Basic information

2012/0146(COD) COD - Ordinary legislative procedure (ex-codecision procedure) Regulation	Procedure completed
Electronic transactions in the internal market: electronic identification and trust services Repealing Directive 1999/93/EC 1998/0191(COD) Amended by 2021/0136(COD) **Subject** 1.20.05 Public access to information and documents, administrative practice 1.20.09 Protection of privacy and data protection 2.50.04.02 Electronic money and payments, cross-border credit transfers 2.80 Cooperation between administrations 3.30.05 Electronic and mobile communications, personal communications 3.30.06 Information and communication technologies, digital technologies 3.30.25 International information networks and society, internet 3.45.05 Business policy, e-commerce, after-sales service, commercial distribution 4.60.06 Consumers' economic and legal interests 4.60.08 Safety of products and services, product liability	

Key players

European Parliament

Committee responsible	Rapporteur	Appointed
ITRE Industry, Research and Energy	ULVSKOG Marita (S&D)	03/07/2012
	Shadow rapporteur DEL CASTILLO VERA Pilar (PPE) CREUTZMANN Jürgen (ALDE) ANDERSDOTTER Amelia (Verts/ALE) KARIM Sajjad (ECR)	

Committee for opinion	Rapporteur for opinion	Appointed
ECON Economic and Monetary Affairs	The committee decided not to give an opinion.	
IMCO Internal Market and Consumer Protection (Associated committee)	BOULLIER GALLO Marielle (PPE)	21/06/2012

	JURI Legal Affairs	MÉSZÁROS Alajos (PPE)	11/12/2012
	LIBE Civil Liberties, Justice and Home Affairs	ROHDE Jens (ALDE)	20/09/2012

Council of the European Union

Council configuration	Meetings	Date
General Affairs	3330	2014-07-23
Transport, Telecommunications and Energy	3243	2013-06-06
Transport, Telecommunications and Energy	3171	2012-06-07
Transport, Telecommunications and Energy	3278	2013-12-05
Transport, Telecommunications and Energy	3213	2012-12-20

European Commission

Commission DG	Commissioner
Communications Networks, Content and Technology	KROES Neelie

European Economic and Social Committee

Key events

Date	Event	Reference	Summary
04/06/2012	Legislative proposal published	COM(2012)0238	Summary
07/06/2012	Debate in Council		Summary
14/06/2012	Committee referral announced in Parliament, 1st reading		
20/12/2012	Debate in Council		
07/02/2013	Referral to associated committees announced in Parliament		
06/06/2013	Debate in Council		Summary
14/10/2013	Vote in committee, 1st reading		
06/11/2013	Committee report tabled for plenary, 1st reading	A7-0365/2013	Summary
05/12/2013	Debate in Council		
02/04/2014	Debate in Parliament		
03/04/2014	Decision by Parliament, 1st reading	T7-0282/2014	Summary
03/04/2014	Results of vote in Parliament		
23/07/2014	Act adopted by Council after Parliament's 1st reading		
23/07/2014	Final act signed		
23/07/2014	End of procedure in Parliament		
28/08/2014	Final act published in Official Journal		

Technical information	
Procedure reference	2012/0146(COD)
Procedure type	COD - Ordinary legislative procedure (ex-codecision procedure)
Procedure subtype	Legislation
Legislative instrument	Regulation
Amendments and repeals	Repealing Directive 1999/93/EC 1998/0191(COD) Amended by 2021/0136(COD)
Legal basis	Treaty on the Functioning of the European Union TFEU 114-p1
Other legal basis	Rules of Procedure EP 165
Mandatory consultation of other institutions	European Economic and Social Committee
Stage reached in procedure	Procedure completed
Committee dossier	ITRE/7/09803

Documentation gateway

European Parliament

Document type	Committee	Reference	Date	Summary
Committee draft report		PE507.971	04/04/2013	
Amendments tabled in committee		PE510.784	20/05/2013	
Amendments tabled in committee		PE510.822	21/05/2013	
Committee opinion	JURI	PE510.497	26/06/2013	
Committee opinion	LIBE	PE504.331	09/07/2013	
Committee opinion	IMCO	PE508.181	22/07/2013	
Committee report tabled for plenary, 1st reading/single reading		A7-0365/2013	06/11/2013	Summary
Text adopted by Parliament, 1st reading/single reading		T7-0282/2014	03/04/2014	Summary

Council of the EU

Document type	Reference	Date	Summary
Draft final act	00060/2014/LEX	23/07/2014	

European Commission

Document type	Reference	Date	Summary
Legislative proposal	COM(2012)0238	04/06/2012	Summary
Document attached to the procedure	SWD(2012)0135	04/06/2012	
	SWD(2012)0136		

Document attached to the procedure		04/06/2012	
Commission response to text adopted in plenary	SP(2014)471	09/07/2014	
Follow-up document	COM(2021)0290	03/06/2021	
Follow-up document	SWD(2021)0130	03/06/2021	

National parliaments

Document type	Parliament /Chamber	Reference	Date	Summary
Contribution	AT_BUNDESRAT	COM(2012)0238	26/07/2012	
Contribution	PT_PARLIAMENT	COM(2012)0238	26/07/2012	
Contribution	AT_NATIONALRAT	COM(2012)0238	07/09/2012	
Contribution	IT_SENATE	COM(2012)0238	13/09/2012	
Contribution	DE_BUNDESRAT	COM(2012)0238	15/10/2012	
Contribution	CZ_SENATE	COM(2012)0238	07/11/2012	

Other institutions and bodies

Institution/body	Document type	Reference	Date	Summary
EESC	Economic and Social Committee: opinion, report	CES1243/2012	18/09/2012	
EDPS	Document attached to the procedure	N7-0048/2013 OJ C 028 30.01.2013, p. 0006	27/09/2012	Summary

Additional information

Source	Document	Date
National parliaments	IPEX	
European Commission	EUR-Lex	
European Commission	EUR-Lex	

Final act

Regulation 2014/0910
OJ L 257 28.08.2014, p. 0073 Summary

Electronic transactions in the internal market: electronic identification and trust services

2012/0146(COD) - 27/09/2012 - Document attached to the procedure

OPINION OF THE EUROPEAN DATA PROTECTION SUPERVISOR

on the Commission proposal for a Regulation of the European Parliament and of the Council

on trust and confidence in electronic transactions in the internal market (Electronic Trust Services Regulation)

In this Opinion, the EDPS focuses his analysis on **three main issues**: (a) how data protection is addressed in the proposal; (b) data protection aspects of electronic identification schemes to be recognised and accepted across borders; and (c) data protection aspects of electronic trust services to be recognised and accepted across borders.

Notwithstanding his general support for the proposal, the EDPS provides the following general recommendations:

- data protection provisions included in the proposal should not be restricted to trust service providers and should also be applicable to the processing of personal data in the electronic identification schemes described in Chapter II of the proposal,
- the proposed regulation should set a common set of security requirements for trust service providers and electronic identification issuers. Alternatively, it could allow the Commission to define where needed, through a selective use of delegated acts or implementing measures, the criteria, conditions and requirements for security in electronic trust services and identification schemes,
- electronic trust service providers and electronic identification issuers should be required to provide the users of their services with: (i) appropriate information on the collection, communication, and retention of their data, as well as (ii) a means to control their personal data and exercise their data protection rights,
- a more selective inclusion in the proposal of the provisions empowering the Commission to specify or detail concrete provisions after the adoption of the proposed regulation by delegated or implementing acts.

Some specific provisions concerning the mutual recognition of electronic identification schemes should also be improved:

- the proposed Regulation should specify which data or categories of data will be processed for cross- border identification of individuals. This specification should contain at least the same level of detail as provided in annexes for other trust services and should take into account the respect of the principle of proportionality,
- the safeguards required for the provision of identification schemes should at least be compliant with the requirements set forth for the providers of qualified trust services,
- the proposal should establish appropriate mechanisms to set a framework for the interoperability of national identification schemes.

Lastly, the EDPS also makes the following recommendations in relation to the **requirements for the provision and recognition of electronic trust services**:

- it should be specified with regard to all electronic services if personal data will be processed,
- the Regulation should take appropriate safeguards to avoid any overlap between the competences of the supervisory bodies for electronic trust services and those of data protection authorities,
- the obligations imposed on electronic trust service providers concerning data breaches and security incidents should be consistent with the requirements established in the revised e-privacy Directive and in the proposed Data Protection Regulation,
- more clarity should be provided to the definition of private or public entities that can act as third parties entitled to carry out audits or that can verify electronic signature creation devices, as well as on the criteria under which the independence of these bodies will be assessed,
- the Regulation should be more precise in setting a time limit for the retention of the data.

Electronic transactions in the internal market: electronic identification and trust services

2012/0146(COD) - 06/06/2013

The Council took note of progress made on a proposed Regulation intended to enhance trust in electronic transactions by setting up a legal framework for electronic identification and other electronic trust services in the internal market.

Work on this technically complex draft legislation under the Irish Presidency focused primarily on electronic identification and, to a lesser extent, trust services. One **key issue is that of assurance levels for electronic identification**, which are required so that electronic means of identification issued in another Member State can be recognised.

While a number of delegations favour the principle of matching levels as a basis for recognition, other delegations would prefer to have the required assurance levels set out in the Regulation.

There is, however, **broad support amongst delegations for a number of general principles regarding electronic identification**: initial limitation on services provided by the public sector; ensuring interoperability between national identification infrastructures; technological neutrality; and the need for security breaches to be addressed.

A considerable number of other issues will also require further discussion, including:

- liability with respect to electronic identification and trust services;
- treatment of trust service providers from third countries;
- supervision of trust service providers;
- the effect of certain provisions concerning electronic signatures and electronic seals on national and procedural law;
- the concept of "electronic document" and the appropriateness of covering electronic documents in this piece of legislation;
- clarification of definitions;
- the use of "delegated acts" empowering the Commission to adopt related legal acts on non-essential technical aspects of the Regulation;
- the deadline for the entry into force of the Regulation.

Electronic transactions in the internal market: electronic identification and trust services

2012/0146(COD) - 06/11/2013 - Committee report tabled for plenary, 1st reading/single reading

The Committee on Industry, Research and Energy adopted the report by Marita ULVSKOG (S&D, SE) on the proposal for a regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

The committee recommended that the position of the European Parliament adopted in first reading following the ordinary legislative procedure should amend the Commission proposal as follows:

Scope: this Regulation should apply to **notified** electronic identification schemes **mandated, recognised or issued** by or on behalf of Member Sates, and to trust service providers established in the Union. It should also apply to both **qualified and non-qualified** trust service providers established in the Union.

Electronic identification systems: Member States which notify an electronic identification scheme shall forward to the Commission the following information and without undue delay, any subsequent changes thereof: (i) a description of the notified electronic identification scheme and its security assurance level; (ii) information on which entity or entities manage the registration of the appropriate attributes identifiers; (iii) a description of how the requirements of the interoperability framework are met; (iv) a description of the authentication possibility and any technical requirements imposed on relying parties.

Security breach: where there is a breach of security that would affect the reliability of that scheme for cross-border transactions, the notifying Member State shall without undue delay **suspend or revoke** the cross-border function of that electronic identification scheme or that authentication possibility or the compromised parts concerned and inform other Member States and the Commission thereof.

Liability: the amended text introduced a new provision providing that the notifying Member State **shall be liable for any damage** caused to a natural or legal person which could reasonably be expected to arise under normal circumstances as a result of its failure to comply with this Regulation, unless it can show that it has acted with due diligence.

Coordination and interoperability: Member States and the Commission shall in particular prioritize interoperability for e-services with the greatest cross border relevance. The provisions intended to guarantee technical interoperability have to be **technologically neutral** so as not to interfere with the options favoured by Member States when developing their national electronic identification and authentication schemes.

Liability of qualified trust service providers: Members took the view that only qualified trust service providers should be subject to the liability scheme, as in Directive 1999/93/EC. Non-qualified service providers should be covered by the general scheme of civil and contractual liability defined in the national law of each Member State.</Amend>

Qualified trust services providers from third countries: Members wished to refer to the provision of EU personal data protection law which specifies the adequacy of the level of protection afforded by a third country.

Processing of personal data: processing of personal data might be necessary in case of a breach or in order to take appropriate counter measures and should be applied where this is absolutely necessary and be a "legitimate interest" under the Data Protection Directive and thus be lawful.

Disabled persons: trust services provided and end user products used in the provision of those services shall be made accessible for persons with disabilities in accordance with Union law.

Supervisory body: the designated supervisory body, its addresses and the names of responsible persons shall be communicated to the Commission. Supervisory bodies shall be given adequate resources necessary for the exercise of their tasks.

Supervision of trust service providers: qualified trust service providers shall be audited annually by an independent body whose competence to carry out the audit has been demonstrated to confirm that they and the qualified trust services provided by them fulfil the requirements set out in this Regulation, and shall submit the resulting compliance audit report to the supervisory body. Such audit shall also be carried out following any significant technological or organizational changes. If, after three years, the annual audit reports raise no concerns, the audits shall be carried out every two years only.

'EU' qualified trustmark: Members introduced the possibility for qualified trust service providers to use an EU trustmark to present and advertise the qualified trust services which they offer that meet the requirements laid down in this Regulation.

Parliament already called for the creation of a trustmark in its resolution of 11 December 2012 on completing the Digital Single Market.

Electronic documents: Members stated that an electronic document shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic format. A document bearing a qualified electronic signature or a qualified electronic seal, shall have the **equivalent** legal effect of a paper document bearing a handwritten signature or a physical seal, where this exists under national law, provided the document does not contain any dynamic features capable of automatically changing the document.

Implementing measures and delegated acts: the proposed Regulation empowers the Commission in many provisions to adopt delegated acts or implementing measures. Members have reservations to an approach that relies upon acts and measures so heavily. They proposed amendments that will restrict the proposed acts strictly to technical implementation of the legal act in question in a uniform manner.

Electronic transactions in the internal market: electronic identification and trust services

2012/0146(COD) - 04/06/2012 - Legislative proposal

PURPOSE: to enhance trust in electronic transactions in the internal market and ensure the mutual recognition of electronic identification, authentication, signatures and other trust services across borders.

PROPOSED ACT: Regulation of the European Parliament and of the Council.

BACKGROUND: building **trust in the online environment** is key to economic development.

The existing EU legislation, namely Directive 1999/93/EC on a Community framework for electronic signatures, essentially covers electronic signatures only.

There is **no comprehensive EU cross-border and cross-sector framework for secure, trustworthy and easy-to-use electronic transactions** that encompasses electronic identification, authentication and signatures.

The Digital Agenda for Europe identifies existing barriers to Europe's digital development and proposes legislation on e-signatures and the mutual recognition of eIdentification and authentication, establishing a clear legal framework so as to eliminate fragmentation and the lack of interoperability, enhance digital citizenship and prevent cybercrime. Legislation ensuring the mutual recognition of electronic identification and authentication across the EU is also a key action in the Single Market Act, as well as the Roadmap for Stability and Growth. The European Parliament stressed the importance of the security of electronic services, especially of electronic signatures, and of the need to create a public key infrastructure at pan-European level, and called on the Commission to set up a European validation authorities gateway to ensure the cross-border interoperability of electronic signatures and to increase the security of transactions carried out using the internet.

The aim of this proposal is to **enhance existing legislation** and to expand it to cover the mutual recognition and acceptance at EU level of notified electronic identification schemes and other essential related electronic trust services.

IMPACT ASSESSMENT: three sets of policy options were assessed, dealing respectively with (1) the scope of the new framework, (2) the legal instrument and (3) the level of supervision required. The preferred policy option proved to be **enhancing legal certainty**, boosting coordination of national supervision, ensuring mutual recognition and acceptance of electronic identification schemes and incorporating essential related trust services. The impact assessment concluded that doing this would lead to considerable improvements to legal certainty, security and trust in terms of cross-border electronic transactions, resulting in less fragmentation of the market.

LEGAL BASIS: Article 114 of the Treaty on the Functioning of the European Union (TFEU).

CONTENT: the proposed regulation seeks to **enable secure and seamless electronic interactions** between businesses, citizens and public authorities, thereby increasing the effectiveness of public and private online services, e-business and electronic commerce in the EU.

The main points of the proposal are as follows:

1) Electronic identification: the proposal provides for the **mutual recognition and acceptance of electronic identification** means falling under a scheme, which will be notified, to the Commission on the conditions laid down in the Regulation. It does not oblige Member States to introduce or notify electronic identification schemes, but to recognise and accept notified electronic identifications for those online services where electronic identification is required to get access at national level.

Electronic identification schemes shall be eligible for notification **if all five of the following conditions** are met:

- the electronic identification means are issued by, on behalf of or under the responsibility of the notifying Member State;
- the electronic identification means can be used to access at least public services requiring electronic identification in the notifying Member State;
- Member States must ensure an unambiguous link between the electronic identification data and the person concerned;
- the notifying Member State ensures the availability of an authentication possibility online, at any time and free of charge. No specific technical requirements, such as hardware or software can be imposed on the parties relying on such authentication;

- Member States must accept liability for the unambiguity of the link (i.e. that the identification data attributed to the person are not linked to any other person) and the authentication possibility (i.e. the possibility to check the validity of the electronic identification data).

The proposal also aims to **ensure the technical interoperability of the notified identification schemes** through a coordination approach, including delegated acts.

2) Trust services: the proposal sets out the **principles relating to the liability of both non-qualified and qualified trust service providers.** It builds on Directive 1999/93/EC and **extends entitlement to compensation of damage** caused by any negligent trust service provider for failure to comply with security good practices which result in a security breach which has a significant impact on the service. It also describes the mechanism for the recognition and acceptance of qualified trust services provided by a provider established in a third country.

3) Supervision: the proposal (i) requires Member States to establish **supervisory bodies**, clarifying and enlarging the remit of the latter with regard to both trust service providers and qualified trust service providers; (ii) introduces an **explicit mechanism of mutual assistance between supervisory bodies** in Member States to facilitate the cross-border supervision of trust service providers; (iii) introduces an obligation for both qualified and non-qualified trust service providers to implement appropriate technical and organisational measures for the security of their activities ; (iv) sets out the conditions for the supervision of qualified trust service providers and qualified trust services provided by them ; (v) provides for the establishment of trusted lists containing information on qualified trust service providers who are subject to supervision and to the qualified services they offer.

4) Electronic signature: the proposal enshrines the rules related to the legal effect of natural persons' electronic signatures, introducing an explicit obligation to **give to qualified electronic signatures the same legal effect as handwritten signatures.** Furthermore, Member States must ensure the cross-border acceptance of qualified electronic signatures, in the context of the provision of public services.

The proposal also sets out: the requirements for qualified signature certificates and the requirements for qualified electronic signature creation devices; the conditions for qualified validation services, and the condition for the long-term preservation of qualified electronic signatures.

5) Electronic seals: the provisions concern the legal effect of electronic seals of legal persons. A specific legal presumption is bestowed on a qualified electronic seal which guarantees the origin and integrity of electronic documents to which it is linked.

6) Electronic time stamp: a specific legal presumption is bestowed on qualified electronic time stamps with regard to the certainty of the time.

7) Electronic documents: there is a specific legal presumption of the authenticity and integrity of any electronic document signed with a qualified electronic signature or bearing a qualified electronic seal. With regard to the acceptance of electronic documents, when an original document or a certified copy is required for the provision of a public service, at the least electronic documents issued by the persons who are competent to issue the relevant documents and that are considered to be originals or certified copies in accordance with national law of the Member State of origin, shall be accepted in other Member States without additional requirements.

8) Website authentication: the proposal ensures that the authenticity of a website with respect to the owner of the site will be guaranteed.

BUDGETARY IMPLICATION: EUR 9 408 million for the period 2014-2020 (human resources). The specific budgetary implications of the proposal relate to the tasks allocated to the European Commission. The proposal has no implications on operational expenditure.

DELEGATED ACTS: the proposal contains provisions empowering the Commission to adopt delegated acts in accordance with Article 290 of the Treaty on the Functioning of the EU.

Electronic transactions in the internal market: electronic identification and trust services

2012/0146(COD) - 07/06/2012

The Commission **presented to ministers a new draft regulation** to enable cross-border and secure electronic transactions in the EU, adopted on 4 June 2012.

The draft regulation:

- lays down rules for electronic identification and electronic trust services for electronic transactions with a view to ensuring the proper functioning of the internal market;
- establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic delivery services and website authentication;
- contribute to building trust and confidence in the on-line market for goods and services and therefore to the completion of the internal market and growth.

Electronic transactions in the internal market: electronic identification and trust services

2012/0146(COD) - 23/07/2014 - Final act

PURPOSE: to enhance trust in electronic transactions in the internal market and ensure the mutual recognition of electronic identification, authentication, signatures and other trust services across borders.

LEGISLATIVE ACT: Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

CONTENT: this new Regulation provides a **common foundation for secure electronic interaction between citizens, businesses and public authorities**, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the Union and enhancing trust in electronic transactions in the internal market.

In doing so, the Regulation:

- lays down the conditions under which Member States recognise electronic identification means of natural and legal persons falling under a notified electronic identification scheme of another Member State;
- lays down rules for trust services, in particular for electronic transactions; and
- establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication.

System for mutual recognition of electronic identification: the new rules require member states to recognise, under certain conditions, means of electronic identification of natural and legal persons falling under another Member State's **electronic identification scheme which has been notified to the Commission**. It is up to the Member States to choose whether they want to notify all, some or none of the electronic identification schemes used at national level to access at least public online services or specific services. These rules only cover **cross-border aspects** of electronic identification, and issuing means of electronic identification remains a national prerogative.

Conditions for mutual recognition: the principle of mutual recognition should apply if the notifying Member State's electronic identification scheme **meets the conditions of notification** and the notification was published in the Official Journal of the European Union.

The obligation to recognise electronic identification should only apply when the public sector body in question uses the assurance level '**substantial' or 'high'** in relation to accessing that service online.

This Regulation should provide for the **liability** of the notifying Member State, the party issuing the electronic identification means and the party operating the authentication procedure for failure to comply with the relevant obligations under this Regulation.

In the case of a **breach of security**, the notifying Member State shall, without delay, suspend or revoke that cross-border authentication or the compromised parts concerned, and shall inform other Member States and the Commission.

Member States should **cooperate with regard to the security and interoperability** of the electronic identification schemes at Union level through the exchange of information and the sharing of best practices between Member States.

Timeline for mutual recognition: those Member States which so wish may join the scheme for recognising each others' notified e-identification means as soon as the necessary implementing acts are in place. This is expected to take place on 18 September 2015 at the latest. The mandatory mutual recognition is expected to kick off in the second half of 2018.

Trustworthy services: Directive 1999/93/EC of the European Parliament and of the Council dealt with electronic signatures without delivering a comprehensive cross-border and cross-sector framework for secure, trustworthy and easy-to-use electronic transactions. This Regulation enhances and expands the acquis of that Directive.

More specifically, the new Regulation also **introduces, for the first time, EU-wide rules concerning trust services**, such as the creation and verification of electronic time stamps and electronic registered delivery services, or the creation and validation of certificates for website authentication.

Trust services which comply with the regulation can **circulate freely** within the single market. In addition, an EU trust mark will be created to identify trust services which meet certain strict requirements. Trust services provided by trust service providers established in a **third country** shall be recognised as legally equivalent to qualified trust services provided by qualified trust service providers established in the Union where the trust services originating from the third country are recognised under an agreement concluded between the Union and the third country in question or an international organisation.

Where feasible, trust services provided and end-user products used in the provision of those services shall be made accessible for **persons with disabilities**.

An **EU trust mark** should be created to identify the qualified trust services provided by qualified trust service providers. The use of the trust mark will be voluntary.

Supervisory body: Member States should designate a supervisory body or supervisory bodies to carry out the supervisory activities under this Regulation.

Supervisory bodies should cooperate with data protection authorities, for example by informing them about the results of audits of qualified trust service providers, where personal data protection rules appear to have been breached.

Supervision of qualified trust service providers: qualified trust service providers should be audited, at least every 24 months, at their own expense by a conformity assessment body

The Commission shall **review** the application of this Regulation and shall report to the European Parliament and to the Council no later than 1 July 2020.

ENTRY INTO FORCE: 17.09.2014. The Regulation shall apply from 1 January 2016.

DELEGATED ACTS: the Commission may adopt delegated acts to adopt the regulatory technical standards. Power to adopt such acts is conferred on the Commission for **an indeterminate period of time from 17 September 2014**. The European Parliament or the Council may formulate objections to a delegated act within a period of **two months** of notification of that act (that period may be extended by two months). If Parliament or Council raise objections, the delegated act will not enter into force.

Electronic transactions in the internal market: electronic identification and trust services

2012/0146(COD) - 03/04/2014 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted by 534 votes to 76, with 17 abstentions, a legislative resolution on electronic identification and trust services for electronic transactions in the internal market.

Parliament adopted its position at first reading following the ordinary legislative procedure. The amendments adopted in plenary are the result of an agreement negotiated between the European Parliament and the Council. They amend the proposal as follows:

Purpose: the Regulation seeks to enhance trust in electronic transactions in the internal market by providing **a common foundation for secure electronic interaction between businesses, citizens and public authorities**, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the Union.

A "**trust service**" means an electronic service normally provided for remuneration which consists in:

- the creation, verification, and validation of electronic signatures , electronic seals or electronic time stamps, electronic registered delivery services and certificates related to these services or
- the creation, verification and validation of certificates for website authentication or
- the preservation of electronic signatures, seals or certificates related to these services.

Scope: this Regulation should apply to **electronic identification schemes notified** by Member States, and to trust service providers established in the Union. This Regulation does not apply to the provision of trust services used exclusively within closed systems resulting from national legislation or from agreements between a defined set of participants.

This Regulation should be applied in full compliance with the principles relating to the **protection of personal data** provided for in Directive 95/46/EC.

Mutual recognition: electronic identification systems notified according to the Regulation should specify the assurance levels**"low", "substantial" and/or "high"** for electronic identification means issued.

The obligation to recognise electronic identification means should only apply when the public sector body in question uses the assurance level "substantial" or "high in relation to accessing that service online.

Notification of electronic identification systems: systems notified by the Member States should be accompanied by, among other things, the **following information**: (i) a description of the notified electronic identification scheme, including its assurance levels and the issuer(s) of electronic identification means under that scheme; (ii) the applicable supervisory regime and information on liability regime with respect to the party issuing the electronic identification means, and the party operating the authentication procedure; (iii) information on the entity or entities which manage the registration of the unique person identification data.

Security breach: when either the electronic identification scheme notified or the authentication is breached or partly compromised in a manner that affects the reliability of the cross border authentication of that scheme, the notifying Member State should **suspend or revoke without delay that cross border authentication** or the compromised parts concerned and inform other Member States and the Commission.

Liability: Parliament and the Council introduced a new provision whereby the notifying Member State, the party issuing the electronic identification means, as well as the party operating the authentication procedure, would be **liable for damage caused intentionally or negligently** to any natural or legal person for failing in a cross border transaction to comply with its obligations under the Regulation.

The intention or negligence of a qualified trust service provider should be **presumed** unless he proves that the damage occurred without the intention or negligence on his part.

Cooperation and interoperability: the national electronic identification schemes notified should be interoperable. The interoperability framework should aim to be **technology neutral** and should not discriminate between any specific national technical solutions for electronic identification within the Member State. Member States should cooperate as regards the interoperability of electronic identification systems and the security of electronic identification systems.

Third country trust service providers: according to the amended text, trust services provided by trust service providers established in a third country should be recognised as legally **equivalent** to qualified trust services provided by qualified trust service providers established in the Union if the trust services originating from the third country are recognised under an **agreement** concluded between the Union and third countries or international organisations.

Accessibility for persons with disabilities: where feasible, trust services provided and end-user products used in the provision of those services should be made accessible for persons with disabilities

Supervisory body: Member States should designate a supervisory body or supervisory bodies to carry out the supervisory activities under this Regulation. Member States should be also able to decide, upon a mutual agreement with another Member State, to designate a supervisory body in the territory of that other Member State.

Supervisory bodies should cooperate with data protection authorities, for example by informing them about the results of audits of qualified trust service providers, where personal data protection rules appear to have been breached.

Supervision of qualified trust service providers: qualified trust service providers should be audited, **at least every 24 months**, at their own expense by a conformity assessment body.

EU trust mark: an EU trust mark should be created to identify the qualified trust services provided by qualified trust services providers. The use of an EU trust mark by qualified trust service providers should be voluntary and should not lead to any other requirement than those already provided for in this Regulation.

By **1 July 2015,** the Commission should, by means of implementing acts, lay down specification relating to the form and in particular the presentation, composition, size and design of the EU trust mark for qualified trust services.