GSMA COMMENTS

on the implementation of a pan-European framework on electronic identification and trust services for electronic transactions in the internal market

19 March 2015

Introduction

The GSMA strongly supports the eIDAS regulation (the 'Regulation') which will provide legal and regulatory certainty across Member States and stakeholders for digital identification and trust services. The Regulation will help boost economic growth in Europe and the promotion and deployment of e-ID schemes across Member States and will open up a new set of business opportunities for the mobile industry.

To achieve this will require the **right balance between protecting privacy and security and ensuring that business and innovation can flourish within a truly uniform single market**. Care should be taken to ensure that economic growth and development are not impeded by disproportionate and unnecessary regulation and that **technology neutrality remains a fundamental principle and objective throughout the implementation of the Regulation.**

Mobile operators are well equipped to play a key role in providing eID and related trust services on mobile devices and on the SIM card. In order to contribute to the preparation of the secondary legislation associated with the eIDAS regulation, the GSMA has set the following four key principles in relation to the implementing acts referred to in the Regulation:

1. **Assurance levels based on well-established global standards.**
2. **Principle-based and not over-prescriptive interoperability framework**.
3. **Technology neutral specifications.**
4. **Appropriate supervision measures.**

These principles together with the supporting comments are outlined in this paper and GSMA hopes they will serve as constructive input to the European Commission's work when further developing implementing acts, as well as to the discussions of the eIDAS Expert Group.

Specific Comments

1. Levels of assurance for electronic identification means

Key Principle #1: Assurance levels based on well-established global standards.

Any harmonised specifications and procedures of assurance levels for electronic identification means and electronic trust services should be based on international standards, because they play an important role in fostering interoperability, not only at European level, but also in a broader international context. Assurance levels should therefore be based on ISO 29115 as it is the only international standard available in the domain of assurance levels for electronic identification means.

When developing the implementing act referred to in Article 8(3) of the Regulation regarding the minimum technical specifications and procedures of assurance levels for electronic identification means, the European Commission should take the following into account:

- **Reference to standards** – ISO 29115 is very comprehensive and the only international standard available in the domain of assurance levels for electronic identification means and should be directly referenced in the implementing act. A harmonised approach to levels of assurance will encourage the notification and adoption of minimum security measures in the provision of electronic identity schemes across borders and across sectors in the EU. ISO 29115 covers the key areas of the Identity ecosystem – from ID Proofing, to credential storage and credential transport - and also provides a detailed catalogue of the threats to 'Identity lifecycle steps' and measures that can be taken to address them. Moreover, ISO 29115 is largely adopted by industry players in the value chain including internet players, the Open ID foundation and GSMA mobile network operator members.

- **Specification of assurance levels** – It is important to make clear differentiations between Low, Substantial and High assurance levels, especially when specifying identity proofing and verification, electronic identification means management, authentication mechanism, as well as security and risk management practices. Furthermore, it is highly recommended that such specifications adopt an outcome-based approach whereby functional requirements are based on core principles and objectives rather than strict definitions. This will ensure flexibility and technology neutrality vis-à-vis technological developments, avoiding the application of outdated standards that might hinder the development of more innovative solutions. When levels of assurance are clearly specified and understood, trusting parties can more easily categorize their services and use electronic identification schemes. For example,

they can choose to only accept schemes which match the required security level for a service, resulting in a dramatic increase in customer satisfaction and overall trust in the ecosystem.

- **Clarity of definitions** - Definitions should be based on the concepts set out in ISO 29115 and any adaptation of these concepts should be clearly justified. Furthermore, it is important to avoid vague concepts when defining the meaning of the authentication factor and its possible variations (e.g. dynamic vs static). Authentication factor definition which implies the usage of a factor that does change between authentications might refer to one-time-password. If this is the case, then it would be a significant step backwards in usability and would rule out PIN and biometric based authentication factors.

2. Interoperability Framework

Key Principle #2: Principle-based and not over-prescriptive interoperability framework.

Technical and operational arrangements of the interoperability framework for electronic identification schemes should not be over-prescriptive, but be principle-based and take into account the criteria and minimum standards already applied within the Regulation. The GSMA welcomes the implementation of the principle of privacy by design within the interoperability framework of electronic identification schemes, because risks can be mitigated by the implementation of this principle and by the use of anonymisation, pseudonymisation, data encryption and other protection measures.

When developing the implementing act referred to in Article 12(8) of the Regulation regarding the technical and operational arrangements of the cross-border interoperability framework for the purpose of setting uniform conditions to ensure the interoperability of electronic identification schemes, the European Commission should take the following into account:

- **Data privacy and confidentiality** - The GSMA strongly recommends that, alongside sufficient transport layer protection, message layer protection is also used (e.g. using encrypted messages, adding signature, adding message checksums, etc.). This way a higher level protection of privacy and confidentiality can be ensured.

- **Protection against malicious attacks** – In order to enable efficient communication, pre-agreement of the protection profile (e.g. encryption algorithms, key length, keys, etc.) should be allowed between the nodes participating in data exchange, or it should be possible to securely discover the protection profile.

- **Message format for the communication** - The message format should use a model of '*Header* + *Payload*', so that the *Header* (i.e. supplemental data placed at the beginning of a block of data being stored or transmitted) can include sufficient metadata to add context for *Payload* (i.e. the message content). The *Header* composition should follow a clear and unambiguous specification in order to allow proper processing of person identification data.

- **Requirements of person identification data** - The requirements that should be met by the minimum set of person identification data uniquely representing a natural or legal person should be clearly set out in this implementing act.

- **The Cooperation Network** - An important task for the Cooperation Network, as clearly stated in the Recitals of the Regulation, is to maintain technology neutrality by ensuring that no additional costs or technical requirements are imposed on relying parties established outside their territory. This is an important issue to ensure a truly European digital single market with no barriers to cross border electronic transactions.

3. Formats of e-Signatures

Key Principle #3: Technology neutral specifications.

Specifications of electronic signature for public services should remain technology neutral and independent of the underlying technology and procedure that is used to deliver those services. It is GSMA's view that while the objective of the Regulation is to remain technology neutral and future-proof, a reference to a specific technology may defeat this important objective.

When developing the implementing act referred to in Article 27(5) of the Regulation regarding the formats of advanced electronic signatures recognised by public sector bodies or reference methods where alternative formats are used, the European Commission should take the following into account:

- **Technology neutrality** – The GSMA believes a technology neutral approach should be used so that non-PKI based alternatives may also be considered. The extent to which an advanced electronic signature is compliant with the Regulation's requirements is dependent on several factors. Advanced electronic signatures, for example, can be delivered with or without a PKI infrastructure i.e. PKI is only one technology option, albeit commonly used. Similarly, both the context and the degree of risk of the signature may have an impact on its security levels.

- **Mapping of electronic signatures** - The GSMA strongly recommends that a high level, non-mandatory and simplified guideline to map electronic signature per level of assurance and per-use case is developed. The GSMA believes that mapping the standards, electronic signature types and profiles with the levels of assurance is necessary. This would help to foster a technology neutral way of associating and using electronic signatures, provide greater legal certainty and harmonization across trust services providers and relevant stakeholders with beneficial effects on trust within the wider ecosystem and overall market development.

4. Supervision (Notification / Trusted Lists)

Key Principle #4: Appropriate supervision measures.

Proportional, appropriate and context based supervision of identity and trust services providers both at national and cross border level is a building block for achieving trust in the wider eco-system. Additionally, consistency of implementation with other current regulatory developments is vital in order to avoid compliance duplication and over prescriptive rules.

When developing the implementing acts referred to in Article 9(5) of the Regulation regarding notification and in Article 22(5) of the Regulation regarding the trusted lists, especially when it considers supervision schemes applied to trust service providers and the electronic trust services they provide, the European Commission should take the following into account:

- Accountability and due diligence requirements for trust service providers should be based on an outcome-based approach whereby functional requirements are based on the core principles and objectives already included in the Regulation.
- Privacy is an important consideration for citizens, business and governments. A consistent privacy and data protection framework is key not only to achieve a level playing field for players in the market, but also to build trust in the identity ecosystem. In the emerging digital identity and trust service market, the protection of privacy and security is a key issue. In order to foster investment in trustworthy solutions and avoid risks such as identity theft or misuse of the electronic medium, it is critical that the implementing acts are not over-prescriptive and a right balance between privacy and security is achieved to ensure both business efficiency and fair competition.

- Appropriate reporting and management of security breaches and loss of integrity are fundamental to building trust in the identity ecosystem. The GSMA, therefore, appreciates the European Commission's proposal to standardise the format and procedures of supervisory authorities for reporting mechanisms. However, current regulatory developments on security breaches should not be duplicated and it is important to take into account that:
    - EU Member States have already implemented notification regimes for loss of integrity and breach of security impacting the operation of public telecommunications networks and services (Article 13a of the revised Framework Directive) as well as breaches of personal data (Article 4 of the revised e-Privacy Directive).
    - The proposed comprehensive data protection reform in the General Data Protection Regulation (GDPR) will extend the notification obligation to sectors other than telecommunications.
    - The proposed Network and Information Security Directive (NIS) will also require competent authorities to submit summary report to the cooperation network on the notifications received and action taken.

About the GSMA

The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with more than 250 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and Internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai and the Mobile 360 Series conferences.

To learn more about our **Personal Data** programme, please visit:
http://www.gsma.com/personaldata/

To read our **mobile identity regulatory overview**, please visit:
http://www.gsma.com/personaldata/wp-content/uploads/2015/01/Personal-Data-Regulatory-Overview-2014.pdf