Standardisation efforts in lighweight cryptography

Riaal Domingues

February 2, 2014

Outline

- Motivation for standardisation.
- Keeloq.
- Standardisation processes and structures at ISO.
- What is in the ISO standards currently?
- Lessons learned from Keeloq.
- Interesting problems to consider.

Motivation for standardisation

Why do we standardise?

Popular answers to the question

- Interoperability is usually seen as the main driver in standardisation.

Motivation for standardisation

Why do we standardise?

Popular answers to the question

- Interoperability is usually seen as the main driver in standardisation.
- What is required to be interoperable?

Motivation for standardisation

Why do we standardise?

Popular answers to the question

- Interoperability is usually seen as the main driver in standardisation.
- What is required to be interoperable?
  - Same protocols, algorithms etc.

Motivation for standardisation

Why do we standardise?

Popular answers to the question

- Interoperability is usually seen as the main driver in standardisation.
- What is required to be interoperable?
  - Same protocols, algorithms etc.
- Much more is actually required:

Motivation for standardisation

Why do we standardise?

Popular answers to the question

- Interoperability is usually seen as the main driver in standardisation.
- What is required to be interoperable?
  - Same protocols, algorithms etc.
- Much more is actually required:
  - Message formats.

Motivation for standardisation

Why do we standardise?

Popular answers to the question

- Interoperability is usually seen as the main driver in standardisation.
- What is required to be interoperable?
  - Same protocols, algorithms etc.
- Much more is actually required:
  - Message formats.
  - (Non-cryptographic) protocols.

Motivation for standardisation

Why do we standardise?

Popular answers to the question

- Interoperability is usually seen as the main driver in standardisation.
- What is required to be interoperable?
  - Same protocols, algorithms etc.
- Much more is actually required:
  - Message formats.
  - (Non-cryptographic) protocols.
  - System security issues (e.g. How keys are stored and their protection).

Motivation for standardisation

Why do we standardise?

Popular answers to the question

- Interoperability is usually seen as the main driver in standardisation.
- What is required to be interoperable?
  - Same protocols, algorithms etc.
- Much more is actually required:
  - Message formats.
  - (Non-cryptographic) protocols.
  - System security issues (e.g. How keys are stored and their protection).
- The latter type of standardisation becomes industry specific.

Motivation for standardisation

Why do we standardise?

Industry answers to the question

- Economics and marketing.

Motivation for standardisation

Why do we standardise?

Industry answers to the question

- Economics and marketing.
- Having your own mechanism adopted by standards organisation brings in money and reputation (e.g. RSA, Sony).

Motivation for standardisation

Why do we standardise?

Industry answers to the question

- Economics and marketing.
- Having your own mechanism adopted by standards organisation brings in money and reputation (e.g. RSA, Sony).
- National pride (e.g. Do not want to offend any particular country).

Motivation for standardisation

Why do we standardise?

Industry answers to the question

- Economics and marketing.
- Having your own mechanism adopted by standards organisation brings in money and reputation (e.g. RSA, Sony).
- National pride (e.g. Do not want to offend any particular country).
- World Trade Organisation.

Motivation for standardisation

Why do we standardise?

Purist answer to the question:

Motivation for standardisation

Why do we standardise?

Purist answer to the question:

To provide well studied and scrutinized cryptographic mechanisms to industry. The cryptogtraphi mechanisms can be incorporated safely into industry solutions without industry requiring crypto experts. Industry should be specialising in building systems.

Motivation for standardisation

Why do we standardise?

Purist answer to the question:

To provide well studied and scrutinized cryptographic mechanisms to industry. The cryptogtraphi mechanisms can be incorporated safely into industry solutions without industry requiring crypto experts. Industry should be specialising in building systems. **Is this really true, or perhaps too idealistic?**

A lesson from history

Keeloq

Why was Keeloq developed?

A lesson from history

Keeloq

Why was Keeloq developed?

- Mid 80's there was a practical problem (threat and reality): Garages, gates and cars were opened by scanning for access codes.

A lesson from history

Keeloq

Why was Keeloq developed?

- Mid 80's there was a practical problem (threat and reality): Garages, gates and cars were opened by scanning for access codes.
- Obvious solution is to encrypt the code.

A lesson from history

Keeloq

Why was Keeloq developed?

- Mid 80's there was a practical problem (threat and reality): Garages, gates and cars were opened by scanning for access codes.
- Obvious solution is to encrypt the code.
- Industry constraint: Space available, both in protocol (32-bit maximum) and on the chip.

A lesson from history

Keeloq

Why was Keeloq developed?

- Mid 80's there was a practical problem (threat and reality): Garages, gates and cars were opened by scanning for access codes.
- Obvious solution is to encrypt the code.
- Industry constraint: Space available, both in protocol (32-bit maximum) and on the chip.
  - The original industry constraint was 32-bit block and key lengths. The designer argued for 64-bit for both. Block length was constrained by the code space available.

A lesson from history

Keeloq

Why was Keeloq developed?

- Mid 80's there was a practical problem (threat and reality): Garages, gates and cars were opened by scanning for access codes.
- Obvious solution is to encrypt the code.
- Industry constraint: Space available, both in protocol (32-bit maximum) and on the chip.
  - The original industry constraint was 32-bit block and key lengths. The designer argued for 64-bit for both. Block length was constrained by the code space available.
- No academic solution was available, and not much time as we cannot wait 22 years while possessions are stolen).

A lesson from history

Keeloq

Why was Keeloq developed?

- Mid 80's there was a practical problem (threat and reality): Garages, gates and cars were opened by scanning for access codes.
- Obvious solution is to encrypt the code.
- Industry constraint: Space available, both in protocol (32-bit maximum) and on the chip.
  - The original industry constraint was 32-bit block and key lengths. The designer argued for 64-bit for both. Block length was constrained by the code space available.
- No academic solution was available, and not much time as we cannot wait 22 years while possessions are stolen).
- Solution was Keeloq (Both code and counter to be ecrypted).

A lesson from history

Keeloq

Why was Keeloq developed?

- Mid 80's there was a practical problem (threat and reality): Garages, gates and cars were opened by scanning for access codes.
- Obvious solution is to encrypt the code.
- Industry constraint: Space available, both in protocol (32-bit maximum) and on the chip.
  - The original industry constraint was 32-bit block and key lengths. The designer argued for 64-bit for both. Block length was constrained by the code space available.
- No academic solution was available, and not much time as we cannot wait 22 years while possessions are stolen).
- Solution was Keeloq (Both code and counter to be ecrypted).
- This was in other words a requirement for a lightweight block cipher.

A lesson from history

Keeloq

Was this the right way to do it?

Standardisation bodies that deal with crypto

Summary

There are many standardisation bodies that produce standards on crypto. Note that not all of them produce International standards.

- NIST (Neither International nor National)
- ETSI (Regional)
- ITU
- IETF
- ISO/IEC
- IEEE

Relationship between academia, industry and standardisation bodies

Academia, industry and standardisation bodies do not exist in isolation.

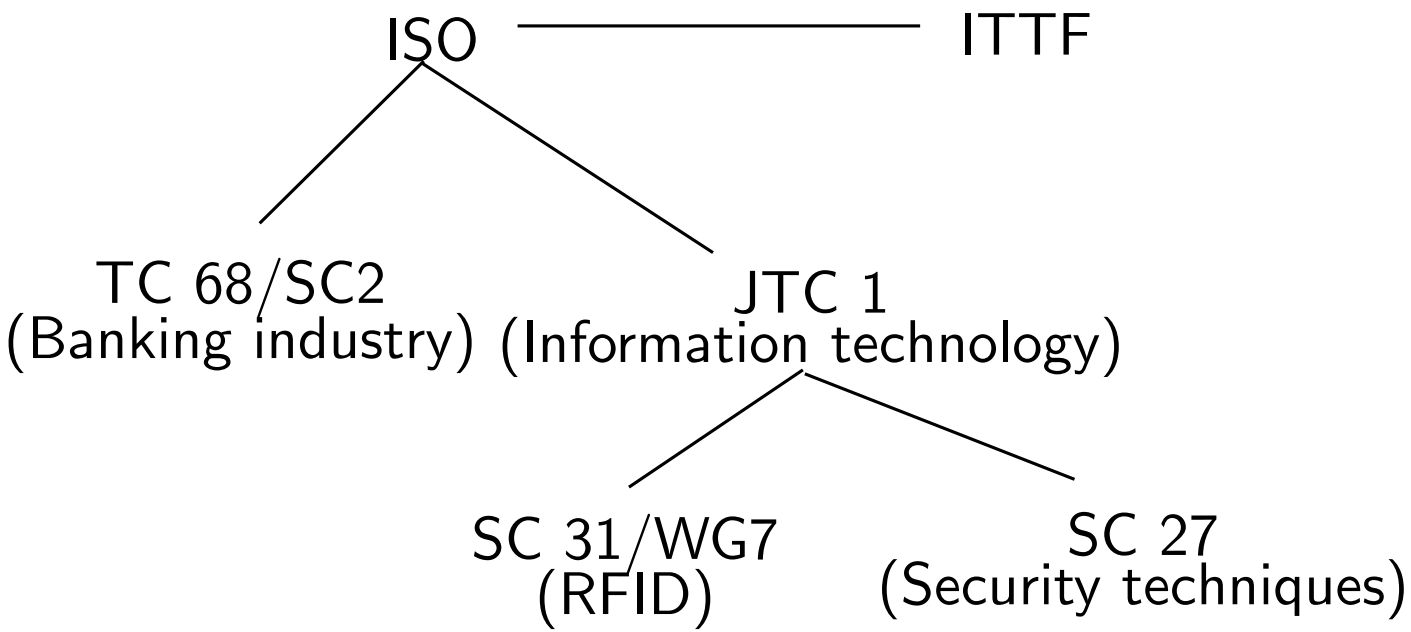
- Academia
  - Explore new horizons.
  - Develop sound theory.
  - Test practice.
- Industry
  - Apply technology developed by Academia.
  - Identify future current problems and find solutions.
- Standardisation
  - Looks for the commonalities to standardise within various industries.
  - Takes its inputs from Academia and Industry and tries to match them.

Relationship between academia, industry and standardisation bodies

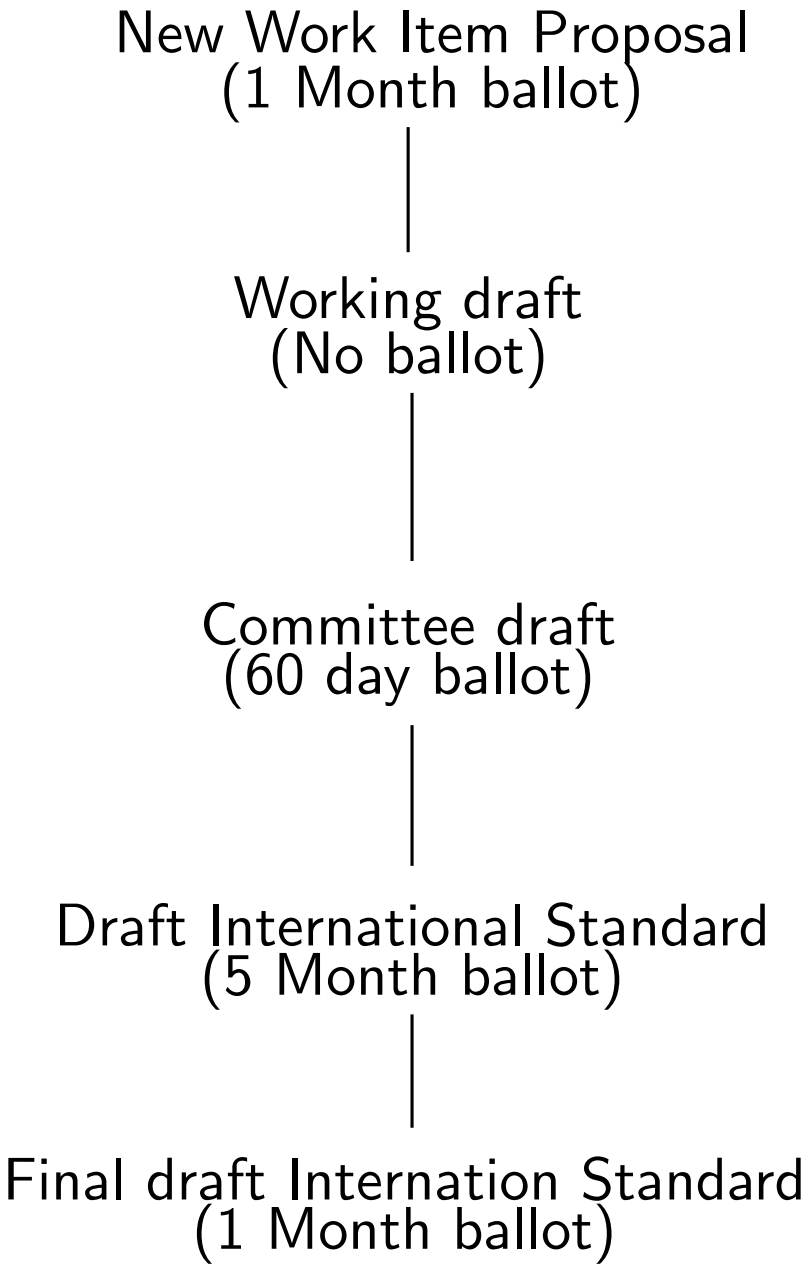
Is there enough communication and understanding between these entities?

ISO structure

Where does the general primitives (building blocks) get standardised?



ISO process of standardisation



Lightweight cryptography standards within ISO/IEC

Breakdown

Lightweight standards developed in ISO JTC 1/ SC 27: ISO/IEC 29192 Lightweight cryptography. It is a 4 (5) part standard.

- Part 1: General
- Part 2: Block ciphers
- Part 3: Stream ciphers
- Part 4: Mechanisms using asymmetric techniques
- (Part 5): Lightweight hash functions (under development)

Part 1: General

This part defines what lightweight cryptography is. It also defines some metrics for hardware used for comparison of different mechanisms.

- Lightweight cryptography is cryptography that has been tailored for a specific environment.
- Minimum security strength must be at least 80-bits.
- Establishes GE formally as a metric and requires all mechanisms tailored for hardware to provide metrics.

Part 2: Block ciphers

- PRESENT
- CLEFIA

Part 3: Stream ciphers

- Enocoro-80
- Enocoro-128V2
- Trivium

Part 4: Mechanisms using asymmetric techniques

- CryptoGPS (Lightweight asymmetric identification scheme and can be implemented making use of "coupons")
- ALIKE (Asymmetric mechanism for authentication and key exchange based on a variant of RSA).
- IBS (Identity based signature scheme and third party is involved in computing of distanct signature keys).
- ELLI (Elliptic Curve Lightweight)(unilateral authentication scheme based on elliptic curves. (Siemens is actually using this in RFIDs. Currently being added as an ammendment).

Part 5: Hash function

- PHOTON
- SPONGENT

A lesson from history

Keeloq

Implications from breaking Keeloq.

- Keeloq was broken (required 2^{16} ciphertexts).
- (Arguably) break is not a problem per se, as it compromises only one individual system.

A lesson from history

Keeloq

Implications from breaking Keeloq.

- Keeloq was broken (required 2^{16} ciphertexts).
- (Arguably) break is not a problem per se, as it compromises only one individual system.
- Caveat: Break leads to compromise of the master key, which makes faking other devices easy.
- Lesson: Key management is a problem.

A lesson from history

Replacing Keeloq

Designer approached Microchip (now in the US) and offered to design a new lightweight cipher. Microchip however declined.

Standards in support of Lightweight cryptography ISO/IEC

There are various standards in support of lightweight cryptography (as currently seen by SC 27 at least).

- ISO/IEC 11770 Key management (actually key agreement/exchange).
- ISO/IEC 9798 Entity Authentication (Basic entity authentication protocols).
- No standard that covers the symmetric setting Keeloq required for key management (perhaps no primitive either).

Lessons from history

What are the lessons to be learned from Keeloq

- There are "gaps" between Academia, standardisation bodies and industry. Better communication on problems and solutions are required.

Lessons from history

What are the lessons to be learned from Keeloq

- There are "gaps" between Academia, standardisation bodies and industry. Better communication on problems and solutions are required.
- If lightweight cryptography is "purpose designed", we have to consider more frequent redesign/refinement in industry.

Lessons from history

What are the lessons to be learned from Keeloq

- There are "gaps" between Academia, standardisation bodies and industry. Better communication on problems and solutions are required.
- If lightweight cryptography is "purpose designed", we have to consider more frequent redesign/refinement in industry.
- Standardisation processes may be too slow for industry (academic development combined with standardisation can take too long).

Lessons from history

What are the lessons to be learned from Keeloq

- There are "gaps" between Academia, standardisation bodies and industry. Better communication on problems and solutions are required.
- If lightweight cryptography is "purpose designed", we have to consider more frequent redesign/refinement in industry.
- Standardisation processes may be too slow for industry (academic development combined with standardisation can take too long).
- Key management in general needs to be studied. Lightweight cryptography failures may be catastrophic due to cryptographic system design issues.

Lessons from history

What are the lessons to be learned from Keeloq

- There are "gaps" between Academia, standardisation bodies and industry. Better communication on problems and solutions are required.
- If lightweight cryptography is "purpose designed", we have to consider more frequent redesign/refinement in industry.
- Standardisation processes may be too slow for industry (academic development combined with standardisation can take too long).
- Key management in general needs to be studied. Lightweight cryptography failures may be catastrophic due to cryptographic system design issues.
- At least in ISO standards in SC 27, there is not enough guidance on cryptographic system design.

Lessons from history

What is lightweight cryptography in reality?

Lessons from history

What is lightweight cryptography in reality?

- Cryptography is not seen as an investment, but an expense.
- Lightweight cryptography is seen as "How little can I get away with"?

This is not only true for the primitives itself, but also all primitives put together to form a cryptographic system.

Lessons from history

What should we do?

Lessons from history

What should we do?

- Lightweight crypto may require shorter refreshment cycles.

This is not only true for the primitives itself, but also all primitives put together to form a cryptographic system.

Lessons from history

What should we do?

- Lightweight crypto may require shorter refreshment cycles.
- Industry must be willing to refresh cryptographic primitives faster.

This is not only true for the primitives itself, but also all primitives put together to form a cryptographic system.

Lessons from history

What should we do?

- Lightweight crypto may require shorter refreshment cycles.
- Industry must be willing to refresh cryptographic primitives faster.
- The SLOW standardisation process needs much shorter cycles.

This is not only true for the primitives itself, but also all primitives put together to form a cryptographic system.

Lessons from history

What should we do?

- Lightweight crypto may require shorter refreshment cycles.
- Industry must be willing to refresh cryptographic primitives faster.
- The SLOW standardisation process needs much shorter cycles.
- The different parties need more overlap in communication and understanding (and a LOT LESS secrecy).

This is not only true for the primitives itself, but also all primitives put together to form a cryptographic system.

Lessons from history

What should we do?

- Lightweight crypto may require shorter refreshment cycles.
- Industry must be willing to refresh cryptographic primitives faster.
- The SLOW standardisation process needs much shorter cycles.
- The different parties need more overlap in communication and understanding (and a LOT LESS secrecy).
- Academia is flooded with cryptographers, so most cryptographers trained today will be practicing cryptographers. We need to make sure they know how to handle security tradeoffs.

This is not only true for the primitives itself, but also all primitives put together to form a cryptographic system.

Lessons from history

What should we do?

- Lightweight crypto may require shorter refreshment cycles.
- Industry must be willing to refresh cryptographic primitives faster.
- The SLOW standardisation process needs much shorter cycles.
- The different parties need more overlap in communication and understanding (and a LOT LESS secrecy).
- Academia is flooded with cryptographers, so most cryptographers trained today will be practicing cryptographers. We need to make sure they know how to handle security tradeoffs.
- Develop more theory to support risk models.

This is not only true for the primitives itself, but also all primitives put together to form a cryptographic system.

Interesting problems to solve

The following problems might be interesting to solve more formally.

- Key management (key distribution)

Interesting problems to solve

The following problems might be interesting to solve more formally.

- Key management (key distribution)
- Real world lightweight implementations.

Interesting problems to solve

The following problems might be interesting to solve more formally.

- Key management (key distribution)
- Real world lightweight implementations.
- Exploits in the encrypted communication protocols.

Interesting problems to solve

The following problems might be interesting to solve more formally.

- Key management (key distribution)
- Real world lightweight implementations.
- Exploits in the encrypted communication protocols.
- Assumptions on bad randomness.

Interesting problems to solve

The following problems might be interesting to solve more formally.

- Key management (key distribution)
- Real world lightweight implementations.
  - Exploits in the encrypted communication protocols.
  - Assumptions on bad randomness.
- Risk analysis frameworks for cryptographic systems.

End

Questions / Remarks