




# OMB Control #0693-0043 - ITL Cryptography Software Collection Screen Shots

Preview / Test Mode   

[Show/Hide Comments](#) [Customize Style](#) [Invite Others to Test](#) [Settings](#)

## Use of Cryptography Survey

The National Institute of Standards and Technology (NIST) is researching ways of making it easier for developers to build cryptography into their products. As part of this research, NIST has created this pilot survey about your organization's use of cryptography and cryptography standards in software that you are developing. We plan to use these questions as the basis of a phase two 30-minute structured interview. Written responses at this point will help us to focus the research effort.

- Please answer the survey questions on behalf of your group or organization unit.
- You are welcome to forward a copy of the survey to others in your organization who develop products that use cryptography and cryptography standards. We are interested in their responses as well!
- Please provide additional information for any question as you see fit.

This survey uses the word "products" to describe any hardware, software, or system that your organization is developing. A product may be for internal use, for sponsors, or customers.

For additional information, please refer to [Use of Cryptography Survey Information Sheet](#)

This collection of information contains Paperwork Reduction Act (PRA) requirements approved by the Office of Management and Budget (OMB). Notwithstanding any other provisions of the law, no person is required to respond to, nor shall any person be subject to a penalty for failure to comply with, a collection of information subject to the requirements of the PRA unless that collection of information displays a currently valid OMB control number. Public reporting burden for this collection is estimated to be 60 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed and completing and reviewing the collection of information. Send comments regarding this burden estimate or any aspect of this collection of information, including suggestions for reducing this burden, to the National Institute of Standards and Technology, Attn: Mary Theofanos, maryt@nist.gov, (301) 975-5889.

OMB Control No. 0693-0043  
Expiration Date: 12-31-2018

[Next](#)

Use of Cryptography Survey Screen 1

## INFORMATION SHEET

Project Title: ITL-16-0011 - Usable Cryptography a Survey

### Key Researchers:

NIST Principal Investigators: Mary Theofanos, Phone: (301) 975-5889, Email: [mary.theofanos@nist.gov](mailto:mary.theofanos@nist.gov)  
Simson Garfinkel, Phone (301) 975-8516, Email: [Simson.garfinkel@nist.gov](mailto:Simson.garfinkel@nist.gov)

### RESEARCH DESCRIPTION

This study is being performed to understand how organizations design and implement crypto applications. It will investigate organization's use of cryptography by determining: sources of crypto implementations, testing and evaluation approaches, challenges when incorporating crypto in products, and standards used in developing products. The research is funded and conducted by the National Institute of Standards and Technology (NIST).

### Requirements for Participation

In order to participate in this research project, you must be at least 18 years old and have experience in developing products that include cryptography.

### Study Procedures

You will be given a survey consisting of 12 questions. All of your questionnaire responses will be recorded without any identifiers. The survey should take you no more than 20 to 30 minutes.

We expect to have approximately 1,000 participants complete this phase of the study.

### Confidentiality:

You will be assigned a participant reference code that will be used for all data in this project. Your identity will be protected to the extent permitted by law, including the Freedom of Information Act. The Office for Human Research Protections (OHRP) of the U.S. Department of Health and Human Services, members of the NIST Institutional Review Board (IRB), appropriate NIST researchers, and other appropriate Federal employees may review the records of this study. The study data will be used by the research team to develop guidance on cybersecurity and privacy training and administration. All of the data from the survey will be recorded without identifiers. Your data will not be linked back to you in any way. NIST will not create or keep a list that links your reference code to your name or other identifying information. In the freeform questions of the questionnaire, do not include information that may identify you.

### Voluntary Participation

Your participation is voluntary. Refusal to participate will involve no penalty or loss of benefits to which you are otherwise entitled. You are free to withdraw from the study at any time during the experiment, without penalty or loss of benefits to which you are otherwise entitled. If you withdraw from the study, your data will not be removed from the study.

### Potential Risks and Benefits

The risks during performance of the study activities are minimal and not greater than those ordinarily encountered in daily life or in responding to a routine survey. You will not benefit directly by participating in the study. The long-term benefits of this study to society should be improved cryptographic implementations.

### Contact Information:

For questions regarding this study, please contact Mary Theofanos at 301-975-5880, [maryt@nist.gov](mailto:maryt@nist.gov) or Simson Garfinkel, (301) 975-8516, [simson.garfinkel@nist.gov](mailto:simson.garfinkel@nist.gov). For questions regarding your rights as a human subject, please contact Anne Andrews, Director, NIST Human Subjects Protection Office, at (301) 975-5445 or [anne.andrews@nist.gov](mailto:anne.andrews@nist.gov), or Laura Baxter in the Office of the Chief Counsel for NIST, at 301-975-5622, or [laura.baxter@nist.gov](mailto:laura.baxter@nist.gov). Any research-related injury during the study should be reported to Mary Theofanos at 301-975-5880, [maryt@nist.gov](mailto:maryt@nist.gov) or Simson Garfinkel, (301) 975-8516, [simson.garfinkel@nist.gov](mailto:simson.garfinkel@nist.gov).

Use of Cryptography Survey Information Sheet (accessible from link on first page of survey). Note that this is the approved information sheet.

## Use of Cryptography Survey

1. Where is cryptography used in your products? Please select all that apply, and provide your own uses if these are not sufficient:

**Protecting Communications:**

- End-to-end encryption (e.g. HTTPS and S/MIME)
- Networking (e.g. VPNs and line encryptors)

**Protecting Storage:**

- Data-at-rest (e.g. full disk encryption, application-level protected storage)
- Cloud-based protected storage
- High-integrity archives

**Identity and Authentication:**

- Machine identity (e.g. device key pairs)
- Service identity (e.g. certificates for web services)
- Human identity (e.g. PKI-based authentication using smart cards)

**Transactional Security:**

- Database integrity (e.g. storing hash values in a database, or using a block chain or hash tree to prevent records from being omitted)
- Chain-of-custody
- Data matching and deduplication (e.g. comparing hash values to see if files are the same or different)

- Other

If Other, please describe:

Back Next

8%

## Use of Cryptography Survey

2. Please tell us what your product does and how it uses cryptography.

Back Next

17%

Use of Cryptography Survey Screen 3

## Use of Cryptography Survey

### 3. What is the source of the cryptographic implementations used in your products?

**Check all that apply:**

- We use what the hardware, operating system, and standard libraries provide.
- We develop our own cryptographic implementations.
- We contract with others to develop proprietary implementations.
- We use open source implementations that we download from the Internet.
- We purchase commercially available implementations.
- We require users/customers to purchase specific cryptographic implementations to use with our products. (For example, customers purchase cryptographic hardware tokens to use with our authentication system.)
- Other

**If Other, please describe:**

Back

Next

## Use of Cryptography Survey

4. There are many approaches that organizations use for testing, evaluating, and gaining confidence in their cryptographic systems. Which of the following practices are employed by your organization?

Check all that apply:

- We do not formally test our cryptographic implementations, but we would be able to visually observe if data were not being properly encrypted.
- We rely on the reputation of the cryptographic providers.
- We rely on third-party testing - for example, by looking for third-party certification or compliance with testing programs.
- We verify that data can be decrypted after it is encrypted.
- We test the implementation with specific test vectors.
- We visually inspect the source code.
- We perform automated analysis of the software using compiler warnings and formal testing products such as lint, findbugs, and purify.
- We use formal methods to validate cryptographic implementations.
- We search for side-channel leakage of cryptographic material.
- We perform tiger-team attacks on the encrypted data and hash functions.
- Other

If Other, please describe:

Back

Next

33%

## Use of Cryptography Survey

5. On a scale of 1-5, with 5 being the most important, how important is each of the following metrics in evaluating the quality of a cryptographic implementation?

	1	2	3	4	5
Throughput (Gb/s)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Implementation size (e.g. gate count, code size)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Power requirements	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Implementation language (e.g. C++, Java)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Code quality (variable names, comments, modularity)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Documentation quality	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Openness of source code	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
General acceptance of the algorithms	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Popularity of the implementation in other products	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Runtime protection of secrets	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Support for hardware that accelerates cryptographic operation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Support for hardware that supports cryptographic key stores	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Blessed by a local expert	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Evaluation by outside trusted consultants	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Evaluation by third-party testing organizations	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Back Next

67%

Use of Cryptography Survey Screen 6

## Use of Cryptography Survey

6. If you are using a third-party testing organization, which one do you use?

Back Next





## Use of Cryptography Survey

7. What resources do you use to help you select or develop cryptographic implementations?

Check all that apply:

- National/international standards
- Industry specifications
- Internal (corporate) guidance
- Proprietary information
- Reference books
- Academic literature
- Web sites
- Other

If Other, please describe:

Back

Next

Use of Cryptography Survey Screen 8

## Use of Cryptography Survey

8. This question is about the kinds of specific challenges that your organization faces when incorporating cryptography in its products.

In each of the areas, we are interested where cryptography creates challenges that are fundamentally greater or different than other kinds of technology, for example, how the difficulty of using a cryptographic API might be larger than the difficulty of using an API that performs machine translation or database access.

a. Recruiting talent for projects:

b. Managing employees:

c. Obtaining appropriate developer tools:

d. Evaluating employee work:

e. Maintaining products over their lifecycle:

f. Transitioning between end-of-life products and new products:

g. Explaining products to potential customers:

h. Participating in product evaluations:

Back Next

## Use of Cryptography Survey

9. Does your organization use cryptographic standards in developing its products?

**Check all that apply:**

- We don't use cryptographic standards.
- We have an individual (a "standards guru") who reads the standards and makes sure that our products comply.
- We use the standards to inform our design process.
- We use the standards to guide our development process.
- We use the standards to validate our implementation.
- We use test vectors from the standards to validate the cryptographic modules.
- We look for conformance with the standards in the external components that we incorporate into our products.
- We advertise conformance with the standards in our marketing material.
- Other

**If Other, please describe:**

Back

Next



## Use of Cryptography Survey

10. If you use cryptographic standards:

Which ones do you use?

How did you choose them?

Back

Next

83%

## Use of Cryptography Survey

11. What is your job function?

12. May we anonymously quote your responses? If so, how would you like your organization to be described in the survey?

Please do not quote my responses in the survey.

You may quote my responses. Please describe my organization as:

Please email your contact information to [cryptography-survey-2016@nist.gov](mailto:cryptography-survey-2016@nist.gov) if you are interested in participating in phase two interviews.

Back

Submit

92%