

National Institute of Standards and Technology (NIST)
Questionnaire for Developers about use of Cryptography in their software.

1. Explain who will be surveyed and why the group is appropriate to survey.

As part of an in-depth interview study of how software developers use cryptography in the programs that they are developing, the Visualization and Usability Group (VUG), of the Information Technology Laboratory (ITL), of the National Institute of Standards and Technology (NIST) intends to recruit 1000 participants. Participants will be individuals who have first-hand technical knowledge of the domain area. Participants will be recruited from crypto websites, list servers of crypto conferences, workshops, and lists of organizations that develop products using crypto through broadcast emails. The information being requested is not available from public sources, such as software documentation or an inspection of open source software code.

The purpose of this project is to investigate how developers use cryptography in their software and the factors that are used to plan future software development. We believe that by collecting this data we can identify and describe the process by which cryptography is incorporated in software, which will assist us in creating recommendations for making it easier for developers to use encryption correctly and securely.

2. Explain how the survey was developed including consultation with interested parties, pretesting, and responses to suggestions for improvement.

The questionnaire that we developed was based on discussions with cryptography experts at the National Institute of Standards and Technology (NIST). This is the first collection of information of its kind that NIST is aware of.

3. Explain how the survey will be conducted, how customers will be sampled if fewer than all customers will be surveyed, expected response rate, and actions your agency plans to take to improve the response rate.

A link for the online survey will be distributed to partners of the National Cybersecurity Center of Excellence (NCCoE), distributed to NIST academic collaborators, and sent to mailing lists of software developers through broadcast emails. After providing their participation consent, each participant will be directed to an online survey of 12 questions.

The expected response rate of completed surveys will vary by organization. We expect a 100% response rate from NCCoE members, a 50% response rate from our academic collaborators, and less than 4% response rate from mailing lists.

4. Describe how the results of the survey will be analyzed and used to generalize the results to the entire customer population.

We intend to use clustering and grounded theory to create a list of developer practices, concerns, and evaluation techniques. We will compare the qualitative responses across different kinds of developers and organizations to identify commonalities and differences. From these results we

will draft a NIST publication and plan the next phase of our research efforts.