# WHAT SHOULD A HIGH LEVEL OF ASSURANCE BE?

*Eurosmart position on eIDAS Levels of Assurance*

## Table of contents



### Why does the eIDAS Regulation implementation need a real level of assurance high?

The European regulation on electronic identification and trust services (eIDAS) defines the three levels of assurance "low", "substantial" and "high" for electronic identification means issued under an electronic identification national scheme. According to article 8 (2.c) of the regulation, "*assurance level high shall refer to an electronic identification means* […]*, which provides a higher degree of confidence in the claimed or asserted identity of a person than electronic identification means with the assurance level substantial, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to prevent misuse or alteration of the identity*."

**The definition of the assurance levels is a cornerstone of the regulation, as a clear vision of these three levels will provide the necessary trust and allow the development of the digital services related to the electronic identification schemes.**

Eurosmart strongly believes that **no party should be imposed a lower level of security than the one it decided to adopt.** Interoperability should not be at the expense of higher security levels. Moreover, the eIDAS regulation should allow citizens' identity to clearly remain the sovereign responsibility of governments, at a time when the increasing digitalization takes away a part of the identity from the sovereign domain. **European Member States have the responsibility, through the adoption of such a regulation, to implement security safeguards to protect their national citizens from risks related to dematerialized procedures and transactions.**

### What is an appropriate level of assurance high?

**The "Levels of Assurance" Implementing Act shall, for the security requirements related to level "high", rely on the existing scheme of SOGIS-MRA, which already gathers EU Member States and which validity has long been demonstrated.** The reference to SOGIS-MRA to define a level of assurance high would avoid misinterpretation and allow more legal certainty for governments. The SOGIS-MRA scheme is a well-known, complete and structured framework, independent from the suppliers. The security requirement shall be a SOGIS-MRA security certification at **level EAL4+, including AVA_VAN5.**

### Member States should notify a level of assurance high for the benefits they provide

- ✓ **Benefits for the Government**
  - **In terms of liability:** The government liabilities are the same whatever the assurance level is. However, lower levels presenting more risks, they will involve the government in more legal cases.
  - **In terms of security and savings:** security requirements related to the level high strongly reduce the risk of identity fraud, and the additional costs that it implies.
  - **In terms of harmonization**: in 2015, 16 EU Member States have[1] an eID scheme running or in development and are likely to notify to the European Commission a level of assurance high. A government that would only notify lower levels would prevent their citizens from accessing public services of these 16 Member States.
  - **In terms of personal data and privacy protection**: Solutions with a level of assurance high are strongly in line with the requirements set out in the new European Data Protection Regulation, to be adopted in 2015-2016.
- ✓ **Benefits for service providers**
  - **In terms of business opportunity:** a clear definition of a level of assurance high for applications where strong security requirements are needed should open the door to the development of services with a level of assurance substantial, as strong security requirements for the level high would create a clearer distinction with the level below.
  - **In terms of convenience:** A clear distinction between a level of assurance high and the lower levels is necessary to perform risk management analysis and privacy impact assessment.
- ✓ **Benefits for citizens**
  - **In terms of privacy protection:** requirements for the level high allow a better guarantee for the privacy of the citizens; rules in terms of data minimization also constitute an additional hurdle against profiling;
  - **In terms of convenience and mobility:** citizens would benefit from a strong flexibility to authenticate and access services in other EU Member States, in the context of the Digital Single Market.
  - **In terms of evolution of services:** electronic identification will evolve through time, with the development of innovative technologies (increasing use of smartphones to access online services, but also identification to smart cars, smart houses etc.) which will require a level of assurance high.

[1] Finland, Estonia, Belgium, Austria, Sweden, Spain, Italy, Netherlands, Portugal, Lithuania, Germany, Latvia, Czech republic, Ireland, Romania, Slovakia

### What are the use-cases?

Eurosmart believes that the assurance level high has a clear sense for many public and private use-cases:

- ✓ **For the public sector**
  - Logical access to social and pension services;
  - Healthcare, telemedicine and access to health records;
  - Qualified eSignature (e.g. for legal procedures)
  - Electronic change of address;
  - Electronic car registration
- ✓ **For the justice and paralegal actors**
  - Logical access to courts;
  - Legal procedures;
  - Notaries and accounting experts;
  - eRegistered letters;
  - Insurance contracting;
  - eVoting and/or petition for a referendum;
- ✓ **For the private sector**
  - Qualified eSignature (e.g. for contracts)
  - Paying a parking lot in a rent smart car
  - Opening bank accounts online
- ✓ **For the enterprise sector**
  - Online bidding on tender in the public domain

## *About Eurosmart*

*Eurosmart is an international non-profit association located in Brussels and representing the smart security industry for multisector applications. Founded in 1995, the association is committed to improving the quality of the security applications in the world's smart secure devices, to developing smart security standards and to expanding the world's smart secure devices market. Members are manufacturers of smart cards, semiconductors, terminals, equipment for smart cards system integrators as well as application developers and issuers who work in dedicated committees (security management, electronic identity, communication, marketing & technology, mobile trust, product & system security).*

*Eurosmart members are companies (Athena Smartcard, EM Electronic Marin, FNMT-RCM, Gemalto, Giesecke & Devrient, Infineon Technologies, Imprimerie nationale, Inside Secure, LFoundry, Linxens, Morpho, Microsoft, NedCard, NXP Semiconductors, Oberthur Technologies, Samsung, STMicroelectronics, Toshiba), payment systems (Mastercard), laboratories (CEALETI), research organisations (Fraunhofer AISEC), associations (Smart Payment Association, Mobismart, Danish Biometrics) and independent experts (Michel Koenig, Jonas Andersson).*

*Eurosmart is acknowledged as representing "the Voice of the Smart Security Industry".*

*For more information, please visit [www.eurosmart.com](http://www.eurosmart.com)*

**Contact:**
**Oyvind Rastad**
Eurosmart Chairman
Rue du Luxembourg 19-21
B-1000 Brussels
Belgium
eurosmart@eurosmart.com
Tel: + 32 2 506 88 38
Fax: + 32 2 506 88 25