NSM’s cryptographic recommendations

NKS 2024

Thomas Gregersen
NSM center for applied cryptology

Motivation

NSM

Why do we produce cryptographic recommendations?

- We are in touch with many parties in need of specific advice on choosing correct cryptographic mechanisms
- At times, some parties touch upon work where specialist knowledge is needed, but where no such knowledge is present beforehand
- To prepare for talks on these matters, the document serves as a foundation for discussion and as a lookup when needed

The target audience

NSM

- Responsible parties for procurement in need of cryptographic advice
- Responsible parties in cybersecurity
- Developers who need to work on cryptographic matters in general systems
- +++

- In general terms, we target those who are dependent on cryptography but who do not have detailed knowledge of its workings

What can be found in today's recommendations?

NSM

- Recommendations on algorithms and parameter choices
- Recommendations on how to use cryptography:
  - Key management
  - Random number generation

The new version

NSM

- A draft version has been out there for some time [1]
- Was circulated to receive feedback over this summer
- The final version is now ready

- We would like additional feedback even if the document has reached its final form

[1] https://nsm.no/fagomrader/digital-sikkerhet/kryptosikkerhet/kryptografiske-anbefalinger/

Why revise now?

NSM

Relevant quantum computers will break important cryptographic primitives if they reach sufficient maturity

- Quantum-safe algorithms are on their way and will be rolled out in any case
- In turn, this is a natural time for a revision
- We would like our partners to start their process of migration (chart and evaluate their infrastructure, find problematic areas if present)
- Other updates as needed
- Our plans for the migration process are available[2]

[2] https://nsm.no/kvantemigrasjon

What news are included?

NSM

- Recommendations on quantum safe cryptography
- Fewer choices, simplicity as a foundation
- Recommendations on handling passwords
- In our minds a more enlightening text

General advice

- Cryptographic software
- Key management
- Random number generation
- Quantum computers

Symmetric algorithms

NSM

- General-purpose encryption: AES-GCM (Default), ChaCha20Poly1305/AES-GCM-SIV (Alternates),
- Hashing: SHA-3/SHA-2
- Disk encryption: XTS-AES (D)
- MAC: HMAC/KMAC
- KDF: HKDF/KMAC
- Password hashing: PBKDF2 (D), Argon2id (A)

Key agreement

NSM

Our advice for a quantum safe beginning: A hybrid solution

- ECDH
- ML-KEM
- Combine the two to form one shared secret

Hybrid?

Until we feel there is enough trust in ML-KEM, we like hybridisation with an algorithm we know well to avoid single point of failure

Signatures

NSM

Our advice for a quantum safe beginning: Another hybrid solution

- ECDSA
- ML-DSA
- Both signatures must be verified

Alternate signature: SLH-DSA (special cases where it fits, can be used alone)

Protocols

NSM

- There are unsafe combinations of secure algorithms
- Correct parameters are a foundation
- We would like to give sound advice on the use of
  - TLS
  - IPSec (possibly)
  - SSH (possibly)
  - Other things (open to comments from you!)

The road ahead

NSM

- The document will be revised as needed, we will continue to use it as a guideline to the general public
- A version in norwegian will appear later
- You may follow developments[3]
- Please let us know if you have comments (have a look at the final page)!

[3] nsm.no/kryptoanbefalinger

Questions/comments?

Send your feedback to
arne-tobias-malkenes.odegaard@nsm.no

nsm.no