billion ● Aviation: € 30 million - €60 million ● eCommerce: €0.24 billion - €0.47 billion	***Recipient: Online service providers*** *with regards to option 1 measure 4, which provides to extend the person identification data set recognised cross border, option 2 measure 1 which provides to create a new qualified trust service for the secure exchange of data linked to identity and option 2 measure 5 which requires regulated sectors such as energy or finance and the public sector to rely on qualified digital credentials*
Reduced expenditures or damages related to cybercrimes (data theft, online fraud and procedures for online fraud prevention)	Sectoral yearly savings: ● Financial services (overall): €0.85 billion - €1.4 billion ● eHealth: €0.3 billion – € 0.6 billion ● Aviation: €3.5 million - €7 million ● eCommerce: €0.13 billion - €0.26 billion	***Recipient: Online service providers*** *with regards to option 1 measure 4, which provides to extend the person identification data set recognised cross border, and option 2 measure 1 which provides to create a new qualified trust service for the secure exchange of data linked to identity*

	Not quantified	***Recipient: Citizens / end-users*** *with regards to option 1 measure 8 which requires to strengthen the recognition of QWACs (qualified website authentication certificates)*
Reduced compliance costs (related to security certifications, GDPR requirements)	Not quantified	***Recipient: Public authorities*** *with regards to Option 1 measure 5 which requires to strengthen security requirements for mutual recognition*
Savings in compliance costs related to conformity assessments	€12,000-24,000 per each audit procedure	***Recipient: eID providers*** *with regards to option 1 measure 5 which requires to strengthen security requirements for mutual recognition*
Increased revenues from new trust services	For every additional 1% of EU businesses that purchase an electronic archiving solution every year, additional revenue of over €37 million a year for providers	***Recipient: Trust service providers*** *with regards to option 1 measure 6 which provides to introduce a new trust service for e-archiving*
Increased market and business opportunities at the EU level	Not quantified	***Recipient: Trust service providers*** *with regards to option 2 measure 1 which provides to create a new qualified trust service for the secure exchange of data linked to identity, option 2 measure 3, and option 3 measure 1* ***Recipient: Wallet app providers*** *with regards to option 3 measure 1*
Increased personal data protection and online security	Not quantified	***Recipient: Citizens / end-users*** *with regards to option 1 measure 4, measure 5,measure 7 and*

		measure 8, as well as option 2 measure 1 and measure 6 and option 3 measure 1, measure 2 measure 3 and measure 4 (all sub-options)
Increased interoperability	Not quantified	***Recipient: Citizens / end-users, Trust service providers and online service providers*** *with regards to option 2 measure 3 and option 3 measure 2 (all sub-options)*
Increased legal value and recognition across the EU	Not quantified	***Recipient: Citizens / end-users, Trust service providers and online service providers*** *with regards to option 2 measure 4*
Enhanced digital inclusion	Not quantified	***Recipient: Citizens / end-users*** *with regards to option 1 measure 1, which provides to establish an obligation for member states to offer eIDs and to notify them under eIDAS*
	Indirect benefits	
Increased access to public services through secure eIDs	Not quantified	***Recipient: Public authorities, Citizens & Government eID providers*** *with regards to option 1 measure 1, which provides to establish an obligation for member states to offer eIDs and to notify them under eIDAS* ***Recipient: eID providers*** *with regards to Option 3 measure 1*
Savings from reduced administrative burden	Overall, between €350 and €400 million per year	***Recipient: citizens / end-users*** *with regards to option 1 measure 4 which provides to extend the person identification data set recognised cross border, and option 2 measure 1 which provides to create a new qualified trust service for the*

		secure exchange of data linked to identity
	Not quantified	***Recipient: public authorities*** *with regards to option 2 measure 2 requiring Member States to make available data stored in authentic sources for the secure exchange of data linked to identity*
Increased and more trustworthy cross-border data exchange	Not quantified	***Recipient: Online service providers*** *with regards to option 2 measure 1 which provides to create a new qualified trust service for the secure exchange of data linked to identity*
	Not quantified	***Recipient: public authorities*** *with regards to option 2 measure 2 requiring Member States to make available data stored in authentic sources for the secure exchange of data linked to identity, and option 2 measure 3 covering the related standards*
Enhanced offer in the Trust Services market	Not quantified	***Recipient: citizens / end-users*** *with regards to option 1 measure 6 which provides to introduce a new trust service for e-archiving*
Increased awareness of EU citizenship	Not quantified	***Recipient: citizens / end-users*** *with regards to option 2 measure 1 which provides to create a new qualified trust service for the secure exchange of data linked to identity*

Figure 19 - Overview of costs for preferred Options (first part)

		Public authorities		TSPs		Gov. eID providers	
	Type of costs	One-off	Recurrent	One-off	Recurrent	One-off	Recurrent
Increased administrative burden (mandatory offer of eID and notification, additional peer reviews) *(Policy option 1 Measure 1)*	Direct cost	between €40-€100 million to develop a fully-fledged eID scheme (Member States not having deployed one)					
Increased administrative burden (mandatory offer of eID and notification, additional peer reviews) *(Policy option 1 Measure 1)*	Direct cost	€0,52 - €1.3 million (cumulative for 13 Member States)					
	Indirect cost	€1.2 million (in the next two years, cumulative for all Member States)					

		Public authorities		TSPs		Gov. eID providers	
	Type of costs	One-off	Recurrent	One-off	Recurrent	One-off	Recurrent
Compliance with eIDAS related obligations *(Policy option 1 Measure 1)*	Direct cost	€9.7 million (envisaged only for 13 Member States)					
Committee work for standardisation *(Policy option 1 Measure 4)*	Indirect cost	€300,000				Not quantified	
Committee work for international standard-setting *(Policy option 2 Measure 3)*	One-off	€1-2 million					
Committee work for international standard-setting *(Policy option 3 Measure 2 for all sub-options)*	One-off	€1-2 million (only if new standards have to be developed)					

		Public authorities		TSPs		Gov. eID providers	
	Type of costs	One-off	Recurrent	One-off	Recurrent	One-off	Recurrent
Compliance costs due to adapting to a certification-based approach *(Policy option 1 Measure 7)*	One-off			Not quantified			
Compliance costs due to certification *(Policy option 1 Measure 5)*	Indirect cost	€228,000					
Familiarisation costs due to new procedures and measures *(Policy option 2 Measure 1)*	Direct cost	€315,000					
Enforcement and administrative costs due to the introduction of new trust	Direct cost		Around €8.1million				

		Public authorities		TSPs		Gov. eID providers	
	Type of costs	One-off	Recurrent	One-off	Recurrent	One-off	Recurrent
services *(Policy option 1 Measure 6)* *(Policy option 2 Measure 1)* *(Policy option 3 Measure 1, sub-option 1)*							
Compliance costs linked to the introduction of eArchiving *(Policy option 1 Measure 6)*	Direct cost			€545,000 per provider	€255,000 per provider		
Compliance costs linked to the introduction of a new qualified trust service *(Policy option 2 Measure 1)*	Direct cost			€545,000 per provider	€255,000 per provider		
Technical costs for upgrading	Indirect cost	€6.1 million					

		Public authorities		TSPs		Gov. eID providers	
	Type of costs	One-off	Recurrent	One-off	Recurrent	One-off	Recurrent
the eIDAS national infrastructures *(Policy option 1 Measure 3)*							
Technical costs to ensure protection of personal data and data minimisation *(Policy option 2 Measure 6)*	Direct cost	Not quantified		Functional Separation: €30,000 per provider Structural Separation: €730,000 for qualified Trust service providers	Structural Separation: €30,000 per year for qualified trust service providers		
Technical costs related to IT integration to the API integration *(Policy option 2 Measure 1 & 2)*		€625 million	€162 million per year				

Figure 20 - Overview of costs for preferred Options (second part)

		Online services providers		CABs		Wallet app providers	
	Type of costs	One-off	Recurrent	One-off	Recurrent	One-off	Recurrent
Familiarisation costs due to the introduction of a new qualified trust service *(Policy option 2 Measure 1)*	Direct cost			€339,000			
Familiarisation costs due to the introduction of a European Digital Identity WalletApp *(Policy option 3 Measure 1, sub-option 1)*				€339,000			

		Online services providers		CABs		Wallet app providers	
	Type of costs	One-off	Recurrent	One-off	Recurrent	One-off	Recurrent
Compliance costs related to the adoption of QWACs *(Policy option 1 Measure 8)*	Indirect cost		€550 per year, per provider				
Technical costs related to IT integration to the API *(Policy option 2 Measure 1 & 2)*	Direct cost	from €18,000 to €27,000 per provider					
Compliance costs related to certification and standardisation *(Policy option 3 Measure 1)*	Direct cost					€545,000 per provider	€255,000 per provider
Compliance costs related to obtaining security certification						€80-100k per provider	

		Online services providers		CABs		Wallet app providers	
	Type of costs	One-off	Recurrent	One-off	Recurrent	One-off	Recurrent
(Policy option 3 Measure 3)							
Operational costs related to onboarding of providers of credentials and services *(Policy option 3 Measure 1)*						Not quantified	Not quantified
Marketing and customer support costs *(Policy option 3 Measure 1)*						Not quantified	Not quantified

ANNEX 4: ANALYTICAL METHODS

This annex provides the basic elements of the methodology adopted for the construction of a macro-economic model for the simulation of the economic effects of investments in the provision of eID services. From the point of view of the official statistical information, production of eID services are included in the Telecommunication sector accounts.

The research objective is to evaluate the impact of investments in the provision and use of eID services on the produced output and on employment in the other sectors in the economy.

The analysis relies on an estimated/calibrated general equilibrium model, whose supply-side is based on input-output relationships among industries, and the demand side is fully specified under the hypothesis of monopolistic competition among industries, such that firms are price-setters, i.e. they consider a mark-up over their own marginal costs in their pricing decisions, and demand is defined considering the full set of industry-specific relative prices.

Production takes place considering an input-output production technology in which the input mix is chosen optimally based on the relative prices of intermediate factor inputs. The telecommunication sector is isolated and included into the several production functions, such that a simulated investment decision affects each sector both directly and indirectly through the other sectors' responses. The impact in each sector is captured by an increase in the telecommunication input, leading to production effects and substitution effects, and the latter driven by the relative price changes.

1. The model

The model used is a large-scale **Input-Output Dynamic Stochastic General Equilibrium Model (IO-DSGEM)** consisting of an Input-Output structure for the supply side and of a symmetric demand side, and which assumes monopolistic competition. This provides an instrument that allows an internally consistent evaluation of the potential macroeconomic effects of investment in the provision and adoption of eID services at a high level of macroeconomic detail. The model used does not belong to the stream of dynamic stochastic general equilibrium models (DSGE) used by central banks and economic institutions for the assessment of monetary and fiscal policies. These in general are built in order to maximize their ability to trace the dynamic effects of the policies on aggregate macroeconomic data. The Input-Output-based DSGE (IO-DSGE) model used for this report is a multi-sector model in which the production side is described by input-output relations characterized by variable input coefficients, whose time variation depends on the productive factor's relative prices. This approach shares with the standard DSGE model the following features: (i) the behaviors of the agents in the model are dynamic (obtained by the micro-foundation of the behavioral equations), and (ii) all variables are endogenous and the exogenous component (i.e. sector-specific total factor productivity, preference wedges on the consumption side, policies) takes a fully stochastic specification.

As compared to CGE models, the IO-DSGE model maintains the high level of detail of the variables being included and an internally consistent theoretical representation of the behavioral relations on the sectoral supply and demand side. A distinguishing feature of the IO-DSGE model is the fully dynamic and endogenous representation of the variables, and the consideration of policies and structural shift factors as stochastic processes. Given the dynamic specification of behaviors and the explicit representation of expectations, the approach used for the report is expected to provide, with respect to standard DSGEs, a more flexible and accurate description of the responses of the model economy to the policies being implemented, without losing the level of detail which is typical of CGEs.

A further difference with respect to CGEs is that, in stochastic models the sources of variability are "randomly drawn shocks from a zero-mean distribution" (i.e. they are unexpected, or unanticipated, by rational agents), whereas in CGE models they are known in advance, should the agents populating the stylized economy be described as rational (this is not always the case

in the different model experiences). In an IO-DSGE model simulation setting, this difference can be shut-down by using a deterministic definition of the shocks (policies). In this case, policies are assumed to be declared in advance to their implementation, such that their dynamics are fully anticipated by the rational agents.

To enhance the generality of results, a flexible translog production technology employing 16 factor inputs is adopted for each of the two-digit NACE classification (Rev. 1.1) [1] addressed in the analysis. The attractive feature of the translog functional form is that it imposes no *a priori* restrictions on substitution and price elasticities (Berndt, 1990), that can be derived from the estimated parameters of the implied cost share functions.

On the demand side, following a standard approach (see Blanchard and Kiyotaki (1987)), sector-specific demand and price setting functions are analytically derived under the hypothesis of monopolistic competition.

Given the limited sample size and the nonlinearity of the key output production functions and of the related cost shares, the Bayesian estimator is employed to parameterize the supply side of the model. The parameterization of the demand side is instead calibrated.

1.1 The supply-side

On the supply side, we define the production technology employing N simultaneous-equations, where N is the number of sectors in the economy (disaggregated according to the NACE classification system, with N=58). Each production function defines the amount of output that can be produced for given amounts of inputs, and satisfies the non-negativity, linear homogeneity and concavity properties. Each produced commodity serves equivalently as a final consumption good and as an intermediate input.

Sector *j*'s (with j = 1, 2 ..., N) production function includes: energy inputs (*E*), materials (*M*), services (*S*), capital services from ICT assets (*ICT*), capital services from non-ICT assets (*K*) and labour (*L*). The production inputs evaluated at their basic costs are obtained by aggregating NACE sectoral inputs h = 1, ..., I_X as $p_i X_{ij} = \sum_{h=1}^{I_x} p_{h,i} X_{h,ij}$, with i = 1...6 (i.e. the six inputs *E*, *M*, *S*, *ICT*, *K*, *L*), where *X* denotes the amount of input *i* used in sector *j*, *p* denotes prices, and upper-case letters denote quantities.

The nominal value of sectoral output of industry *j* is given by the revenue function:

$$p_Y Y_j = f\left(p_E E_j, p_M M_j, p_S S_j, p_{ICT} ICT_j, p_K K_j, p_L L_j\right) \quad (1)$$

To simplify the analysis, we assume constant return to scale and single-output technologies. Under these conditions, the production function and the cost function match each other. In other words, even though one function is defined with respect to quantities, and the other with respect to prices, both convey the same information about the production technology. Because of this duality property between production and cost functions, the total cost function of (1) can be written as:

$$C_j = g(p_E, p_M, p_S, p_{ICT}, p_K, p_L) \quad (2)$$

On these formal premises, results strongly depend on substitution among factor inputs. This implies that the definition of the partial elasticities of substitution plays a key role. In order to

[1] NACE is a 4-digit activity classification used by the European Union since 2002. More details are available at: http://ec.europa.eu/eurostat/ramon/relations/index.cfm. The classification of economic activities according to NACE is totally coherent with ISIC and can be considered its European counterpart. Concordance tables from NACE to ISIC are available at: http://www.foost.org/database/nace/nace-en_2002c.php.

enhance the generality of the analysis (by allowing that inputs demands depend on the level of output), we assume a non-homothetic translog cost function[2], which is given by:

$$ln(C_j) = ln(\alpha_{0j}) + \sum_{i=1}^{6} \alpha_{ij} ln(p_i) + \frac{1}{2}\sum_{i=1}^{6}\sum_{k=1}^{6} \gamma_{ikj} ln(p_i) ln(p_k) + \alpha_{Yj} ln(Y_j) + \frac{1}{2}\gamma_{YYj} ln(Y_j^2) + \sum_{i=1}^{6} \gamma_{iYj} ln(p_i)\, ln(Y_j) \quad (3)$$

where $\gamma_{ikj} = \gamma_{kij}$, Y_j denotes sector *j*'s output and C_j is the total cost. To obtain homogeneity of degree 1 in prices conditional on Y_j, the following restrictions are imposed:

$$\sum_{i=1}^{6} ln(\alpha_{ij}) = 1 \quad (4)$$

$$\sum_{i=1}^{6} ln(\gamma_{ikj}) = \sum_{i=1}^{6} ln(\gamma_{kij}) = \sum_{i=1}^{6} ln(\gamma_{iYj}) = 0 \quad (5)$$

Note that alternative specifications can be obtained by imposing additional restrictions to the translog production function (3). First, the homothetic property, i.e. that inputs demand does not depend on the level of output can be imposed by assuming $\gamma_{iYj} = 0 \ \forall \ i$ = 1...6; second, homogeneity of a constant degree in output $1/\alpha_{0Yj}$can be obtained if the condition $\gamma_{iYj} = 0$ is added to the homotheticity condition; third, constant returns to scale are obtained when, in addition to the restrictions above, $\alpha_{Yj} = 1$; fourth, the Cobb-Douglas production function is obtained when, in addition to all the above restrictions, $\gamma_{ikj} = 0$ $\forall i,k$ = 1...6.

Because of data availability and potential gains in efficiency, the cost production function (3) is better estimated indirectly, by solving it with respect to the cost shares. These are derived from cost-minimizing input demand equations, obtainable by differentiating (3) with respect to input prices and employing the Shephard's Lemma:

$$\frac{\partial ln(C_j)}{\partial ln(p_i)} = \frac{p_i}{C_j}\frac{\partial C_j}{\partial p_i} = \frac{p_i X_{ij}}{C_j} = \alpha_{ij} + \sum_{k=1}^{6} \gamma_{kij} ln(p_k) + \gamma_{iYj} ln(Y_j) \quad (6)$$

where $C_j = \sum_{i=1}^{6} p_i X_{ij}$. By denoting the cost share $p_i X_{ij}/C_j$ with S_{ij}, i=1...6, the following cost share equations for the six inputs (*E,M,S,ICT,K,L*) are:

$$S_{Ej} = \alpha_{Ej} + \gamma_{EEj} ln(p_E) + \gamma_{EMj} ln(p_M) + \gamma_{ESj} ln(p_S) + \gamma_{EICTj} ln(p_{ICT}) + \gamma_{EKj} ln(p_k) + \gamma_{ELj} ln(p_l) + \gamma_{EYj} ln(Y_j)$$

$$S_{Mj} = \alpha_{Ej} + \gamma_{Mj} ln(p_E) + \gamma_{MMj} ln(p_M) + \gamma_{MSj} ln(p_S) + \gamma_{MICTj} ln(p_{ICT}) + \gamma_{MKj} ln(p_k) + \gamma_{MLj} ln(p_l) + \gamma_{MYj} ln(Y_j)$$

$$S_{Sj} = \alpha_{Ej} + \gamma_{SEj} ln(p_E) + \gamma_{SMj} ln(p_M) + \gamma_{SSj} ln(p_S) + \gamma_{SICTj} ln(p_{ICT}) + \gamma_{SKj} ln(p_k) + \gamma_{SLj} ln(p_l) + \gamma_{SYj} ln(Y_j)$$

$$S_{ICTj} = \alpha_{Ej} + \gamma_{ICTEj} ln(p_E) + \gamma_{ICTMj} ln(p_M) + \gamma_{ICTSj} ln(p_S) + \gamma_{ICTICTj} ln(p_{ICT}) + \gamma_{ICTKj} ln(p_k) + \gamma_{ICTLj} ln(p_l) + \gamma_{ICTYj} ln(Y_j)$$

$$S_{Kj} = \alpha_{Ej} + \gamma_{KEj} ln(p_E) + \gamma_{KMj} ln(p_M) + \gamma_{KSj} ln(p_S) + \gamma_{KICTj} ln(p_{ICT}) + \gamma_{KKj} ln(p_k) + \gamma_{KLj} ln(p_l) + \gamma_{KYj} ln(Y_j)$$

$$S_{Lj} = \alpha_{Lj} + \gamma_{LEj} ln(p_E) + \gamma_{LMj} ln(p_M) + \gamma_{LSj} ln(p_S) + \gamma_{LICTj} ln(p_{ICT}) + \gamma_{LKj} ln(p_k) + \gamma_{LLj} ln(p_l) + \gamma_{LYj} ln(Y_j)$$

[2] The translog cost function is basically a second order Taylor approximation to an arbitrary cost function.

(7)

This system of equations has 48 parameters (eight in each of the six equations) for each *j* sector (with *j* = 1...56). By imposing the 15 symmetry restrictions, $\gamma_{ikj} = \gamma_{kij}$, $\forall i,k$ = 1...6, and the eight homogeneity restrictions in input prices, $\sum_{i=1}^{6} ln(\alpha_{ij}) = 1$, $\sum_{i=1}^{6} ln(\gamma_{ikj}) = 0$ $\forall k$ = 1...6, $\sum_{i=1}^{6} ln(\gamma_{kij}) = 0$, we reduce the number of parameters to be estimated to 25 (for each sector *j)*. Moreover, since for simulation purposes constant returns to scale are preferred, we also estimate a version of the system above in which we impose the six additional restrictions $\sum_{i=1}^{6} ln(\gamma_{iYj}) = 0$ $\forall i$ = 1...6. These restrictions reduce further the number of parameters to be estimated to 18 for each *j* sector (the restriction $\sum_{i=1}^{6} ln(\gamma_{iYj}) = 0$ becomes redundant).

The Hicks-Allen partial elasticities for the general dual cost function can be computed as $\sigma_{ik} = (C/C_i)(C_{ik}/C_k)$, while the price elasticities can be computed as $\epsilon_{ij} = \partial ln(X_i)/\partial ln(p_k) = (\partial X_i/\partial p_k)(p_k/X_i) = S_k\sigma_{ik}$. Under translog function assumption, the partial and own elasticities turn out to be:

$$\sigma_{ik} = \frac{\gamma_{ik}+S_iS_k}{S_iS_k}$$

(8a)

$$\sigma_{ii} = \frac{\gamma_{ii}+S_i^2-S_i}{S_i^2}$$

(8b)

whereas price elasticities can be calculated as:

$$\epsilon_{ik} = \frac{\gamma_{ik}+S_iS_k}{S_i}$$

(9a)

$$\epsilon_{ii} = \frac{\gamma_{ii}+S_i^2-S_i}{S_i}$$

(9b)

1.2 The demand-side

On the demand side, the demand for good *j* (D_j) is given by:

$$D_j = \left(\frac{p_j}{p}\right)^{-\varepsilon} D$$

(10)

where $p = \left[\sum_{j=1}^{N} p_j^{1-\varepsilon}\right]^{\frac{1}{1-\varepsilon}}$ is the price index resulting from the Dixit-Stiglitz aggregator, ε denotes the (demand) elasticity of substitution among differentiated products, and $D = \left[\sum_{j=1}^{N} D_j^{\frac{\varepsilon-1}{\varepsilon}}\right]^{\frac{\varepsilon}{\varepsilon-1}}$ is aggregate demand. At each point in time, only a fraction of prices are re-optimized, whereas the remaining fraction is held fixed at the previous time level. Reset prices (optimal) are defined by maximizing profits subject to the supply equations and (12) and turn out to depend on the sectoral marginal cost MC_j. In the aggregate:

$$p_{j,t} = \theta \frac{\varepsilon}{\varepsilon-1} MC_{j,t}(1-\theta)p_{j,t-1}$$

(11)

where θ is a convolution of parameters summarizing the (complement to one) of the degree of nominal price rigidity, $\varepsilon/\varepsilon-1$ is the price mark-up from monopolistic competition and $MC_{j,t}$ are marginal costs in sector *j*. Goods market equilibrium is satisfied when demand equals supply

for each product-factor *j*. Under flexible prices hypothesis, the symmetric equilibrium holds period by period.

The instantaneous and cumulated effects on output and employment can be evaluated in terms of both percentage deviations from control (i.e. a situation in which no investment/adoption occurs) and in terms of variations of volumes, i.e. output value effects (in Euros), and employment effects (in jobs).

The estimation requires detailed statistical information on sectoral outputs and inputs, i.e. industry by industry input-output tables, publicly provided by the Eurostat (European System of Accounts - ESA 95), while other operational variables and data are obtained from the Eurostat Structural Indicators and from the STAN - OECD database. A detailed description of the statistical information is provided in the next section.

2. Estimation

The econometric methodology used - given the shortage of data availability over the time dimension and the small number of degrees of freedom over the sectional dimension - is the Bayesian seemingly unrelated regression equation (SURE) estimator. The Bayesian Monte-Carlo integration method ensures convergence in estimation while maintaining consistency even with small samples.

The scope of Bayesian estimators is to get the posterior distribution for model parameters conditioning on prior beliefs on models, structural parameters, and sample information. The methodology thus nests a formalized prior distribution for the *q*-th Model's parameters and the conditional distribution (pseudo-likelihood) to get the posterior density. This is obtained by employing the Bayes' rule.

The posterior distribution of interest is the result of a weighted average of prior non sample information and the conditional distribution (i.e. the empirical information). Weights are inversely related to, respectively, the variance of the prior distributions and the variance of the sample information ("precisions"). Thus, formalizing a tight prior will result in highly constrained estimation, while a diffuse prior will result in weakly constrained estimation. Asymptotically, the conditional distribution (objective information) dominates the prior distribution (subjective information) and the posterior distribution of the parameters collapses to their pseudo-true values. This property ensures that the relevance of priors in posterior estimates vanishes as the sample size increases. A further feature of the Bayesian estimator that is particularly important in standard applications is that its small sample performances outperform those of the FIML estimator (Geweke et al., 1997; Fernandez-Villaverde and Rubio-Ramirez, 2004).

The posterior density of interest is a complex nonlinear function of the deep parameters, thus its analytical calculation is not generally feasible analytically. For this reason, we calculate the posterior distribution via numerical integration. Operationally, the Bayesian MCMC posterior estimates are obtained adopting a two steps procedure, employing the Kalman smoother to approximate the conditional distribution and the Gibbs sampler implemented in BACC to perform Monte Carlo integration.

Measures of sectoral outputs and inputs require industry by industry input-output tables which are provided by the Eurostat (European System of Accounts - ESA 95). Other variables are obtained from the Eurostat Structural Indicators and from the STAN - OECD database.

3. Data

The model parameterization is obtained from the information provided by a panel of years and sectors. The data are available from 1995. According to the 2-digit NACE classification systems, 58 production sectors are included in the estimates and in the model simulation (NACE-P is omitted because of data constraints). These 58 economic sectors cover all the economic activities, that is, only mentioning the macro-areas (1-digit NACE): *Agriculture, hunting and forestry (A), Fishing* (B), *Mining and quarrying* (C), *Manufacturing* (D),

Electricity, gas and water supply (E), *Construction* (F), *Wholesale and retail trade, repair of motor vehicles, motorcycles and personal and household goods* (G), *Hotels and restaurants* (H), *Transport, storage and communication* (I), *Financial intermediation* (J), *Real estate, renting and business activities* (K), *Public administration and defense; compulsory social security* (L), *Education* (M), *Health and social work* (N), *Other community, social and personal service activities* (O).

The econometric analysis relies on the following set of data:

- values of the 1-digit 17 inputs used (including labour) at purchaser prices
- values of the 2-digit sectoral output at basic prices
- inputs' prices (except labour)
- labour compensation

All this information is obtained by three main data sources:

(1) OECD – *STAN* STructural ANalysis Database;
(2) Eurostat - Industry, trade and services – Industry and construction Industry;
(3) ESA 95 Table – Input-output tables – Eurostat.

Inputs and Outputs at basic prices are obtained from all the sectors (A/01-Q/99) ESA 95 Table - Input-output tables - Eurostat: Supply and Use Tables, Current Prices. Two-digit NACE aggregation system. This dataset is key in the definition of the model structure, i.e. of the number of production sectors, relative prices and demand functions being considered in the model, as well as for the model estimation stage. The supply, the use and the merged input-output tables provide a detailed picture of the interdependencies of the production system. In particular, information on the use of goods and services (products) and the output generated in each production is provided by the supply and use tables.

The symmetric input-output table is a transformation of the supply and use tables under a fully consistent classification system[3].

The supply table illustrates where in the production system goods and services are produced; in other words, it offers information on the supply of goods and services by type of product of an economy in each year. By column, information on the production programme for each sector is provided, i.e. the domestic output of primary and secondary productions is reported. The principal activities of each industry are identifiable in the main diagonal of the matrix table, whereas the off-diagonal elements provide information on secondary activities.

The use table conveys information on the use of goods and services by product, by type of use for intermediate consumption (i.e. where intermediate consumption by industry is paired to final consumption by individuals) and by industry. Its structure can be described as follows: by columns, the input structure of each industry is reported; by row, instead, the use of different products and primary inputs is shown for each production sector. The costs of production can be obtained in the table's columns for each sector and the total cost of each product can be obtained from the sum across columns for each row. The total output measured at basic prices for each sector is reported as sum across rows for each column.

The use input-output table is the results of intersections between (rows) product and value added and (columns) sectors and individuals as final users (exemplified in Table 2.1). The rows report the use of goods and services by sector (intermediate consumption) and by individuals (final consumption). The columns of sectors reflect the production structure (used inputs) of each specific sector.

[3] The classification used for the included sectors is the "General Industrial Classification of Economic Activities within the European Communities" (NACE), whereas the classification employed for products is the 'Classification of Products by Activity' (CPA), which are one the counterpart of the other.

Figure 21 - Structure of a use I/O table of an economic system composed by only 3 sectors (Agriculture, Manufacture and Transport)

	Sectors			Final users	TOTAL
Products	**Agriculture**	**Manufacture**	**Transport**		
Cereals Textiles Transport services	Intermediate consumption			Final consumption by product	**Total consumption by product**
Value added	Value added by sector				**Total Value added**
TOTAL	**Total output by sector**			**Total consumption by final users**	

In the example reported in **Error! Reference source not found.** below, 10% of the cereal production is used as input in the productive process of agriculture and 33% in manufacture. 57% is consumed by individuals. With respect to columns, the transport sector employs 50% of textiles and 50% of transport services for the total production of 15 units.

Figure 22 - Example of a use I/O table of an economic system composed by only 3 sectors (Agriculture, Manufacture and Transport)

	Sectors			Final users	TOTAL
Products	**Agriculture**	**Manufacture**	**Transport**		
Cereals	10	33	0	57	**100**
Textiles	5	67	5	41	**118**
Transport services	21	23	5	19	**68**
Value added	2	5	5		**12**
TOTAL	**38**	**128**	**15**	**117**	

The combination of the supply and the use tables gives the symmetric input-output table, which requires a transformation procedure in order to move from the product by industry system of the supply and use tables to the product by product system or the industry by industry system.

It is worth stressing that, given the single output technology hypothesis, which implies that a sector produces a single product/service, the only needed information for the purposes of our analysis is the use input-output tables (made by 58 rows and 17 columns).

Price deflators for the industries/productions of the Supply and Use Tables are obtained from different sources' data elaborations and harmonization. Data from STAN are sometimes aggregated at a less detailed ISIC level. In this case, average prices as given by STAN in the ISIC category are used. For instance, agriculture and fishing that are in the ISIC_group 01_02 are distinct categories in NACE. To this purpose, the same price (given by STAN) within the ISIC_group 01_02 was associated to the two categories 01 and 02 in the NACE classification. The associated price is the average of the prices in sectors agriculture and fishing weighted by the relative output shares. In the specific of the various sectors, the following data sources are considered:

- Agriculture, hunting and forestry (A/01-02): OECD - STAN - Two-digit ISIC aggregation system
- Fishing (B/05): OECD - STAN - Two-digit ISIC aggregation system
- Mining and quarrying (C/10-14): OECD - STAN - Two-digit ISIC aggregation system
- Manufacturing (D/15-37): Eurostat - Industry, trade and services - Industry and construction - Industry - Production price indices - Two-digit NACE Rev. 1 aggregation system
- Electricity, gas and water (E/40-41): OECD - STAN - Two-digit ISIC aggregation system
- Construction (F/45): OECD - STAN - Two-digit ISIC aggregation system
- Wholesale and retail trade; repair of motor vehicles, motorcycles and personal and house-hold goods (G/50-52): OECD - STAN - Two-digit ISIC aggregation system
- Hotels and restaurants (H/55): OECD - STAN - Two-digit ISIC aggregation system

- Transport, storage and communication (I/60-64): OECD - STAN - Two-digit ISIC aggregation system
- Financial intermediation (J/65-67): OECD - STAN - Two-digit ISIC aggregation system
- Real estate, renting and business activities (K/70-74): OECD - STAN - Two-digit ISIC aggregation system
- Public administration and defence; compulsory social security (L/75): OECD - STAN - Two-digit ISIC aggregation system
- Education (M/80): OECD - STAN - Two-digit ISIC aggregation system
- Health and social work (N/85): OECD - STAN - Two-digit ISIC aggregation system
- Other community, social and personal service activities (O/90-93): OECD - STAN - Two-digit ISIC aggregation system
- Activities of households (P/95): OECD - STAN - Two-digit ISIC aggregation system
- Extra-territory organizations and bodies (Q/99): OECD – STAN - Two-digit ISIC aggregation system

Employment is obtained as a result of some elaborations. Data from all sectors (A/01-Q/99) STAN - Two-digit ISIC aggregation system - Total employment (number of persons employed) are sometimes aggregated at a less detailed ISIC level than in the I/O tables. In these cases, STAN provides the aggregate value for employment, i.e. total workers in the ISIC category are used, and these aggregates are spread into the relevant subcategories by using a schedule of weights based on relative output shares obtained from the NACE sub-categories.

Labour compensation data are obtained from the all sectors (A/01-Q/99) OECD - STAN - Labour compensation - Two-digit ISIC aggregation system. Labour compensation represents the wage rates, which include: i) basic wages, cost-of-living allowances, and other guaranteed and regularly paid allowances) + ii) overtime payments + iii) bonuses and gratuities regularly paid + iv) remuneration for time not worked + v) bonuses and gratuities irregularly paid + vi) payments in kind + vii) employer contribution to statutory social security schemes or to private funded social insurance schemes + viii) unfunded employee social benefits paid by employers.

ANNEX 5: COMPLEMENTARY INFORMATION

CHAPTER 1: INTRODUCTION

HOW EIDAS WORKS

Based on internal market principles, the eIDAS Regulation does not harmonise national eIDs but relies on their mutual recognition implemented through a notification process. Once a Member State has notified a national eID scheme to the Commission, Member States' experts will peer review the scheme and issue an opinion as regards the compliance of the scheme with the criteria set out in the eIDAS Regulation[4], implementing acts and guidelines[5]. Only Member States can notify eID schemes and this is done on a voluntary basis. eID schemes by private sector providers can be notified under eIDAS only if they are recognised by, or provided on behalf of a Member State. Following a federated approach and the principle of technological neutrality, the eIDAS Regulation does not establish common technological standards but binds together technically diverse national eIDs in three levels of assurance (low, substantial and high[6]) as long as they follow certain minimum criteria and functional requirements for each of those levels. Once an eID scheme has successfully passed the notification process, it should be mutually recognised for cross-border use in all Member States.

Member States are not obliged to offer their citizens and businesses to use eIDs to enable secure access to online public services, but if they do, they should also accept eIDs issued in other Member States (provided that the above notification process is respected). For the system to work, national eID schemes need to be interoperable. As the regulation does not harmonise technical standards, an interoperability framework[7] with technical nodes ("eIDAS nodes") has been established to ensure that the different national eID schemes notified under eIDAS can "speak to each other" and cross-border identification of users is successful. Therefore, even when notified eIDs fulfil the eIDAS legal requirements, lack of connection to the nodes can make the cross-border function unusable.

In eIDAS, Member States are encouraged to also allow private online service providers to rely on national eID means - including notified ones - for identification or authentication purposes when needed to access their online services. The notifying Member State defines the terms of access to the authentication means, including access to the interoperability network of notified eID schemes.

In addition to eID, the eIDAS regulation also provides a legal framework for trust services. There are different trust services under eIDAS that serve different purposes: electronic signatures, electronic seals, time stamps, electronic delivery services and website authentication certificates. Unlike for eIDs, trust services do not need to go through any peer review or evaluation by other Member States. eIDAS establishes the legal framework and market rules to ensure that trust services are provided and recognised across borders with the same legal effect in all Member States as their traditional equivalent paper-based processes. In this regard, it also defines clear common rules for liability and burden of proof for the use of trust services. It provides the highest probative value and legal certainty only to qualified trust services (which are equivalent to the physical / paper-based ones). Due to their cross-border recognition, qualified trust services and qualified trust service providers (as opposed to non-qualified) are subject to a strict supervision by Member States' dedicated authorities.

4 Article 9 of eIDAS lays down the notification process

5 Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework; Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification; Commission Implementing Decision (EU) 2015/1984 of 3 November 2015 defining the circumstances, formats and procedures of notification.

6 Article 8 of the eIDAS regulation

7 Article 12 of the eIDAS regulation

Trust service providers that intend to provide qualified trust services shall submit to a supervisory body a notification of their intention to be recognised under eIDAS, jointly with a conformity assessment report issued by a conformity assessment body. These are typically private-sector certification companies. The supervisory body shall verify whether the trust service provider and the trust services intend to provide comply with the requirements laid down in eIDAS, and if confirmed, they are included on the national trusted lists. Member States maintain national lists of qualified providers of trust services and of qualified services they provide, which are communicated to, and published by the Commission. The basis of the conformity assessment are the functional requirements of the eIDAS Regulation, supported by secondary legislation and available technical standards, although many of these have not been explicitly referenced and harmonised by adopting implementing acts. The eIDAS Regulation relies on international standards defined by recognized standardisation organisations such as ETSI, CEN, ISO, etc. The Commission supports the use of ETSI/ CEN standards. The standards are frequently updated and published. Today, there are ETSI/ CEN standards for trust services in almost all relevant areas[8,9,10,11].

DEMAND FOR DIGITAL IDENTITY SOLUTIONS

Cost efficiency: One of the main benefits of using digital identity solutions is the potential for efficiency gains, both in private and public sectors. For example, the banking sector's digital champions'cost/income rate is 4 percentage points better and return on equity 1,9 percentage points higher than their incumbent peers[12]. The value of strong user authentication, in particular, is to allow service providers to communicate with their customers online with confidence and cut costs of bricks and mortar. The difference in cost of the online and physical channels can be threefold[13].

User experience: Managing multiple digital identities has become a considerable burden for users, who are often asked to create a digital identity for each service they want to access. Most of these identities are not interoperable and their number will constantly increase due to the digitalisation of organisations. According to research conducted by the Ponemon Institute, nearly 50% of consumers have been unable to execute an online transaction due to forgetting their password[14]. This has led to the emergence of new digital identity solutions that are self-managed, or managed by a third party external to the service provider[15]. Convenience is also triggering an increasing demand for mobile-based solutions[16] along with rapidly increasing mobile penetration[17]. European citizens expect their eID to function on their mobile phone[18], with the result that mobile-based digital identity solutions and digital wallets (where users can store passwords or other identity data) are increasingly popular on the market.

Authentication solutions to private online services, using third-party authentication services (e.g. using a Facebook or Google account to log in to different services), are becoming more common

8 Advanced electronic signatures must comply with one of the following ETSI technical specifications: ETSI TS 103 171 v.2.1.1. with the exception of clause 9, ETSI EN 319 132-1 V1.1.1, ETSI TS 103 173 v.2.2.1. with the exception of clause 9, ETSI EN 319 122-1 V1.1.1, ETSI TS 103 172 v.2.2.2. with the exception of clause 9, ETSI EN 319 142-1 V1.1.1

9 Associated signature container must comply with the following ETSI technical specifications: ETSI TS 103174 v.2.2.1, ETSI EN 319 162-1 V1.1.1

10 Advanced electronic seals must comply with one of the following ETSI technical specifications: ETSI TS 103 171 v.2.1.1. with the exception of clause 9, ETSI EN 319 132-1 V1.1.1, ETSI TS 103 173 v.2.2.1. with the exception of clause 9, ETSI EN 319 122-1 V1.1.1, ETSI TS 103 172 v.2.2.2. with the exception of clause 9, ETSI EN 319 142-1 V1.1.1

11 Associated seal container must comply with the following ETSI technical specifications: ETSI TS 103174 v.2.2.1, ETSI EN 319 162-1 V1.1.1

12 https://www2.deloitte.com/content/dam/Deloitte/ce/Documents/financial-services/ce-digital-banking-maturity-2020.pdf

13 https://www.fintechfutures.com/files/2018/10/Backbase_The-ROI-of-Omni-channel_Whitepaper-2.pdf

14 Gigya: Social Login 101: Everything You Need to Know About Social Login and the Future of Customer Identity (2015)

15 Gartner: Innovation Insight for Bring Your Own Identity (2019)

16 Since 2016, mobile has overtaken desktop as the main means of accessing websites, with a market share of 53% in 2018: StatsCounter. (2020). Desktop vs Mobile Market Share Worldwide

17 Estimated to reach 88% in 2025: ENISA. (2019). eIDAS compliant eID Solutions

18 This is supported by the results of the Open Public Consultation in which 90% of respondents consider the ability to use their eID on their mobile phone as very important or somewhat important.

in eCommerce. This way of authenticating offers convenience, improves conversion rates (due to not forgetting passwords) and helps save costs on password resets[19].

Security and trustworthiness: While convenient solutions such as those offered by platforms are most popular, they lack the level of assurance of identity required by certain sectors (public sector, health, financial etc.) and increasingly expected by users concerned about their data protection and privacy. According to a Gigya survey, more than 80% of consumers admit to having quit an online registration form because they were uncomfortable with the amount or type of information requested[20]. A recent Eurobarometer survey shows that 88% of consumers wish for more control over their data[21]. Moreover, high-profile data security breaches has highlighted the need to counter evolving cyber risks and is driving innovation in secure digital identity solutions[22]. Technologies such as artificial intelligence, internet of things, data analytics, biometrics, blockchain and mobile technology intersect to establish and verify a claimed identity. Juniper Research reports regulatory technology spending exceed $127 billion by 2024[23]. These technological developments have also resulted in an increasing role and demand for solutions enabling the identification of non-human entities (e.g. IoT devices).

Secure authentication is opening up service possibilities at a scale that would otherwise not be possible. For example, the very high uptake of BankID[24] (95% usage to access public services) has made it possible to provide digital e-Health services for almost all citizens in Sweden, offering services such as: patient journal, vaccinations, doctor appointments, e-prescriptions, secure messages, test results (including COVID tests), travel expenses, change of regular doctor.

PROVIDERS OF DIGITAL IDENTITY SOLUTIONS

Several eID schemes are based on a federation of private sector identity providers, either under the direction of or independent from the government, with examples including notified schemes under eIDAS such as SPID[25] in Italy and ITSME[26] in Belgium, as well as schemes not notified under eIDAS like BankID[27] in Sweden. Derived identities (i.e. identities derived from official ID documents) such as Verimi[28] are also emerging[29]. Based on patent surveys there are clear indications that the platforms are considering this approach.

The social login market features several market players such as Facebook (including Instagram), Google Sign-In, LinkedIn, Twitter and Amazon. These five have an aggregated market share of 87% of social logins in Europe[30]. One competitive advantage enjoyed by these players appears to be linked to the amount of data they store and can share about their users to service providers, and the related convenience for users to use these log-in services instead of engaging in a new registration. Amazon is emerging as the main identity provider across eCommerce websites thanks to its capacity to streamline the checkout process[31]. Facebook Login, Google Sign-in, Twitter Sign-in, Instagram Login and LinkedIn Login are used by over 50.000 service providers as solutions to allow users signing in into their websites[32].

19 According to Forrester, one password reset may cost up to $70: https://www.onelogin.com/blog/is-password-reset-the-pebble-in-your-businesses-shoe
20 Gigya 2014 Privacy & Personalization Survey (2014)
21 Eurobarometer 503, Attitudes towards the impact of digitalisation on daily lives, December 2019,
22 The European Union Blockchain Observatory and Forum Blockchain And Digital Identity Blockchain For Government and Public Services. (2019) Blockchain and Digital Identity
23 Juniper Research whitepaper "Opportunities for AI in regtech"
24 BankID is the leading electronic identification n Sweded, developed by a number of large banks for use by public authorities and companies.
25 SPID – Public Digital Identity System (https://www.agid.gov.it/en/platforms/spid)
26 ITSME (https://www.itsme.be/en/)
27 BankID (https://www.bankid.com/en/)
28 Verimi (https://verimi.de/en/)
29 Deloitte, VVA, Spark Legal Network, Ecorys. (2020). Study to support the evaluation of eIDAS - First Interim Report. Unpublished.
30 LoginRadius: Digital Identity Trends (2019)
31 Gigya: Social Login 101: Everything You Need to Know About Social Login and the Future of Customer Identity (2015)
32 https://stack.g2.com/

Dedicated digital identity companies: In addition to ITSME, SPID and BankID mentioned above, some of the solutions available include: Yoti (UK)[33], SisuID (FI)[34], GlobalID (CH), Onfido (UK), Chekk (HK), Janrain (US), Gigya (IL).

Digital identity networks: Included within this category are "**derived identity" providers**, which draw on existing digital identities to create a new, more user-friendly one. Examples of this type of solution are provided by Mastercard (US), Verimi (DE) and Yes (CH).

Identity as a service providers: Solutions available on the market are provided by operators including Atos (Evidian,FR), Auth0 (US), Broadcom (CA Technologies,US), ForgeRock (US), IBM (US), Idaptive (US), Micro Focus (UK), Microsoft (US), Okta (US), OneLogin (US), Optimal IdM (US), Oracle (US), Ping Identity (US), SecureAuth (US)[35].

MARKET STRUCTURE

Figure 23 - Market Structure today

33 https://www.yoti.com/

34 https://www.biometricupdate.com/201912/finnish-ministry-tests-sisuid-biometrics-nixu-restructures-amsterdam-team

35 These services are delivered to a service provider through a remote connection from a third-party provider, as opposed to the feature being managed on site and by in-house personnel alone. Solutions provided by such cloud service providers may be more reliable and robust than in-house security and authentication systems. Solutions available on the market are provided by operators including https://www.gartner.com/en/documents/3956209/magic-quadrant-for-access-management

Figure 24 - Development of Market Structure

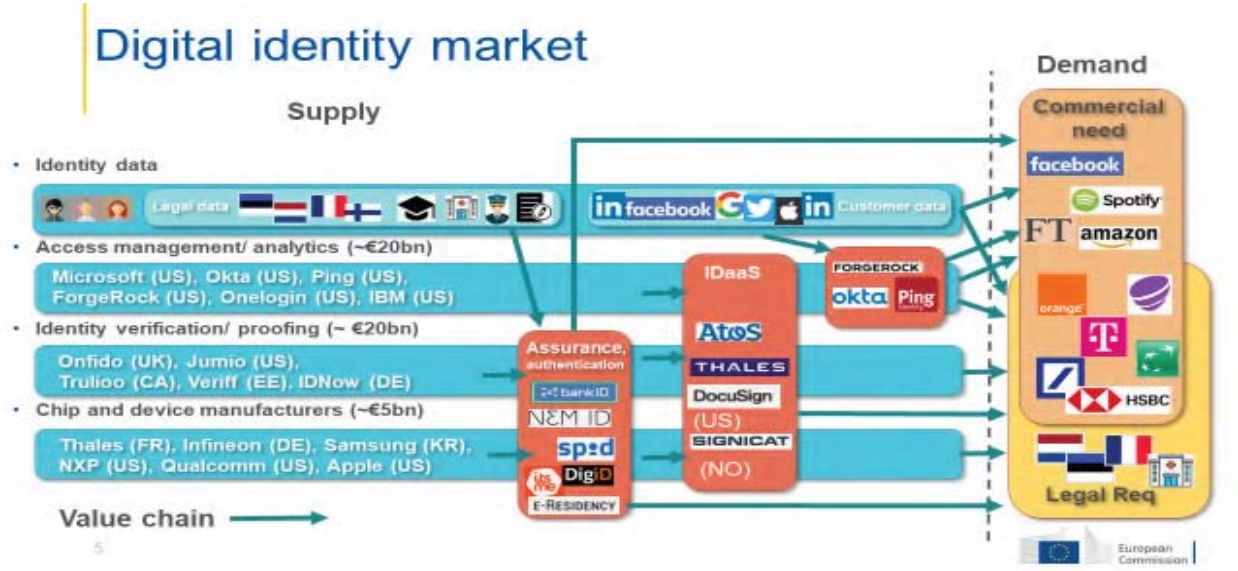


Figure 25 - Digital wallets

CHAPTER 2: PROBLEMS AND DRIVERS

OVERVIEW OF THE IMPLEMENTATION OF THE EIDAS REGULATION ACROSS MEMBER STATES

As regards eID: Since the entering into force of the eID part of the Regulation in September 2018, 14[36] Member States have notified at least one eID scheme, and four[37] Member States have notified multiple schemes. In total, 19 eID schemes have been notified so far[38]. By March 2021 three Member States[39] have pre-notified their schemes. Since there is no obligation to notify eID schemes under the eIDAS Regulation, several Member States with national eID schemes in place have so far not notified them. The reasons for slow uptake by Member States are manifold and depend on the specific national situation and includes legal incompatibilities, technical interoperability issues, absence of national schemes, and lack of resources or political interest in notifying national schemes. For example, some Member States believe that the functional

[36] The United Kingdom notification of UK.GOV Verify (on 2 May 2019) is not included in this analysis.

[37] Belgium, the Netherlands, Italy and Portugal. A number of notified eID schemes includes multiple eID means (e.g. in case of Estonia the eID card and Mobiil-ID, amongst others)

[38] State of Play 8 September 2020: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Country+overview

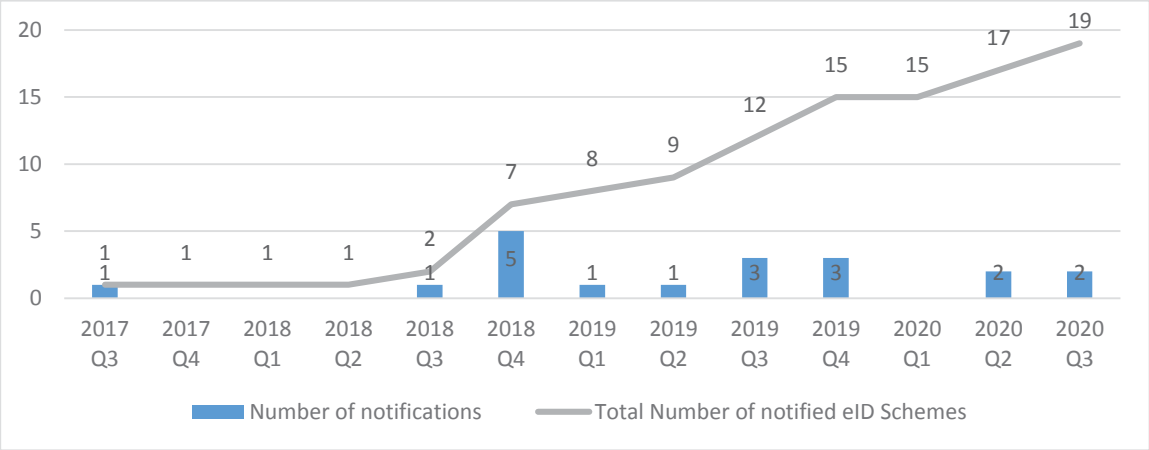
[39] Sweden, France and Malta

requirements of the Regulation leave to much room for discretion with respect to appropriate security levels.

Figure 26 - Overview of the notified and pre-notified eIDs under eIDAS[40] (State of play April 2021)

Overview of notified eID schemes under eIDAS							
Country		eID scheme	Publication in OJ	Country		eID scheme	Publication in OJ
	Germany	National ID card	26.9.2017		Czech Republic	National ID card	13.9.2019
	Italy	SPID	10.9.2018		Netherlands	eHerkenning	13.9.2019
		National ID card	13.9.2019			DigiD	21.8.2020
	Spain	National ID card	7.11.2018		Slovakia	National ID card	18.12.2019
	Luxembourg	National ID card	7.11.2018		Latvia	eID karte, eParaksts	18.12.2019
	Estonia	ID card, Mobiil-ID, e-Residency	7.11.2018		Denmark	NemID	8.4.2020
	Croatia	Personal ID card (eOI)	7.11.2018		Lithuania	National ID card	21.8.2020
	Belgium	Citizen eCard	27.12.2018		*Sweden*	Swedish eID - BankID Freja eID	*Pre-notified*
		FAS/itsme	18.12.2019				
	Portugal	National ID card	28.2.2019		*France*	FranceConnect+	*Pre-notified*
		CMD - mobile	8.4.2020				
	UK	*GOV.UK Verify*	*2.5.2019*		*Malta*	Identity Malta	*Pre-notified*

Figure 27 - Progress of notifications of eID schemes[41]



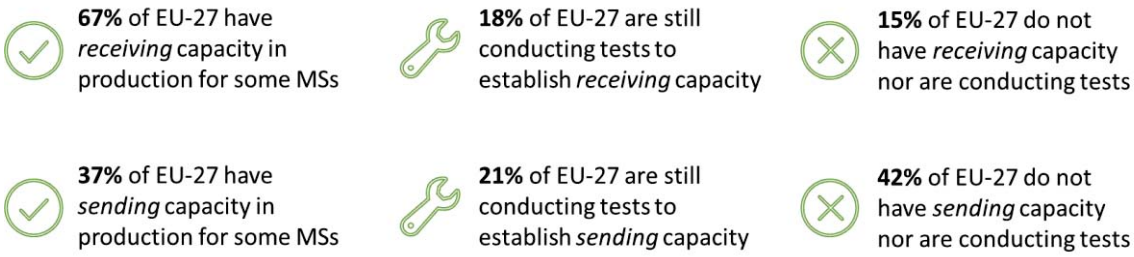
The **eIDAS Network** for eID consists of the eIDAS nodes established at Member State and EU level, including EFTA EEA Countries (Iceland, Liechtenstein, and Norway), and interconnects the notified eID schemes connected to the eIDAS node at national level. The information linked to the status of the eIDAS node is hard to collect as it based on the self-reporting of EU and EFTA EEA countries. Each country has to first develop the receiving function of the node, allowing cross-border users to use their notified eID scheme to access online public services within the country of the node. For countries that have already notified an eID scheme, the

[40] State of play April 2021 – detailed list of currently pre-notified or notified eID schemes including their origin, title, means provided, levels of assurance, status and date of publication in the OJEU is available at: https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS

[41] This graph is based on the data available on CEF digital and include the notification of UK : https://ec.europa.eu/cefdigital/wiki/x/iw3oAg

sending functions also needs to be developed so that the holders of the notified eID scheme can use it abroad. Most eIDAS nodes are in production but some are not fully operational. Generally, Member States are prioritising the development of their receiving function. The sending function might only be developed once a country has effectively pre-notified an eID scheme.

Figure 28: eIDAS node sending and receiving capacity across EU[42]



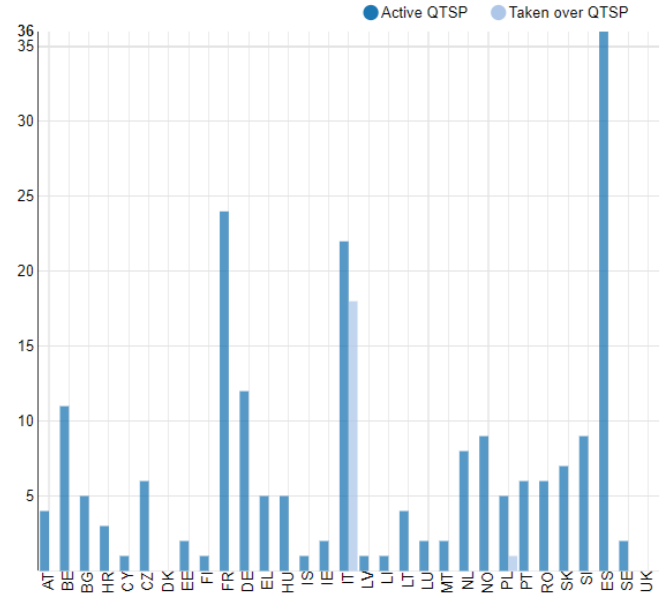
As regards trust services: the number of cross-border authentications and especially the number of receiving transactions provides an estimate on the current usage of notified eID schemes, as it is related to the number of use cases where citizens request access to an online service across borders.

As regards trust services, the eIDAS Regulation has successfully established legal certainty on the liability and burden of proof and international aspects, and on legal effects of trust services, but some issues remain.

Both the **availability and take-up of trust services** in Europe have been increasing since the introduction of the eIDAS Regulation, however, there are differences among Member States and among the different trust services. Availability and take-up are overall very low in some Member States. There are currently 202 active qualified trust service providers[43] operating in 28 of the 31 EU and EEA/EFTA countries. Qualified eSignatures are the service provided most on the market (158), followed by qualified time stamps (114) and qualified eSeals (107). Out of the five core trust services (Qualified certificate for electronic signature, Qualified certificate for electronic seal, Qualified time stamp, Qualified certificate for website authentication, Qualified electronic registered delivery service), the latter service is the most limited one, featuring only 20 active services in seven Member States[44] at present. The eIDAS Regulation has successfully defined the legal effects and provided a well-functioning framework for the provisioning of qualified trust services, electronic signatures, electronic seals, electronic time stamps, electronic registered delivery services and electronic documents across borders.

[42] Source: European Commission, cross-border interoperability testing, collaborative platform of EU experts (not accessible to the public)
[43] State of play in April 2021: https://webgate.ec.europa.eu/tl-browser/#/dashboard
[44] BE, BG, DE, ES, FR, NL,SI,

Figure 29 - Active QTSPs in 29 countries[45]



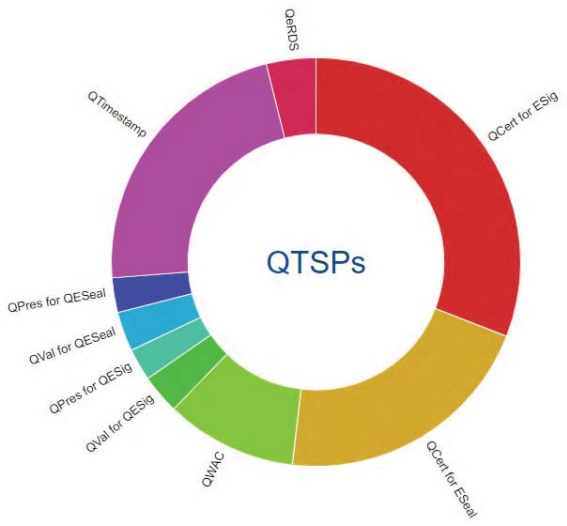


Figure 30 - Qualified trust services in Europe[46]

Type of Qualified Trust Service	Nr of active QTS	Nr of EU and EFTA EEA countries in which the QTS is active	EU and EEA/EFTA countries in which the Qualified Trust Service is active
Qualified certificate for electronic signature	152	28	AT, BE, BG, HR, CY, CZ, EE, FI, FR, DE, EL, HU, IS, IE, IT, LI, LT, LV, LU, MT, NL, NO, PL, PT, RO, SK, SI, ES
Qualified time stamp	109	23	AT, BE, BG, HR, CZ, EE, FR, DE, EL, HU, IE, IT, LV, LT, LU, NL, NO, PL, PT, RO, SK, SI, ES
Qualified certificate for electronic seal	102	24	AT, BE, BG, HR, CY, CZ, EE, FR, DE, EL, HU, IE, IT, LV, LT, LU, NL, NO, PL, PT, RO, SK, SI, ES
Qualified certificate for website authentication	51	20	AT, BE, BG, HR, CZ, FI, FR, DE, EL, HU, IT, LU, NL, NO, PL, PT, RO, SK, SI, ES
Qualified electronic registered delivery service	20	7	BE, FR, DE, NL, PL, SI, ES
Qualified validation service for qualified electronic signature	15	10	BE, BG, CZ, FR, LT, PL, SI, SK, ES, SE
Qualified validation service for qualified electronic seal	15	10	BE, BG, CZ, FR, LT, PL, SK, SI, ES, SE
Qualified preservation service for qualified electronic seal	13	9	BG, CZ, FR, HU, MT, PL, RO, SK, ES
Qualified preservation service for qualified electronic signature	12	7	BG, CZ, FR, HU, MT, PL, RO, SK, ES

THE USAGE OF NOTIFIED EID BY PUBLIC AND PRIVATE SECTORS

The decentralised nature of the eIDAS network makes it difficult to obtain specific data on the usage of notified eID schemes by public and private sectors. Few Member States have put in place modules allowing to keep track of the statistics of usage of their eIDAS nodes. To assess the usage of notified eID schemes, a number of criteria at the supply and demand side are relevant:

[45] If there exist active QTSPs that have been taken over by other entities, this number of active taken-over QTSPs are presented in a different color, separately from the active ones. Active taken-over QTSPs are defined as those qualified trust service providers who have ceased issuing new trusted tokens (e.g. not issuing qualified certificates anymore), and whose remaining obligations regarding these tokens (e.g. managing the revocation requests and status of these qualified certificates) have been taken over by another entity. (State of play April 2021: https://webgate.ec.europa.eu/tl-browser/#/dashboard)

[46] Statistics sourced from Trusted List Browser (https://webgate.ec.europa.eu/tl-browser/#/) on 8 September 2020

- A critical mass of eID schemes must be notified;
- Relying parties must be connected to the national nodes;
- Private service providers must be entitled to access the domestic node, foreign nodes and notified identity providers;
- Citizens and businesses must have a need to access a service across borders and must be aware about the possibilities to use their national eID for this purpose;

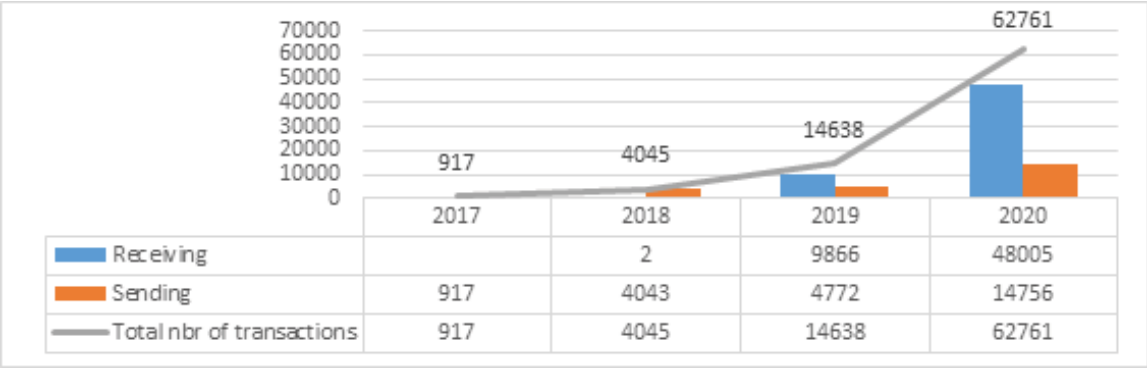
A limited number of Member States have provided the number of relying parties connected to their eIDAS node and the situation can vary considerably between Member States depending on size and organisation of their public services: in some countries, each municipality provides some specific services and would therefore need to connect to the national node while in other countries, key public services are provided centrally.

However, the number of services connected to the national nodes is considerably smaller than the number of services declared as being accessible via the domestic eID scheme. On the basis of available data it seems that only about half of the services accessible through domestic eID are connected to the national eIDAS node.

Figure 31 - Number of relying parties connected to the national eID scheme[47]

Member State		2017	2018	2019	2020	Comments
Belgium (FAS)			1000			Public services only
Czech Republic (eID card)					79	
Germany (eID card)					95	
Netherlands (DigID)				663	*(Target: 12 000)*	
Netherlands (eHerkenning)		260	330	393		
Italy (SPID)	Public				4 478 *(Target: 10 000)*	Data from 30/07/2020 Data from 03/06/2020
	Private				11	
Portugal			150		202	Public and private
Luxembourg	Public		>200			
	Private		6			

Figure 32: Evolution of the number of yearly cross-border authentications in Austria, Czechia, Estonia, Netherlands, Luxembourg, and Sweden



To assess the potential cross-border usage for public services, different proxies can be used. According to Eurostat, in 2019, less than 4% of EU citizens of working age were residents of another EU Member State than where they hold their citizenship. In principle, they should be able to use one eID to access public services in both Member States. In addition, there are online

[47] Study SMART 2019/0046 evaluating the European Regulation 910/2014 (eIDAS Regulation) has been commissioned by the European Commission Directorate-General for Communications Networks, Content and Technology H4 (DG CNECT H4) and performed by Deloitte , VVA, Spark and ECORYS, pg. 38

public services where user authentication is needed and that can be used by e.g. tourists (about 30% of EU population travel yearly to another Member State) such as buying tickets for public transport, museums or subscribing to bike rentals.

It is likely that the number of public services connected to the eIDAS network remains very low, since citizens access to services will continue to depend on technical and architectural choices made by Member States on their national identity systems. For instance, it is expected that some Member States will not change their approach not to centralise their eGovernment services on central platforms or gateways (e.g. Estonia), thus not offering their citizens a good access to the eIDAS network and an effective recognition of notified eID schemes. Similarly, it is expected that the number of cross-border authentications to remain very low, particularly when compared to the usage of the eIDs at national level.

To assess the overall potential of eID use, we can rely on existing use as proxies. Available data from some Member States (e.g. NO, SE, EE, LV, LT), where user authentication solutions are widely re-used by different service providers, authenticating oneself with a legal identity is done roughly around 20 times per month, of which 1 occurs in the public sector. If that relationship is extrapolated to the EU level, we can assume the potential for EU to be roughly 100 billion user authentications per year of which 5 billion in the public sector. On the basis of these assumptions, for example, if we expect 3% of people living in another Member State to only use eIDAS in the current scope, the potential of eIDAS authentications in this case would be 150 million per year.

In relation to the articulation of relationships between eIDAS and private sector service providers, these are expected to remain suboptimal. Even if all notifying Member States potentially open their eIDAS nodes to the private sector services providers across the Union, the diversity of national conditions for the use of the national eID infrastructures will still make it very difficult for the service providers to build a sustainable business plan or to accurately estimate the potential of this openness to expand their business cross-border. Moreover, given the difficulty raised by the constraint to harmonize the various approaches followed at national level, a revenues model and establishing clear liability rules would be difficult to construct.

CHAPTER 5: OPTIONS

Development and Distribution of the European Digital Wallet

Regardless of the sub-option for deployment retained, the following types of activities would need to be carried out:

- Develop a **mobile application** for each platform (Google Play Store, Apple App Store, Microsoft Store, Huawei AppGallery, other). The app would have to meet the relevant requirements of the respective app stores;
- Design the **security architecture** of the app so that it meets the level of security required under EU law (see below) to provide the European Digital Wallet, which would include the capacity to store cryptographic keys. It would be up to the service provider to decide whether to rely on an embedded hardware element in the device (eSE) or an embedded SIM card (eSIM). In the case of eSE, mobile device manufacturers would have to provide access to the eSE. For SIM cards, agreements with all relevant mobile network operators would have to be reached.

The app provider would also need to envisage agreements with relevant credential issuers and service providers covering aspects on liability[48], invoicing, interoperability, availability, support

[48] Depending on the sub-option for deployment retained, respective rules on liability set in the eIDAS Regulation would also apply - article 11 (implementation by Member States) or 13 (implementation by the private sector).

etc.; Specific governance arrangements to ensure consistent and effective implementation may have to be agreed as part of the reference framework for the European Digital Identity Wallet (see measure 2 below).

The provider would need to take organisational measures to deal with incidents and offer customer support for credential providers, service providers and end-users[49].

Onboarding / linking of the European Digital Wallet with official identities

After downloading the Wallet App from an app-store, the Wallet provider would ensure the wallet can be linked to the user's notified eID for the service to be recognised at qualified level and ensure it can receive and exchange qualified attributes and credentials or allow the user to create qualified e-signatures. Two possibilities exist to establish this link, depending on whether the user's country of residence has already notified a national eID scheme under eIDAS or not:

A national eID scheme has already been notified under eIDAS:

2 The European Digital Identity Wallet providers will digitally link the wallet with the user's national eID. No additional identity proofing or on-boarding process will be necessary.

A national eID scheme has not been deployed and has not yet been notified under eIDAS:

3 The link can be established by physical appearance or equivalent remote verification means, subject to rules that require high level of assurance. Technical references for these procedures will be set in implementing acts[50].

[49] For example, the provider would need to set a process for dealing with complaints and disputes concerning all actors. Incidents might be related to fraud (for example if a user's identity is being used by someone else to sign in to your service), service delivery (for example if users cannot use your product or service because it's temporarily unavailable) or data breach.

[50] This link could for instance be established by means of qualified identity credentials offered by a qualified trust service provider through procedures which are externally audited, verified and supervised by national competent authorities to meet requirements which reach the equivalent quality, security, assurance and reliability requirements than those applicable to notified eID means of level high. Alternatively, qualified certificates for signatures created with a certified qualified signature creation device could also secure the onboarding process.

Figure 33 --- The on-boarding process:

CHAPTER 6: IMPACTS

Detailed analysis of the costs and benefits entailed by the measures put forward in the context of Options 1-3.

BASELINE SCENARIO (POLICY OPTION 0)

Policy option 0 represents the baseline scenario, in which the Commission would not propose any changes to the current legislation, and the eIDAS Regulation and its framework would therefore remain in force. In this legislative context, the following measures can be brought forward.

- **Gatekeepers to offer access and interoperability with notified eIDs (as per Digital Markets Act)**

Costs

As highlighted in the Impact Assessment for the Digital Markets Act, compliance costs for the **gatekeepers** would be insignificant when compared to their revenues and could be absorbed by gatekeepers with little incentive for them to pass on costs to business users or to consumers. Indirect (other than compliance) costs may be higher, but the impact of such changes is difficult to quantify.

Supervision of gatekeepers complaint-handling etc. are likely to create certain costs for **public authorities**.

Benefits

Online service providers are protected against lock-in and could choose to offer the use of trusted eIDs, as an option for identification to their services. The measure would positively impact the protection of personal data online since notified eIDs do not require their disclosure.

- **Require Member States to limit identification data transmission to only the data necessary for a particular transaction**

Costs

Technical adaptations are likely to create limited costs for **public authorities**.

Benefits

If successfully adapted, the future Interoperability Framework and the eIDAS technical specifications, would positively impact on the citizens' and companies' opportunities to share only the identity attributes required for the transaction at stake. Similarly, online service providers would not be able to request more data than needed for that specific transaction. The measures would also empower users to send anonymous credentials, without disclosing the identity of the person and pseudonymisation, thus avoiding profiling opportunities for eID providers.

This measure will also positively impact on **citizens' and companies'** trust in public authorities, and contribute to make users - in particular citizens and SMEs - aware of the value brought by the EU citizenship.

Simplify and improve notification and peer-review processes

The following actions could be taken under the baseline:

4 a simplification of the notification process by opening the possibility to reuse the same standards/technological solutions ("blocks") already peer-reviewed or otherwise certified and notified by other Member States in the context of other notifications (the measure implies amendment of secondary legislation).

5 strengthened focus on interoperability: This action would design the peer reviews to allow for better focus on interoperability issues, such as the conformity and readiness of the eIDAS nodes which would need to be operational before notification (the measure implies amendment of secondary legislation).

6 strengthening of the peer-review guidance: This action would improve the consistency of peer reviews by strengthening the guidelines that support the peer-reviews processes (e.g. Guidance on the Levels of Assurance, Guidance for notification under eIDAS Regulation). In order to ensure consistency in scope, depth and length of peer reviews, guidelines would e.g. reference objective assessment criteria identified by standards, once available (e.g. related to the use of biometrics, remote identification, and mobile schemes).

7 harmonise peer-review reports: This action would establish a template for peer review reports to ensure harmonisation in terms of assessment granularity. Summaries could be made publicly available to increase transparency and trust, with due consideration to Member States' views on the confidential information (the measure implies amendment of secondary legislation).

8 introduce Conformity Assessment Reports: Certification carried out by conformity assessment bodies (as it is currently the case for trust services) issuing conformity assessment reports may be used by the Member States to support their claims during the peer-reviews on the alignment of the schemes or of parts of them with the requirements of the Regulation on the interoperability and the security of the notified electronic identification (Article 7, Article 8 and Article 12 of the eIDAS Regulation). Prior-certification would facilitate the endorsement of the notified schemes by the Cooperation Network. This action would be in synergy with Measure 6 under Option 1: Strengthen security requirements for mutual recognition described below (this measure and implies the amendment of the Regulation and of the secondary legislation).

9 establish clear rules for the notification of 'federated' schemes (i.e. schemes that are composed of several identity providers and a variety of eID means) and clarify which changes to an existing eID scheme would require a new peer review (the measure implies amendment of secondary legislation).

10 introduce dispute settlement mechanisms: This action would establish a dispute settlement mechanism internal to the eIDAS governance between Member States in relation to issues linked to the security or interoperability of the pre-notified eID schemes. The aim is to facilitate agreement on the assessment of interoperability and security of notified eID schemes. Since the opinions of the Cooperation Network are not binding, alternative mechanisms need to be established whenever divergences between Member States appear and consensus is not in reach (the measure implies amendment of secondary legislation).

Costs

Currently, an eID scheme only becomes effectively available under the eIDAS network almost 2 years after the notification, which, as noted in the evaluation of eIDAS, is widely seen as taking too long[51]. A more efficient peer review process would reduce the time and complexity (and implicitly the costs) of the notification process (estimated by stakeholders to cost, on average, around €40,000 to €100,000 per notification[52]) and result in less workload for the Cooperation Network. Costs would be entailed by the coordination of the Member States in amending the implementing acts on the procedural arrangements for cooperation between Member States on electronic identification (2015/296) and on defining the circumstances, formats and procedures of notification (2015/1984).

Benefits

A more harmonised and transparent approach would shorten the time for notification of eIDs by Member States and provide citizens faster with the benefits of the mutual recognition of eID schemes. Citizens would be empowered to make more informed choices, based on a better understanding of the possibilities offered by the eIDAS solutions.

- **Harmonise Supervisory Procedures for Trust Services**

Costs

We expect that costs will involve in a first stage coordination work among **national competent authorities** needed to discuss and approve the scope of harmonisation and standardisation activities, with the support of the Commission. Given the current divergent approaches across Member States on issues such as remote identification, significant standardisation work may be needed at the European level to develop the ensuing guidance.

It is expected that **conformity assessment bodies** will incur costs stemming from the adoption of **new routines** triggered by the new standards and **familiarisation costs** of the staff with the new implementing acts and procedures.

Benefits

Clearer and more harmonised rules on audits are likely to reduce the need for **Supervisory bodies** to re-audit QTSPs that have already been audited by accredited conformity assessment bodies, as well as reduce time and resources spent reviewing and requesting changes to the conformity assessment reports. Harmonising and standardising the audit procedures is expected to reduce considerably the number of (re)audits carried out by supervisory bodies.

Once binding harmonized standards for all conformity assessment bodies across Europe are available, it is also expected that the previous difficulties raised by "forum shopping" by **QTSPs** and divergent approaches in the severity of audits in Europe would be alleviated.

[51] Deloitte, VVA, Spark Legal Network, Ecorys. (2020). Study to support the evaluation of eIDAS

[52] The estimate corresponds to the range of expenditure provided by Member states participating in a survey conducted for the evaluation of the eIDAS Regulation. It is based on 5 data points. Additional data points were collected through the interviews conducted as part of the supporting study, which are consistent with the range estimated.

Tackling the legal uncertainty across the EU triggered by the possibility opened by the eIDAS Regulation to leave to the discretion of Member States the assessment on the equivalence of **remote identification** methods with the physical presence would generate significant **internal market benefits**, driven by the speed and convenience and cross-border reach of the remote processes.

The common position put forward by the **Forum of European Supervisory Authorities** (FESA)[53] on the review of eIDAS lends support to the strong consensus on the need for greater harmonisation on key trust services aspects of the Regulation. Only one country (AT) expressed concerns with regard to the possible cost implications of these reforms for the **national competent authorities**.

The measures to increase the harmonization/coherence of trust services are expected to trigger benefits for **TSPs** (qualified and non-qualified) essentially linked to a clearer regulatory framework and the lack of ambiguities in the accreditation and conformity assessment processes. This would reduce national divergence in the qualification of TSPs in different countries and of their qualified trust services and therefore supporting a level playing field.

Introducing harmonized requirements on remote identification would support **citizens** to avoid the difficulties raised by practical situations - such as the need to renew their certificates or to receive technical support – for which, under many national legislations, they are required to be physically present in the country of issuance. Overall, this was one of the measures gathering the most support among stakeholders, with 43% of respondents to the open public consultation identifying it as a key corrective action to be taken.

Savings are also expected in relation to the **conformity assessment body** accreditation procedures. It is also likely that the stable framework would foster an increase of conformity assessment bodies' revenues, while the definition of a standard conformity assessment report is also likely to provide more clarity on the requirements to be assessed and to reduce the amount of time requested to complete the report.

POLICY OPTION 1.

- **Measure 1: Mandatory Notification facilitated by a streamlined notification procedure**

Costs

In relation to the future mandatory notification, the major costs of this measure will be borne by the 13 remaining **Member States** who have not yet notified an eID scheme. All other Member States will bear only marginal costs linked to adapting the authentication service to their Public Administrations to ensure the recognition of new notified eIDs. Some of the Member states will have to invest in their eID system before notifying it, particularly those not having a fully-fledged eID system, as well as bear the costs of the notification process estimated at between €520,000 and €1.3 million across the 13 Member states.

The costs for **Member States public authorities** to develop a fully-fledged eID scheme from scratch would be shaped by specific cost drivers linked to inherent country characteristics as well to the overall system design or technology chosen. To provide an indicative range of investments: around €40-60 million were invested for the Finnish eID scheme; €72 million

[53] "Harmonization in conformity assessment of Qualified Trust Services (QTSs) is essential for building actual trust in trust services and for mutual recognition of trust services. Harmonization of accreditation and Conformity Assessment Reports (CARs) will allow fair competition between the CABs and will reduce the incentive for QTSPs aiming at the lowest price. Clear and transparent accreditation and certification schemes will foster the uptake and global reach of the eIDAS Regulation. The credibility of conformity assessments and the quality of the CARs will enhance adoption of harmonized accreditation and certification schemes. It will enable TSPs to better make a weighed choice in selecting a CAB without having to make concessions on the quality of the CARs."

expenditures over 3 years in the Netherlands[54], while 100 € million estimate was provided by Sweden. However, the remaining Member States who have not yet notified an eID already deploy various types of eGovernment platforms or trusted and secure eID systems allowing their citizens access to public services.[55]

The additional cost to **Member States** caused by the mandatory notification will be linked to the implementation of the eIDAS related obligations (interoperability, connection to the eIDAS network). These costs are estimated at €9.7 million for the 13 countries.

Depending on the timeline set for complying with this obligation, **Member States** (eIDAS Cooperation Network) may see an increase in administrative burden triggered by peer reviews, estimated at around €1.2 million in the next two years. The measures aiming to streamline the notification and peer-review processes (particularly under the baseline) are expected to at least partially offset this increased workload. The **European Commission** is also expected to experience additional pressure due to its supporting roles in the peer-reviews and notifications processes.

Benefits

The notification of the eID schemes would be smoother by the streamlining the current procedures under the Regulation. The time needed from the pre-notification of an eID scheme until its publication in the Official Journal of the EU or to the delay for the application of mutual recognition following such publication would shorten.

This measure would reinforce the mutual recognition principle and **Member States** would see their role as providers of primary and secure legal identities fully recognised. As the trust and convenience in using such eIDs on regular basis will increase, a certain rise in the use of public services both at national and European level is expected. This will however reach a "plateau" firstly due to the statistical limitation carried by the number of European citizens living abroad and, even more, due to the systemic deficiencies of eIDAS which are likely to persist even when notifications multiply (see the description under the baseline scenario section).

Mandatory notification would make **citizens and companies** of the notifying countries the first direct beneficiaries of such a measure. The direct effect for them would be to see their digital freedoms expanding considerably by being able to authenticate (at least) to public e-services provided in other EU Member States.

- **Measure 2: Establish a requirement for Member States to allow private online service providers across the EU to rely on notified eIDs**

Costs

Notified eIDs should be adapted to fit the use-cases in the private sector. This may require costs for **Member States / public authorities** which could widely vary and cannot be quantified. For instance, only three[56] notified schemes provide sufficient attributes today required for onboarding of natural persons in the financial sector (i.e. to open a bank account) and none provide all attributes for legal persons.

Estimates developed as part of previous EU interoperability projects suggest that building software from scratch to connect to an eIDAS node would imply a one-off cost to **online service**

54 Dutch Report: (2012) Rekenhof - De elektronische identiteitskaart (eID) Toegangssleutel voor de burger tot e-government: (eID) For the Finnish and Swedish data: collected during targeted interviews by PwC for the purposes of the supporting study.

55 Member States are still in the process of implementing eID systems, mostly smartcard-based: Bulgaria, Cyprus, Greece, Poland, Romania, Slovenia. To be noted that the future Regulation 2019/1157 on strengthening the security of ID cards and residence documents obliges Member States to have an identity card with the security features specified therein by August 2021. Member States could build on the new identity cards and notify them as eID means under the eIDAS Regulation.

56 Signicat (2017) The rise of digital identities: Plugging the 'digital gap' in financial services onboarding. Out of 13 schemes notified at the time of the research. The number has now increased to 19.

providers for putting in place the required infrastructure (the global cost for a relying party could amount to €42,000[57]).

Benefits

An upgraded interoperability framework that enables more cost-efficient, direct service provider connectivity with the eIDAS network is likely to increase private sector take-up. This would trigger savings for **private sector service providers** that decide to adopt these schemes in their workflows when the needed attributes come with the national eID.

- **Measure 3: Establish a common cost-model and liability rules to facilitate private online service providers to rely on notified eIDs**

Costs

This measure will generate costs to **Member States** related to upgrading the operational capacity of eIDAS Nodes - in particular with respect to likely additional security, reliability and data protection requirements - to efficiently and securely handle increased levels of traffic, estimated at €6.1 million across the EU 27 (an average €225,000 per Member State).

Benefits

The mutual recognition principle would be reinforced and **Member States** would see their role as providers of primary and secure legal identities be fully recognised also in the context of online cross-border transactions. As the trust and convenience in using such eIDs on regular basis will increase, a rise in their use in public services both at national and European level is expected.

Since some **Member States** monetise the offer for national eIDs for private relying parties while others provide the service free, developing a common costing model for the use cross border of notified eIDs by the private sector would avoid unfair competition and fragmentation of the EU authentication and attribute exchange market within the eIDAS network and between Member States by preventing "cherry-picking". Similarly, overloading of certain national infrastructures would be avoided.

The development of a comprehensive and balanced cost and liability framework model is expected to incentivise use of the national eIDs by **private online providers**. The clearer the contractual conditions on liability and prices online service providers would be charged for accessing the eIDAS network, the better chances are for them to see opportunities and adhere to such a system. A hypothetical annual growth in transactions between 20% and 33% over the 5 years following implementation can be estimated to generate revenue between €17 million and €53 million and between €816 million and €2.5 billion depending on the assumed revenue per transaction and cost model chosen by Member State.

- **Measure 4: Extend the person identification data set recognised cross border**

Costs

This activity could certainly benefit from the effort made and the lists of attributes already defined in the Member States[58] or internationally[59] where the use of national eID by private sector service providers is facilitated and supported. Some stakeholders expect that no significant costs to **Member States** will arise given the fact that work on an extension of the list of attributes is already in progress within the eIDAS technical subgroup (20.000 EUR per Member State)[60]. However, as revealed by recent work of the eIDAS technical subgroup on the

57 LEPS Project. (2018). *D7.2 Report on Cost Benefit Assessment*

58 See for example the list of attributes defined in Italy for SPID https://www.agid.gov.it/sites/default/files/repository_files/regole_tecniche/tabella_attributi_idp_v1_0.pdf

59 See for example the approach in the UK https://www.gov.uk/government/publications/attributes-in-the-uk-digital-identity-and-attributes-trust-framework

60 Based on views gathered through a survey of Cooperation Network members (see the supporting study for further details)

topic and as expressed by certain stakeholders during the public consultation[61], finding an agreement between Member States on the attributes and on their technical and semantic expression is challenging (e.g. the "nationality" attribute, currently discussed has different interpretations in various countries). Significant standardisation work will also be necessary and, based on stakeholder views, is likely to create one-off costs of around €300,000[62].

The connection to the eIDAS Node of the relevant national registers/systems that contain the required attributes at national level (for instance a patient identifier) might imply additional costs for the **Member States**, depending on how their eIDs are organised. The attributes enablement costs could be minimised by leveraging on dedicated EU funding schemes, building for instance on funding in the context of the Digital Europe Programme

Similarly, the interoperability framework would need adjustments to allow direct integration by **private sector service providers**.

Benefits

The measure will benefit **Member States authorities** by providing a predictable legal framework for the trustworthy and structured exchange of other attributes than the minimum data-set currently used to authenticate for public services.[63]

The Member States providing feedback on this measure in the public consultation generally recognised the potential benefits of this measure on private sector re-use of notified eID schemes, data management and privacy. Similarly, some Member States (BE, LU, NL) explicitly highlight the positive impact on extending the list of attributes to facilitate eID matching (increasing data accuracy) and better uphold the principle of data minimisation.

The minimum dataset typically provided by **Member States** only contains citizens' personal attributes. Therefore, a wide array of cross-border services would be enabled by an extension of the minimum data-set which facilitating seamless access to services in a non-discriminatory way, reducing non-trade barriers to the internal trade of digital goods and services, thus fostering the internal market integration for the benefit of citizens.

Providing a legal reference for the exchange of subsets/supersets of the minimum dataset with an assigned level of assurance via the eIDAS network would reduce associated administrative burden and costs for users to fetch and provide pre-defined authentic documents or attestations (e.g. birth certificate to prove the age) in a number of use cases and transactions with public and private sector service providers.

Comments received from businesses consulted in relation to the proposed extension of the list of attributes were generally positive[64]. Many views from the financial sector recommended complementing the list with customer due diligence attributes, so that CDD processes can be further digitised.

Measure 5: Strengthen security requirements for mutual recognition

Costs

A number of countries already rely on ICT security certification for their eID means when they take the form of the electronic identity cards (e.g. France, Austria, Estonia, Italy, Spain, Poland, etc.). However, ICT security certification is not widely used for other type of eID means. The **Member States** that already require ICT security certification for their eID means will not incur significant additional costs. In addition, for the notifying Member States there will be cost for

61 See for example FESA. (2020). Position Paper On the review of the eIDAS Regulation FESA's answer to the European Commission's consultation

62 Based on views gathered through a survey of Cooperation Network members (see the supporting study for further details)

63 For instance, more than two out of three Member States replying to a survey conducted for the evaluation of eIDAS disagree that the current minimum dataset allows to uniquely identify both natural and legal persons.

64 The majority of stakeholders participating in the interviews were supportive of this measure, and 47% per cent of respondents to the Deloitte / PwC Survey also indicated that this measure would bring greater benefits than costs.

the completion of a conformity assessment report for the eID scheme which is in the order of 80/100K€. For other countries, the conformity assessment process may require more material changes to existing methodologies, possibly creating up-front costs. The cost of familiarisation with the changes for supervisory bodies could amount to roughly €228,000 across the EU 27.

As highlighted by some stakeholders, there is a risk that certification may affect innovation if certification standards fall behind technological advances. This could however be prevented through effective standards review mechanisms and the coexistence of alternative means in absence of standards, as it is already provided in eIDAS for qualified signature creation devices[65]. This potential negative effect may also be offset by the positive contribution of certification to interoperability (as has been the case for e-signatures), which may instead act as enabler for greater innovation.

Benefits

Generally, ICT security certification would result in increasing trust and security in the eID solutions. Conformity assessment and ICT security certification would directly address the current difficulties raised by the lack of agreement between Member States on the criteria that make, for instance, mobile scheme resistant to high level security attacks and making it easier for **Member States** to prove the compliance of the notified eID schemes with the eIDAS security requirements (as defined in the relevant Implementing Acts)[66], thus contributing to the efficiency savings discussed above. Some of the Member States consulted (DE, FR, CZ, and HR) expect a reduction of the costs and delays linked to a lack of a commonly agreed methodology and a reinforced role of eIDAS as a horizontal regulation for electronic identification. ICT security certification would also ensure better alignment of the governance of the eID part of the Regulation with the set-up already in place for the trust services (audits, regular revisions of standards, etc.), which would improve the coherence of the overall eIDAS enforcement efforts.

Citizens would benefit from an increased public trust in eID products, services or processes providing a certified level of cybersecurity.

Relying on a harmonized conformity assessment reports as well as on well-functioning voluntary ICT security certification process would not only significantly shorten the timing and costs of notification processes for **Member States,** but also increase the appetite of private sector to use notified eIDs for access to their services. Even if private sector identity solutions are currently not regulated under eIDAS, a common criteria certification scheme being established under the Cybersecurity Act would contribute to establishing an objective reference and a commonly agreed assessment methodology of the market security requirements.

Savings (estimated at €12,000-24,000 per year per audit for each provider) would be generated for **eID providers** as a result of less extensive re-auditing of new components, relying on elements that have already been certified for use in other applications.

Measure 6: Introducing new Trust Services

Costs

The introduction of a new qualified trust service for **e-archiving** would incur costs linked to familiarisation for **supervisory bodies** as well as enforcement and administrative costs for **Member States** (see below for Option 2, measure 1). There might also be certain interoperability costs which would be absorbed under Digital Europe Programme specific activity on e-archiving.

[65] Art. 30(3) of eIDAS

[66] COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means

Trust Service Providers would see a modest increase in compliance costs including for qualification, particularly those that already fulfil many of the QTSPs requirements. Based on the costs borne by QTSPs for existing services and excluding the economies of scale that would be achieved by already qualified TSPs, the average cost would be around €545,000 per provider for initial qualification and €255,000 on a recurrent basis.

Benefits

The creation of e-archiving as a trust service under eIDAS will enable **Trust Service Providers** (many of them are already providing this service) to enhance trust in their service offer by inclusion in the European trusted lists of this service, likely resulting in increased consumer awareness of and demand for the service. For every additional 1% of businesses purchasing an eArchiving solution - for Trust Service Providers could generate additional revenue estimated at €37 million a year. In addition, the possibility to provision such a service on the whole EU market will give opportunities for economy of scale both on the service being provided – thus becoming more economic and efficient – as well as on the usage by businesses (in particular SMEs) that have to rely diverging nationally services.

Citizens could benefit from the introduction of a new trust service for e-archiving complementing the qualified preservation of qualified electronic signatures. The new trust service will likely stimulate competition, thus the end users will benefit from more competitive services and lower costs.

- **Measure 7: Strengthening the Recognition of QWACs (Qualified Website Authentication Certificates)**

Costs

The measure to ensure that users can use QWACs will come with a cost of around €550 per year, which will need to be sustained by all **online service providers** using it.[67]

While they are not service providers, in respect of **web-browsers**, recognition of QWACs may entail certain impacts, however costs are likely to be limited as the related procedures are already carried out or are part of their standard procedures.

Benefits

Qualified Web Authentication Certificates will increase trust and reduce fraud in the online environment for the **benefit of the user and business in general**. A high level of trust in who is behind a website is particularly important related to **online services provided by public and private sectors**, e.g. e-commerce, e-banking and e-health. The use of QWACs would also support the principle of transparency as set out in Article 13 and 14 of the General Data Protection Regulation and strengthen data protection.

- **Measure 8: Harmonise the certification process for remote electronic signing**

Costs

In terms of costs, harmonised certification would **eID providers** to adapt to new processes and requirements, which would likely imply additional resources in the short term. The switch to a Common criteria (CC) certification is seen as increasing costs of the time needed to develop, modify, integrate, certify the solution, certify and audit the service, and in particular to rapidly patch any identified security vulnerabilities and deploy updates. This might place better resourced providers in the market in an advantageous position.

Benefits

[67] This estimate was calculated in the supporting study.

Based on data gathered for the eIDAS Expert group, greater harmonisation in this area finds generally support among qualified signature creation device vendors and qualified trust service providers, who would be most directly impacted by it.

Standardisation of the certification process would support fair competition and increase the security of trust services for end users. A unified framework that makes reference to EU-wide standards would bring more coherence in remote signing, ensure greater transparency and compliance of solutions with the eIDAS Regulation and better guarantee the security of sever signing systems. As a result of greater harmonisation, the acceptance of mobile trust services in the market would also be enhanced.

POLICY OPTION 2.

- **Measure 1: Creating a new Qualified Trust Service for the secure exchange of data linked to identity**

Costs

For **public authorities** in their capacity as national supervisory authorities of Trust Services under the eIDAS Regulation, establishing a new trust service will incur a one-off cost linked to familiarisation of around €315,000 for all supervisory bodies. The estimated recurrent annual costs of enforcement for supervisory bodies are on average €282,000 per supervisory body[68] or around €8 million across all Member States[69].

There may be modest increases in administrative costs related to cooperation between **Member States** (cross-border cooperation activities on trust services - €25,000 to €90,000 for public authorities) for the purpose of harmonisation of supervision rules and procedures. A new trust service could also result in a modest increase in international cooperation costs for Member States.

The measure would introduce regulatory obligations for **qualified trust service providers** of data linked to identity of: 1) One-off costs of initial accreditation for providing qualified schemes; estimates for these costs varied significantly among the stakeholders consulted, converging on an estimated average of €545,000[70]; 2) Recurrent compliance costs estimated by stakeholders at on average €255,000[71] annually and 3) Technical costs from the need to bring the attribute service up to the standards prescribed by the Regulation which cannot be estimated as they are entirely dependent on the technical standards which are not defined yet.

Part of the **compliance costs** would be linked to the identity proofing of the users, which is an important part of customer onboarding processes.

Qualified trust service providers will be enabled to access authentic sources to extract relevant digital data. Given the different advancement of digitization of government data linked to identity, QTSPs may have to bear the costs of digitalising the credentials to be exchanged. These costs would be embedded in their business model.

Creating a new qualified trust service for the exchange of data linked to identity also brings other market players established in the EU which are active in providing identity today under the framework of the revised eIDAS Regulation as non-qualified trust service providers. Compliance costs, cost of accreditation and cost associated with access to authentic sources will

68 This is the average cost incurred by SBs for supervisory activities as reported by respondents to the survey of SBs conducted for the evaluation of eIDAS. The figure is based on 9 data points.

69 This estimate was calculated in the supporting study.

70 This is the average cost of administrative expenses linked to achieving and maintaining the qualified status reported by respondents to the survey of TSPs conducted for the evaluation. The figure is based on 16 data points from QTSPs that are large private organisations, public organisations and micro-enterprises or SMEs.

71 This is the average annual cost of administrative expenses linked to compliance with eIDAS reported by QTSPS responding to the survey of TSPs conducted for the evaluation of eIDAS. The figure is based on 12 data points from QTSPs that are large private organisations, public organisations and micro-enterprises or SMEs.

not apply to **non – qualified trust services providers**, as they are not currently subject to ex-ante supervision.

Costs incurred by **online service providers** are mainly related to IT integration to the APIs. The initial cost will vary depending on the level of integration sought, the specific use case and the number of standard components that can be used. Relying parties need to upgrade their portals and carry out adjustments to have a new system of verified credentials and attestations.

The stakeholders consulted provided insights to the business model for the exchange of credentials. The key point is that it is not the "order" or the citizen that shall pay to earn the credentials, but rather the online service providers requesting the verification that would pay the trust service provider. The company ITSME offering electronic identify services in Belgium charges €3.04/user/year, in addition to set-up costs, maintenance & support fees[72].

Conformity assessment bodies will incur costs associated with the work in the standardisation committees, the adoption of new routines and the amount of money spent by each to familiarise staff with the new implementation acts and procedures which is €339,000 for Conformity Assessment Bodies.

Benefits

Trust service providers offering secure exchange of data linked to identity will benefit from a significant increase in the potential use base and a level playing field enhanced by legal certainty and common rules established at the EU level. The framework is likely to promote new market opportunities for trust service providers (public and private) of all types of credentials, such as transport companies (car keys, subscriptions), universities (diplomas), business registries (company info), financial institutions (credit cards), credit rating agencies (credit rating info on natural and legal persons) etc.

Assuming all European citizens will engage in around 38 online transactions[73] per years involving both identification and the exchange of data linked to identity, the total number of transactions estimated at EU level would be between 11bn and 17bn[74].

Stakeholder consultations suggest that the creation of "unique" credentials building on specific services, particularly at low levels of assurance, would offer the most profitable opportunities. Issuance of commonly used credentials (e.g. driving licences) is perceived as low-margin; by contrast, more attractive opportunities are likely to open up in designing credentials that are tailored to specific use cases and draw on a unique service that the provider themselves have created

The creation of attributes as a trust service will provide more possibilities for the **citizens** to actively manage attributes, credentials and attestations (e.g. gender, age, professional qualifications etc.), increasing user control of data related to his/her digital identity and enabling personalised online services in a trusted environment where online privacy can be ensured and data is protected[75]. This measure would also improve trust in how attributes, credential ad attestations are handled by **online service providers**. The OPC suggests significant stakeholder interest in this measure, with 41% identifying the introduction of new private sector digital identity trust services for identification, authentication and provision of attributes.

Increased access to secure and convenient digital identity authentication services for **citizens** based on trustworthy digital identity attributes issued and guaranteed by Member States would

72 See https://business.itsme.be/fr/

73 The figure is based on the 3,8 number of yearly transactions using eID at domestic level in EU Member States from the Deloitte evaluation report. Based on stakeholder consultation we appraised that around 10 times more transactions are estimated in transactions linked to the private sector.

74 The European population using online services ranges annually between 297.8 million and 451.9 million, we estimate that overall annual transactions passing through the eIDAS network in the EU 27 + UK ranges between 1.117 million and 1.694 million.

75 European Commission. (2020). Inception impact assessment.

also encourage greater access to services, lead to more digital identification enabled online transactions cross border and reducing the administrative burden associated with identifying digitally for access to online services and providing verifiable proofs and evidences when required either by private or public institutions saving on average 20 hours per year[76].

Based on comparable business models from the payment cards system we expect that citizens will not pay for the service. In specific cases where the value of the credential benefits mostly the user, it may happen that the trust service provider requests a fee from the user rather than or in addition to the online service provider.

Greater trustworthy and secure exchange of digital identity attributes will also increase data security for **IoT devices**, once identified and linked to a person by electronic means. In 2021, the market will increase to nearly 11.6 billion IoT devices; by 2025 it is estimated that there will be more than to 21 billion IoT devices[77]. Trust Services can intervene at a first level to certify the identity of the interconnected objects, guaranteeing their reliability from a technological point of view and providing additional security safeguards on the data provided by **end users**. These measures are necessary considering that attacks on IoT devices increased by more than 300% in the first half of 2019 and the risk of IoT devices being used as intermediaries is expected to increase[78]. About one fifth of respondents to the public consultation also singled this out as a measure that should be taken.

This option would have a positive effect on existing notified **national eID providers** regarding the take-up of their solutions, as qualified trust service providers will need to rely on them.

Creating a trust service for the secure exchange of data linked to identity would support secure exchange of this information in the context of a wide range of private service use cases , such as customer due diligence/evidential identity information in the banking sector, allowing the possibility of reusing parts of the very costly Customer Due Diligence processes but also those cases that do not have strong requirements for customer identity verification but still require proof of attributes (e.g. age) and attestations.

An increase in the offer of trusted credentials would, make it possible for **online service providers** to cut the costs of verification and storage of attributes and attestations (e.g. because of substitution of paper attestations by their digital equivalents), increase data accuracy and trustworthiness, which reduces risk of costly errors and fraud[79] (see data in Annex 6, section 2[80]), offer more personalized services, as services providers would be able to acquire more relevant information about their users in a cost-efficient way thanks to more effective exchange of attributes and reduce operating costs and enhanced end user convenience. Reduced cost of internal processes varies across sector, estimated for financial services, eHealth and the Aviation sector.[81])

The costs savings for **online service providers** in relying on trust service providers for credentials and attribute verification would depend on the business model adopted and the indicated fees. Taking as an example the provision of degree certificates as digital credentials, it is estimated that this would create a market opportunity worth €130 million in revenue over the 5 years following implementation. The measure would multiply benefits far beyond this, given the potential for a vast number of paper-based credentials to be issued as digital ones.

It is likely that the introduction a new trust service would contribute to a reduction in fraud and related economic impacts where secure digital identity means are not yet used. According to the

76 McKinsey & Company. (2019). Digital identification: A key to inclusive growth
77 Norton. (2020). *The future of IoT: 10 predictions about the Internet of Things*
78 Collard, A. (2019). *Large-Scale IoT Attack Coming*. Gadget. 6 December 2019. https://gadget.co.za/large-scale-iot-attack-coming/
79 Experian. (2018). *The 2018 Global Fraud and Identity Report*
80 This estimate was calculated in the supporting study and detailed in *Annex A. Notes on calculations* of the study
81 This estimate was calculated in the supporting study and detailed in *Annex A. Notes on calculations* of the study

2019 Identity Fraud Study from Javelin Strategy & Research, the shift to embedded chip cards is helping to contain existing card fraud.

There are substantial cost savings for **online service providers** in relying on new trust services linked to identity. At the moment the extent to which Service Providers can currently depend on governmental eID-s varies substantially by Member States. Where such solutions cannot be relied upon, Service Providers need to manage their users' identification and authentication themselves either physically or digitally. The cost of these activities typically includes branch upkeep, paying for video ID solutions, procuring eID means such as PIN calculators, smartcards or other types of tokens, training employees etc.[82]

Figure 34 - Potential reduction in fraud losses per year

Sector	Potential reduction in fraud losses per year
Financial services	Lower bound adoption scenario (5%/20%) €0,85 billion, Upper bound adoption scenario (10%/33%) €1.4 billion
eHealth	Lower bound adoption scenario (5%/20%) €0,3 billion, Upper bound adoption scenario (10%/33%) €0.6 billion
Aviation	Lower bound adoption scenario (5%/20%) €3.5 million, Upper bound adoption scenario (10%/33%) €7 million
eCommerce	Lower bound adoption scenario (5%/20%) €0,13 billion, Upper bound adoption scenario (10%/33%) €02.6 billion

Figure 35 - Reduced Operating Costs per year

Sector	Reduced Operating Costs Per year
Financial services	0.41 billion – €0.81 billion (low adoption scenario) €0.68 billion in savings on on-boarding and wider CDD/KYC compliance with 20% adoption – €1.36 billon with 33% adoption (High adoption scenario).
eHealth	€1.26 billion in the wider health sector with 5% adoption (low adoption scenario) to €2.51 billion with 10% adoption (high adoption scenario).
Aviation	With 5%-10% adoption by airlines, savings would amount to between €30 million (low adoption scenario), €60 million (High adoption scenario) per year from more efficient identity checks, reduced costs of fines/other costs from inaccurate passenger identification
eCommerce	Cost savings between €0.24 billion and €0.47 billion per year with 5-10% adoption

Measure 2: Require Member States to grant access to authentic data to qualified providers of the new trust service for the secure exchange of data linked to identity

Costs

Allowing **qualified trust service providers** access to data stored in authentic sources with prior consent of the user would require the development at EU level of standardised Application Programming Interfaces (APIs) enabling integration from target public administrations across Europe. The costs for developing the API would be of around €30.000.[83] The development does not include the costs for standards setting of the API itself. These shall be commissioned to standardisation bodies or organisation composed by trust service providers, academia and stakeholders with skills and experience in defining standards for API such as the Cloud

[82] From open-source software-based solutions to integrated service offerings from Customer Relationship Management (CRM) or Human Resources (HR) platform providers

83 This does not include data integration costs and overheads.. This estimate was calculated in the supporting study and detailed in *Annex A. Notes on calculations* of the study

Signature consortium[84]. The work, however, will benefit from and build upon already existing relevant standards.

Each **public authority** would incur in integration costs to the API (around €18,000 to €27,000[85]) which is a cost linked to digitization of public services and not directly linked to the eIDAS Regulation and, also, recurrent costs related to annual infrastructure assessment and maintenance. For all EU, the overall total costs for Member states for integration would be of around 625 M € while the recurrent costs are expected to be overall 162 M € per year

By leveraging on the compliance obligations of the European legislation on open data and re-use of public sector information, the public sector can recover the marginal costs incurred[86] or the costs related to the processing of the request for re-use[87].

Benefits

The main benefit for **public administrations** is linked to the possibility to rely on digitial identity autentication attributes and credentials sourced from verified and trusted surces in other Member States, further supporting the application of the once only principle cross border. This will reduce the administrative burden and enhance trust when reliance can be based on a trusted framework at the European level.

- **Measure 3: Setting security requirements and common technical standards for the secure exchange of data linked to identity**

Costs

Public authorities would face typical cost related to international standard-setting decisions, which rely on committee work in synergy with standardisation bodies or multi-stakeholder consortium. The overall costs may range between €1-2 million for public authorities[88]. However, this effort may benefit from and build upon already existing relevant standards. Ongoing international standardization activities are already well-advanced, so costs may be reduced significantly.

eID providers are also expected to face technical costs due to compliance with the standards which cannot be estimated as they are entirely dependent on the technical specification resulting from the standardisation committees' work.

Benefits

This measure is expected to increase interoperability in the use of data linked to identity at the EU level, easing the use of digital authentication services cross-border and therefore bringing positive spill overs on the EU internal market. The adoption of common technical standards would significantly help **Trust Service Providers** by making the trust services market harmonized at the EU level.

Finally, to the benefit of **online service providers and business**, the adoption of this measure would support secure exchange of data linked to identity also in the context of a wide range of private service use cases, such as customer due diligence in the banking sector, positively affecting also those cases that do not have strong requirements for customer identity verification but still require proof of attributes (e.g. age) and attestations.

- **Measure 4: Define the legal effect of digital identity credentials**

84 The Cloud Signature consortium (www.cloudsignatureconsortium.org, is a success story defining technical specifications for cloud-based digital signature adopted not only by EU trust service providers but going globally to other service providers and government institutions.

85 Refer to Annex A note on data and calculation of costs and benefits, Policy Option 2: "Technical Integration costs to the API".

86 See Article 6 of Directive (EU) 2019/1024 of June 2019 on open data and the re-use of public sector information]

87 See Article 6 of the Proposal for a Regulation on European data governance (Data Governance Act)

88 This is mainly made by the cost of hiring highly specialised technical staff to work on developing the standards for a number of months, estimated in consultation with experts in standard development and negotiation at EU level. For further details, please see the supporting study.

Costs

The main direct costs stem from amending the eIDAS regulation in order to modify existing provisions and/or include new ones pertaining to the legal effect of digital identity credentials, which would mainly be borne by **public authorities** (the European Commission and national competent authorities).

Benefits

This measure provides for new opportunities, namely that digital identity credentials will be admitted as evidence in legal proceedings across all Member States on a non-discriminatory basis (they could not be rejected only for being in electronic form). Similarly, they will be recognised across the EU. This is likely to result in wide-ranging positive impacts on the value and legal certainty of identity credentials, thus encouraging cross-border transactions.

Firstly**, end users** would benefit from increased recognition of digital identity credentials for accessing public and private services in different Member States, leading to greater secure exchange of such credentials as well as improved access to cross-border services in Europe. Online service providers would also see benefits as increased use of digital identity credentials would diminish the costs of verification and storage of attributes and attestations (e.g. because of substitution of paper attestations by their digital equivalents). Moreover, increased usage by end users and increased legal certainty would have positive spill-overs on the market for EU trust services as a whole, more potential customers and less unpredictability about legal validity and liability.

- **Measure 5: Regulated sectors such as energy or finance and the Public Sector would be required to rely on Qualified digital credentials**

Costs

The costs relevant for the **public sector** would mainly include costs related to IT integration. Public service providers would need to upgrade their portals and carry out adjustments to have a new system adapted to the verified credentials and attestations. The initial cost will vary depending on the level of integration sought, the specific use case and the number of standard components that can be used.

The same goes for the **online service providers**, they will incur costs associated to allowing users to rely on their own digital identity attributes for authentication purposes in regulated sectors. IT integration costs are highly dependent on the system to be integrated and technical/organisational context where it needs to be implemented. Hence, it is not possible to estimate this cost in the absence of specific details on those characteristics. Similar costs would also be incurred by other non-regulated online service providers allowing users to rely on own digital identity attributes

IT integration costs may be significantly lowered if common solutions like the CEF building blocks[89] are used. In the case of electronic identity attribute services, this would imply the definition of common technical specifications, including specific EU profiles of existing standards, and could include the provision of EU common software components and services.

Benefits

The concerned actors would benefit from the legal certainty brought by the use of attributes and credentials issued by the **qualified trust service providers**, thus reducing their compliance costs linked to the obligation to identity their customers and limiting their exposure in relation to possible damages to be paid for the misuse of identity data.

89 See https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/CEF+Digital+Home A Building Block is an open and reusable digital solution. It can take the shape of a **framework**, a **standard**, a **software**, or a **software as a service (SaaS)**, or any combination thereof and are made freely available for Governments and businesses to rely on if they so choose. CEF buildings blocks have been financed and endorsed by the European Commission under the Connecting Europe Facility (CEF) Programme.

Measure 6: Legal requirements to ensure the protection of personal data

Costs

Qualified trust service providers would face additional **costs** from implementing the personnel and infrastructure changes required to comply with **the data protection provisions**, although these would very much depend from the existing structure and underlying business of the provider. For those companies that are already offering digital identity services on a stand-alone basis, there would not be significant costs.

Functional separation (logical data segregation) is considerably less resource intensive than structural separation. For a logical segregation of data of a medium size infrastructure it came down to around 25.000 € to 30.000 €[90]. Also, **non-qualified providers** would be subject to this data protection measure and will have to bare the same costs to functionally separate identity data from other data. For a structural separation, the estimated one-off cost of €730,000 plus a recurrent annual cost of €30,000 for operational support, business, communications and accounts was estimated.

A significant proportion of respondents to the Deloitte / PwC survey (41%) were positive towards measures to strengthen data protection and privacy, perceiving their benefits to be greater than their cost.

Structural separation is already in place for banks that are also **identity providers**. For instance, in the case of the Nordic BankID scheme, identity services have been structurally separated from other banking operations. Structural separation should not apply to data generated by the trust service provider core business essential for the provision of this new trust service, but to data collected by aggregation or through third parties.

For the provision of qualified digital identity attributes **qualified trust service providers** would face costs from fulling the requirement of structural separation. These costs could be comparable to the costs incurred in regulated sector such as telecom and energy requiring structural separation (physical data segregation).

Benefits

The data protection measure requiring that **digital identity providers** not to use identify data for other purposes and keep identity data separate from other data, would increase clarity over how data is shared and support that authentication processes are in line with GDPR[91]. It would also provide citizens with increased control over the use of identity data and thereby protect against identity theft. It will help address a key point of concern for many citizens related to progressive profiling and the accumulation of personal data in the hands of service providers. These measures would support the benefits for citizens derived from the more specific rules proposed for large online platform (Gatekeepers) in accordance with the Digital Market Act. This would also preserve user cost. It has been estimated that a user would require 244 hours per year to read the privacy statements of all the visited websites[92].

POLICY OPTION 3

Measure 1: Providing a user-controlled secure European Digital Identity Wallet App (all sub-options)

Costs

[90] Based on estimates from internal confidential PwC professional activities in cybersecurity field.

91 PwC (2016) Study on eID and digital onboarding: mapping and analysis of existing onboarding bank practices *across the EU*

92 A.M. McDonald and L.F. Cranor (2008), *The Cost of Reading Privacy Policies*, in Journ. of L. & Pol. Inform. Soc., Privacy Year Review, p. 540-565

As far as **online service providers** are concerned, the costs will depend on the business model (see below under impacts on Wallet providers). In the commonly used business model, the costs are borne by the service provider / relying party. As mentioned for Option 2, IT integration costs will be needed to adjust to a system accommodating verified credentials.

In scenarios where service providers consume identity attributes "on the spot" from the user's mobile device screen (by verifying the authenticity of the credential through a QR code, barcode, NFC etc.), service providers may need to acquire devices such as mobile phones, tablets etc. to be able to verify the authenticity of the presented credential.

Regardless of the organisation providing the wallet, the costs for **providers of identity credentials** will vary depending on how the providers will adjust their business model and service offer, as their ability to increase volume of transactions and develop new services may at least compensate for any loss of revenue linked to the need to share fees with the Wallet provider (see below section on wallet providers).

Development and Maintenance Costs

Cost estimates have been based on the following resources needs: A permanent staff of 25-30 full-time employees (for any area, at least 5 employees are required to ensure continuity of operations). The start of operations will require more investments into tools and system components, like test suites, app developments and the system test environment, while maintenance is of course lower.

In effect, in total about 10.5 m € could be assumed for the first three years.[93] This cost has been estimated by the Commission on the basis of available data as a rough estimate for the first-time development.[94] If developed libraries would be provided to other wallet providers, their development and maintenance cost could be reduced.

In terms of providing readiness to deal with incidents and offer customer support, tasks related to help desks for end-users as well as ID providers and service providers and maintaining the security and functionality of the App are already considered in the table below. As reported there, service desk costs are estimated at €77,500 at the specification stage and € 310,000 at the roll-out and maintenance stages (with the latter representing a recurrent annual cost), while incident response will require an investment of € 310,000 at the roll-out stage and €155,000 per year for maintenance .Procuring an app from the private sector may offer substantial savings as the average cost to develop an app is reportedly below €90.000, varying between around €35.000 and up to €420.000 or higher.

In case the European Digital Identity Wallet App is secured by means of a SIM card, it would imply to sign agreements with relevant mobile network operators, requiring legal, organisational and technical relationships with telecom companies. Developing a mobile application for each platform (Google Play Store, Apple App Store, Microsoft Store, Huawei AppGallery, other) can also incur cost.

Figure 36 - European Digital Identity Wallet – Development and Maintenance Costs: A total cost of about 10.5 m € is estimated for the first three years of deployment

Year 1	Year 2	Year 3
Specification &Development	**Dev & Roll out**	**Maintenance**

93 Expected Average Cost by FTE : 155.000 EUR. For comparison: The budget for the DE Optimos 2.0 project that also included the development of a secure wallet was €5M.

94 See detailed cost estimates in annex 6, section 5.

Technology Stack	FTEs	Cost	FTEs	Cost	FTE	Cost
Project Management	2	310,000 €	2	310,000 €	1	310,000 €
eID SWAPP	4	620,000 €	4	620.000 €	3	620.000 €
3rd party embedding	2	310.000 €	2	310,000 €	1	155,000 €
EU eID (Q)VCP integration	3	465.000 €	3	465,000 €	1	155,000 €
Service Provider integration	3	465,000 €	3	465,000 €	1	155,000 €
TOTAL		2,170,000 €		2,170,000 €		1,085,000 €

EU_eID Support Services	FTEs	Cost	FTEs	Cost	FTE	Cost
Project Management	1	155,000 €	1	155,000 €	1	155,000 €
Service Desk	0.5	77,500 €	2	310,000 €	2	310,000 €
Risk& Security management	1	155,000 €				
Interoperability testing (incl. Test system)	0.5	77,500 €	3	465,000 €	2	310,000 €
Community Building Service (Stakeholder management)	2	310,000 €	3	465,000 €	2	310,000 €
Specifications team	0.5	77,500 €	1	155,000 €	3	465,000 €
Incident response	0	0 €	2	310,000 €	1	155,000 €
Training services	0	0 €	2	310,000 €	1	155,000 €
TOTAL		852,500 €		2,170,000€		1,860,000 €

Business Development	FTEs	Cost	FTEs	Cost	FTE	Cost
Project Management and Overall Coordination	1	155,000 €	1	155,000 €	1	155,000 €
Operations income	1	155,000 €	0.5	77,500 €	0.5	77,500 €
Budgeting & Accounting	0.5	77,500 €	1	155,000 €	1	155,000 €
Legal (SLAs, contracts etc.)	0.5	77,500 €	0.5	77,500 €	0.5	77,500 €
TOTAL		465,000 €		465,000 €		465,000 €
Total	5	3,487,500 €	5	4,805000 €	5	2,201,000 €

Conformity Assessment Costs

The costs of possible certification (or 'conformity assessment') of the Wallet App provisioning would be similar to currently incurred by trust service providers under eIDAS. As presented under other options, these consist of:

- One-off costs of initial qualified status. Estimates for these costs varied significantly among the stakeholders consulted, due in part to the size of the provider, sector and number of services offered. The average administrative costs linked to qualification are €545,000.
- Recurrent compliance costs. Stakeholder estimates for these costs were also wide-ranging, with figures suggesting annual costs are on average €255,000.

Security Costs

To secure the European Digital Identity Wallet App, several hardware security options can be considered. These options include the storage of cryptographic keys. For this storage several options and requirements exit, including:

- the mobile phone of the user should contain a so-called secure element (SE) for the secure storage of cryptographic codes. This secure element should be an embedded hardware element in the device (eSE) or an embedded SIM card (eSIM).
- this secure element should be accessible by the provider of the European Digital Identity Wallet App. In the case of embedded SE, the provider would have to request mobile device manufacturers to provide access to the eSE or to the MNOs (or the eUICC subscription provider) to provide access to the eSIM, which can be difficult to obtain for a small actor.
- standards for the secure operation of the Wallet App on a SE, as well as standards for the certification of the SE should be available.

The development and evaluation of an open SE-based ecosystem requires cooperation with several partners. Currently, about a third of mobile devices feature each of the SE options. Availability of devices with an eSIM is currently limited to high-end models[95], though their availability is expected to increase substantially in the medium term. Stakeholder interviews carried out by the Commission indicated that it can be expected that at least one of the required technical features will be supported by most mobile phones. (see overview below)

Ongoing standardisation work is likely to speed up the development of this market. Of special interest is the draft ISO 23220 "Card and security devices for personal identification – Building blocks for identity management on mobile devices" and GSMA standard on Secure Applications for Mobile (SAM).

With the availability of these standards in the course of 2021/2022, it is likely that conditions 2 and 3 above will be fulfilled in the short / medium term. Once industry standards for the access to and communication with a secure element in the identity environment are available it is likely that the associated hardware will be made accessible by device manufacturers.[96]

Figure 37 - GSM DEVICE MARKET DETAILS

GSM Device Market (million items sold)	**2021**	**2022**	**2023**	**2024**	**2025**

95 https://esim2fly.com/esim-supported-devices/

96 E.g. currently SE are open with Samsung phones only.

FEATUREPHONES	369.4	351.4	335.9	319.8	303.8
SMARTPHONES	1416.9	1508.7	1600.6	1668.5	1717.2
ALL PHONES	1786.3	1860.1	1936.5	1988.3	2021.0
SOURCE: SA, GLOBAL HANDSET / SMARTPHONE / FEATURE PHONE SALES FORECAST FOR 88 COUNTRIES : 2007 TO 2025					

SECURITY CONTROLLER PRODUCTS WHICH MAY BE ABLE AND USED TO HOST AN EID APPLICATION (million items sold)	**2021**	**2022**	**2023**	**2024**	**2025**
eSE: NFC EMBEDDED SECURE ELEMENT SMART CARD IC MARKET (SOURCE: ABI_-_SECURE_SMART_CARD_AND_EMBEDDED_SECURITY_IC_TECHNOLOGIES_MARKET_DATA_Q1_2020)	482.6	492.3	498.3	503.1	
eSIM (stand-alone and eCD; there may be an overlap with eSE figures above). Source: IFX internal assessment	296.6	349.4	391.2	498.5	642.4

Note: feature phones are expected to integrate neither an eSIM nor an eSE

Onboarding Costs

To make the Wallet app usable the provider would need to have an active role in onboarding both credential providers and service providers to the ecosystem. There are over 11000 identity providers in the public sector and about 13400 in the private sector with the number of service providers being similar.[97] [98] To enable users to request identity credentials through the App, the App provider may agree with credential providers described in options 1 and 2 to build the necessary integrations and agree terms. Where Wallet App providers support provisioning of multiply kinds of identity credentials to a variety of service providers, it may be expected of it to facilitate billing between credential and service providers.

Marketing and Customer Support Costs

Even though the wallet will be used by end-users, its success depends on the uptake of service providers, which can help substantially with marketing and awareness raising. Due to the high requirements on security, the provider would need to maintain readiness to deal with incidents and offer customer support for credential providers, service providers and end-users.

Business Model

Personal Wallets are developed by more and more ID providers from the public and the private sectors.[99] In recent years, a number of banks have started to provide Wallet Apps, such as Rabobank in NL and Sparkassen in DE while there are also open Wallet Apps such as mTasku in EE or the Optimos 2.0 project in DE currently under development.

[97] SDG MS readiness study by Deloitte

[98] https://www.ecb.europa.eu/stats/financial_corporations/list_of_financial_institutions/html/index.en.html

[99] Examples include Thales and the UK Government. More examples have been added in annex 6, section 4.

It will be important to develop a sustainable business model for the wallet. This business model will depend on the sub-option chosen for the deployment. While the business model would not be prescribed by the Regulation, under all sub-options the App provider would seek to cover costs by billing online service providers relying on the digital identity services and/or providers of digital identity services (trust services providers in Option 2). (see annex 6, section 8)

Based on existing business models, it is unlikely that consumers would be ready to directly pay for the app. Considering the set-up costs, and a 0,1 eurocents revenue per transaction, roughly between 50 and 83 million transactions would be needed to cover the development and roll-out costs in one year.

For reference, BankID (7,9M users) was used 3,3bn times in Sweden in 2018100 and Smart-ID (2,9M users) was used over 65M times in the Baltic countries in December 2020[101]. Under sub-option 2, part of the costs may be covered from public funds, but making revenue from provisioning of the wallet may be limited, depending on national approaches. Member States would most probably hire contractors to develop the App and related solutions, potentially through a governmental/EU agency.

Existing Identity Providers that issue digital identity means to their users (such as governments, financial institutions, telcos etc.) may find developing of a European Digital Identity Wallet App (on their own or on behalf of governments depending on the Sub-Option) a financially sustainable alternative to existing means, especially if it offers revenue opportunities. In addition, under sub-option 3.1., mobile phone manufacturers (such as Apple, Samsung, Google, Huawei, Oppo etc.), app developers and Secure Element providers may find business opportunities in developing a European Digital Identity Wallet App or updating existing ones to meet security requirements.

European Digital Identity Wallet App providers may have an advantage compared to existing digital identity means providers although they can also act as platforms for the provision of their services. For chip manufacturers there are opportunities related to the likely increase in sales for secure elements (SE), general market development will also depend on the identification of devices.

Figure 38 - BUSINESS CASE OF THE EUROPEAN DIGITAL IDENTITY WALLET

	Platforms		**National eID / eIDAS**		**EUeID Wallet**	
Customer base	++	Global	-	National	++	all EU citizens
Use by Service providers	++	Global, limited to low security private use cases	+/-	Public Services / high security private use cases	**USP**	all EU service providers (public & private)
Cost for customer and	**USP**	Free of charge for service provider and customer	**?**	Potentially subsidized	-	**Depends on business**

100 https://www.bankid.com/assets/bankid/stats/2018/statistik-2018-12.pdf

101 https://www.smart-id.com/

Service Prov.						**model**
Support for all assurance levels	XX	Not supported	ok	As required by the supported services	**USP**	To be positioned to support all eIDAS levels
Data protection / Security	-	Questionable	ok	Probably supported	++	„Best-in-class“
Market Power	--	Service Provider dependency	ok	Probably Impartial	++	Impartial

Benefits

The European Digital Identity Wallet would **enable citizens to manage their different identities and all credentials** that they receive from various sources (e.g. education, employment, municipality, state, professional associations, leisure, etc.) anywhere in the EU.

Wallets offer citizens and businesses a personal space for the user to manage identity attributes and credentials and would support transactions requiring all levels of assurance. The link to secure and highly trusted, official national eID could not be offered by the private sector solutions, including those offered by the online platforms. In addition, the possibility to protect personal data through a user-controlled privacy by design concept and impartiality towards service providers is also a unique advantage on the market. A mobile based wallet would also deliver similar **user experiences** for end-users to e.g. Apple or Google Wallets, allowing for a visual representation of credentials.

Data from countries where digitalisation is most advanced suggests an **increase in use-cases** and market demand for trusted and secure digital identification solutions. For instace, in Norway, BankID offers a trusted personal wallet space to manage e.g. a patient journal, medical tests, doctor appointments, e-prescriptions, secure messages etc. The important uptake of BankID on high level of assurance (90% +) has made it possible to provide digital e-Health services for almost all citizens.

In addition, the measure also takes a more explicit **privacy-by-design** approach that could yield additional benefits in terms of data protection and privacy. The wallet would reduce the need for intermediaries in the transactions, enabling the citizen to communicate directly with the service and credential providers.

Finally, a universally issued EU eID to all European citizens based on a secure wallet trusted app, (provided upon citizens' request), is expected to increase data security and reduce **the likelihood of identity theft,** based on the app's SSI functional design and strict requirements on security for providers. The wallet would enable more secure sharing of the data compared to other identity management systems, while the data architecture would make use of secure elements.

Depending on market uptake and Government funding, having the wallet provided by multiple private providers (sub-Option 1) might result in reduced costs for the user and/or improved service due to competition between the providers.

Where governments offer secure eID-s for use also in the private sector, it can be regarded as a public service and therefore allowing for substantial cost savings compared to Member States where the private sector would need to cover the costs of getting a wallet from the market. The costs of identity proofing and customer onboarding processes, more generally, are substantial and are expected to be significantly reduced if providers have access to secure and convenient eIDs to onboard customers.

The European Digital Identity Wallet App would need to be competitive in this regard, both in terms of price, coverage among potential customers and ease of onboarding. However, it is important to mention that coverage among customers and price are a result of the Wallet App provider's ability to associate all relevant credential providers and marketing the solution among potential users. The Wallet App provider's sales and marketing savvy is therefore a critical component of the success of option 3.

The wallet is expected to lower considerably the high abandonment rate[102] when users get to the online shopping cart (eCommerce sector it is documented that on average there is around 69%.) Twenty-eight per cent of respondents mentioned as the second most important reason for dropping out the fact that the site requests them to use a specific account.

By allowing to accurately establish the identity of the customers, the wallet is also expected to mitigate losses from fraud, errors and fines linked to inaccurate customer identification and verification. The high level of assurance eIDs associated to eIDs would make that possible. Moreover, identity theft would be also tackled, thus preventing substantial financial loss to European citizens. European consumers are particularly targeted by sophisticated fraudulent scams each year, both offline and online. According to data gathered by Finanso.se, 56% of Europeans have experienced at least one type of fraud in the last two years. One-third of them became victims of identity theft, making it the second most-common type of fraud in Europe. The savings from reduced fraud could be substantial in a range of sectors requiring customer identification (see Annex 6).

Overall, in Member States where eIDs are ubiquitous (e.g. Scandinavia, Baltic countries, Benelux), these benefits have been to an extent already realized thanks in part to existing eID means, but only at national level. The main value proposition of European Digital Identity wallet App lies precisely in its cross-border dimension complementing the outreach of national eID means. The effects would be particularly felt where identity proofing and access management markets are not mature yet. According to Deloitte's 2020 digital banking maturity study, only 34% of banks offer fully digital account opening and 23% offer remote identification and verification. There is a substantial gap between the champions and latecomers for both opening a bank account through the mobile channel (55% vs 5%) and internet channel (58% vs 20%)[103]. The situation is similar with governments: more than 90% of citizens submitted forms to government online (a process that typically requires user identification and authentication) while for two countries the number is less than 40%[104].

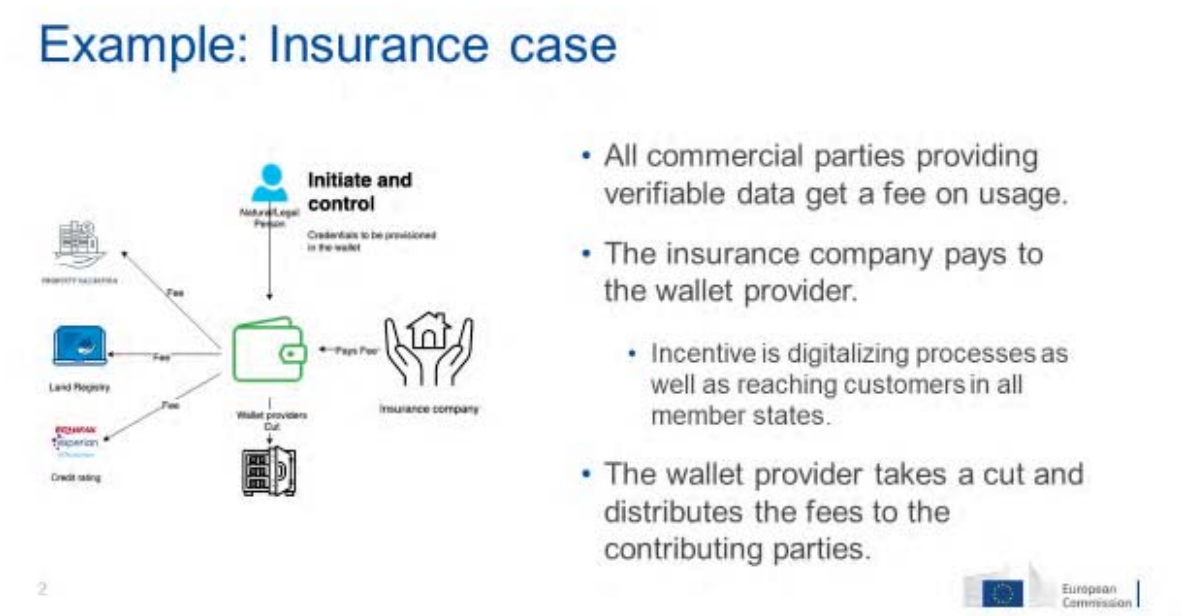
Further market opportunities may stem from the incentive to design new services connected to the Wallet App. Specific areas where new services may emerge include identification and authentication of non-human entities: IDC estimates that, in 2025, there will be 41.6 billion connected IoT devices, generating 79.4 zettabytes (ZB) of data. The time and costs of onboarding devices is seen today as a market barrier. The initiative would likely encourage providers to fill this market gap and invest in developing innovative services in this area. The Wallet App would allow users to store attestations of attributes of "things" securely linked to their identity.

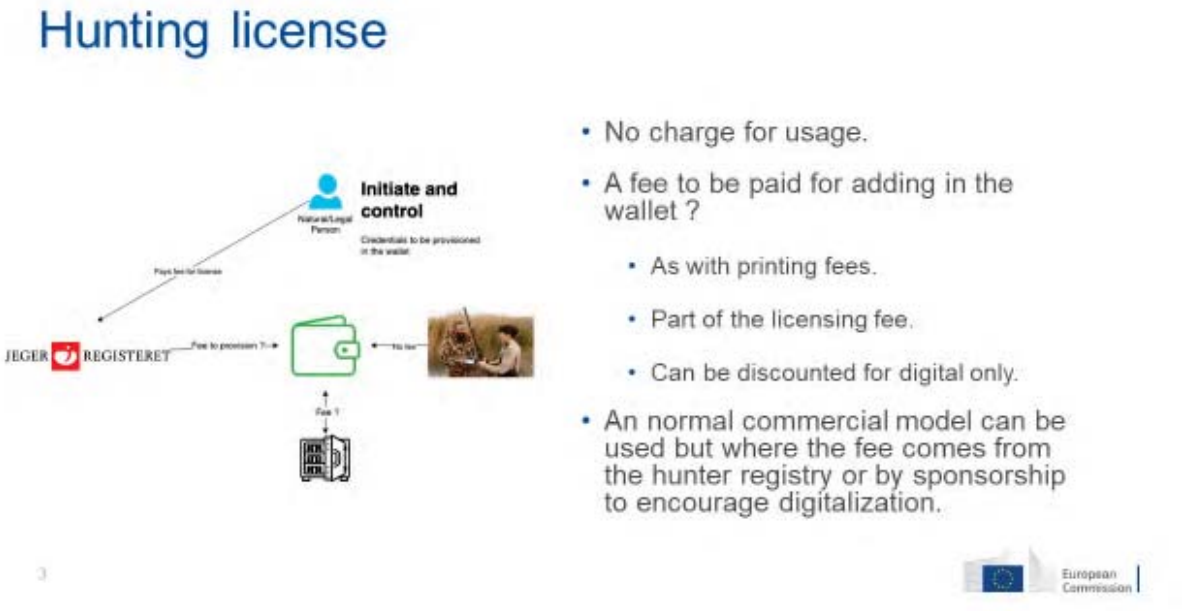
102 This value is an average calculated based on these 41 different studies containing statistics on e-commerce shopping cart abandonment: https://baymard.com/lists/cart-abandonment-rate

103 https://www2.deloitte.com/content/dam/Deloitte/ce/Documents/financial-services/ce-digital-banking-maturity-2020.pdf

104 https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=67084

Figure 39 - Use Cases of the European Digital identity Wallet (Examples)





- **Measure 1 (sub-option 1): Creating a new Qualified Trust Service for the provision of a user-controlled secure European Digital Identity WalletApp**

Costs

National supervisory authorities of Trust Services under the eIDAS Regulation will incur similar supervisory costs as mentioned in Option 1 and 2 for dealing with a new trust service (see above).

Costs / Benefits

Similar to option 2, the benefit for conformity assessment bodies is on the revenue opportunities side. Assuming that (i) each conformity assessment body employs only one person to learn the administrative processes and this person is able to pass this on to colleagues, costs associated to familiarisation of the requirements related to the new trust service are estimated to be

approximately €339,000 (around €12,000 per conformity assessment body). In any case these costs will be rolled over to Wallet Providers.

- **Measure 1 (sub-option 2): mandatory extension of notified eID schemes, or mandatory provision of a user-controlled secure European digital identity Wallet App by Member States**

Costs

Supervisory costs could be higher than under sub-option 1 as all Member States would have to notify a wallet while the unit cost of supervision can be assumed to be the same.

Costs / Benefits

Similar to option 1, Member States may assess the conformity of their wallets with conformity assessment bodies in order to achieve greater conformity of implementation of standards, in which case the impact is similar to Sub-Option 1. The number of wallets to be assessed may be similar to sub-option 1.

In case governments provide the wallet, (sub-option 2) costs are expected to be the same envisaged in the wallet providers section described above.

- **Measure 2: Defining Common Standards for a European Digital Identity Wallet App**

Costs

The development of a standardised SE-based ecosystem from scratch requires substantial coordination efforts between all relevant parties. In order to set common standards, public authorities will face costs related to international cooperation activities which are estimated to be similar to those outlined under Option 2 Measure 3, (namely overall costs ranging between €1-2 million). Existing relevant standards and ongoing international standardization activities may significantly reduce the efforts.

Depending on the standards and technical requirements adopted, Wallet App providers are expected to face compliance costs. These are difficult to quantify before the definition of the above-mentioned technical requirements, but it could be reasonably assumed that would be mainly associated to ensuring a SE-based solution.

Ongoing standardisation work is likely to speed up the development of the SE market, as demonstrated by the global work on the ISO 23220 "Card and security devices for personal identification – Building blocks for identity management on mobile devices".

Once industry standards for the access and communication related to a secure element in the identity environment are available, it is likely that this will incentivise the manufacturers to provide access to the associated hardware.

Benefits

The definition of common development and security standards to deploy the EU Digital Identity Wallet App will provide consistent user-experience and transparency about its security requirements and functionalities. This will positively affect citizens and end-users as they could benefit from the same functionalities of the Wallet App regardless of the provider.

Wallet App providers would benefit from a harmonized level-playing field, without incurring in national legislative barriers. This could also ensure interoperability and an effective cross-border market for the App, positively affecting the Digital Single Market.

STANDARDISATION

Standards are required to establish acceptance criteria to be used by conformity assessment bodies and supervisory authorities, in order to judge or challenge the soft- and hardware used by wallet providers, as well as the procedures and legal and organisational set-up of wallet

providers. Once functional requirements for the Wallet are set, the Commission will have to work with Member States on suitable technical references and standards.

Of special interest is draft ISO 23220 "Card and security devices for personal identification – Building blocks for identity management on mobile devices", currently very advanced (amongst others) by American and global market players. This first part ISO23220 will influence other artefacts (like those of GSMA) that could be identified as reference standards. Other parts (2 to 6) that will potentially cover higher levels of the stack, up to 'certification' and 'trust model'. Other standards of interest have been proposed by World Wide Web Consortium (W3C) including the Verifiable Credential data model and FIDO2 WebAuthn, the Internet Engineering Task Force (IETF) and the FIDO (Fast IDentity Online") Alliance and GlobalPlatform. Besides standards, further profiles and specifications (such as that for the verifiable credential API) will be needed for reasons of interoperability and security.

Specifications, profiles and standards for to allow access data stored in authentic sources and the provision of verifiable credentials and presentations will have to be identified for PO2, and PO3 will additionally need standards for hard and software (including protocols) for the secure storage on devices. Testing of new types of mobile devices was carried out by the MNO who operated the SIM-ecosystem. This was extremely costly and impacted the business case negatively. As long as hardware features relevant for the SE based services are not included in applicable specifications used in certification of mobile devices (e.g. Global Certification Forum), testing mobile devices for their feasibility for the wallet applet will remain costly.

Option 3 imposes no set-technology. Technical solutions can be implemented on different platforms (iOS, Android) and utilising different form factors for secure elements.

Measure 3 (all sub-options): Security requirements

Costs

Since the measure consists in the use of a targeted certification scheme developed under the Cybersecurity Act[105], the costs could be deemed similar to measure 6 under Option 1 (also reliant on the introduction of EU-wide ICT security certification applicable to eID means under the same act). The main costs would therefore stem from the need to get certified under the new scheme (also in the order of 80/100K€) which in this case would be incurred by the Wallet App providers.

Benefits

The benefits of this measure would match those reported under measure 6/option 1. Firstly, by strengthening the security of the Wallet App and introducing more transparent criteria, certification would increase citizens/end users' trust in using the Wallet App. Secondly, despite the initial net cost of getting certified falling on Wallet App providers, in the longer term the measure would provide an efficient way for providers to demonstrate compliance. More importantly, a clear and common assessment methodology and criteria would reduce the risks of delays in the process and non-harmonized interpretation of security requirements across Member States.

[105] REGULATION (EU) 2019/881 introduces a European cybersecurity certification scheme. Art 54(3) provides: "Where a specific Union legal act so provides, a certificate or an EU statement of conformity issued under a European cybersecurity certification scheme may be used to demonstrate the presumption of conformity with requirements of that legal act."