Online security - Seamless personal authentication
(authentication for all)

RULES OF CONTEST

Version 1.1

10 October 2017

1. THEME: SEAMLESS PERSONAL AUTHENTICATION - AUTHENTICATION FOR ALL

1.1 Objectives pursued

The Internet has come to play an integral part in the lives of many European citizens. A large majority of people believe and even accept that there is no alternative other than to provide personal information if they want to obtain products or services online. The reliance on digital technology and the transfer of personal data to enable the use of online services come with substantial security risks to people and their smart objects, such as online fraud and identity theft.

We are now entering a new era of digital services where these concerns will increase as important aspects of our lives (such as personal relations) are being shared though social networks, when the way we interact with the world around us is changing as everything gets connected and the boundaries between the physical and the digital worlds are progressively blurring, and when we start to see connected smart objects that become autonomous and incorporate self-adapting and intelligent decision making capabilities. In this new technological revolution, we should bring people into the focus by enabling them (independently of age, financial or physical status) to equally participate in all digital services, have full access to cyberspace, and have control and liability for their smart objects (e.g. smart mobile devices and household appliances, wearable gadgets, smart cars). To shape this Next Generation human-centric and trustworthy Internet, we first need to develop innovative ways to enable all people with their linked objects to easily prove their identities, their mutual relationships, privileges and rights. In other words we need innovative authentication solutions where connectivity will become an opportunity and not a burden to people.

Password protection has been the default method of authentication online to date. This simple mechanism has many advantages, but the use of usernames and passwords in practice is severely flawed in both security and usability. Other solutions typically employed in conjunction with passwords in a multi-factor approach (e.g. smart cards, PKI - Public Key Infrastructure certificates, biometrics, RFIDs - Radio Frequency Identification Devices), usually improve the robustness of the authentication. However, the increased security of multi-factor authentication (MFA for short) has come at the price of limited usability and privacy concerns for individuals and increased costs for providers. Users often find multi-factor authentication cumbersome and a burden in terms of time and effort. This burden is then transferred to providers who find it challenging to register or even retain users. In addition to this limitation, providers are also confronted with the high costs of MFA as the method often requires additional hardware.

Another significant concern for citizens is privacy. A number of authentication methods, such as the ones based on biometric traits or digital quasi-identities such as social network/platform accounts, rely on the collection of large amounts of sensitive personal data. However, these approaches typically fail to assure citizens' trust by giving visibility over how this collected data is used and stored.

Thus there is a clear need for a simple, secure and privacy-friendly way of seamlessly authenticating individuals and their smart objects online.

Solutions to this particular challenge should overcome the shortfalls of current technologies, and should bring enhanced convenience, security, privacy, accuracy, openness, efficiency and effectiveness in authentication.

This Horizon 2020 Prize aims to stimulate further research and innovation within the European Union in online authentication. The contest has the ultimate goal of fostering the widespread adoption and access of services and products provided within the Digital Single Market of the European Union where cyber security, privacy and liability are the priorities. This prize also complements the activities of the Cybersecurity contractual Private Public Partnership (cPPP)[1], which aims to develop Europe's strengths in cybersecurity and digital privacy.

[1] https://ecs-org.eu/cppp

1.2 Expected results

An information and communication technologies (ICT) solution that enables citizens and their smart objects to seamlessly authenticate themselves across a wide range of applications and devices. The solution should be easy to use, reliable, robust against cyber-attacks, privacy-friendly and compatible with widely used technologies as well as affordable. It should be also open enough so that it could be easily audited, enhanced, tailored, developed and/or integrated. In addition, it should be ready to benefit a wide range of the EU population, from healthy to impaired citizens of all ages.

The innovative solution should enable people and the smart objects they own to seamlessly authenticate (i.e. prove their relationships, identities, privileges and rights) among each other and across a wide range of services, applications, systems and devices within IoT ecosystems. The solution should also overcome the shortfalls of existing authentication technologies including challenges of group authentication (multiple users authenticating e.g. to the same smart objects in IoT and cloud ecosystems). It should be ready to benefit a wide range of the EU population and the variety of objects they own (e.g. smart cars/appliances/terminals/devices) while respecting and promoting the objectives of relevant EU legislation (e.g. eIDAS[2], NIS Directive[3], GDPR[4]).

2. PRIZE AMOUNT

A total budget of 4.000.000 EUR is available for this prize, offering 3 (three) awards as follows:

- 2.800.000 EUR for the winner(s).
- 700.000 EUR for the 1st runner-up.
- 500.000 EUR for the 2nd runner-up

3. DEADLINES & ADMISSIBILITY

Deadlines	
Opening of the submission:	**28th September 2017**
Closing date for submission:	**27th September 2018 at 17:00:00 CEST**[5]
Evaluation and solutions demonstration:	**November-December 2018**
Prize award:	**December 2018**

Joint applications by a group of participants are admitted. In this case, the participants must appoint a 'lead participant' to represent them towards the Commission. The participants will be jointly responsible and must all fulfil and respect the conditions set out in these Rules of Contest.

Applications must be submitted by the (lead) participant via the Participant Portal Submission Service.

Applications must be readable, accessible and printable. Incomplete applications may be considered inadmissible if essential elements are missing (see General Annex B to the Main Work Programme).

The page-limit for your prize application (Part B) is: 100 pages (excluding annexes and appendices).

Sample application forms will be available on the Participant Portal Reference documents page.

---

[2] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[3] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

4 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[5] Central European Summer Time = Brussels local time

4. ELIGIBILITY

4.1 Eligibility criteria

The contest is open to any legal entity (including natural persons) or group of legal entities established in an EU Member State or in a country associated to Horizon 2020.

Please note however that special rules may apply for entities from certain countries (see General Annex C to the Main Work Programme).

Please also be aware that participants that have already received an EU or Euratom prize cannot receive a second prize for the same activities.

4.2 Exclusion criteria

Participants will be excluded if they (or one of them):

- are subject to an administrative sanction (i.e. exclusion)[6]
- are in one of the following situations[7]:
  - bankrupt, being wound up, having their affairs administered by the courts, entered into an arrangement with creditors, suspended business activities or subject to any other similar proceedings or procedures under national law (including persons with unlimited liability for the participant's debts)
  - declared in breach of social security or tax obligations by a final judgment or decision (including persons with unlimited liability for the participant's debts)
  - found guilty of grave professional misconduct[8] by a final judgment or decision (including persons having powers of representation, decision-making or control)
  - convicted of fraud, corruption, involvement in a criminal organisation, money laundering, terrorism-related crimes (including terrorism financing), child labour or human trafficking (including persons having powers of representation, decision-making or control)
  - shown significant deficiencies in complying with main obligations under a procurement contract, grant agreement or grant decision financed by the EU or Euratom budget (including persons having powers of representation, decision-making or control)
  - found guilty of irregularities within the meaning of Article 1(2) of Regulation No 2988/95 (including persons having powers of representation, decision-making or control)
- have misrepresented information required for participating in the contest or fail to submit such information
- were involved in the preparation of the prize documents and this entails a distortion of competition.

6 See Articles 131(4) and 106(1) Financial Regulation.

7 See Articles 138(2) and 106(1), 107 of the Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council of 25 October 2012 on the financial rules applicable to the general budget of the Union and repealing Council Regulation (EC, Euratom) No 1605/2002 (OJ L 218, 26.10.2012, p.1).

8 Professional misconduct includes: violation of ethical standards of the profession, wrongful conduct with impact on professional credibility, false declarations/misrepresentation of information, participation in a cartel or other agreement distorting competition, violation of IPR, attempting to influence decision-making processes or obtain confidential information from public authorities to gain an advantage.

5. AWARD CRITERIA

The proposed solution should fulfill the following minimum requirements:

- Independently of technological choices (e.g. biometrics, PKIs, wearable computing devices, ear-electroencephalography signal readers, brain computing interfaces), relevant standards for design, development, implementation and testing need to be followed as much as possible as well as technology-related relevant standards (e.g. for biometrics: the ISO/IEC JTC 1/SC 37, ISO-19795) whenever applicable.

- Compliance with relevant EU legislation (e.g. eIDAS, NIS Directive, GDPR) should be demonstrated.

The prize will be awarded to the entry that in the opinion of the jury demonstrates a solution that best addresses the following nine (9) cumulative criteria:

5.1 Significant contribution

The proposed solution should demonstrate measurable advancement beyond the state-of-the-art at least in the following dimensions: security, privacy, usability, interoperability, accuracy, performance and EU legislation compliance in group authentication (of people with their smart objects) in IoT ecosystems.

5.2 Usability

The proposed solution needs to be compliant with relevant usability standards (e.g. ISO 9241-11) whenever applicable. It should be as accessible as possible, and participants should state which accessibility requirements they do meet, and be able to demonstrate this as part of their usability tests (see below).

Participants need to have conducted usability tests of their solution and report the results in their application.

The usability tests should show the solution in at least 3 different usage scenarios requiring user authentication, and cover a wide range of users (in terms of age, skills, physical/mental abilities) and the smart objects they own (e.g. appliances, smart mobile terminals). Usability tests should include the process of activating the user account and/or his/her credentials.

5.3 Reliability

The proposed solution should demonstrate and provide evidence of how it addresses at least the following aspects and how it is compared with existing solutions:

- Completeness and robustness of the authentication mechanism.

- Soundness, accuracy and speed of the authentication mechanism. False acceptance rate (FAR), false detection rate (FDR) and equal error rate (EER) must be provided based upon large scale objective measurements (independently of the scenarios).

- Resistance to known attacks relevant to reliability (e.g.: replay attacks).

- Adequacy for usage on continuous authentication.

- Reliability should be based upon collected data using specific measures (e.g. MTBF - Mean Time Between Failure, MTTF - Mean Time To Failure).

- Maintenance capabilities, justifying and describing the maintenance strategy/policy that will be adopted (e.g. Corrective, Preventive, Scheduled, Predictive, Proactive).

Participants should submit clear proofs for statements/measures regarding reliability and maintenance and provide the necessary means required for the jury to reproduce results during evaluation, either by describing the test suites that were used, or by providing access to the datasets and experimental apparatus (e.g., scripts or programs in a repository), along with parameter configurations.

Operational availability measures need also to be provided by participants, based upon relevant industrial/ICT recognized terms (e.g. downtime, uptime).

5.4 Security

The proposed solution should include a detailed security analysis of the proposed authentication scheme. The application must include a detailed system architectural model, functional flows (e.g. communication flows), security and privacy requirements and proofs / means on how they will be implemented. All assumptions on which the security/privacy is based on should be clearly specified. The application must also include detailed implementation, integration and deployment specifications addressing the security requirements and measuring the security, privacy and accountability properties.

If applicable, cryptographic secrets management schemes and the length of cryptographic material should be analysed and documented. Proofs for cryptographic protocols should be included and particularized with well-known cryptographic primitives.

The provided implementation of the proposed authentication token/solution should have undergone: risk analysis (threat/impact/vulnerability/risk); extensive penetration testing; implementation of: appropriate attack protection strategy (e.g. in case of biometrics utilise the PAD, ISO/IEC 30107-1) and mitigation strategy development (selection/implementation of controls); and static code analysis. State of the art tools, approaches and/or best practices (e.g. the OWASP Testing Guide) should be used for this purpose. The application must contain well summarized penetration testing reports (including the utilized procedures and tools, and the results) and how to reproduce them. The provided implementation should withstand resilience against all applicable and well known state-of-the-art attacks.

Either physical/cyber risk assessment (including risk mitigation) reports or relevant certifications (e.g. CC, ISO27005, ISO27009) should be submitted.

If applicable, biometric based methods used in the proposed solution should also be clearly documented in the application.

The proposed solution should not endanger the health of the user.

5.5 Privacy and data protection

Strong authentication may also be a key privacy mechanism when used to ensure that only a data subject, or authorised parties, may access private information. But serious privacy concerns may arise from the specific ways in which authentication is performed and/or if specific measures are applied aiming at mitigating the data protection and privacy risks.

While by definition authentication requires to demonstrate the identity of an entity or a person, such mechanism should at the same time guarantee that the user's privacy and protection of his personal data is respected in compliance with EU data protection rules, the Data Protection Directive[9] and implementing national laws as well as with the General Data Protection Regulation 2016/679/EU[10], which rules will become applicable as of 25th May 2018.

Privacy and data protection aspects that the proposal addresses will be evaluated, with specific focus on the principles of (a) data protection by design and (b) data protection by default applied with the overall objective of achieving a successful privacy-friendly design of an authentication system.

(a) Data protection by design

The participant should demonstrate how the proposed solution integrates appropriate technical and organisational measures, designed to implement data-protection principles (e.g. the “right to be forgotten”, the “right to ask”), including data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements and data protection rights of the potential users of this solution.

[9] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; Official Journal, L 281 , 23/11/1995 P. 0031 - 0050

[10] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal, L 119, 4/5/2016, P. 1-87

(b) Data protection by default

The participant should demonstrate how to appropriately implement technical and organisational measures for ensuring that, by default, only personal data which are necessary for the specific purpose of authentication are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

5.6 Applicability

The proposed solution should work across a relevant collection of technologies and applications scenarios from at least two of the following critical sectors: health, transport, finance, telecom, governmental and energy. It should illustrate how it can be leveraged in multiple IoT ecosystems and business models.

Participants should strive to bring approaches as broad as possible i.e. authenticating various persons (e.g. different ages/ physical characteristics) with a variety of their objects (e.g. smart toys, wearables, appliances) in all relevant combinations.

5.7 Compatibility

The proposed solution should work across a relevant set of hardware devices and of operating systems (OS) of different kinds and should ensure muti-source capability.

For example: sensor node (e.g., with tinyOS, Rtlinux OSes), smart phone/tablet (e.g. with iOS, Android OSes), laptop, desktop, server (e.g., with Windows, Linux, MacOS OSes) and cloud computing environments (e.g. OpenStack).

The proposed solution should be compatible with other widely used technologies (e.g. WIFI, Bluetooth).

5.8 Affordability

The proposed solutions should be affordable for deployment in large scale and cost-effective, requiring low implementation and infrastructure costs for service providers and for end users.

The proposed solution should illustrate this by providing estimated costs (in EURO currency) for the end user and for the service provider, for four scales of deployment: 100 users, 1.000 users, 100.000 users and 10 Million users.

Participants should document essential cost elements of the proposed solution (e.g. IPR royalties, minimal hardware required).

When relevant, one-time costs and recurrent costs should be documented. Recurrent costs should be estimated per year.

The participant should provide justification for the assumptions supporting the cost values.

5.9 Openness

The extent of openness in the proposed solution should be maximum (e.g. open source).

Participants should strive to clearly and extensively document their technical solution (e.g. document the source code, the APIs, the Software Development Kit, manuals, videos) in order that it could be easily audited, enhanced, tailored, developed and/or integrated.

6. DOCUMENTS

The mandatory supporting documents are set out in the application form.

Participants may be asked at a later stage for further documents (for legal entity validation, bank account validation, ethics review, declaration of honour on exclusion grounds, etc.).

7. PROCEDURE

If there are more than 12 applications, there will be a pre-selection phase to select the best 12 applications to pass to jury review. Otherwise, all applications will pass directly to jury review.

The pre-selection panel and jury usually have a different composition, but jury members may participate in the pre-selection panel.

The jury evaluation is planned to take place in November-December 2018.

The pre-selection panel/jury will evaluate each application against the 9 award criteria: and score them as follows (half marks are possible, decimals are not):

Criterion	Threshold	Maximum points
1. Significant contribution	18	23
2. Usability	6	8
3. Reliability	5	8
4. Security	11	14
5. Privacy and data protection	10	13
6. Applicability	5	8
7. Compatibility	5	8
8. Affordability	5	8
9. Openness	6	10
Total	**71**	**100**

For applications with the same score, the pre-selection panel/jury will determine a priority order according to the following approach: The score for the criterion No 4 will be given a weight of 2 and the score for criterion No 5 will be given a weight of 1.5. If two or more applications tie for the first rank, the price will be equally divided and awarded to all the applications in the tie.

The 5 best applications will be invited as finalists for a hearing with the jury, where they will have to demonstrate their solution on a prototype running in an operational environment.

On the basis of the evaluation by the jury, the Commission will decide on the award of the prize.

All participants will be informed at the end of 2018 on the outcome of their application.

8. OTHER CONDITIONS

8.1 Payment arrangements

The prize money (EUR 2.800.000, 700.000 and 500.000 for the winner(s), the 1st runner-up and the 2nd runner-up resp.) will be paid to the (lead) participant in one instalment after the award ceremony by bank transfer, provided all the requested documents have been submitted.

8.2 Publicity — Promoting the prize — Visibility of EU funding

8.2.1 Publicity by the winner(s)

The finalist(s) and the winner(s) must promote the prize and its results, by providing targeted information to multiple audiences (including the media and the public) in a strategic and effective manner.

Unless the Commission requests or agrees otherwise or unless it is impossible, any communication activity related to the action (including in electronic form, via social media, etc.) must:

(a) display the EU emblem and

(b) include the following text:

> "This action/activity/person was finalist for/winner of the Horizon Prize seamless authentication for all from the European Union's Horizon 2020 research and innovation programme".

When displayed together with another logo, the EU emblem must have appropriate prominence.

Within two years after the award, (each of) the winner(s) must post the award in at least 100 websites, publish award outcomes in at least 10 scientific publications, and demonstrate the awarded system in at least 20 international scientific events/exhibitions/fora.

For the purposes of their obligations, the finalist(s) and winner(s) may use the EU emblem without first obtaining approval from the Commission.

This does not, however, give it the right to exclusive use.

Moreover, they may not appropriate the EU emblem or any similar trademark or logo, either by registration or by any other means.

8.2.2 Publicity by the Commission

The Commission may use, for its communication and publicising activities, information relating to the action, documents notably summaries for publication as well as any other material, such as pictures or audio-visual material that it receives from the participants (including in electronic form).

The Commission will publish the name of the finalist(s) and the winner(s), their origin, the amount of the prize and its nature and purpose — unless they have requested to waive this publication (because disclosure risks threatening their security and safety or harm their commercial interest).

Photos and videos taken by the Commission either in preparation of the award ceremony or during the award ceremony are the sole property of the Commission.

8.3 Dissemination and exploitation of results

The winner(s) must comply with the obligations set out in Title III of the Horizon 2020 Rules for Participation Regulation No 1290/2013[11]

For more information and best practice, see Articles 23a-31 of the H2020 AGA — Annotated grant agreement.

[11] Regulation (EU) No 1290/2013 of the European Parliament and of the Council of 11 December 2013 laying down the rules for participation and dissemination in "Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020)" (OJ L 347, 20.12.2013 p.81).

8.4 Processing of personal data

8.4.1 Processing of personal data by the Commission

Any personal data will be processed by the Commission under Regulation No 45/2001[12] and in accordance with the Participant Portal privacy notice(s).

All finalist(s) and winner(s) consent that the Commission publishes the following information:

- name
- Member State of origin (address or NUTS 2 region)
- their activities in relation to the award of the prize (via the summary for publication they provided)
- prize amount

in whatever form and medium.

8.4.2. Processing of personal data by the participants

The participants must process personal data in compliance with applicable EU and national law on data protection (including authorisations or notification requirements, if any).

8.5 Ethics

The activities must be carried out in compliance with:

(a) ethical principles (including the highest standards of research integrity) and

(b) applicable international, EU and national law.

No prize will be awarded for activities carried out outside the EU, if they are prohibited in all Member States.

The participants must ensure that the activities have an exclusive focus on civil applications.

The participants must ensure that the activities do not:

(a) aim at human cloning for reproductive purposes

(b) intend to modify the genetic heritage of human beings which could make such changes heritable (with the exception of research relating to cancer treatment of the gonads) or

(c) intend to create human embryos solely for the purpose of research or for the purpose of stem cell procurement, including by means of somatic cell nuclear transfer.

Research activities involving human embryonic stem cells (hESC) are moreover subject to the conditions set out in the Statement of the Commission related to research activities involving human embryonic stem cells.

The participants must respect the highest standards of research integrity — as set out, for instance, in the European Code of Conduct for Research Integrity[13].

For more information and best practice, see the Participant Portal Online Manual, the Guidance — How to complete your ethics self assessment and the Guidance note — Research focusing exclusively on civil applications.

---

12 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.01.2001, p. 1).

13 European Code of Conduct for Research Integrity of ALLEA (All European Academies) and ESF (European Science Foundation) of March 2017 http://ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020-ethics_code-of-conduct_en.pdf.

8.6 Security

The activities must be carried out in compliance with Commission Decision 2015/444, i.e. security-sensitive information must be **EU-classified**, if its unauthorised disclosure could adversely impact the interests of the EU or of one (or more) of its Member States. Applications that are too security-sensitive cannot be awarded a prize.

For more information and best practice, see the Guidance — Guidelines for the classification of information in research projects, the Guidance — Guidelines for the handling of classified information in EU research projects, the Guidance note — Potential misuse of research results and the Guidance note — Research involving dual use items.

8.7 Conflict of interests

The participants must take all measures to prevent any situation where the impartial and objective award of the prize is compromised for reasons involving economic interest, political or national affinity, family or emotional ties or any other shared interest ('conflict of interests').

They must inform the Commission without delay of any situation constituting or likely to lead to a conflict of interests and immediately take all the necessary steps to rectify this situation.

The Commission may verify that the measures taken are appropriate and may require additional measures to be taken by a specified deadline.

8.8 Liability for damages

The Commission cannot be held liable for any damage caused to the participants or to third parties as a consequence of the prize, including for gross negligence.

The Commission cannot be held liable for any damage caused by any of the participants in the context of the prize.

8.9 Checks, audits and investigations

The Commission, the European Anti-Fraud Office (OLAF) and the European Court of Auditors may carry out checks, audits and investigations in relation to the prize.

8.10 Withdrawal of the prize — Recovery of undue amounts

The Commission may withdraw the prize after its award and recover all payments made, if it finds out that:

(a) false information, fraud or corruption was used to obtain it

(b) a winner was not eligible or should have been excluded

(c) a winner is in serious breach of its obligations under these Rules of Contest.

8.11 Administrative sanctions

If a participant has committed irregularities or fraud or has made false declarations, the Commission may also:

(a) exclude the participant from all future contracts, grants and contests financed from the EU or Euratom budget for a maximum of five years (or 10 years in case of repetition) and/or

(b) impose a financial penalty between 2% and 10% of the value of the prize (or between 4% and 20% in case of repetition).

8.12 Cancellation of the contest

The Commission may cancel the contest or decide not to award the prize — without any obligation to compensate participants —, if:

(a) no applications are received

(b) the jury does not find a winner

(c) the winner is not eligible or must be excluded or

(d) the objective of the contest has already been achieved.

8.13 Complaints

Complaints against decisions negatively affecting the rights of a participant or winner can be brought before the General Court — or, on appeal, the Court of Justice of the European Union — under Article 263 of the Treaty on the Functioning of the EU (TFEU).

9. CONTACT

For more information, please see the prize website.

In case of questions, please contact cnect-a2-prize@ec.europa.eu.